SparkyLinux: Neues Leben für alte 32-Bit-Rechner S. 6

02.2023

linuxUSER

linuxUSER 02 AUDIO-WORKSHOP • CORSAIR K70 • FLATPAK • SPARKYLINUX • ZIGBEE • SICHER IM VPN

Anonym durchs Internet, verschlüsselter Zugriff auf das heimische Netz

SICHER IM VPN

Grundlagen: VPN-Technik anschaulich erklärt S.14

Privacy: VPN-Dienste im direkten Vergleich S. 18

OpenVPN: Fernzugriff ins LAN per Bridging S. 24

VPN-Server: Wireguard und OpenVPN im Test S. 32

Bookmarks voll im Griff: Floccus und Linkace S. 38

Effiziente plattformübergreifende Synchronisation mit Floccus, selbst gehostetes Archivieren und Organisieren mit Linkace

USB-Multiboot-Tools S. 46

Mobilen Werkzeugkasten für die Systemwartung bequem bauen

Audio-Workshop S. 72

Optimale Hard- und Software für Podcaster, Youtuber und Musiker

Flatpak-Aktualisierung mit Pfiff S. 80
Komfortables automatisches Update per Systemd-Service und Cronjob

Wayland, Flatpak und Pipewire S. 54
Wie die neuen Technologien unter OpenSuse dem Anwender die Arbeit erleichtern können

www.linux-user.de

EUR 7,99 Deutschland | EUR 8,50 Österreich | sfr 13,20 Schweiz | EUR 9,20 Benelux | EUR 10,00 Spanien | EUR 10,00 Italien

4 195111 007997 02

Leute, lasst uns gehen

Carina Schipper
Redakteurin

Sehr geehrte Leserinnen und Leser,

Im Sommer 2014 traten zwei Dinge gleichzeitig in mein Leben: Twitter und Elon Musk, beide im Kontext meines Volontariats. Die Plattform entwickelte sich für mich rasch zu einer Mischung aus RSS-Feed und Unterhaltungsmedium. Passierte irgendetwas, machte es auf Twitter in scheinbar rasender Geschwindigkeit die Runde. Als Journalistin lernte ich damit umzugehen und verbrachte meine Zeit dort deutlich lieber als auf Facebook mit seinen überhandnehmenden Werbe-Posts oder in reinen Business-Netzwerken wie Linkedin.

Mitte der 2010er-Jahre tummelte sich auf Twitter längst auch Elon Musk. Ich erinnere mich gut, wie ich nach Tweets von ihm suchte, um meinem Chefredakteur für einen Artikel zur damals gerade angekündigten Tesla-Gigafactory in Nevada zuzuarbeiten. Über den Boss der Elektroautofirma wusste ich wenig. Er hatte sich Energieeffizienz auf die Fahnen geschrieben, das klang nicht allzu schlecht. Danach verlor ich Musk etwas aus den Augen, trotz seines Raumfahrtprogramms SpaceX. Für mich war er irgendein Technikvisionär, der prinzipiell brauchbare, wenngleich dezent utopische Ideen hatte. Spätestens die jüngste Vergangenheit beweist: Ich lag daneben.

Ende Oktober 2022 hat der Multimilliardär meinen Lieblingskurznachrichtendienst übernommen. Sein Image hat bei mir schon im Zuge des Wirbels um die Tesla-Fabrik in Brandenburg gelitten, doch was er als Twitter-Chef zumindest bis zum Redaktionsschluss unseres Magazins veranstaltet, stößt bei mir auf nichts außer blankes Unverständnis. Zunächst proklamiert er, auf Twitter die Redefreiheit stärken zu wollen, anschließend sperrt er willkürlich Nutzerkonten, darunter zahlreiche Journalisten. Hatespeech will er auch bekämpfen. Da wirkt es auf mich durchaus befremdlich, wenn Musk beispielsweise den Account Donald Trumps reaktivieren lässt.

Ein anderes Phänomen, das sich beim Überfliegen der Tweets des selbst ernannten „Chief Twit" offenbart, ist sein Hang dazu, die Community abstimmen zu lassen. Das sieht ja so schön demokratisch aus. Beim Verkünden der Resultate antwortet Musk gern mit „Vox populi, vox Dei". Die Stimme des (Twitter-)Volks ist also die Stimme Gottes? Da fehlen mir tatsächlich die Worte und ich bin vollends verwirrt. Ein echtes Highlight markiert in diesem Zusammenhang das Ergebnis seiner Umfrage, ob er Twitter-Chef bleiben sollte. Die Nutzerschaft aka Gott ist wohl dagegen.

Als gleichsam bizarr, absurd und traurig unterhaltsam empfinde ich Musks Technik- und Personalentscheidungen. Nachdem er zahlreiche Entwickler feuerte (um festzustellen, dass kaum noch welche für den Betrieb seiner Plattform übrig blieben), meldete „Der Standard" am 14. Dezember, dass Twitter-Angestellte wohl zumindest teilweise keinen Zugriff mehr auf wichtige Github-Repositories hätten. Angesichts dieses Wirrwarrs ließ mich ein Post einer meiner Twitter-Kontakte kürzlich doch etwas schmunzeln. Sinngemäß stellte der die Frage danach, was wohl schneller zum Ende von Twitter führen würde: hausgemachte technische Probleme oder der anhaltende Nutzerschwund?

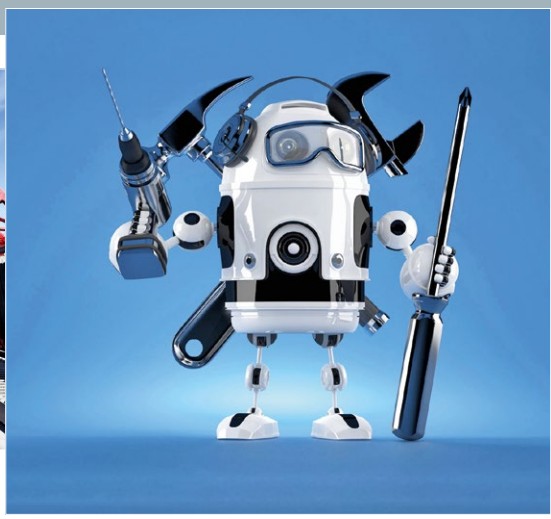
Das Abwandern der Menschen zu freien Alternativen wie Mastodon kann ich gut nachvollziehen. Als Alternative erscheint auch mir Mastodon interessant, nicht allein wegen seines Open-Source-Konzepts. Mich interessieren dort auch Instanzen wie *social.linux.pizza*. Obendrein ziehen viele meiner Twitter-Kontakte dorthin um. Zudem gibt es komfortable Tools, mit deren Hilfe Sie Ihre Follower und Personen, denen Sie selbst folgen, mitnehmen können, wie Fedifinder oder Debirdify.

Ob und wann ich meine Zelte bei Twitter abbreche, kann ich noch nicht sagen. Aus meiner Sicht lohnt es sich aber auf jeden Fall, noch tiefer in die Welt von Mastodon und Co. einzutauchen – schließlich entsteht mit dem Fediverse gerade etwas, was in seinen Anfängen an die des Internets erinnert.

Herzliche Grüße,

Carina Schipper

Weitere Infos und interessante Links
www.linux-user.de/qr/47825



14 Ein **Virtual Private Network** ist kein Hexenwerk. Unser Grundlagenartikel erklärt ausführlich die wichtigsten Technologien und Protokolle.

24 Mit **OpenVPN** baut man den Zugang ins heimische Netz meist per Routing auf. Die Alternative Bridging bietet jedoch einige entscheidende Vorteile. Dafür gilt es allerdings, an den richtigen Stellen anzupacken.

46 Wir stellen drei Tools vor, mit denen Sie **multibootfähige USB-Sticks** erzeugen, von denen Sie je nach Bedarf verschiedene Distros booten.

Heft-DVD

Aktuelles

Schwerpunkt

Schwerpunkt

Praxis

6 Möchten Sie einem angestaubten 32-Bit-PC mit einer topaktuellen Distribution neues Leben einhauchen, dann empfiehlt sich unbedingt ein Blick auf **SparkyLinux MinimalGUI**.

54 Die **OpenSuse-Tipps** untersuchen diesmal, was die neuen Technologien Wayland, Flatpak und Pipewire dem Anwender konkret bringen.

66 Im boomenden Markt für die Heimautomation spielt **Zigbee** eine prominente Rolle. Mithilfe eines Raspbee-II-Moduls verwandeln Sie einen Raspberry Pi im Handumdrehen in eine Steuerzentrale für entsprechende Geräte.

72 Unser **Audio-Workshop** zeigt, mit welcher Hard- und Software Podcaster, Youtuber und Musiker bei der Produktion optimale Ergebnisse erzielen.

Bilderwand

Mit Fgallery 1.9 erzeugen Sie unkompliziert statische Bildgalerien fürs Web

Wer seine Fotos und Bilder digital archiviert, der möchte sie oft auch gern online präsentieren. Viele Galerien basieren jedoch auf einem PHP- oder Python-Framework und setzen ein Datenbank-Backend voraus. Nicht so das in Perl geschriebene Fgallery: Es erzeugt aus einer Bildersammlung eine simple, statische Webgalerie; eine Datenbank ist nicht erforderlich. Dadurch fällt der Ressourcenbedarf sehr gering aus. Damit eignet sich das Tool für den Einsatz auf SoCs oder günstigen vServern. Zur Navigation bindet Fgallery Java-basierte Steuerelemente in die jeweiligen Seiten ein.

Zum Erzeugen einer neuen Galerie geben Sie beim Aufruf das Quellverzeichnis mit den Bildern sowie das Zielverzeichnis für die Galerie an. Außerdem vergeben Sie einen Namen für die Galerie. Beim Anlegen richtet Fgallery die Bilder einheitlich aus und sortiert sie bei der Anordnung nach dem jeweiligen Zeitstempel. Zudem erzeugt es passend skalierte Vorschaubilder, standardmäßig in 90-prozentiger Qualität. Mit dem Parameter `--quality` können Sie eine andere Qualität vorgeben. Bei Porträts lässt sich mit `-f` das Vorschaubild auf das jeweilige Gesicht zuschneiden. Auf leistungsfähigen Rechnern können Sie mit `-j` die Verarbeitung parallelisieren. Das Zielverzeichnis müssen Sie abschließend nur noch ins Dokumentenverzeichnis des Webservers übertragen.

```
Terminal - vollbracht@vmhost11: ~/extract/LU022023/fgallery-1.9
vollbracht@vmhost11:~/extract/LU022023/fgallery-1.9$ ./fgallery -h
Usage: ./fgallery [options] input-dir output-dir [album name]
  -h, --help            this help
  --version             output current fgallery version
  -v                    verbose (show commands as being executed)
  -s                    slim output (no original files and downloads)
  -i                    include individual originals
  -c methods            caption extraction methods (txt,xmp,exif,cmt or none)
  -o                    do not auto-orient
  -k                    do not modify source files, keep originals
  -t                    do not time-sort
  -r                    reverse album order
  -p                    do not automatically include full-sized panoramas
  -d                    do not generate a full album download
  -f                    improve thumbnail cutting by performing face detection
  -j N                  set process-level parallelism
  --max-full WxH        maximum full image size (1600x1200)
  --max-thumb WxH       maximum thumbnail size (267x200)
  --min-thumb WxH       minimum thumbnail size (150x112)
  --no-sRGB             do not remap preview/thumbnail color profiles to sRGB
  --quality Q           preview image quality (0-100, currently: 90)
  --index url           specify the URL location for the index/back button
vollbracht@vmhost11:~/extract/LU022023/fgallery-1.9$
```

Fgallery liefert im Verzeichnis `view/` ein eigenes Standarddesign für die Galerie mit. Es umfasst neben CSS-Einstellungen auch die Javascript-Elemente für die Navigation in der Galerie und lässt sich als Vorlage für eigene Layouts nutzen. Die aktuelle Version von Fgallery kommt mit UTF-8 und Leerzeichen in der Kommandozeile besser zurecht. Daneben unterstützt sie die neueste Version von 7-Zip und verarbeitet Graustufenbilder besser.

Lizenz: GPLv2

Quelle: https://www.thregr.org/~wavexx/software/fgallery/

Muschelersatz

Die alternative Shell Fish 3.5.1 wartet mit vielen Komfortfunktionen auf.

Sinnvolle Arbeit in der Konsole setzt eine leistungsfähige Shell voraus. Neben den Platzhirschen Bash und Zsh gibt es mit der Friendly Interactive Shell, kurz Fish, eine weitere Alternative. Die Fish setzt sich zum Ziel, eine einfache und übersichtliche Bedienung zu ermöglichen. Dazu stellt sie viele nützliche Funktionen bereit. Während sich ältere Versionen der Shell in den Repositories vieler Distributionen finden, müssen Sie das aktuelle Release selbst kompilieren.

Die Fish wirkt zunächst wie jede andere Shell, der Unterschied zeigt sich jedoch spätestens bei der ersten Eingabe: Die Fish bietet standardmäßig eine leistungsfähige Autovervollständigung samt integriertem Syntax-Highlighting. Unvollständige Befehle hebt sie während der Eingabe rot hervor, die Vervollständigung leiten Sie wie gewohnt durch einen Druck auf die Tabulatortaste ein.

```
Terminal - [vmhost11] ~/e/LU022023
vollbracht@vmhost11 ~/e/LU022023> fi
fiascotopnm          (Convert compressed FIASCO image to PGM, or PPM)
fig4latex                                                (command link)
filan                                  (Multipurpose relay (SOcket CAT))
file                                                (Bestimmt den Dateityp)
file-rename                                                  (command)
fincore                (Speicherseiten der Dateiinhalte im Kern zählen)
find                (In einer Verzeichnishierarchie nach Dateien suchen)
findaffix                                 (Interactive spelling checking)
findhyph                                                (Unbekanntes Thema)
findmnt                                                (Ein Dateisystem finden)
find-all-symbols-11                 (Manual page for find-all-symbols 11)
fish-3.5.1/                                                    (directory)
fish_add_path
fish_breakpoint_prompt
fish_clipboard_copy
fish_clipboard_paste
fish_commandline_append
fish_commandline_prepend
fish_command_not_found
fish_config
fish_default_key_bindings                                (emacs-like key binds)
fish_default_mode_prompt                                (Display vi prompt mode)
rows 1 to 22 of 53
```

Zudem schlägt die Shell selbstständig eine Liste von Befehlen vor, auf die das eingegebene Muster zutrifft. Darin können Sie navigieren und das gewünschte Programm auswählen. Die Autovervollständigung greift bei einigen Befehlen auch bei der Parameterangabe, etwa bei `find`. Dabei benutzt die Fish eine Autosuggestions-Funktion, die bei den Vervollständigungsvorschlägen auch auf die Befehlshistorie zurückgreift.

Wie die Bash ermöglicht auch die Fish ein Shell-Skripting. Die verwendete Syntax weicht aber bei Funktionen, Schleifen oder Verzweigungen von der gängigen Bash-Syntax ab. Hilfe finden Sie auf der Projektseite, auf Github oder in der mitgelieferten Manpage. Die Fish legt ihre Konfiguration im Verzeichnis `$HOME/.config/fish/` ab. Hier können Sie auch eigene Vervollständigungskonfigurationen oder zusätzliche Funktionen ergänzen.

Lizenz: GPLv2

Quelle: https://github.com/fish-shell/fish-shell

Formwandler

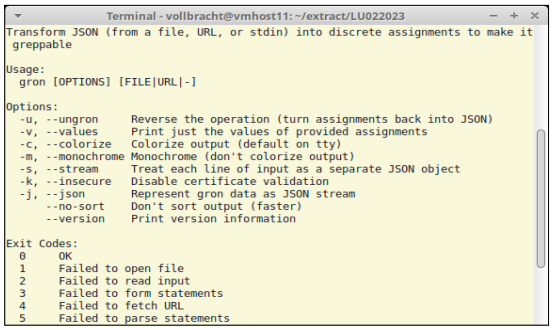
JSON-Dateien lassen sich mit Gron 0.7.1 zur Weiterverarbeitung aufbereiten.

Die Javascript Object Notation JSON hat sich in den letzten Jahren als Allzweckformat für Konfigurationsdateien und den Datenaustausch etabliert. Mit klassischen GNU-Werkzeugen ist das Aufbereiten von JSON-Dateien zur Weiterverarbeitung jedoch schwierig. Hier springt das Go-Programm Gron in die Bresche. Es wandelt JSON-Dateien in ein zeilenbasiertes Format um, was die Weiterverarbeitung erleichtert. Manche Distributionen bringen ältere Versionen des Tools mit, Binärpakete der aktuellen Version stehen auf Github bereit. Wer die 32-Bit-Variante von Pi OS verwendet, geht dabei allerdings leer aus.

Sie steuern Gron komplett über Aufrufparameter. Für eine einfache Umwandlung geben Sie dem Programm lediglich den Namen der zu verarbeitenden Datei mit. Stattdessen können Sie Gron aber auch per Weiterleitung über die Standardeingabe mit JSON-Inhalten beschicken. Selbst die Angabe einer URL und damit das direkte Verarbeiten beim Herunterladen ist möglich. Da Gron das Ablegen der Inhalte in eine Datei nicht unterstützt, müssen Sie seine Ausgabe zum Speichern in jedem Fall umlenken.

Das Tool bereitet seinen Output durch Highlighting optisch auf, was zwar die Lesbarkeit verbessert, bei der Umleitung in eine Datei jedoch stören kann. Mit `–m` erzwingen Sie gegebenenfalls eine monochrome Ausgabe. Zudem sortiert Gron den Output alphabetisch. Für eine höhere Arbeitsgeschwindigkeit deaktivieren Sie das mit `––no–sort`.

Bei einer URL als Eingabequelle kann die Überprüfung des TLS-Zertifikats für Probleme sorgen. Geben Sie beim Aufruf den Parameter `–k` mit, überspringt Gron die Prüfung und startet unverzüglich mit dem Verarbeiten der Daten. Interessant ist daneben auch der Parameter `–u`, mit dem Sie die Ausgabe eines Gron-Durchlaufs wieder in eine gewöhnliche JSON-Datei umwandeln.



Lizenz: MIT

Quelle: https://github.com/tomnomnom/gron

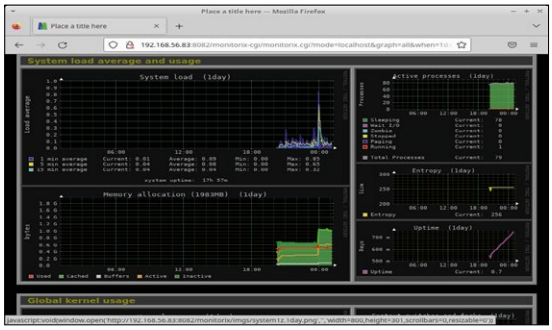
Überwacher

Mit Monitorix 3.15.0 behalten Sie die Auslastung des Systems langfristig im Blick.

Lastparameter wie Speicherverbrauch, Datendurchsatz oder CPU-Nutzung erfassen Konsolenprogramme wie Netstat oder Htop nur als Momentaufnahme. Wer alle Daten bequem im Webbrowser betrachten möchte und dabei die Auslastung über einen gewissen Zeitraum erfassen will, für den ist das Perl-basierte Monitorix genau das Richtige. Es erfasst zahlreiche Systemdaten wie Plattenzugriffe, Netzwerkverkehr, Anzahl der verbundenen Benutzer oder auch Prozessor- und Speicherauslastung. Ältere Releases des Tools finden sich in den Repositories vieler Distributionen, die aktuelle Version müssen Sie von Hand installieren. Sind alle benötigten Perl-Module vorhanden, genügt dazu ein Make, gefolgt vom verwendeten Init-System. Hier unterstützt Monitorix neben Systemd auch SysV und Upstart.

Vom Systemdienst gestartet, behält es im Hintergrund alle in der Konfigurationsdatei `/etc/montorix/monitorix.conf` angegebenen Dienste im Auge. Standardmäßig kann Monitorix über 60 verschiedene Aspekte des Systems im Auge erfassen, darunter auch Daten von Diensten wie Fail2ban, Postgres oder Squid. Die gesammelten Daten legt es als RRD-Datei im Verzeichnis `/var/lib/monitorix/` ab. Das ermöglicht zeitabhängige Auswertungen, etwa für komplette Wochen oder Monate. Für den bequemen Webzugriff bringt Monitorix eine eigene Engine mit, die an der Loopback-Schnittstelle auf Port 8080 lauscht. In der Konfiguration können Sie mit den Parametern `host` und `port` eine andere Schnittstelle festlegen.

Die Konfigurationsdatei bietet darüber hinaus zahlreiche weitere Einstellungsmöglichkeiten. Informationen dazu liefern Manpage und Projektseite. Die aktuelle Version des Tools korrigiert eine Reihe von Fehlern und bringt verbesserte Lock-Optionen für den Zugriff auf RRD-Dateien mit. (*Uwe Vollbracht/jlu*)



Lizenz: GPLv2

Quelle: https://github.com/mikaku/Monitorix

Dateien zum Artikel herunterladen unter

www.linux-user.de/dl/47816

VPN-Anbieter im Vergleich

Wenig Wahl, viel Qual

Wer sicher im Internet unterwegs sein will, braucht VPN – so suggerieren es die Anbieter. Wir gehen der Sache auf den Grund. Moritz Tremmel

README

Anbieter, die VPN als die Wunderwaffe für Anonymität im Internet und das Wahren der Privatsphäre verkaufen, gibt es inzwischen wie Sand am Meer. Doch das kann die Technik allein gar nicht leisten. Mehr noch: Viele der Anbieter tracken ihre Kunden selbst und führen damit das ganze System ad absurdum.

Mit wenigen Klicks das Internet sicher, anonym und vor Hackern geschützt nutzen: Das versprechen viele VPN-Anbieter auf ihren Webseiten. Alle Daten würden durch eine moderne Verschlüsselung geschützt, wirbt etwa NordVPN. Dabei sind die Versprechen aber meist die Pixel nicht wert, mit denen sie auf unseren Bildschirmen erscheinen: Viele der Werbeversprechen kann ein Virtual Private Network (VPN) per se gar nicht einlösen. Nicht etwa das Internet wird auf magische Weise komplett verschlüsselt, wie es mancher Werbespruch suggeriert, sondern nur der Tunnel zwischen dem eigenen Rechner oder Smartphone und dem Server des VPN-Anbieters – und dem gibt man seinen gesamten Internet-Traffic vertrauensvoll in die Hand.

Dabei tummeln sich gerade unter den VPN-Anbietern etliche sinistre Gestalten, denen man spätestens auf den zweiten Blick seine Privatsphäre vielleicht lieber nicht anvertraut. Wir zeigen, warum für uns viele VPN-Anbieter gar nicht erst infrage kommen und wie wir dann doch empfehlenswerte Anbieter fanden, obwohl auch sie nur einen kleinen Baustein zu mehr Privatsphäre im Netz beitragen.

Sicherer durch VPN?

Die erste und wichtigste Frage, die sich bei der Wahl eines VPN-Anbieters stellt: Wofür brauche ich das überhaupt? Die häufig beworbene zusätzliche Sicherheit durch den verschlüsselten VPN-Tunnel dürfte den meisten Nutzern jedenfalls keinen Sicherheitsvorteil bringen. Sie schützt ja nur den Übertragungsweg zwischen dem eigenen Gerät und dem VPN-Anbieter. Danach laufen die Inhalte ganz normal durchs Internet.

Eine vollständige Verschlüsselung zwischen dem Absender und dem Ziel einer Internet-Verbindung lässt sich nur realisieren, wenn diese Client und Server untereinander aushandeln. Genau das pas-

siert heute auch meist: Die Mehrzahl der Webseiten wird über HTTPS mit einer TLS-Verschlüsselung ausgeliefert und ist damit vor mitlesenden Dritten und auch vor Manipulation der Daten geschützt. Verbleibenden Risiken kann man beispielsweise mit dem HTTPS-Only-Mode von Browsern wie Firefox oder Chrome begegnen, die vor unverschlüsselten Verbindungen warnen.

Bei der Kommunikation via Messenger oder bei Videokonferenzen sollten die Daten zudem nicht nur mit der oben genannten Transportverschlüsselung gesichert werden, sondern zusätzlich mit einer Ende-zu-Ende-Verschlüsselung. Letztere sorgt dafür, dass sich die Inhalte auf den Servern der Anbieter nicht mitlesen lassen, sondern nur von den Sendern und Empfängern gesehen werden. Auf eine solche Ende-zu-Ende-Verschlüsselung setzen beispielsweise Signal, Threema, Whatsapp, Wire oder Matrix mit Clients wie Element oder Fluffychat.

Verschlüsselungsebenen

VPNs bieten hier nur eine weitere Verschlüsselungsebene, die zwar nicht schadet, aber nur vor sehr speziellen Angriffen schützt – beispielsweise, wenn andere Nutzer geteilter WLANs die aufgerufenen Domains mitschneiden, denn die werden bis dato trotz Transportverschlüsselung weiterhin übertragen. Dasselbe gilt für Provider. Sie können obendrein dazu gezwungen werden, unverschlüsselte Verbindungen zu kapern und Staatstrojaner auszuliefern, um das Gerät eines Betroffenen zu infizieren.

Das ist schon passiert, und auch im Verfassungsschutzgesetz steht eine entsprechende Regelung. Es dürfte aber für normale Internet-Nutzer ein eher unwahrscheinliches Szenario sein, gegen das zudem besagter HTTPS-Only-Mode schützt. Gegen ausgefeiltere Techniken, die auf eine interaktionslose Infektion über gesendete Nachrichten setzen, hilft das alles jedoch nichts.

Die durch ein VPN hinzugewonnene Sicherheit ist also eher homöopathisch. Gegen Hacker, als E-Mail-Anhang oder Messenger-Nachricht bei uns eintrudelnde Schadsoftware sowie weitere mögliche Internet-Gefahren hilft ein VPN trotz aller Versprechen schlicht nicht.

Etwas besser sieht es beim Datenschutz aus, auch wenn hier die Werbeversprechen der VPN-Anbieter genauso großspurig wie falsch ausfallen.

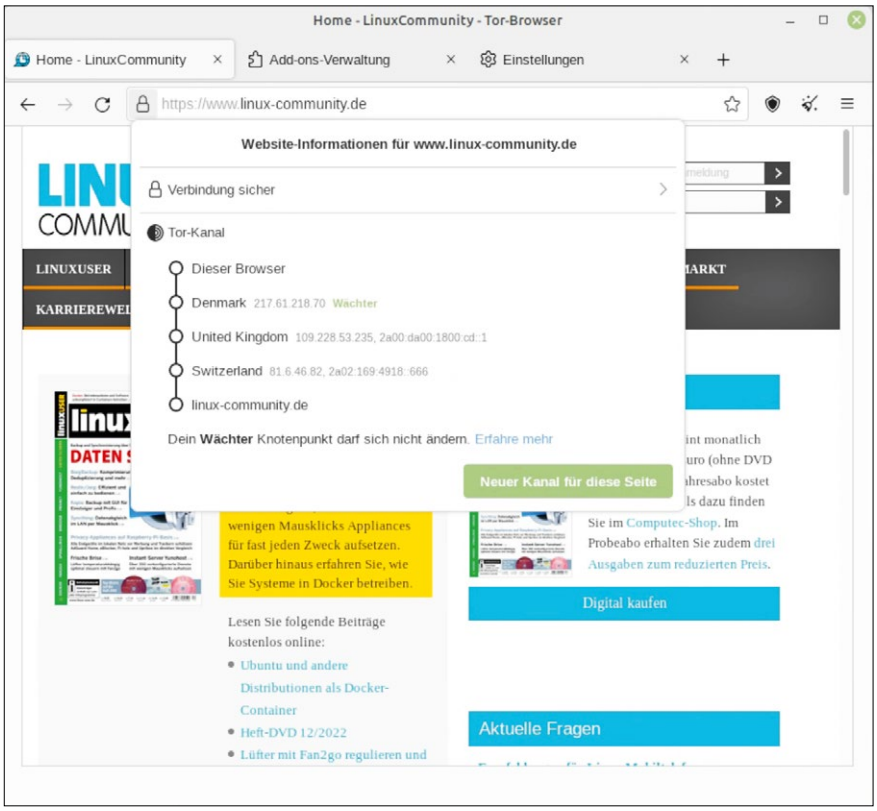
Wenn der Anbieter trackt

Neben der Sicherheit ist ein zentraler Slogan die Privatsphäre. So verspricht der VPN-Dienst Private Internet Access etwa: „Nie war Datenschutz so schnell." Cyberghost geht noch eine Stufe weiter und wirbt mit „absoluter Privatsphäre auf allen Geräten". Diese Versprechen kann ein VPN jedoch nicht einlösen, denn technisch lässt sich der Datenschutz durch den VPN-Anbieter auf eine Funktion reduzieren: die eigene IP-Adresse hinter der des VPN-Diensts zu verbergen.

Damit können die Nutzer ihre IP-Adresse und den ungefähren Standort verstecken, der sich aus ihr ableiten lässt (Location Privacy) – das war es dann aber eigentlich auch schon. Denn die unzähligen Tracking-Unternehmen wie Google, Facebook, Admob und viele andere, die uns durch das Internet und die Apps auf unseren Rechnern und Smartphones verfolgen, nutzen dafür kaum unsere IP-Adresse. Vielmehr setzen sie auf Cookies, Fingerprinting und Logins, um uns wiederzuerkennen. Hinzu kommen Tracking-Skripte in Webseiten, um unsere Interessen und unser Verhalten zu analysieren.

Das ist übrigens der Grund, warum der Anonymisierungsdienst Tor einen eigenen Browser zur Verfügung stellt und nicht nur eine Software, mit der man sich mit dem Netzwerk verbindet. Der Tor Browser 1 versucht, auf allen Systemen möglichst gleich auszusehen, damit Datenkraken die Nutzer nicht unterscheiden können. Das sorgt im Zusammenspiel mit ausgefeilter Technik letztlich auch für die Anonymität.

Entsprechend dient ein VPN nur als ein Baustein für mehr Privatsphäre im Internet. Daneben gilt es noch viele andere Dinge zu beachten. Das beginnt bei den verwendeten Diensten (und damit einem Verzicht auf Google), setzt sich in Form diverser Datenschutzeinstellungen im Browser fort und reicht bis hin zu Tracking-Blockern und werbefreien Pur-Abos.



1 Der Anonymisierungsdienst Tor bietet mit dem Tor Browser eine erheblich höhere Anonymität als lediglich ein Virtual Private Network.

Google Analytics

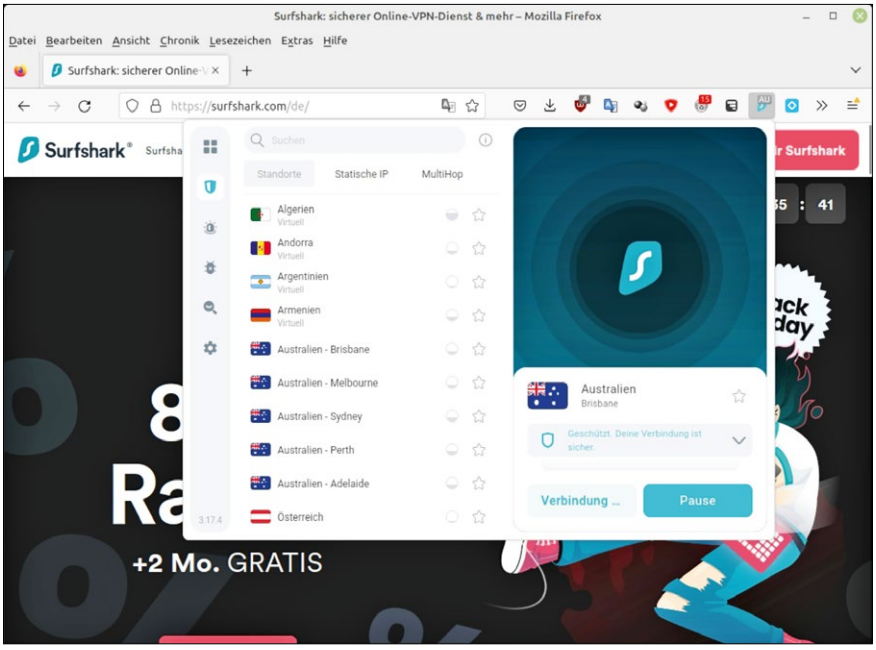
Die Installation eines VPNs allein sorgt also keineswegs für absolute Privatsphäre, mit der sich einfach weiter Google und Facebook nutzen lassen. Im Gegenteil: Viele VPN-Anbieter integrieren sogar eben jene Tracking-Unternehmen in ihre Webseiten und Apps, vor denen man die Privatsphäre doch schützen will.

Laut der Datenschutzerklärung von Cyberghost gibt das Unternehmen Daten für „Kundenanalysen und Betrugsprävention" an Drittanbieter weiter, darunter Google Analytics und Appsflyer. Beide Tracker finden wir auch in einer Analyse der App mit dem Exodus-Privacy-Projekt, das Android-Apps auf Tracking-Bibliotheken hin untersucht. Wir erinnern uns: Cyberghost bewirbt seine Dienste mit „absoluter Privatsphäre", auf der Webseite heißt es markig: „Privatsphäre ist in allem drin, was wir tun – nicht nur in unserer VPN-App für Android."

Auch die Webseite sowie die Android-App von NordVPN enthalten etliche Tracker. Eine Kurzanalyse 2019 ergab, dass die App sowohl eine eindeutige Werbe-ID für App-übergreifendes Tracking an eine Tracking-Firma übermittelte als auch die E-Mail-Adresse der Nutzer. An Drittunternehmen gab NordVPN unter anderem auch detaillierte Informationen zum Gerät weiter, darunter etwa Akkustand und Mobilfunkanbieter.

Auch viele andere Webseiten sowie die Android-Apps von VPN-Anbietern verwenden Tracking-Dienste, darunter fast immer Google Analytics. Das gilt nicht nur für Cyberghost und NordVPN, sondern auch für die häufig von VPN-Testseiten empfohlenen Anbieter ExpressVPN, Surfshark 2, IPVanish und Hide My Ass (HMA). Beim VPN-Anbieter Private Internet Access (PIA) fanden wir zwar Tracker auf der Webseite, die App hält der Anbieter jedoch frei davon. Nicht selten enthalten auch die Bezahlseiten, wo man meist eine E-Mail-Adresse und Zahlungsdaten angeben muss, solche Tracker.

Es verwundert durchaus, wenn Dienste und Anwendungen, die eigentlich die Privatsphäre schützen sollen und damit sogar offensiv hausieren gehen, gleichzeitig Tracking-Dienste von Google und Co. in ihren Webseiten und Apps einsetzen. Damit haben sich die genannten Anbieter für uns erledigt, für mehr Privatsphäre und Sicherheit sind sie dementsprechend einfach nicht zu gebrauchen. Dabei sind teilweise nicht nur die Dienste mit Vorsicht zu genießen, sondern auch die Betreiber selbst.



2 VPN-Anbieter wie Surfshark werben zwar mit vielen Server-Standorten, häufig handelt es sich dabei aber um virtuelle Server oder Weiterleitungen.

VPN mit Gruselfaktor

Innerhalb der letzten Jahren wechselten manche VPN-Anbieter immer wieder ihre Besitzer. So legte sich beispielsweise die Firma Kape zahlreiche VPN-Anbieter zu: 2017 Cyberghost für 10 Millionen US-Dollar, ein Jahr später Zenmate für 5 Millionen US-Dollar und ein Jahr später Private Internet Access für 127 Millionen US-Dollar. 2021 folgte dann schließlich der Kauf von ExpressVPN für ungefähr eine Milliarde US-Dollar.

Dabei hatte Kape, das bis 2018 Crossrider hieß, ursprünglich nicht viel mit Privatsphäre am Hut. Während Cyberghost sich vom ersten Tag an auf Datenschutz und Sicherheit konzentrierte, begann Crossrider als ein Unternehmen, das Browser-Erweiterungen vertrieb und Ad-Tech-Produkte entwickelte. „Genau das Gegenteil von dem, was wir gemacht haben", schrieb Cyberghost in einem Blog-Eintrag anlässlich der Übernahme im Jahr 2017. Einer der Crossrider-Gründer hatte zudem gute Beziehungen zum Geheimdienst Unit 8200, dem israelischen Äquivalent zu NSA und GCHQ. Die Namensänderung in Kape war laut CEO Ido Erlichman ein Versuch, sich von den kontroversen „vergangenen Aktivitäten" zu distanzieren.

Auch der Anbieter Perfect Privacy wartet mit einer recht kruden Vergangenheit auf. Die zwei Gründer, die den VPN-Dienst jahrelang betrieben, gehörten der rechtsextremen Szene an, wie ein Gerichtsprozess in Österreich im Jahr 2012 ergab. Außer dem VPN-Anbieter sollen sie auch zahlreiche Neonazi-Webseiten betrieben haben.

Gekaufte VPN-Tests

Interessanterweise werden die VPN-Anbieter, die wir bisher genannt und für uns ausgeschlossen haben, häufig auf VPN-Bewertungsseiten empfohlen. Wie neutral diese Berichte und Tests sind, bleibt allerdings unklar. Immerhin finanzieren sich die Seiten häufig durch Partnerprogramme mit eben jenen VPN-Anbietern. Die VPN-Review-Webseiten VPNmentor und Wizcase gehören sogar Kape, dem oben genannten Eigentümer etlicher VPN-Anbieter. Die Top drei der empfohlenen VPN-Dienste auf den bei-

den Webseiten sind ExpressVPN, Cyberghost und Private Internet Access. Alle drei gehören Kape – ein Schelm, wer Böses dabei denkt.

Wie sinnvoll solche VPN-Tests sind, die beispielsweise die Geschwindigkeit, die Anzahl der Server und die verfügbaren Länder vergleichen, ist ohnehin fraglich. Das viel gewichtigere Argument für einen VPN-Anbieter ist, ob man ihm wirklich seinen Netzwerkverkehr anvertrauen möchte und ob er diesen auch wie versprochen nicht mitloggt. Doch das lässt sich schwer oder gar nicht in einem Test abbilden.

In den vergangenen Jahren gab es jedenfalls immer wieder Fälle, in denen Logs von VPN-Anbietern, die angeblich keine Daten loggen, in Ermittlungsverfahren genutzt wurden. 2011 wurde ein Mitglied der Hackergruppe Lulzsec mithilfe von Logs des VPN-Anbieters Hide My Ass für einen Hack bei Sony überführt. 2016 nutzten US-Ermittler Daten des Anbieters IPVanish in einem Fall von Kindesmissbrauch, 2017 überführte das FBI einen Cyberstalker mithilfe von Logs des Anbieters PureVPN. Der versuchte, den Vorfall damit zu erklären, dass es verschiedene Arten von Logs gebe und sein Privacy-Versprechen sich nur auf einen Teil davon bezogen habe.

Transparenz durch Audits

Doch woher soll man wissen, ob ein Anbieter mitloggt oder nicht? Schließlich kann man als Nutzer nicht in die Server hineinschauen. Manche VPN-Anbieter lassen daher ihre Systeme und Apps auditieren, um Sicherheitslücken zu finden und zu schließen und sich zudem bestätigen zu lassen, dass die Systeme privatsphärefreundlich arbeiten und eben keine Daten loggen. Mullvad [3] und IVPN beauftragen hierfür regelmäßig das Berliner Pentesting-Unternehmen Cure53 und veröffentlichen dessen Ergebnisse.

So bestätigte Cure53 Mullvad bei einem Infrastruktur-Audit, dass auf den VPN-Servern keinerlei personenbezogenen Daten oder anderweitige Probleme für die Privatsphäre der Nutzer gefunden wurden. Auch IVPN attestieren die Prüfer in einem Audit seine No-Log-Policy. Beide Anbieter ließen auch ihre Apps auditieren.

Auch ProtonVPN, der VPN-Dienst von Protonmail, hat sowohl seine Apps als auch das Versprechen keine Logs zu speichern auditieren lassen. Der Anbieter aus der Schweiz wirbt mit einer strikten No-Log-Policy. Allerdings loggte auch die Mutter Protonmail die IP-Adressen nicht mit, bis das Unternehmen im Fall eines französischen Klimaaktivisten dazu gezwungen wurde, sie zu erfassen und an die Behörden zu übergeben.

„Nach geltendem Schweizer Recht werden E-Mail und VPN unterschiedlich behandelt, und ProtonVPN kann nicht gezwungen werden, Benutzerdaten zu protokollieren", betont das Unternehmen jedoch in einem Blog-Eintrag. Laut eines Transparenzberichts der Firma mussten bisher auch bei gerichtlichen Anfragen keine IP-Adressen herausgegeben werden. Der Report wurde allerdings seit zwei Jahren nicht mehr aktualisiert.

Sparsame VPN-Anbieter

Bei den meisten VPN-Anbietern muss man sich mit einer E-Mail-Adresse registrieren, so auch bei ProtonVPN. Einen völlig anderen und deutlich datensparsameren Weg schlagen Mullvad und IVPN ein: Sie generieren ohne die Abfrage weiterer Daten lediglich eine Account-ID.

Um auch beim Bezahlen möglichst keine Daten zu hinterlassen, nehmen beide Anbieter Bargeld an. Hierzu gilt es, einen Barcode auszudrucken und gemeinsam mit dem Geld per Brief nach Berlin (IVPN) oder Schweden (Mullvad) zu senden. Das Porto hält sich in beiden Fällen mit 0,85 respektive 1,10 Euro in Grenzen, das Zustellen dauert nur wenige Tage. Auch ProtonVPN bietet eine Barzahlung an. Die lässt sich allerdings nicht einfach beim Bezahlvorgang auswählen, sondern erfordert eine gesonderte Support-Anfrage. Neben Bargeld nehmen alle drei Anbieter auch Zahlungen mittels Kryptowährungen, Kreditkarten oder Paypal an.

Die Werbeversprechen fallen bei diesen drei Anbietern deutlich weniger großspurig aus, obgleich ProtonVPN mit einem privaten Browser-Verlauf wirbt und damit, dass „Passwörter und vertrauliche Daten sogar bei öffentlichen oder nicht vertrauenswürdigen Internet-Verbindungen sicher bleiben". Auch Mullvad behauptet, dass „Hacker und Tracker […]

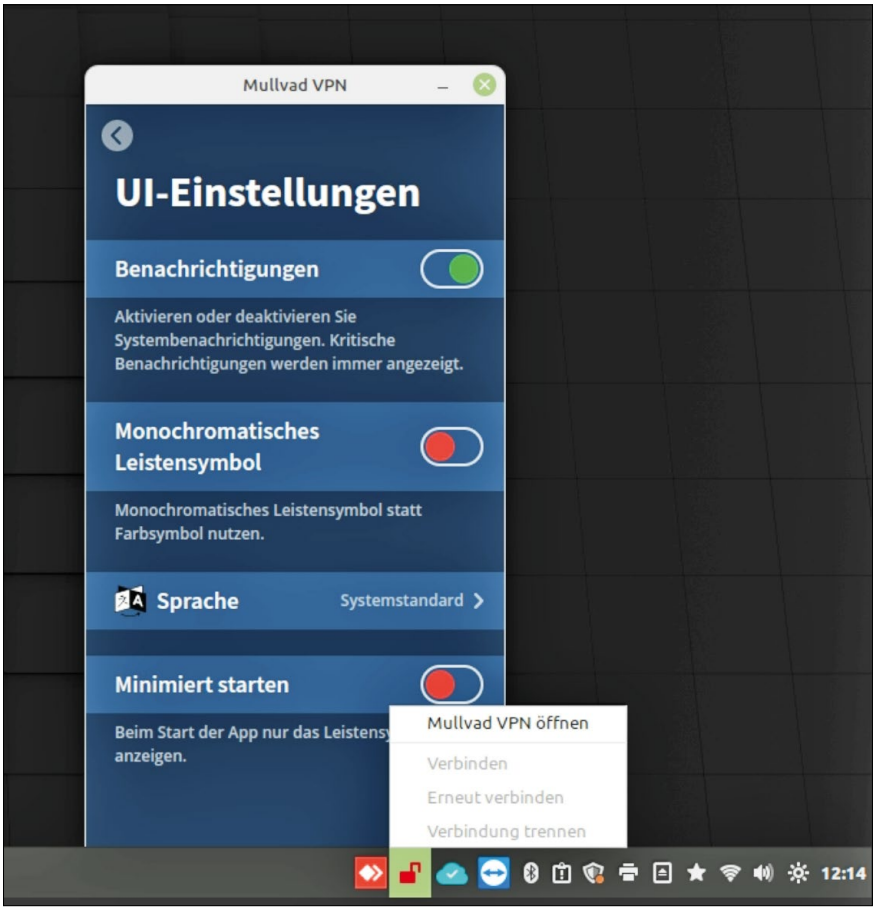
keine Chance“ hätten. Abgesehen von diesen überzogenen Aussagen fallen die Erklärungen auf den Webseiten sonst jedoch weitgehend sachlich aus.

Noch besser macht das IVPN: Der Anbieter problematisiert zwar die Überwachung im Internet, hält aber schon im zweiten Satz fest, dass „ein VPN dieses Problem nicht allein lösen kann“. Ebenfalls auf der Startseite wirft er sogar die Frage auf, ob der Kunde wirklich ein VPN braucht und erklärt, dass VPNs nutzlos oder bestenfalls ineffektiv sind, um Privatsphäre online zu sichern oder sich vor Tracking von Google oder Facebook zu schützen. Diese Ehrlichkeit ist im kommerziellen VPN-Markt, in dem selbst seriöse Anbieter mit überzogener Werbung arbeiten, wahrscheinlich einmalig.

Server in der Cloud?

Ein weiterer wichtiger Punkt, den Sie bei der Auswahl eines VPN-Anbieters berücksichtigen sollten, sind die Server. Verwendet ein Anbieter virtuelle Server in der Cloud eines anderen Anbieters, erhält der letztlich auch die Kontrolle über die Daten der Nutzer. Entsprechend sollten VPN-Anbieter immer mindestens auf dedizierte Server setzen, die sie bei einem Rechenzentrum gemietet haben. Noch besser ist Co-Location, also eigene Hardware, die in ein Rechenzentrum gebracht wird, oder gleich ein eigenes Rechenzentrum. Die beiden letzten Optionen gibt es jedoch eher selten.

Mullvad, ProtonVPN und IVPN setzen keine virtuellen Server ein. ProtonVPN gibt an, vornehmlich gemietete Server zu verwenden, an drei Standorten kommen jedoch für die Secure-Core-Server eigene Geräte zum Einsatz. Auch Mullvad verwendet sowohl eigene als auch gemietete Server und gibt das jeweilige Eigentumsverhältnis in seiner Server-Liste auf der Webseite an. IVPN wiederum setzt nur auf gemietete, dedizierte Server.



3 Der schwedische Anbieter Mullvad, den auch Mozilla als VPN-Lösung anbietet, lässt seine Apps und die Infrastruktur regelmäßig durch externe Unternehmen prüfen.

Wireguard statt OpenVPN

Mit Wireguard kam ein neues, schlankes VPN-Protokoll auf, das mittlerweile auch in den Linux-Kernel Einzug hielt. Im Unterschied zu dem in die Jahre gekommenen OpenVPN kommt Wireguard mit einem Bruchteil des Codeumfangs und deutlich weniger, dafür aber sehr sicheren Optionen aus. So lässt sich beispielsweise nicht zwischen etlichen Verschlüsselungsverfahren wählen, sondern es gibt schlicht einen einzigen Standard mit sicheren modernen Algorithmen wie Curve25519 und Chacha20-Poly1305. Kurz: Wireguard arbeitet deutlich schneller und sicherer als OpenVPN.

Allerdings wurde Wireguard für klassische VPN-Szenarien wie die Verbindung in ein Firmennetz oder auf Server entwickelt und nicht für einen Tunnel ins Internet, wie ihn die hier betrachteten VPN-Anbieter offerieren. So verlangt Wireguard einen initialen Schlüsselaustausch und weist passend zum Schlüssel immer dieselbe interne/lokale IP-Adresse zu. Zudem behält Wireguard die IP-Adressen der verbundenen Geräte bis zum Neustart der Software im Arbeitsspeicher.

Entsprechend müssen VPN-Anbieter Anpassungen vornehmen. So löschen Mullvad und IVPN die IP-Adressen nicht mehr verbundener Geräte aus dem Arbeitsspeicher und rotieren über ihre Apps regelmäßig die Wireguard-Schlüssel, wodurch auch die interne IP-Adresse wechselt. ProtonVPN hingegen setzt das sogenannte Double-NAT-Verfahren ein, das die IP-Adresse der Nutzer zu einer Session-IP umschreibt.

Die IP-Adressen der Nutzer können beispielsweise per WebRTC geleakt werden. Entsprechend sollte man es im Browser deaktivieren oder auf privatsphärefreundliche Einstellungen abändern. Entsprechende Tests bieten Mullvad und IVPN auf ihren Webseiten an.

Open-Source-Apps

Im Unterschied zu vielen anderen VPN-Anbietern verzichten Mullvad, IVPN und ProtonVPN nicht nur auf Tracker in ihren Apps, sondern stellen diese auch als quelloffene Software bereit. Neben Windows, MacOS und Linux unterstützen die drei VPN-Anbieter auch iOS und Android.

Bei Letzterem finden sich die Apps nicht nur in Googles Play Store, sondern auch im alternativen App Store F-Droid.

Bei Mullvad handelt es sich um ein inhabergeführtes Unternehmen aus Schweden, das sich der Privatsphäre im Internet verschrieben hat. Gegründet wurde es 2009 und gehört zu den Early Adopters in Sachen Wireguard, das es bereits mehrfach finanziell unterstützt hat. Die beiden Eigentümer geben an, das Unternehmen weiterführen und nicht verkaufen zu wollen. Unter Datenschützern hat sich Mullvad in den vergangenen Jahren einen Namen als Privacy-VPN gemacht. Auch der von Mozilla angebotene VPN-Dienst setzt auf Mullvad und dessen Server-Netz.

Das Unternehmen IVPN gründeten 2009 einige ehemalige IT-Security-Studenten der Universität London. Es sitzt in Gibraltar, das zu Großbritannien gehört, aber unterhält darüber hinaus Räumlichkeiten in Berlin und ist ebenfalls inhabergeführt. Bei IVPN wie bei Mullvad findet die Softwareentwicklung öffentlich auf Github statt, und das Team wird auf der Webseite genannt. Bei IVPN stellen sich die Angestellten sogar vor. IVPN und Mullvad geben an, nicht für Reviews zu bezahlen, und lehnen Werbung und Überwachung über Google und ähnliche Firmen ab.

ProtonVPN sitzt in der Schweiz und gehört zu Protonmail. Letzteres wurde im Zuge der Snowden-Leaks 2013 von Angestellten des Forschungsinstituts CERN gegründet. Anfangs finanzierte sich das Unternehmen unter anderem über eine Crowdfunding-Kampagne, später auch über Venture-Kapital. Zur Kommunikation mit seinen Kunden setzt ProtonVPN auf die externe Plattform Zendesk.

Lediglich IVPN gibt an, seine komplette Infrastruktur inklusive des E-Mail-Servers selbst zu betreiben, während Mullvad in Sachen Mailserver ausgerechnet auf Google-Dienste zurückgreift. Mullvad und IVPN betreiben neben Twitter- auch Mastodon-Konten. Preislich schlagen alle drei mit ungefähr 5 Euro pro Monat zu Buche.

Fazit

Eines haben fast alle VPN-Anbieter gemeinsam: Sie wollen dem Nutzer einreden, dass er sie unbedingt braucht. Dabei scheuen sie nicht davor zurück, unhaltbare Versprechen in die Welt zu setzen, die auch jenseits von Privatsphäre und Sicherheit haarsträubend sind. So wirbt ExpressVPN beispielsweise mit 160 VPN-Server-Standorten in 94 Ländern, hat jedoch in etlichen der angegebenen Länder gar keine Server, sondern nur eine IP-Adresse. So wird etwa der Traffic für den Server-Standort Argentinien über die Niederlande abgewickelt, mit einer argentinischen IP-Adresse.

Den überwiegenden Teil der zahlreichen bunten VPN-Angebote mit ihren wilden Versprechen können Sie von vorneherein ausschließen, zumindest dann, wenn Sie Ihrer Privatsphäre nicht mehr schaden als nützen möchten. Zum Glück gibt es mit Mullvad, IVPN und ProtonVPN auch mehrere seriöse Anbieter, deren Werbeaussagen zwar mitunter ebenfalls grenzwertig ausfallen, bei denen aber immerhin die Technik stimmt. Sie setzen auf das moderne Wireguard-Protokoll und bieten Open-Source-Apps an, die wie ihre Webseiten keine Tracker enthalten. Ihre Apps und Infrastruktur haben sie einem externen Audit unterzogen und gehören keinen Firmen mit seltsamem Hintergrund.

Allerdings spiegeln sich diese Kriterien kaum in den Vergleichstests von VPN-Anbietern wider, bei denen häufig die Eigentümer oder Affiliate-Partner auf die ersten Plätze gelangen. Das mag aber auch daran liegen, dass lieber Geschwindigkeiten gemessen sowie die Server- und Länderanzahl verglichen werden als echter Datenschutz. Der lässt sich ohnehin meist nur falsifizieren und nicht verifizieren, denn am Ende müssen wir auch mit einem Audit auf das Einhalten einer No-Log-Policy vertrauen.

Eine Frage sollte man sich auf jeden Fall vor dem Kauf noch einmal stellen: Brauche ich das wirklich, und wenn ja, wofür? Sicher gibt es gerechtfertigte Anwendungsfälle für ein VPN, zum Beispiel kann es im Zusammenspiel mit anderen Maßnahmen einen Baustein für mehr Sicherheit und Privatsphäre im Netz darstellen. Es lässt sich allerdings ebenfalls zum Umgehen von Zensur oder Geoblocking nutzen oder zum Schutz vor staatlicher Repression. Das klappt jedoch teilweise mit dem spendenfinanzierten Tor-Netzwerk besser. (*tle*)

Weitere Infos und interessante Links

www.linux-user.de/qr/48538

Der Autor

Moritz Tremmel arbeitet seit 2018 als Redakteur im Fachbereich IT-Security bei Golem.de. Er beschäftigt sich auch mit Datenschutz, Überwachung, digitaler Selbstverteidigung und Netzpolitik. Im Rahmen seines Studiums der Politikwissenschaften, Soziologie und Rechtswissenschaften forschte er zu den Auswirkungen von Technik auf das menschliche Zusammenleben. Er ist Mitglied der Digitalen Gesellschaft e.V. und des Chaos Computer Clubs. Früher schrieb er für Netzpolitik.org.

LINUXUSER

IHRE DIGITALE AUSGABE ÜBERALL DABEI!

LinuxUser begleitet Sie jetzt überall hin – egal, ob auf dem Tablet, dem Smartphone, dem Kindle Fire oder im Webbrowser. LinuxUser ist ab sofort immer dabei!

Available on the App Store

JETZT BEI Google Play

amazon apps Available on kindle fire

1x im Shop registrieren – überall mobil lesen.

Mit Ihren Login-Daten erhalten Sie überall Zugriff auf Ihre gekauften Digital-Ausgaben, im Shop-Account, in der Kiosk-Computec-App und auf epaper.computec.de.

shop.linuxuser.de

Lesezeichen mit Floccus und Linkace organisieren

Gesichert und sortiert

Die Hauptaufgaben von Floccus und Linkace bestehen im Synchronisieren und Verwalten von Lesezeichen. Beide belassen alle Daten beim Anwender. Ferdinand Thommes

README

Floccus und Linkace setzen beim Verwalten von Lesezeichen verschiedene Schwerpunkte. Während sich Floccus auf das Synchronisieren unter eigener Kontrolle spezialisiert, geht es bei Linkace um das selbst gehostete, langfristige Archivieren und Organisieren von Bookmarks.

Wer viel im Web unterwegs ist, stößt immer wieder auf Inhalte, die er speichern möchte, um sie später weiter auszuwerten. Traditionell bietet sich dafür die Lesezeichenfunktion der Webbrowser an. Möchten Sie etwa eine Webseite, die Sie unterwegs entdecken, zu Hause am Rechner weiterlesen, bedarf es – nutzt man die Bookmarks des Browsers – einer Synchronisation zwischen den Geräten.

Alle modernen Browser bieten dazu Synchronisationsdienste an. Wir beziehen uns an dieser Stelle exemplarisch auf Firefox Sync. Der Pferdefuß bei diesen Diensten besteht darin, dass die Daten wie Lesezeichen, Passwörter, offene Tabs und mehr auf den Servern des jeweiligen Browser-Anbieters landen. Ohne Mozilla etwas unterstellen zu wollen: Was eignet sich besser als diese Daten, um ein Profil unseres Nutzerverhaltens zu erstellen?

Abhilfe schaffen hier Tools wie die Browser-Erweiterung Floccus oder die selbst gehostete URL-Verwaltung Linkace. Der Schwerpunkt bei Floccus liegt auf der sicheren Synchronisation der Lesezeichen über eine private Cloud-In-

stanz via WebDAV, über Nextcloud oder Google Drive zwischen verschiedenen mobilen und stationären Plattformen und verschiedenen Browsern. Der Fokus von Linkace liegt eher beim Archivieren und der besseren Organisation von Lesezeichen auf eigener Hardware.

Floccus

Betrachten wir zunächst Floccus. Wir wollen unsere in Firefox gespeicherten Lesezeichen zwischen Geräten synchronisieren, ohne dafür den Firefox-Account oder andere externe Dienste zu nutzen, indem wir dazu unsere Nextcloud einbinden. Das bedarf einiger Vorarbeiten.

In Nextcloud müssen Sie eine App mit dem Namen *Bookmarks* ab Version 0.14 1 über die App-Verwaltung oder den Nextcloud App-Store installieren und aktivieren. Zudem müssen Sie im Browser die Erweiterung *Floccus Bookmarks Sync* einrichten. Sie steht darüber hinaus für Android über F-Droid oder den Google Play Store zur Verfügung.

Backup

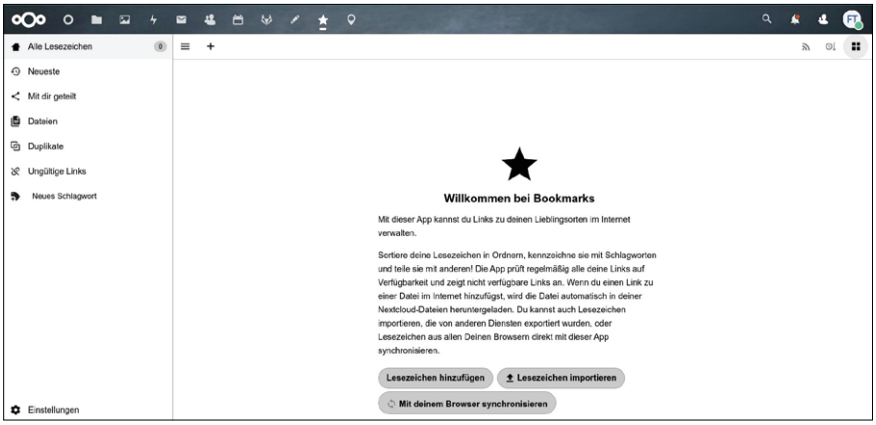
Bevor es mit der Synchronisation losgeht, empfiehlt es sich, ein Backup der Lesezeichen anzulegen. Das gelingt in Firefox über *Einstellungen* | *Lesezeichen* | *Lesezeichen verwalten* | *Importieren und Sichern*. Dort wählen Sie zwischen einer Sicherung als JSON-Datei oder einem Export als HTML. Bei Chromium geht es zunächst ebenfalls in den Einstellungen zu den *Lesezeichen* und dort über das Hamburger-Menü rechts oben zu *Lesezeichen exportieren*. Der Export als HTML ergibt Sinn, da sich die Datei unten links über *Einstellungen* direkt in Nextcloud Bookmarks importieren lässt 2.

An derselben Stelle findet sich auch der Eintrag *Hinzufügen zu Nextcloud*, den Sie mit dem Mauszeiger anfassen und als Bookmarklet in die Lesezeichenleiste des Browsers ziehen 3. Damit lassen sich künftig Lesezeichen direkt in Nextcloud anlegen. Nach der Installation von Floccus gilt es zunächst, ein oder mehrere Konten einzurichten. Ein Konto bei Floccus gilt jeweils nur für einen Lesezeichenordner. Sollen sich die Lesezeichen genauso wie im Browser verhalten, benötigen Sie zumindest zwei Konten. Eines ist für die Lesezeichen selbst, das andere für die Lesezeichen-Symbolleiste.

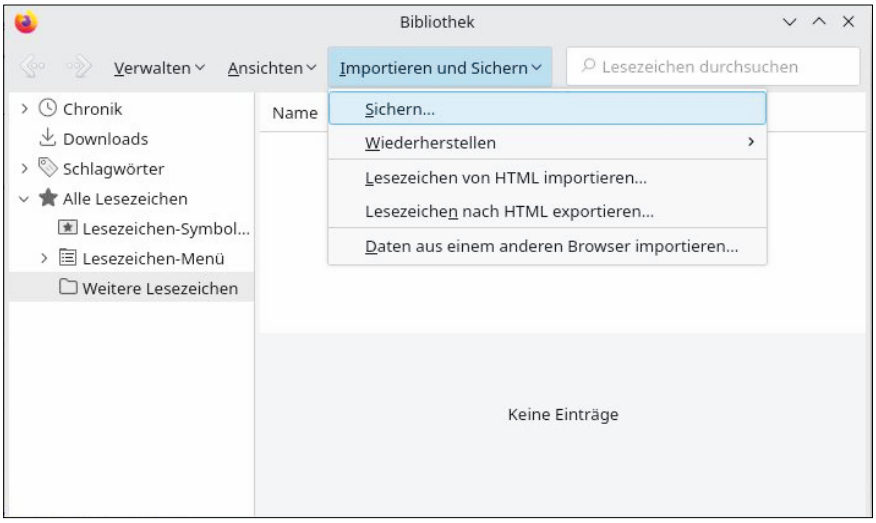
Konten erstellen

Im Einrichtungsfenster eines Kontos steht zunächst die Auswahl zwischen dem generischen WebDAV-Protokoll, Google Drive oder Nextcloud als Zentrale für die Synchronisation an. Wir entschieden uns im Test für Nextcloud 4.

Im nächsten Schritt verbinden Sie sich, indem Sie in der Adressleiste die URL Ihrer Nextcloud angeben 5. Dann legen Sie fest, in welchem Ordner in der Nextcloud Sie die Lesezeichen speichern möchten und welches Verzeichnis des Browsers die Lesezeichen enthält. Dazu



1 Die Bookmarks-App steht als Voraussetzung für den Betrieb von Floccus sowohl in der Nextcloud-Instanz als auch im Nextcloud App-Store zur Installation bereit.

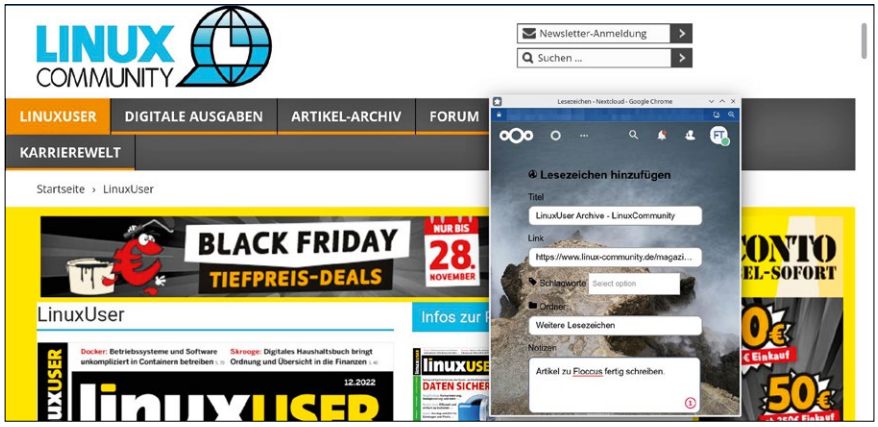


2 In den Einstellungen von Firefox und Chromium sollten Sie als ersten Schritt die vorhandenen Lesezeichen im HTML-Format sichern.

legen Sie Ordner auf der obersten Nextcloud-Ebene an und tragen diese mit Ihrem Namen als Server-Ordner ein, beispielsweise als `/Lesezeichen–FF`. Wichtig ist hier der Schrägstrich am Anfang.

Bei der Frage nach dem lokalen Ordner wählen Sie den zu synchronisierenden Lesezeichenordner aus. Bei Firefox wählen Sie *Lesezeichen-Menü*, bei Chromium *Weitere Lesezeichen*. Ein zweites Konto für die Symbolleisten erhält die Einträge *Lesezeichen-Symbolleiste* (Firefox) oder *Lesezeichenleiste* (Chromium). Im nächsten Fenster legen Sie fest, ob automatisch synchronisiert werden soll und in welchem Zeitintervall 6. Zudem entscheiden Sie, ob dies in beide Richtungen geschieht. Floccus lässt sich per Passwort absichern, das Sie im unteren Bereich über *Zugangsdaten absichern* festlegen.

Analog verfahren Sie nun mit weiteren Geräten, indem Sie dort Floccus installieren und entsprechend konfigurieren. Die Software bietet zur Unterstützung eine Anleitung sowie eine FAQ. Möchten Sie neben den Lesezeichen auch Ihre Addons, den Verlauf sowie geöffnete Tabs synchronisieren, so ist ein selbst gehosteter Firefox-Sync-Server die bessere Wahl, wie ihn Decatec beschreibt.

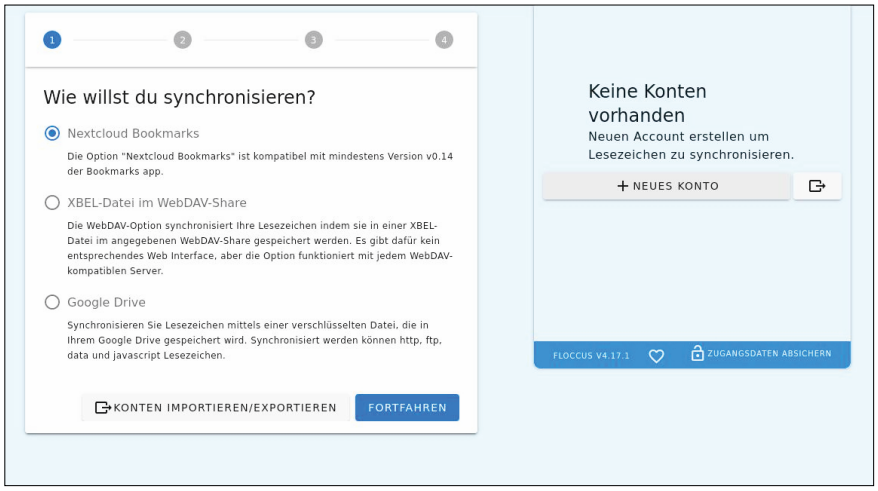


3 Über das Bookmarklet, das in der Lesezeichen-Symbolleiste abgelegt wird, lassen sich mithilfe von Floccus die besuchten Webseiten einfach in der Nextcloud oder einem anderen Speichermedium zur späteren Verwendung ablegen.

Linkace

Bei der Web-Anwendung Linkace geht es nicht um das Synchronisieren der vorhandenen Lesezeichen, sondern um eine eigenständige Sammlung von Bookmarks zum späteren Auswerten und Archivieren. Dafür reicht ein Raspberry Pi allemal aus. Für unseren Test nutzen wir einen Proxmox-Container. Linkace verwendet PHP und benötigt eine Datenbank im Hintergrund. Zur Auswahl stehen MySQL, MariaDB, PostgreSQL oder SQLite. Der schnellste Weg, Linkace aufzusetzen, führt über Docker Compose.

Doch bevor wir zur Installation schreiten, sehen wir uns zunächst an, worauf genau Linkace abzielt und wie es das umsetzt. Die Absicht des deutschen Open-Source-Entwicklers Kevin Woblick besteht darin, dem Nutzer das Speichern, Archivieren, Markieren, Klassifizieren und Wiederfinden von Lesezeichen zu erleichtern. Dazu dient bei Linkace eine auf das



4 Floccus bietet eine Synchronisation wahlweise über Nextcloud, über WebDAV oder – automatisch verschlüsselt – über Google Drive an.

Nötige reduzierte, gut gegliederte und übersichtliche Oberfläche 7.

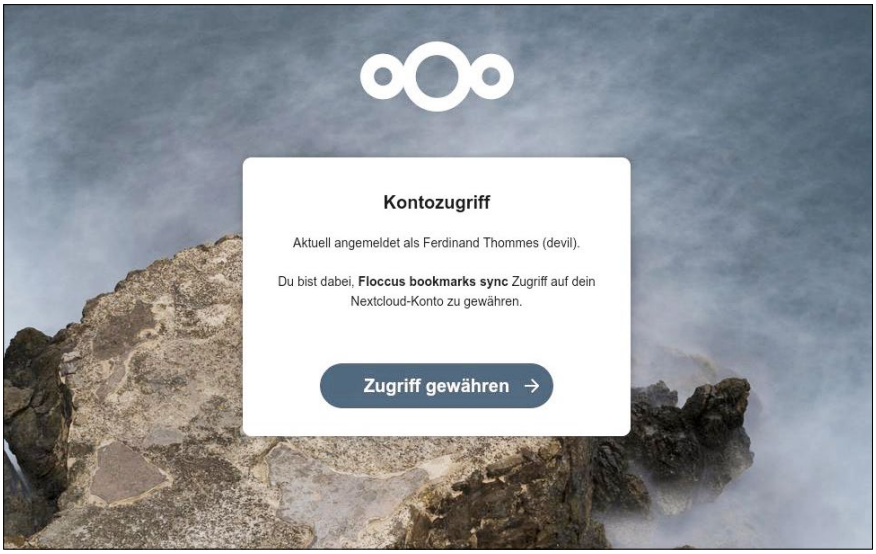
Übersichtlich

Die App bietet drei Wege, neue URLs hinzuzufügen. Zunächst lassen sich die in den Browsern vorhandenen Lesezeichen als HTML importieren. Sie können URLs auch direkt in der Oberfläche eintragen 8. Zudem gibt es ein Bookmarklet, das Sie in die Lesezeichenleiste Ihres Webbrowsers ziehen können, um interaktiv URLs von besuchten Webseiten in der Datenbank abzulegen 9.

Linkace kümmert sich anschließend um gespeicherte URLs. Auf Wunsch prüft die Anwendung diese regelmäßig. Wenn ein Link nicht mehr verfügbar ist oder verschoben wurde, erhalten Sie eine Benachrichtigung inklusive Details. Außerdem können gespeicherte Links in der Wayback Machine des Internet Archive gesichert werden. Alle gespeicherten Links lassen sich als HTML exportieren, in einen Browser importieren oder als Sicherung verwahren. Als zusätzlich unterstützte Backup-Ziele stehen die beiden kostenpflichtigen Dienste AWS und S3 bereit.

Tags und Listen

Zur Klassifizierung von Links dienen Tags und Listen 10. Letztere erfüllen den Zweck, mehrere Links zu einem Thema zu bündeln, während Tags eher der allgemeinen Kategorisierung dienen. Linkace bietet optional auch einen zu aktivierenden Gastzugang, der es erlaubt, alle Links



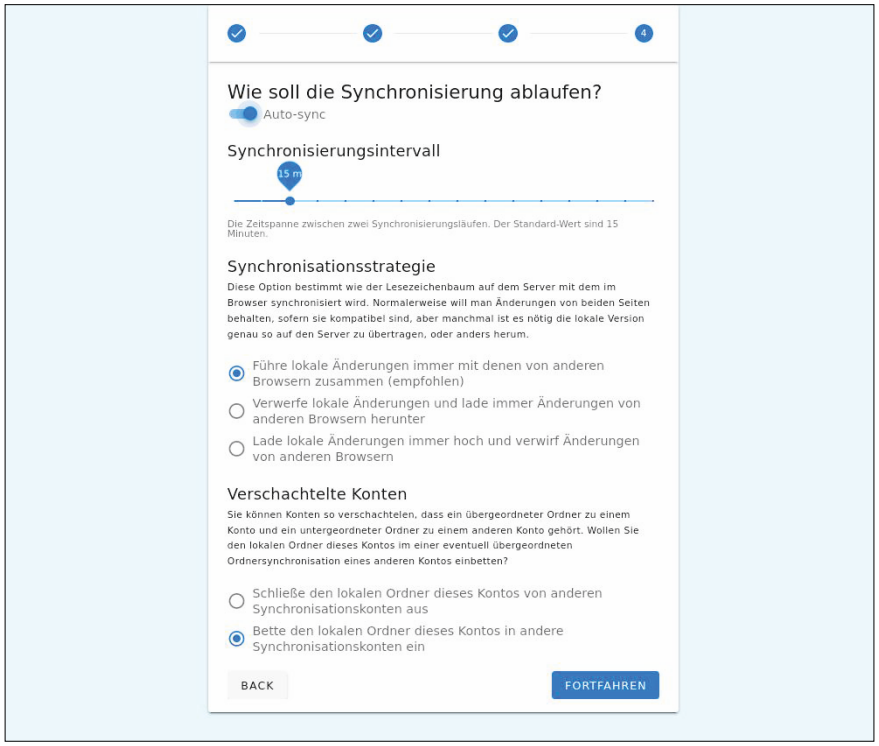
5 Die Verbindung von Floccus mit Ihrer Nextcloud-Instanz ist mit wenigen Klicks erledigt.

Listing 1: Docker einrichten

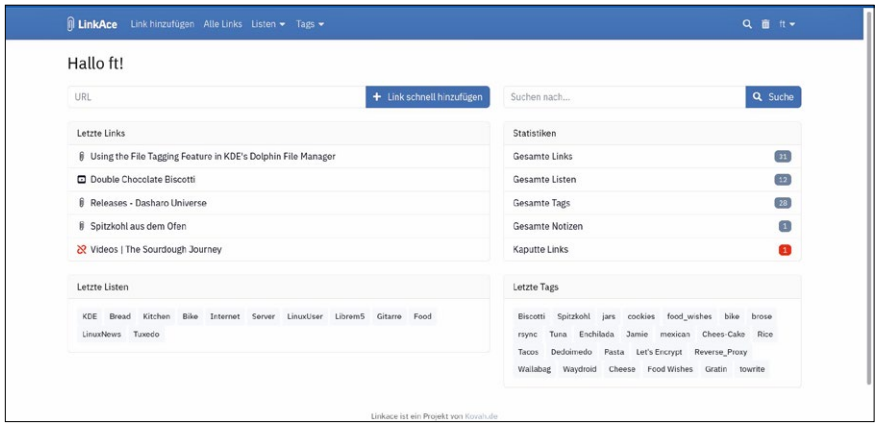
```
01 ### Docker einrichten
02 $ sudo apt update
03 $ sudo apt install apt-transport-https ca-certificates curl
   softwareproperties-common
04 $ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo
   apt-key add -
05 $ sudo add-apt-repository "deb [arch=amd64] https://download.docker.
   com/linux/ubuntu jammy stable"
06 ### Docker-CE einrichten
07 $ sudo apt update
08 $ sudo apt install docker-ce
09 $ sudo systemctl status docker
10 $ sudo usermod -aG docker ${USER}
11 ### Docker Compose einrichten
12 $ sudo curl -L "https://github.com/docker/compose/releases/download/
   v2.13.0/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/
   docker-compose
13 ### Docker-Version ermitteln
14 $ sudo chmod +x /usr/local/bin/docker-compose
15 $ docker-compose --version
```

zu sehen, die Sie nicht als *privat* einstufen. Der Zugriff lässt sich für jeden Link, jedes Tag und jede Liste separat steuern.

Eine weitere Möglichkeit, Links zu teilen, bietet Link Sharing, das derzeit für 20 verschiedene Dienste verfügbar ist. Mit einem API-Schlüssel für die Linkace-API lässt sich die App mit anderen Tools verbinden, die auf die Daten in Linkace zugreifen und diese bearbeiten können.



6 In den Einstellungen von Floccus legen Sie fest, auf welche Weise und wie oft die Synchronisation ausgeführt werden soll.



7 Die gut überschaubare Standardoberfläche von Linkace zeigt übersichtlich die zuletzt eingetragenen Links sowie eine Übersicht über alle Links, Listen und Tags an. Defekte Links werden in Rot aufgelistet.

Installation

Wenn Ihnen das Konzept gefällt, testen Sie Linkace unverbindlich als Demo, bevor Sie zur Installation schreiten. Für das Einrichten auf dem eigenen System gibt es drei Optionen. Der einfachste Weg führt über eine vorbereitete Docker-Compose-Datei, die alle benötigten Komponenten funktionsbereit installiert. Wünschen Sie mehr Einflussmöglichkeiten, verwenden Sie alternativ das Docker-Image von Docker Hub. Als dritte Möglichkeit installieren Sie alle Komponenten manuell auf Ihrem Server.

Wir setzten für unseren Test die Docker-Compose-Methode um, die sich auch für Einsteiger eignet. Als Unterbau diente ein Ubuntu Server 22.04. Um Docker und die zugehörigen Komponenten auf Ihrem Rechner einzurichten, gehen Sie wie in Listing 1 gezeigt vor. Beim Verwenden einer anderen Ubuntu-Version ersetzen Sie die Angabe `jammy` aus Zeile 5 durch den Codenamen des verwendeten Ubuntu-Releases.

Überprüfen Sie auf https://github.com/docker/compose/releases, ob Version 2.13.0 (Zeile 12) noch aktuell ist. Die installierte Version ermitteln Sie mit den Eingaben aus den Zeilen 14 und 15 .

Das weitere Vorgehen beschreibt die Linkace-Dokumentation. Zunächst gilt es, zwischen der einfachen und der erweiterten Version von Linkace zu wählen. Die einfache Version, die die Anwendung und den Webserver in einem Container ausliefert, genügt, wenn Sie Linkace nur lokal in Ihrem Netzwerk nutzen möchten. Für die erweiterte Variante müssen Sie die Software, den Webserver und die Datenbank in getrennten Containern installieren. Das vereinfacht unter anderem das Verwenden eines Reverse Proxy zum Absichern per HTTPS, falls die Anwendung von außen erreichbar sein soll.

Vom Ablauf der Installation verhalten sich beide Varianten gleich, außer dass Sie eine andere Compose-Datei herunterladen. Wir beschränken uns hier auf die einfache Methode. Das Vorgehen zum Verwenden eines Reverse Proxys oder eines Load Balancers in der erweiterten Variante finden Sie ebenfalls in der Dokumentation.

Im ersten Schritt laden Sie `linkace-docker-simple.zip` oder `inkace-do-`

cker-advanced.zip in einen zuvor erstellten Ordner in Ihr Heimatverzeichnis herunter und entpacken die ZIP-Datei. In der einfachen Variante enthält sie neben Lizenzangaben und einem README die Dateien docker-compose.yml und die versteckte Datei .env. Bei der erweiterten Variante kommen die Dateien nginx.conf und nginx.ssl.conf hinzu.

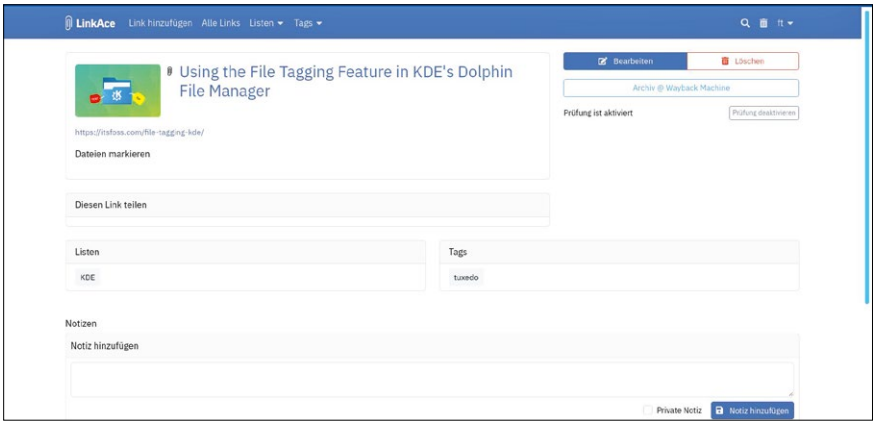
Passwörter setzen

Bevor es weitergeht, müssen Sie in der .env-Datei zumindest die Einträge POSTGRES_PASSWORD und REDIS_PASSWORD ändern. Verwenden Sie eine andere Datenbank als MySQL, dann ersetzen Sie den Namen dort entsprechend. Nach dem Speichern geht es auch schon mit dem Befehl docker-compose up -d in den Endspurt. Das Aufsetzen kann einige Minuten dauern – immerhin rollt der Aufruf die Anwendung, den Webserver und die Datenbank nach den Vorgaben in der Compose-Datei aus. Am Ende erhalten Sie eine URL, um das Web-Interface von Linkace zu starten.

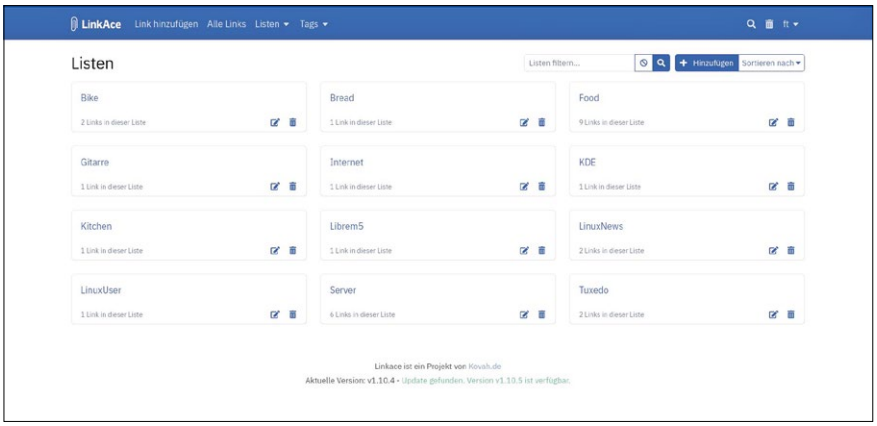
Weitere, teils optionale Schritte vor dem Verwenden von Linkace fasst die Dokumentation im Abschnitt *Post Setup* zusammen. Auf die wichtigsten davon gehen wir im Folgenden ein. Zunächst wechseln Sie oben rechts in die *Einstellungen*. Dort sehen Sie das Bookmarklet, das Sie in Ihre Lesezeichenleiste ziehen. Gleich darunter wartet die Erstellung eines API-Tokens. Darunter erstellen Sie einen Nutzer samt Passwort und E-Mail-Adresse. Falls Sie sich mit Zwei-Faktor-Authentifizierung zusätzlich absichern möchten, finden Sie eine Anleitung in der Dokumentation der *User Settings*.

Im weiteren Verlauf legen Sie Ihre Präferenzen bezüglich Sprache, Zeitformat, Privatsphäre und einiger Voreinstellungen für das Web-Interface fest. Am Ende der Seite entscheiden Sie, ob Sie den Light oder Dark Mode bevorzugen oder den Voreinstellungen der Desktop-Umgebung folgen möchten. Nicht zuletzt entscheiden Sie, auf welchen Social-Media-Plattformen Sie Ihre Links gegebenenfalls teilen möchten.

Neben den *Einstellungen* gibt es noch die sich zum Teil überschneidenden *Systemeinstellungen*. Hier gilt es zunächst, ein Cron-Token zu erstellen. Es dient für periodische Überprüfungen der Links, für Backups und für die Sicherung in der Wayback Machine. Wie Sie einen Cron-



8 Ein Klick auf *Alle Links* zeigt erwartungsgemäß eine Übersicht über alle gespeicherten Links mit einem Thumbnail der entsprechenden Webseite.



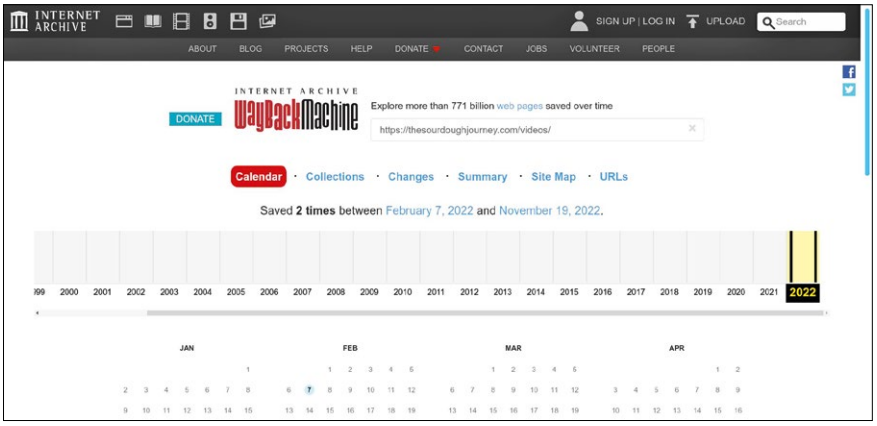
9 Analog zeigt auch ein Klick auf *Alle Listen* alle bisher angelegten Listen an, die sich filtern, bearbeiten oder löschen lassen.

Dateien zum Artikel herunterladen unter

www.linux-user.de/dl/48308

job für Linkace aufsetzen, zeigt der Kasten Cronjob für Linkace.

Linkace bietet beim Sortieren, Suchen und Kategorisieren durchaus mehr Optionen als die übliche Lesezeichenverwaltung im Webbrowser. Sie ändern nach Belieben einzelne Links von öffentlich zu privat und umgekehrt. Jedem Link lässt sich eine Beschreibung hinzufügen. Gelöschte Links verbleiben im Papierkorb, bis Sie ihn leeren. Hinzu kommen RSS-Feeds für private und öffentliche Links. Über ein CLI-Interface lassen sich einige Befehle zur Administration einsetzen. Upgrades von Linkace fallen ebenfalls leicht, wie die Dokumentation belegt.



10 Einen geöffneten Link können Sie nicht nur teilen, bearbeiten und löschen, sondern auch an die *Wayback Machine* senden oder mit einer Notiz versehen. Links unten wird Ihnen der Verlauf zu diesem Link angezeigt.

Fazit

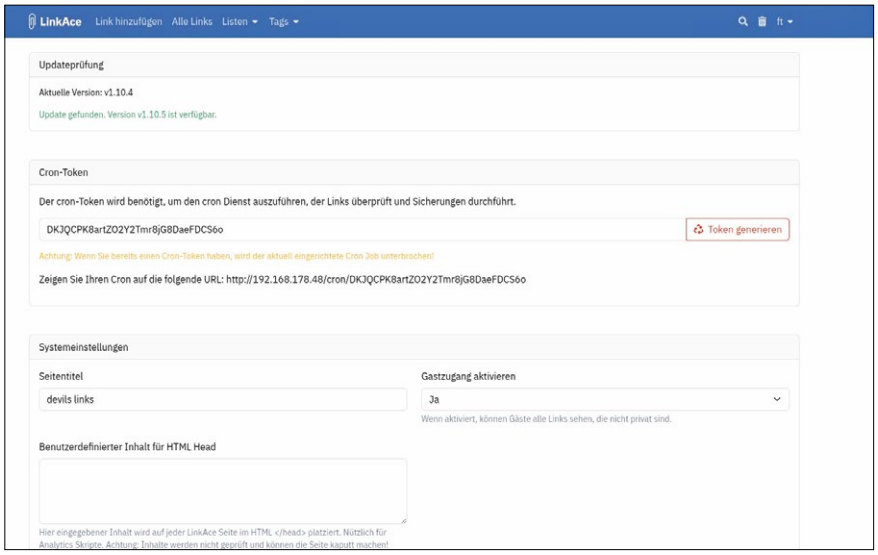
Floccus und Linkace arbeiten an einer besseren Handhabung von Lesezeichen, allerdings mit unterschiedlicher Ausrichtung. Floccus sorgt für eine sichere Synchronisation, bei der Sie die Daten selbst kontrollieren. Linkace konzentriert sich auf eine übersichtliche Verwaltung auch großer Link-Sammlungen. Der Entwickler nimmt auf Github Vorschläge für Funktionen in der anstehenden Version 2 entgegen. Dort finden Sie auch das Forum zur Anwendung. Egal, für welche der beiden Tools Sie sich entscheiden: Es bleibt das gute Gefühl, dass keine Daten in den Clouds von Google, Mozilla oder anderen Cloud-Anbietern landen, sondern alles unter eigener Kontrolle bleibt. (*tle*)

Cronjob für Linkace

Um Links zu überprüfen, sie in der Wayback Machine zu melden und um Backups zu erstellen, benötigt Linkace einen Cronjob. Einen solchen legen Sie am einfachsten über den Befehl `crontag -e` an. Darin legen Sie einen Job wie den folgenden an:

```
* * * * * wget -qO- http(s)://linkace-example.com/cron/WPvv4mxM6nr22Aq4rVf1qEKutsXLTgyw
```

Den Teil hinter `.../cron/` erstellen Sie als Cron-Token in den Sytemeinstellungen 11.



11 In den Einstellungen lässt sich unter anderem ein Token generieren, den Sie für das korrekte Funktionieren zeitgesteuerter Cron-Jobs benötigen.

Weitere Infos und interessante Links

www.linux-user.de/qr/48308

Wayland, Flatpak und Pipewire unter OpenSuse

Auf zu neuen Ufern

Neue Besen kehren bekanntlich gut. Aber trifft diese Binsenweisheit auch auf die neuen technischen Ansätze Wayland, Flatpak und Pipewire zu? Peter Kreußel

README

Was bringt es, von X11 nach Wayland umzusteigen? Lösen Flatpak-Pakete wirklich das Problem, dass selbst OpenSuse Tumbleweed nur veraltete Pakete für bestimmte Programme anbietet? Und lassen sich die Soundprobleme lösen, die viele Nutzer immer noch frustrieren, wenn man Pulseaudio durch das neuere Pipewire ersetzt? Diese OpenSuse-Tipps prüfen den Status Quo.

Von Mitte der 1990er-Jahre bis 2015 blieben einige Grundfesten eines Linux-Systems unverändert: Als grafische Oberfläche lief ein X-Server, sämtliche Software stammte aus den von den Distributionen mitgelieferten Paketen. Ab etwa 2015 stand schließlich zur Debatte, das uralte X-Window-System durch Wayland zu ersetzen. Zu dieser Zeit stellte auch Alexander Larsson mit seinem Paketsystem Xdg-app (heute: Flatpak) generische, auf praktisch sämtlichen Linux-Distributionen lauffähige Softwarepakete vor. Die jüngste und grundlegende Veränderung betrifft das Soundsystem Pulseaudio, das die Distributionen zunehmend durch das neue Pipewire-Framework ersetzen.

Geschlossene Gesellschaft

Eine der größten Einschränkungen, mit denen Linux Windows-Umsteiger konfrontiert, ist die Tatsache, dass sich unter Linux zunächst lediglich für die jeweilige Distribution vorgesehene Pakete installieren lassen. Im Gegensatz dazu funktionieren unter Windows generische `setup.exe`-Dateien über mehrere Versionen des Betriebssystems hinweg.

Das hängt damit zusammen, wie die beiden Systeme mit Hilfsprogrammen umgehen, den sogenannten Bibliothe-

ken: Windows überlässt die Verwaltung der Software selbst und stellt lediglich ein System zur Verfügung, das es erlaubt, mehrere Versionen einer Bibliothek parallel zu installieren. OpenSuse dagegen stellt mit seiner zentralen Paketverwaltung 1 sicher, dass alle Programme dieselbe Version einer systemweit installierten Bibliothek nutzen.

Jede Distribution enthält in jedem Release andere Versionen dieser Hilfsprogramme. In den meisten Fällen bedeutet das, dass Programme für jede Distribution neu aus dem Quellcode kompiliert werden müssen – eine Aufgabe, die nicht immer leicht gelingt und die etliches an Erfahrung voraussetzt. Genau deswegen ist es üblich, das an die Entwickler der Distributionen zu delegieren und die mitgelieferten Pakete zu installieren.

Allerdings wird es für die Distributionen schwieriger, einen möglichst großen Querschnitt der stetig wachsenden Anzahl freier Programme aktueller Versionen zu paketieren: Die Zahl der verfügbaren Programme und das Tempo der Entwicklung in der Welt der freien Software nimmt stetig zu, die Ressourcen der Distributoren eher nicht.

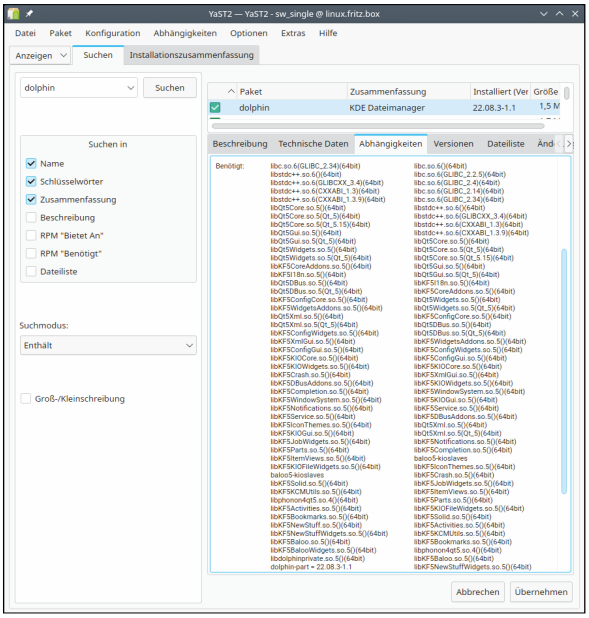
Für die Entwickler einer Software gestaltet es sich ebenfalls aufwendig, fertige Pakete für mehrere Distributionen bereitzustellen: Der Bau von Paketen für RPM-basierte Systeme wie OpenSuse und Fedora, für DEB-basierende Distributionen wie Debian und Ubuntu oder für Arch Linux läuft grundverschieden ab. Selbst Linux-Initiator Linus Torvalds beschwerte sich auf der DebConf 2014 darüber, wie schwierig es sei, seine Tauchcomputersoftware Subsurface 2 unters Volk zu bringen.

Linus glaubte 2014, noch keine geeignete Lösung für das Problem zu kennen. Doch bald darauf standen auf der Webseite von Subsurface neben nativen Paketen für Ubuntu, Debian, Fedora und OpenSuse auch generische Appimage-Pakete bereit, die unter allen Linux-Distributionen funktionieren 3.

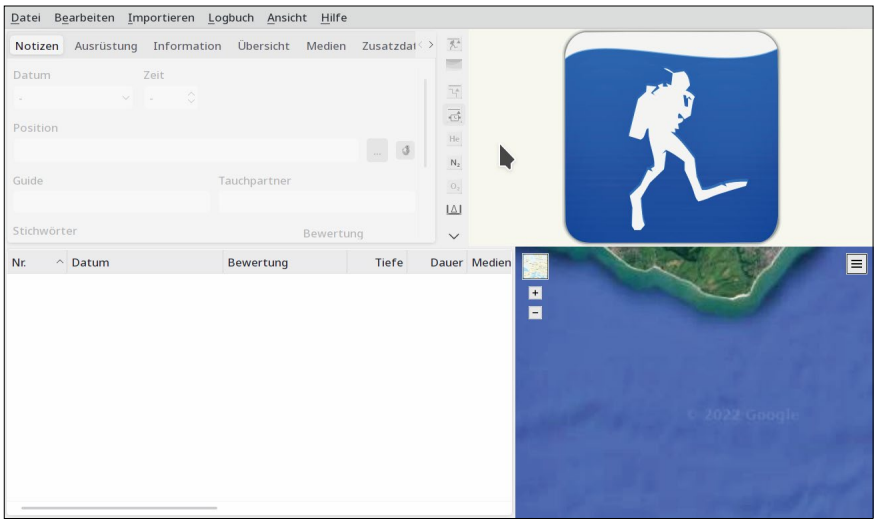
Von hinten aufgezäumt

Appimage-Pakete umgehen das Problem der unterschiedlichen Bibliotheken dadurch, dass sie nicht nur das eigentliche Programm enthalten, sondern auch dessen Abhängigkeiten. Bei einem solchen Paket handelt es sich um ein selbstentpackendes Archiv, das Sie lediglich im Dateimanager anklicken müssen, um das enthaltene Programm zu starten. Appimages greifen ausschließlich auf das Home-Verzeichnis zu und tasten das System nicht an. Deswegen müssen Sie im Regelfall auch keine zusätzliche Software installieren.

Ein Nachteil von Appimage-Paketen liegt in ihrer Größe: Das native OpenSuse-Paket von Subsurface umfasst lediglich 9 MByte, das Appimage dagegen



1 Die zahlreichen benötigten Hilfsprogramme einer Anwendung – hier des KDE-Dateimanagers – stellt eine Distribution für alle Programme in einer einzigen Version bereit.



2 Die von Linus Torvalds initiierte Tauchcomputersoftware Subsurface bietet ein gutes Beispiel dafür, wie schwierig es für Softwareentwickler ist, ihre Programme unter Linux dem Endnutzer zugänglich zu machen.

113 MByte. Das spielt bei einer Handvoll von Programmen hinsichtlich Download und Plattenplatz kaum eine Rolle. Einer der Hauptgründe, weswegen die Linux-Distributionen dennoch den Aufwand betreiben, um nur eine Version jeder der zahlreichen genutzten Bibliotheken installieren zu müssen, liegt in der Hauptspeicherbelegung: Schwergewichte wie Qt erfordern gut und gern einige zig MByte RAM. Teilen sich alle Programme dieselbe Qt-Version, dann lädt das System sie nur ein Mal in den Hauptspeicher. Bei unterschiedlichen Versionen, wie sie bei distributionsübergreifenden Paketen zwangsläufig auftreten, erfolgt das einmal pro laufendem Programm.

Negativ fällt an den ansonsten praktischen Appimages außerdem auf, dass die von OpenSuse laufend bereitgestellten Sicherheitsaktualisierungen für sie nicht greifen: Sie enthalten ja jeweils eine eigene Version der möglicherweise fehlerhaften Bibliothek. Es ist ihnen nicht ohne Weiteres anzusehen, um welche Version es sich dabei handelt.

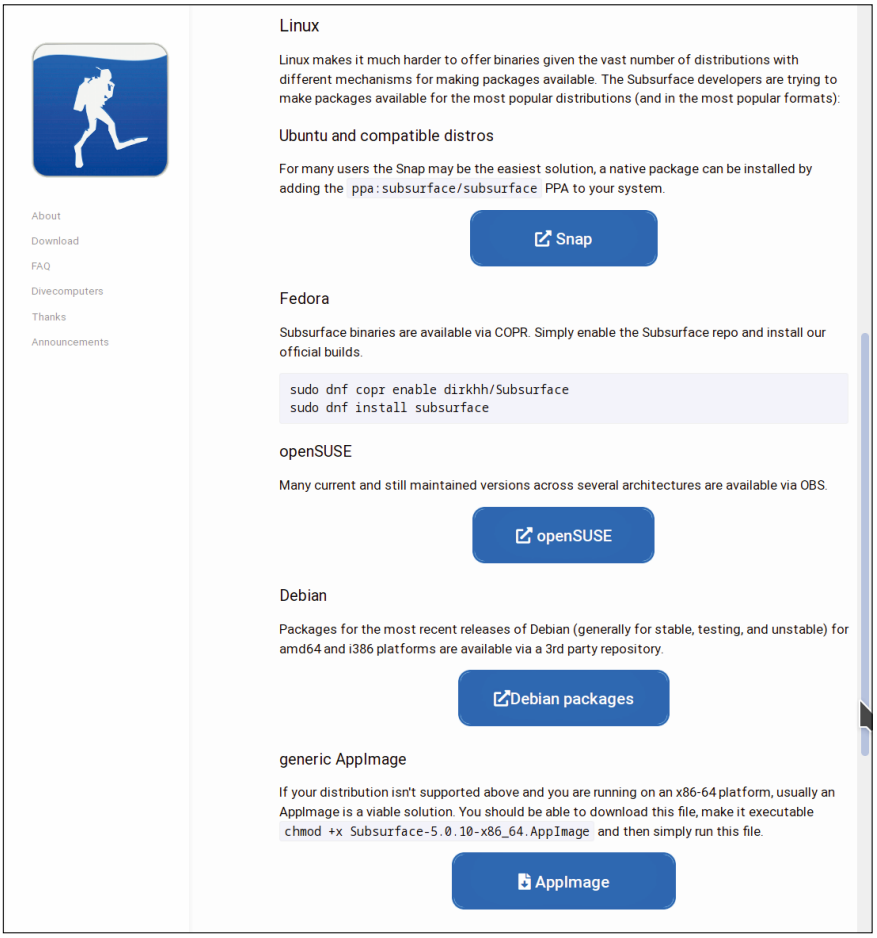
Flatpak gilt gegenüber dem seit 2004 prinzipiell verfügbaren Appimage als vergleichsweise moderneres plattformübergreifendes Paketformat. Es bügelt einen Teil dieser Nachteile durch sogenannte Runtimes aus, also Sammlungen häufig gebrauchter Abhängigkeiten. Daraus bedienen sich die einzelnen Flatpak-Pakete und teilen die Komponenten dann mit anderen Flatpak-Paketen, wenngleich nicht mit dem restlichen System. Die Flatpak-Entwickler versorgen die Runtimes außerdem mit Bugfixes.

Um Flatpaks zu nutzen, installieren OpenSuse-Anwender zunächst das Paket *flatpak* und fügen dann mit den Aufrufen aus Listing 1 das Standard-Flatpak-Repository hinzu und frischen den lokalen Katalog auf. Existieren schon Pakete, dann spielt dieses Update genau wie `zypper up` verfügbare Updates ein.

Etwas überspitzt formuliert installiert Flatpak also ein zweites System parallel zu OpenSuse – eigene Programme mit eigenen Bibliotheken, die es wie OpenSuse zentral pflegt. Flatpak verhält sich wie ein Paketmanager, der Abhängigkeiten automatisch mitinstalliert: `flatpak search` durchsucht das Repository, `flatpak install` installiert ein Paket, `flatpak uninstall` entfernt es wieder. Auch die KDE- und Gnome-Appstores Discover und Gnome Software unterstützen das Paketformat.

Flatpak bietet außerdem eine Container-Architektur, die Programme vom restlichen System abschotten kann: Der Datei- und Netzzugriff lässt sich blockieren oder auf einzelne Verzeichnisse beschränken. Jedes Paket kann diese Mechanismen ein- oder ausschalten. In der Praxis sind sie meist deaktiviert 4.

Standardmäßig fragt Flatpak bei der Installation nach dem Root-Passwort.



3 Die gegenwärtigen Entwickler von Subsurface machen sich die Mühe, gleich vier Linux-Distributionen mit einem eigenen Paket zu bedienen. Alle weiteren Distros deckt das generische Appimage ab.

Listing 1: Flatpak installieren

```
# flatpak remote-add
--if-not-exists flathub https://
flathub.org/repo/flathub.
flatpakrepo
# flatpak update
```

Eine Installation ohne Root-Rechte gestattet die Option `--user`. Das Mischen von systemweiten und benutzerspezifischen Installationen birgt aber den Nachteil, dass das System umfangreiche Runtimes mehrfach herunterladen und aktuell halten muss.

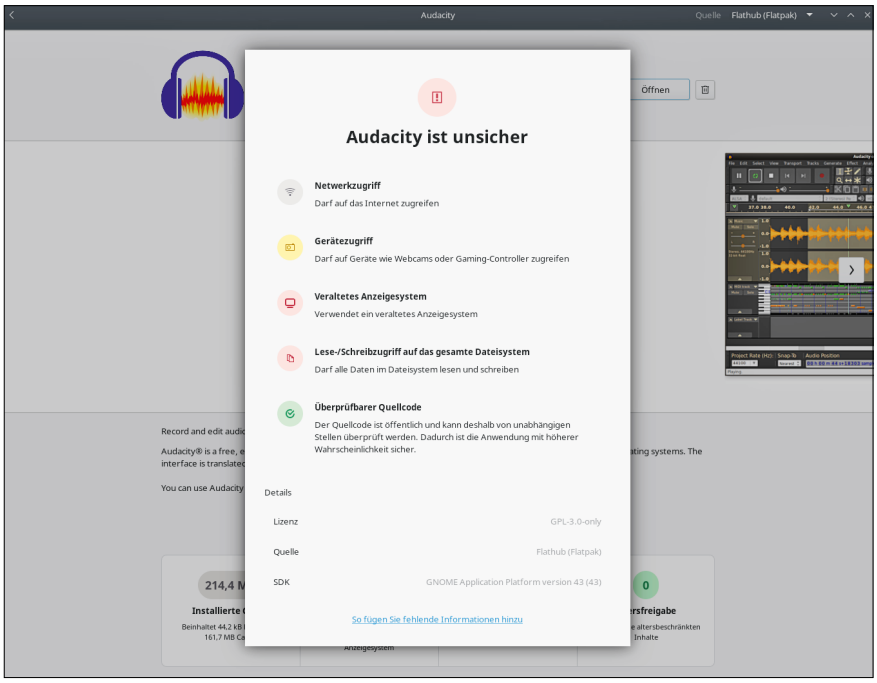
Wer den nötigen Zeitansatz vergleicht, um ein Linux- und ein Windows-System aktuell zu halten, spürt den technischen Vorteil der unter Linux üblichen Praxis, Bibliotheken in exakt einer Version vorzuhalten. Wahr ist allerdings ebenso, dass die Distributionen bei der Pflege ihrer Paket-Repositories mehr und mehr an ihre Grenzen stoßen und Linux-Anwender in Zukunft wohl viele Programme – vielleicht sogar alle, mit Ausnahme zentraler Systemkomponenten – über Flatpak-Pakete installieren werden.

Fenster der Vergangenheit

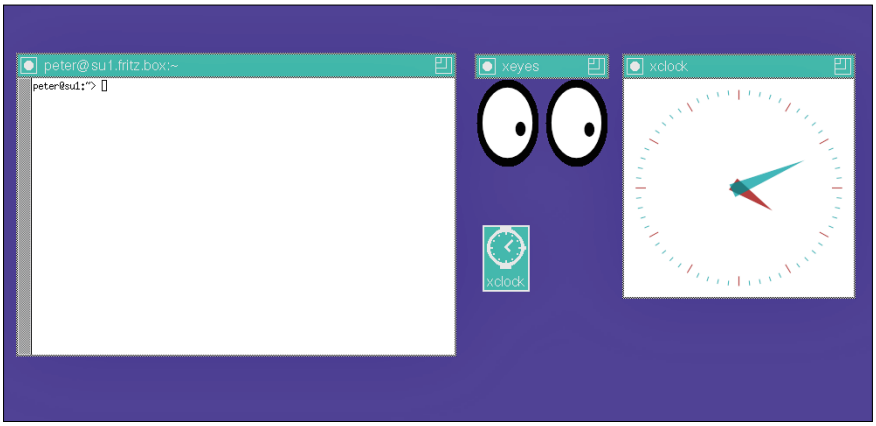
Die Wurzeln des bis heute immer noch eingesetzten grafischen X-Window-Systems, auch bekannt als X11 5, reichen bis ins Jahr 1984 zurück. Sein Konzept, jegliche Kommunikation, auch mit lokalen Anwendungen, über eine Pseudo-Netzwerkschnittstelle abzuwickeln, entstammt dem Zeitalter des Terminalzugriffs auf Großrechner.

Mehr als ein Jahrzehnt lang störte diese archaische Grundstruktur unter Linux niemanden. Zum Problem wurde sie erst im Kontext der etwa 2005 aufkommenden 3D-Desktop-Effekte, die Sie in Abbildung 6 sehen. Bei 3D-Animationen, die mit mindestens 50 Hz Bildschirmwiederholfrequenz ablaufen, führt die zusätzliche Latenz der Pseudo-Netzwerkschnittstelle leicht zum Ruckeln oder zu Blitzern (sogenannten Tearing-Artefakten).

Es gab weitere Gründe, den X-Server in Rente zu schicken: Unter X11 erhalten alle Programme ungeprüft Zugriff auf Maus, Tastatur und Bildschirm. Das macht es zum Beispiel selbst Schadsoftware, die nur mit Benutzerrechten läuft, leicht, Passwörter abzugreifen. Auch

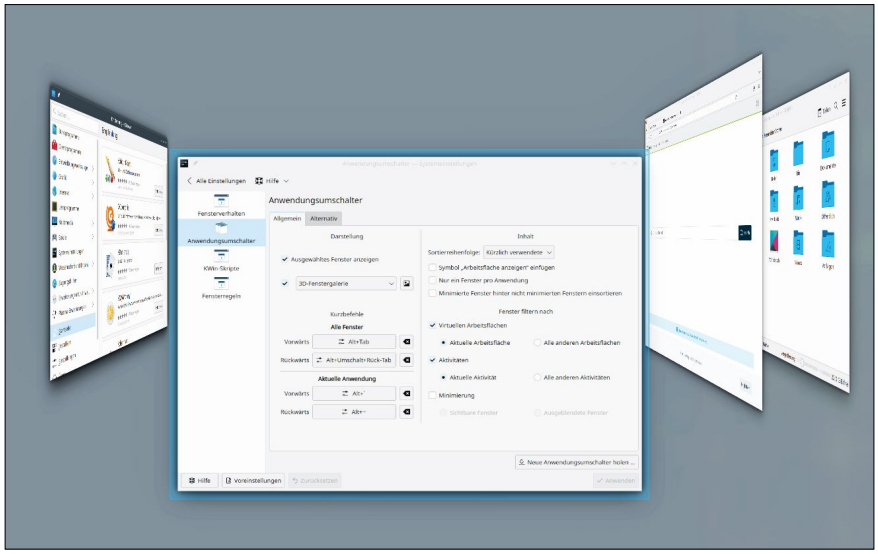


4 Das Flatpak-Paket des Audio-Editors Audacity zeigt exemplarisch, welche zusätzlichen Absicherungsmöglichkeiten Flatpak beherrscht.

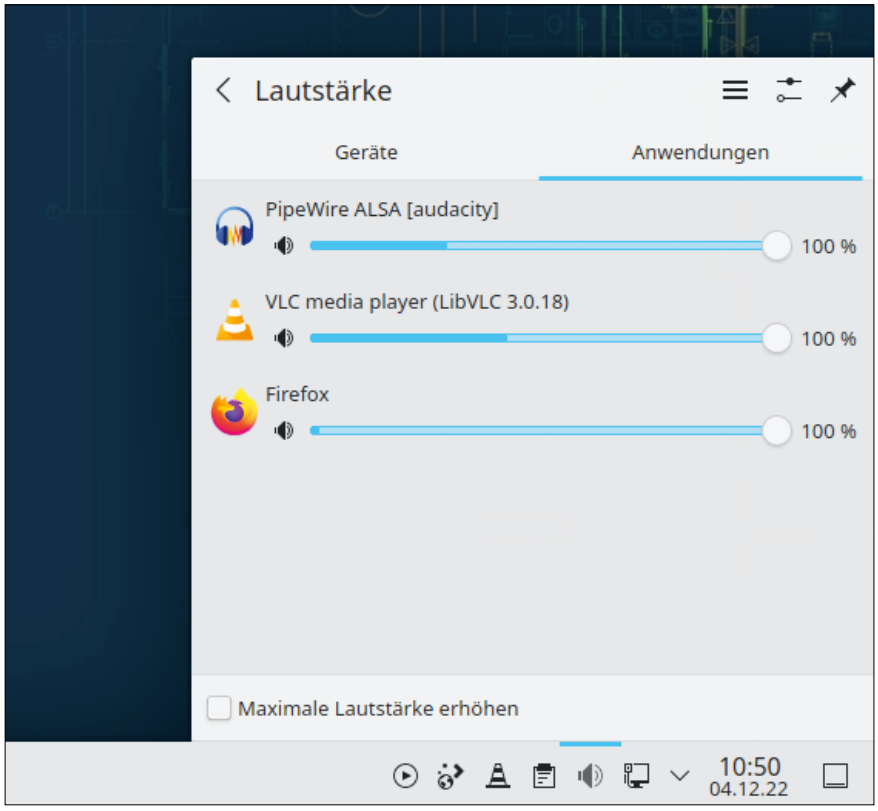


5 Die ressourcenschonenden Zeichenfähigkeiten des X-Servers bieten heute keinerlei Mehrwert mehr: Grafiken ohne Kantenglättung, Farbverläufe und Schatten wirken im 21. Jahrhundert letztlich einfach zu altmodisch.

nutzt kein modernes Programm mehr die Funktionen des X-Servers zur Schriftdarstellung und zum Zeichnen: Ohne Kantenglättung oder halbtransparenten Schlagschatten wirkten damit gezeichnete Oberflächen archaisch. Unnützer Code bedeutet außerdem immer auch ein unnötiges Sicherheitsrisiko.



6 3D-Effekte wie beim heute noch in KDE verfügbaren Anwendungsumschalter *3D-Fenstergalerie* führen unter X11 zu Problemen.



7 KDE und ähnlich auch Gnome regeln dank Pulseaudio nicht nur die Lautstärke der Audiogeräte, sondern auch die der einzelnen Anwendungen.

Der X-Server gestattet es, Bitmaps wie die Oberfläche eines Schalters im Server zwischenzuspeichern, was sich beim Arbeiten via Netzwerk als nützlich erweist. Stürzt aber ein Programm ab, dann bleiben die Grafikressourcen bis zum Neustart von X11 im Speicher. Es gab also genug alte Zöpfe, die einen Neuansatz lohnenswert erscheinen ließen.

Ob sich jedoch der Umstieg von X11 nach Wayland im Moment tatsächlich lohnt, hängt auch davon ab, ob Sie Gnome oder KDE nutzen. Gnome begann bereits 2013 mit der Integration der Wayland-Kompatibilität, während KDE zu dieser Zeit mit dem Wechsel von KDE 4 auf 5 beschäftigt war. Daher läuft Gnome unter Wayland schon seit längerer Zeit stabil, während KDE mit Plasma 5.26.4 in Tumbleweed diesen Zustand gerade einmal mit inzwischen vergleichsweise kleinen Einschränkungen erreicht. Frühere Fehler scheinen immerhin gelöst, wie eine versagende Zwischenablage, nicht mehr zuklappbare Kontextmenüs oder der Effekt, dass KDE bestimmte Anwendungen einfach „vergisst“, sodass sie sich nicht mehr durch Klick auf das Fenster aktivieren lassen.

Fenster der Zukunft

Es kostet Sie so gut wie keinen Aufwand, KDE oder Gnome unter Wayland auszuprobieren: Gnome-Anwender installieren im YaST-Modul *Software* als *Schema* die *Gnome-Desktop-Umgebung (Wayland)*, wobei es eigentlich lediglich um das Paket *gnome-session-wayland* geht. KDE-Anwender hingegen benötigen keine zusätzlichen Pakete.

Zum Starten genügt es, im Anmeldebildschirm als *Arbeitsflächen-Sitzung* entweder *Plasma (Wayland)* oder *GNOME on Wayland* auszuwählen. Sind Sie mit der Stabilität des Desktops unter Wayland nicht zufrieden, wählen Sie bei der nächsten Anmeldung wieder eine *X11-* oder *Xorg*-basierte Sitzung.

Mancher wird sich fragen, welche Vorteile das vergleichsweise unausgereifte Wayland gegenüber X11 letztlich bringen soll. Hier sei erwähnt, dass Wayland die zwei Ziele, mit denen es entworfen

wurde, bereits erreicht: Ausschließlich das Wayland-Programm mit Fokus besitzt Zugriff auf Maus und Tastatur. Auf dem 8-Kern-Rechner des Autors waren zwar auch unter X11 praktisch nie Hänger oder ein Tearing bei den Desktop-Animationen wahrzunehmen, dennoch wirkt der Ablauf der Animationen unter Wayland glatter.

Ressourcen-Einsparungen sind im Moment nicht zu erwarten, da gegenwärtig während einer Wayland-Sitzung sogar zwei Instanzen des X-Servers im Hintergrund laufen: Der Anmeldebildschirm basiert in der Voreinstellung auf X11, auch wenn er eine Wayland-Session starten soll. Außerdem wartet im Hintergrund der Desktop-Sitzung ein X-Server, der sich um noch nicht Wayland-kompatible Programme kümmert. Alle Anwendungen, die auf die Toolkit-Bibliotheken Qt und GTK aufsetzen, sollten dank ihres Unterbaus ohne weitere Veränderungen bereits mit Wayland zusammenarbeiten.

Um zu ermitteln, ob ein Programm im Wayland-Modus läuft, installieren Sie das Paket *xeyes* 5: Folgen seine Augen dem Mauszeiger, wenn Sie ihn über ein Programmfenster bewegen, dann läuft es unter X11. Bleiben sie starr, dann liegt eine Wayland-Anwendung vor. Das demonstriert zugleich, dass dort Benutzereingaben immer nur ein Programm erreichen und für die nicht aktiven Anwendungen verborgen bleiben.

Klang der Zukunft

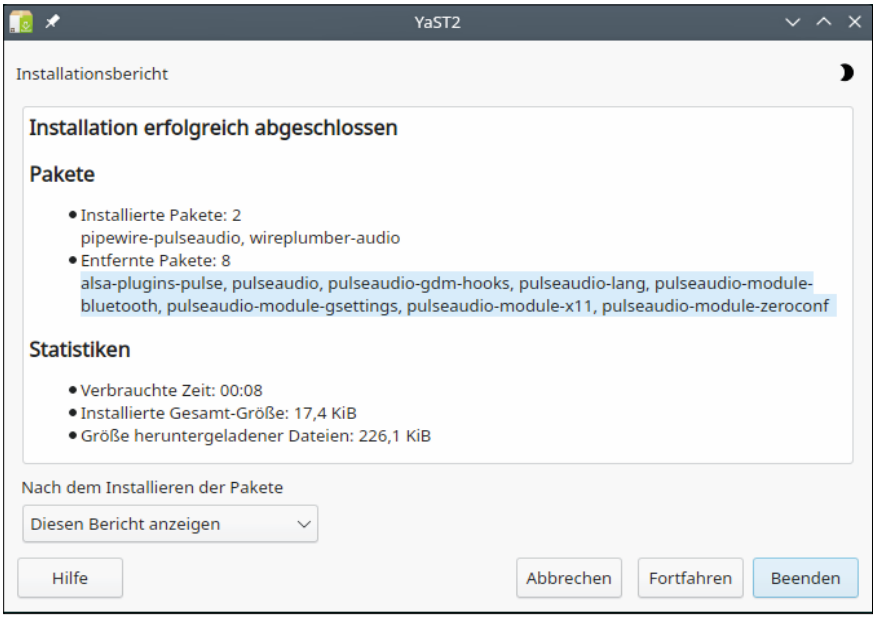
Schon der Linux-Kernel spielt Sound aus verschiedenen Quellen gleichzeitig ab. Seit 2012 benutzt OpenSuse trotzdem den Soundserver Pulseaudio. Die Lautstärkeregler der Desktop-Umgebungen 7 ermöglichen es, die Lautstärke einzelner Programme zu regeln, auf bestimmte Soundkarten umzuleiten oder die Priorität eines nur temporär angeschlossenen USB- oder Bluetooth-Audiogeräts so festzulegen, dass es sofort nach dem Erkennen die Wiedergabe übernimmt. Zu guter Letzt macht die Tatsache Pulseaudio unverzichtbar, dass manche Programme wie Firefox ohne es gar keinen Ton mehr abspielen – bis jetzt, denn mit Pipewire steht ein Nachfolger in den Startlöchern. Tatsächlich gibt es einige Gründe, Pulseaudio durch einen modernen Nachfolger zu ersetzen. Dazu zählt etwa der durchwachsene Ruf von Pulseaudio hinsichtlich Stabilität. Vor allem die Frühphase des Einsatzes unter Ubuntu ab Version 8.04, bei der sich ein Großteil der Bug-Reports im Bereich Audio auf Pulseaudio zurückführen ließ, blieb Linux-Veteranen im Gedächtnis.

Tatsächlich kämpfte der Autor dieses Artikels unaufhörlich mit dem Problem, dass Pulseaudio immer wieder hartnäckig die Einstellungen vergaß, dazu zählt insbesondere die Deaktivierung des in der Grafikkarte integrierten Sound-Devices. Nach dem Umstieg auf Pipewire im August 2021 traten derlei Probleme jedoch nicht mehr auf. Andererseits erforderten bis Anfang 2022 gelegentliche Abstürze des Servers einen Neustart von Pipewire. Die Software gilt noch als instabil; ihre Entwickler rechnen, wie die niedrige Versionsnummer andeutet, noch mit grundlegenden Fehlern.

Zur hohen Nutzerzufriedenheit trotz der frühen Version kommt hinzu, dass Pipewire zwei Fliegen mit einer Klappe schlägt: Es ersetzt nicht nur Pulseaudio, sondern gleichzeitig auch den für den professionellen Aufnahmeeinsatz mit minimalen Latenzen konzipierten Soundserver Jack. Sowohl für Pulseaudio als auch für Jack ausgelegte Programme funktionieren auf Anhieb.

Listing 2: Pipewire starten

```
# systemctl --user enable --now
pipewire.socket
# systemctl --user enable --now
pipewire-pulse.socket
# systemctl --user enable --now
wireplumber.service
```



8 Um zu Pulseaudio zurückzukehren, genügt es, die von YaST bei der Pipewire-Installation als *entfernt* gelisteten Programme wieder zu installieren.

Weitere Infos und interessante Links
www.linux-user.de/qr/47808

Anfangs war Pipewire ausschließlich als Tool für Video-Streaming gedacht, das Videokonferenzprogrammen anders als unter X11 erst nach expliziter Nachfrage das Aufnehmen von Wayland-Fenstern gestattet. Diese Funktion ging mit dem Einbau der Audio-Routing-Fähigkeiten nicht verloren.

Um von Pulseaudio auf Pipewire umzusteigen, installieren Sie die Pakete *pipewire* und *pipewire-pulseaudio*. Dann starten Sie die entsprechenden Dienste mit den Befehlen aus Listing 2. Für eine Rückkehr zu Pulseaudio notieren Sie sich die bei diesem Vorgang deinstallierten Pulseaudio-Pakete, die Sie für unser Beispiel Abbildung 8 entnehmen können.

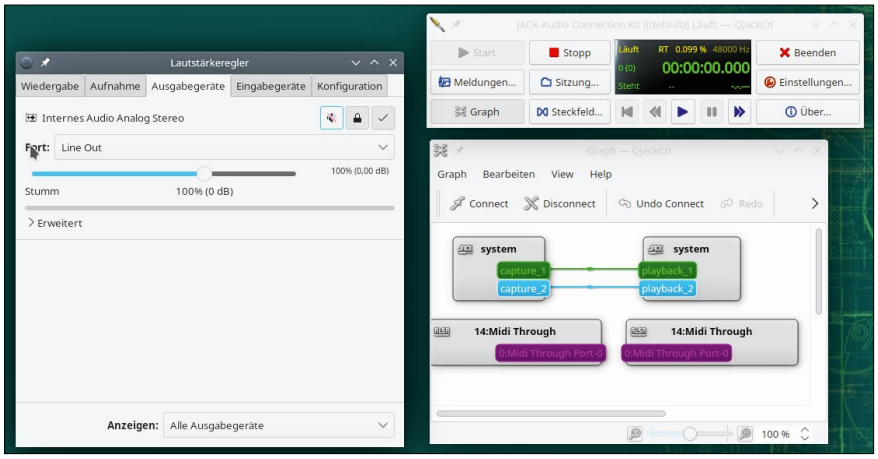
Pipewire befindet sich noch in einer Phase der zügigen Verbesserung, von der Tumbleweed-Anwender profitieren. Die in Leap enthaltene Version 0.3.49 vom März 2022 sollte ebenfalls bereits stabil genug laufen, damit sich ein Umstieg lohnt. Sowohl das altbekannte Verwaltungswerkzeug für Pulseaudio, Pavucontrol, als auch QJackCtl für Jack lassen sich wie gewohnt weiterverwenden 9.

Fazit

Wayland, Flatpak und der neue Soundserver Pipewire schicken sich an, altgediente Techniken wie X11, die distributionsgebundenen RPM-Pakete und Pulseaudio zu ersetzen. Dass den neuen Technologien die Zukunft gehört, scheint dementsprechend unausweichlich.
X11 gilt architektonisch als veraltet und unsicher; selbst seine eigenen Entwickler votieren dafür, es mittelfristig in Rente zu schicken. Viele Distributoren stöhnen unter der Last, immer mehr Programme in aktueller Version anbieten zu müssen. Wenn die Entwickler selbst zunehmend ein generisches Paket ihrer Software für alle Linux-Varianten ausliefern, gelangen Anwender auch dann an die aktuellste Version der Software, wenn die Distributions-Updates hinterherhinken.

Pulseaudio zeigt sich in der Praxis auch nach 10 Jahren Einsatz bei OpenSuse immer noch fehlerbehaftet. Pipewire scheint schon jetzt bei Version 0.3 auf einem deutlich besseren Weg zu sein, wenn es nicht sogar bereits stabiler funktioniert. Es vereinheitlicht darüber hinaus das alltagstaugliche Pulseaudio mit dem auf professionelles Recording zugeschnittenen Jack, was Paul Davis, der Entwickler hinter Jack und dem meistgenutzten freien Musikprogramms Ardour, ausdrücklich lobt.

OpenSuse prescht bei den neuen Techniken weder vor, wie Fedora oder Ubuntu, die Pulseaudio inzwischen durch Pipewire ersetzt haben, noch zwingt es sie dem Nutzer auf. Letzteres versucht etwa Ubuntu, das viele Pakete lediglich noch als Snaps anbietet, also als Ubuntu-spezifisches Pendant zu Flatpaks. Dem Anwender die Wahl zwischen den alten und neuen Technologien zu lassen, wie OpenSuse das tut, ist schon deswegen die richtige Politik, weil Anwendern so der Umstieg ohne großen Aufwand gelingt. (*tle*)



9 Verwaltungsprogramme wie Pavucontrol (links, für Pulseaudio) oder QJackCtl (rechts, für Jack) funktionieren auch mit Pipewire.

Smart Home flexibel per Raspberry Pi steuern

Schalten und walten

Der Markt für die Heimautomation wächst unaufhörlich. Mit entsprechenden Modulen verwandeln Sie Ihren Raspberry Pi in eine smarte Steuerzentrale für Zigbee-Geräte. Erik Bärwaldt

README

Als einer der Pioniere in Sachen Heimautomation mit Zigbee-Komponenten entwickelt das sächsische Unternehmen Dresden Elektronik Ingenieurtechnik GmbH schon seit vielen Jahren Gateway-Module für den Raspberry Pi. Wir klären, was das neue Raspbee-II-Modul kann.

Im Jahr 2022 betrug der Umsatz mit Hausautomationsprodukten in Deutschland knapp 6 Milliarden Euro, Tendenz steigend. Gleichzeitig fällt es immer schwerer, das stetig wachsende Angebot zu überblicken. Häufig sind Lösungen diverser Hersteller untereinander inkompatibel, sodass Kunden nicht das volle Leistungsspektrum der Hausautomation nutzen können.

Doch es geht auch anders: Die Dresden Elektronik Ingenieurtechnik GmbH beschäftigt sich bereits seit rund zehn Jahren mit Lichtsteuerungssystemen auf Basis des Zigbee-Protokolls und bietet für das Smart Home inzwischen zahlreiche Systeme an, die Sie herstellerübergreifend einsetzen können. Für den Raspberry Pi vertreibt das Unternehmen Module für die Hausautomation, die es ermöglichen, ohne teure Gateways und Cloud-Anbindungen die Vorteile des Smart Homes zu genießen.

Beim Raspbee-Modul, das bereits in der zweiten Generation vorliegt, handelt es sich um eine Aufsatzplatine (HAT) für den britischen Kleincomputer, mit deren

Hilfe Sie das System zu einer Steuerzentrale für Smart-Home-Endgeräte wie Leuchten, Alarmsirenen oder intelligente Steckdosen und Schalter umbauen. Dabei unterstützt das Raspbee-II-Modul Endgeräte unterschiedlicher Hersteller, deren Lösungen zur Hausautomation auf dem Zigbee-Protokoll basieren. Dahinter steckt ein Framework für Funknetze, die sich wegen ihres geringen Datenaufkommens und ihres niedrigen Energiebedarfs speziell für die Hausautomation eignen.

Das modular aufgebaute Zigbee-Protokoll lässt sich durch diverse Funktionen erweitern. Manche Hersteller versuchen, Kunden über solche Erweiterungen an sich zu binden, da durch die neuen Funktionen Inkompatibilitäten zu den Geräten anderer Anbieter entstehen und die Anwender somit nicht auf alternative Lösungen umsteigen können. Dem trägt das Zigbee-II-Modul Rechnung, indem die Entwickler Komponenten verschiedenster Hersteller testen und in stetig aktualisierte Kompatibilitätslisten einpflegen.

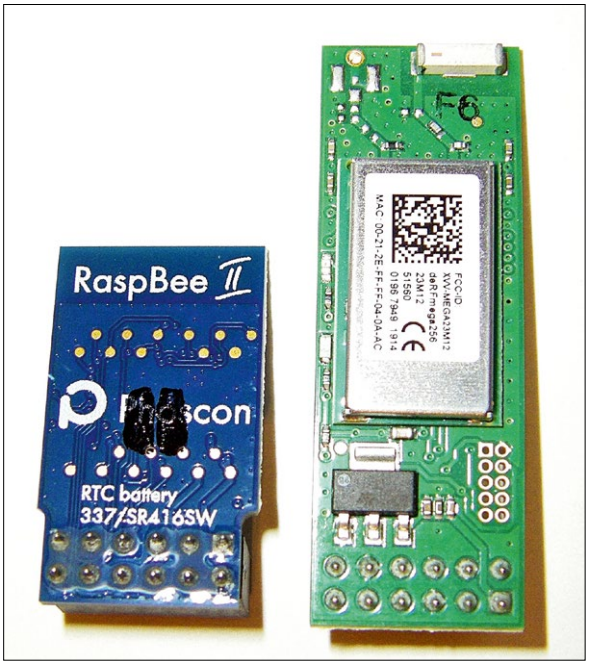
Das jüngste Modul ist im Vergleich zum HAT der ersten Generation nicht nur kompakter, sondern führt außerdem eine wichtige Neuerung ein: Durch eine batteriegepufferte RTC auf dem HAT verrichtet der zur Steuerzentrale für die Hausautomation umfunktionierte Raspberry Pi nun zuverlässig zeitkritische Aufgaben. Bislang funktionierte das System aufgrund der fehlenden Zeitsynchronisation des RasPi beispielsweise bei einem Stromausfall nicht im Zusammenspiel mit zeitgesteuerten Komponenten. Die Batterie soll laut Herstellerangaben mindestens zwei Jahre lang halten und bei täglichem Einsatz des Systems bis zu acht Jahre lang Energie liefern. Es handelt sich dabei um eine austauschbare Knopfzelle 1.

Außerdem bringt das Raspbee-II-Modul einen Leistungsverstärker mit, der eine effektive Reichweite innerhalb von Gebäuden von 30 Metern gestattet. Außerhalb geschlossener Räume sollen bis zu 200 Meter möglich sein. Da Sie bei Zigbee-Installationen ein Mesh-Netz aufsetzen, bei dem Endgeräte wie Leuchten oder intelligente Steckdosen als Repeater agieren, können Sie die Reichweite ohne zusätzliche Hardware weiter erhöhen.

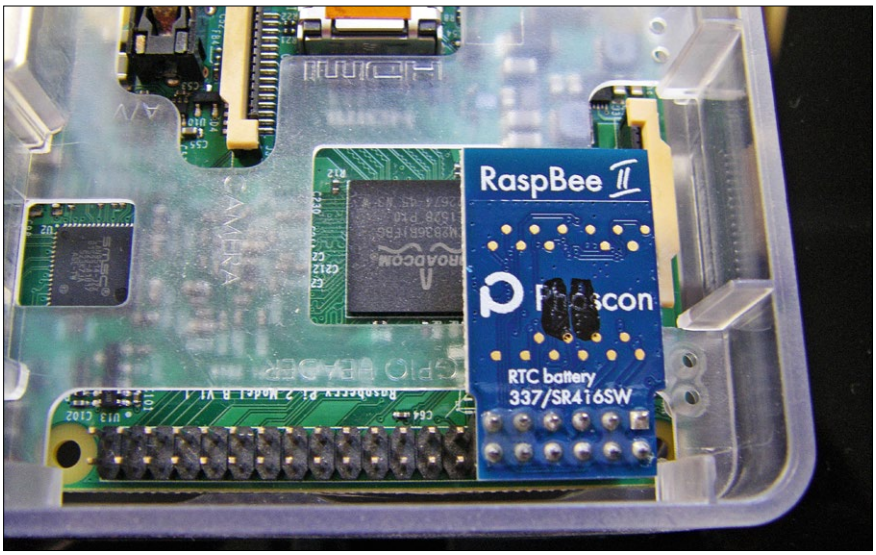
Die Raspbee-HATs werden durch zwei verschiedene Softwarepakete flankiert: Um die Hardware zu konfigurieren, setzen Sie die Plattform deCONZ ein. Das grafische Werkzeug visualisiert Zigbee-Netze, in die Sie Endgeräte unterschiedlicher Hersteller einbinden. Dabei läuft deCONZ im Hintergrund. Die zweite Komponente bildet die Browser-basierte App Phoscon. Sie dient als grafisches Frontend zum Steuern von Lichtinstallationen.

Installieren

Zunächst stecken Sie das Raspbee-II-Modul einfach auf die Stiftleiste des Kleincomputers, und zwar an der zum Slot für



1 Das Zigbee-II-Modul (links) ist im Vergleich zum Vorgänger (rechts) deutlich geschrumpft.



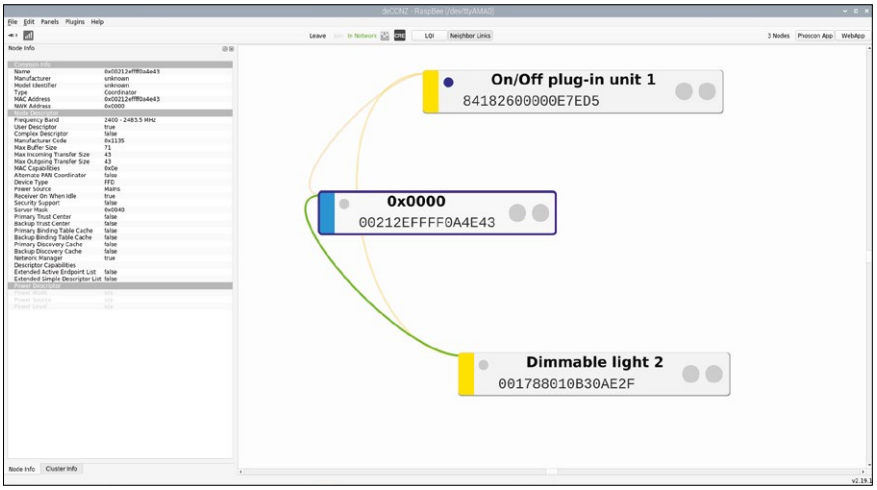
2 Das Zigbee-II-Modul wird am Ende der Kontaktleiste des Raspberry Pi aufgesteckt.

die microSD-Karte befindlichen Seite 2. Das Modul funktioniert mit allen Versionen des Raspberry Pi, sodass Sie zum Beispiel ein älteres Modell für die Hausautomation einsetzen können. Als Betriebssysteme kommen ausschließlich aktuelle Versionen von Raspbian „Buster“ und Pi OS „Bullseye“ infrage.

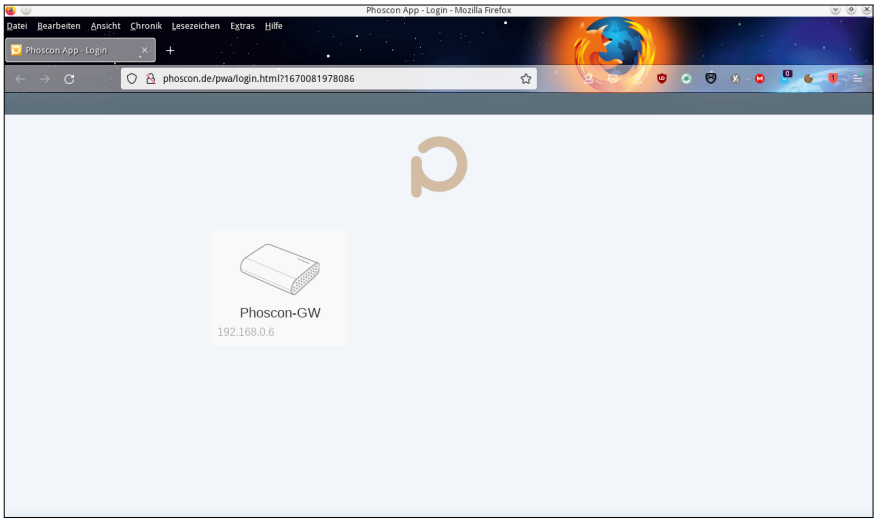
Daneben offeriert der Hersteller insgesamt vier verschiedene Images für microSD-Karten. Sie enthalten ein angepasstes Raspbian „Buster“, auf dem jeweils die Konfigurationsanwendung deCONZ vorinstalliert ist. Bei einem der Abbilder findet sich bereits das Homebridge-Hue-Plugin, mit dessen Hilfe Sie Komponenten des Leuchtensystems Hue von Philips steuern. Die Abbilder verfügen bis auf eines alle über die Raspbian-Arbeitsumgebung, sodass Sie die Konfiguration bequem grafisch ausführen können. Sämtliche Images eignen sich auch für das Raspbee-Modul der ersten Generation.

Die Images mit Desktop-Umgebung umfassen jeweils knapp 880 MByte, das Headless-Abbild ohne Arbeitsumgebung lediglich knapp 395 MByte. Der Anbieter empfiehlt, für alle Images eine schnelle microSD-Karte mit einer minimalen Kapazität von 8 GByte zu nutzen. Sie sollte mindestens den Class-10-Standard erfüllen, um Latenzen im Betrieb zu vermeiden. Alternativ finden Sie auf der Webseite des Anbieters eine ausführliche Anleitung, mit der Sie die für das Raspbee-II-Modul benötigten Softwarepakete in herkömmliche Pi-OS-Abbilder integrieren. Entscheiden Sie sich für die vorgefertigten Abbilder, startet initial automatisch ein Systemupdate sowie die Konfigurationssoftware deCONZ. In deren grafischer Netzdarstellung sehen Sie zunächst nur das vorhandene Gateway 3.

Anschließend öffnen Sie auf einer beliebigen Maschine im lokalen Netz einen Webbrowser und geben dort als Zieladresse die URL http://*RasPi-IP*:80 ein. Nach einer kurzen Startzeit zeigt das Browser-Fenster das Gateway an. Ein Mausklick auf das Gateway-Symbol führt Sie in einen Konfigurationsdialog, in dem Sie ein Passwort für die Anmeldung am Gateway setzen. Zukünftige Einstellungen lassen sich danach nur noch nach dem Einloggen am Gateway vornehmen 4.



3 Im Hauptsegment von deCONZ sehen Sie das Gateway und einzelne Netzkomponenten.



4 Beim Start der Phoscon-App sehen Sie lediglich das Gateway.

Danach fordert Sie die Routine auf, alle ins Zigbee-Netz zu integrierenden Leuchtmittel einzuschalten. Zuvor müssen Sie die Leuchtmittel jedoch auf die Werkseinstellungen zurückgesetzt haben, da das Raspbee-Modul die Komponenten sonst nicht erkennt. Eine Anleitung zum Zurücksetzen der Leuchtmittel liefert Dresden Elektronik für verschiedene Heimautomationshersteller mit.

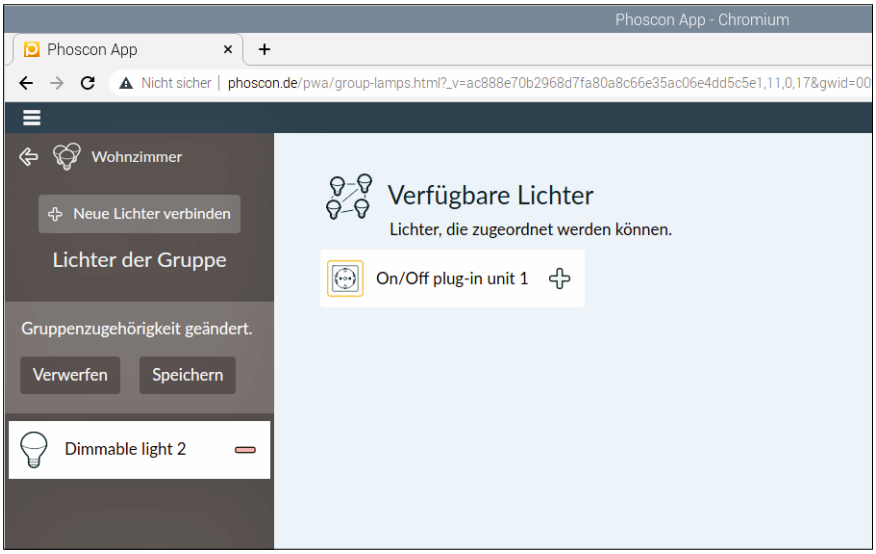
Nach dem Einschalten der Leuchtmittel sucht deCONZ diese und listet sie auf. Dabei zeichnet die Software automatisch Verbindungslinien vom Gateway zu den einzelnen Geräten, um das Mesh-Netz zu skizzieren. Gleichzeitig erscheinen die gefundenen Komponenten in einer Tabelle im Browser-Fenster der Phoscon-App. Ein Klick auf eines der Geräte in deCONZ blendet dessen technische Daten links in einem vertikalen Bereich ein.

Da deCONZ herstellerunabhängig arbeitet, lassen sich Zigbee-kompatible Geräte in Ihr Smart Home einbinden. Vor dem Kauf einzelner Komponenten sollten Sie allerdings einen Blick auf die vom Anbieter bereitgestellte Kompatibilitätsliste werfen, um sicherzugehen, dass die gewünschten Endgeräte mit dem Raspbee-II-System harmonieren.

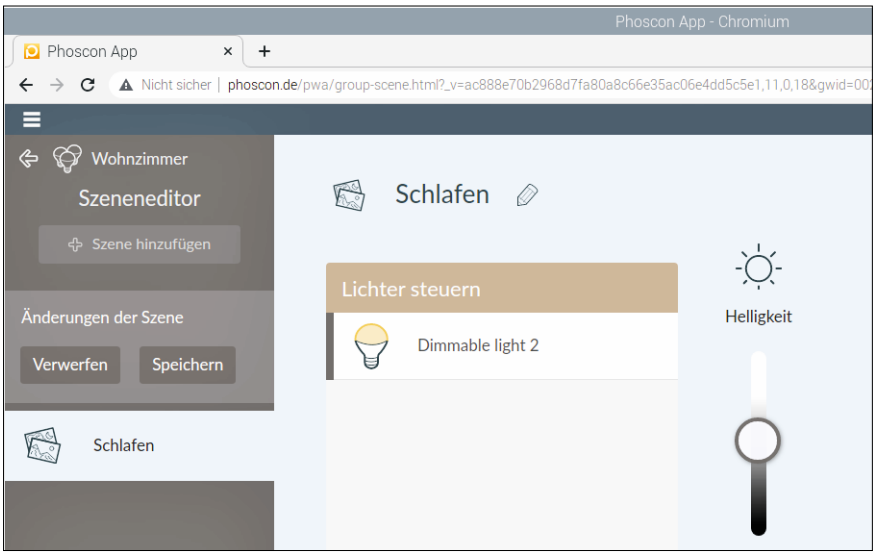
Gruppieren

Sind alle Geräte am Gateway angemeldet, klicken Sie oben links im Browser-Fenster der Phoscon-App auf *Hauptseite*. In einem überlappenden Dialog legen Sie daraufhin eine erste Gruppe an. Gruppen bezeichnen in der Phoscon-App meist unterschiedliche Räume mit Smart-Home-Komponenten.

Nach einem Klick auf *Erste Gruppe erstellen* legen Sie in einem weiteren Dialog einen Gruppennamen fest. Die App unterbreitet ihnen dabei Vorschläge. *Erstellen* Sie die neue Gruppe, gelangen Sie zurück in den Dialog zum Zuordnen der gefundenen Komponenten. Hinter dem Zahnradsymbol unten rechts stoßen Sie auf die Option *Lichter verwalten*. Im da-



5 Grafisch übersichtlich aufbereitet sehen Sie sämtliche Gruppenmitglieder und fügen dem Setup außerdem neue Komponenten hinzu.



6 Der Szeneneditor ermöglicht es, die Geräte individuell zu steuern.

nach eingeblendeten Dialog *Verfügbare Lichter* fügen Sie der Gruppe die gewünschten Komponenten hinzu.

Doch Vorsicht: Einige Komponenten wie Zwischenschalter, die ein herkömmliches Gerät ins Smart Home integrieren, identifiziert die Software ebenfalls als Lichter und listet sie dementsprechend auf. Aussagekräftige Symbole vor den Knoten verraten jedoch, ob es sich um ein Leuchtmittel oder ein anderes Gerät handelt. Mithilfe des Pluszeichens hinter jedem Gerät übernehmen Sie es links in die Gruppenspalte. *Speichern* Sie Ihre Arbeit nach Übernahme aller gewünschten Komponenten in die Gruppe 5.

Szenarisches

Im nächsten Schritt fügen Sie der Installation sogenannte Szenen zu, in denen Sie die Knoten konfigurieren. Dabei lassen Sie etwa Schalter oder Leuchtmittel zeitgesteuert ein- und ausschalten oder im Rahmen des Szeneneditors dimmen.

Über die Option *Szeneneditor* öffnen Sie den Szenendialog, klicken dort auf *Szene hinzufügen* und vergeben einen Namen. Nach einem Klick auf *Erstellen* pflegen Sie anhand der Möglichkeiten, die das aktivierte Gerät unterstützt, die Einstellungen ein und speichern sie 6.

Wechseln Sie zurück ins Gruppenmenü und definieren Sie nun anhand des Dialogs *Zeitsteuerungen*, wann das Tool welche Szene in der jeweiligen Gruppe aktivieren soll. Über *Zeitsteuerungen* | *Zeitsteuerung* stellen Sie in einem gesonderten Fenster gegebenenfalls einen Alarm oder einen Timer inklusive Namen ein.

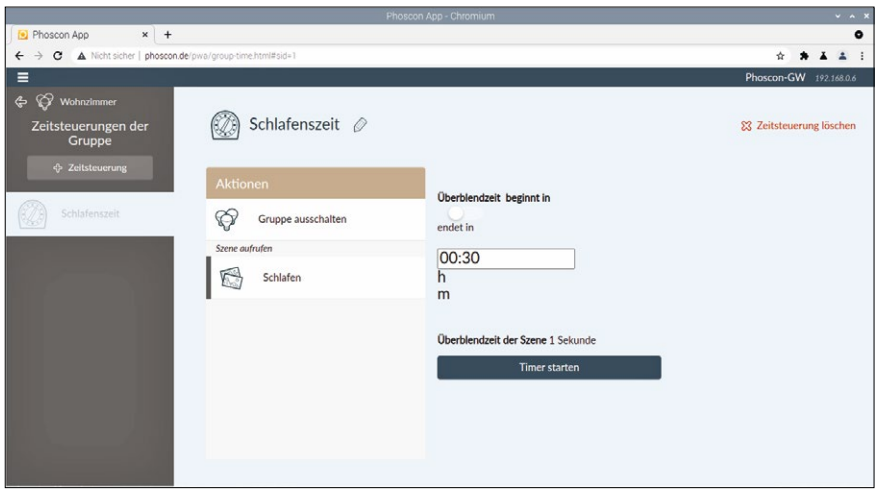
Nach dem *Erstellen* finden Sie sich im Konfigurationsdialog für die Zeitsteuerung wieder. Hier bestimmen Sie, welche Szene zu welchem Zeitpunkt mit welcher Aktion verknüpft wird. Dabei geben Sie zudem die Länge der Überblendzeiten vor und können den *Timer starten* 7.

Wiederholen Sie diese Prozedur für alle Räumlichkeiten, in denen sich Komponenten des Zigbee-Netzes befinden. Die einzelnen Geräte werden ab sofort zuverlässig automatisiert gesteuert.

Fazit

Mit dem Raspbee-II-Modul und den Programmen von Dresden Elektronik gehören Probleme mit Endgeräten, die dem Zigbee-Standard entsprechen, nahezu der Vergangenheit an. Die Software unterstützt viele der auf dem Markt verfügbaren Geräte. Auch ältere Systeme lassen sich, sofern sie nicht durch proprietäre Erweiterungen der Schnittstellen Inkompatibilitäten auftreten, ohne manuelle Konfiguration in eine Heimautomationsinfrastruktur integrieren.

Dabei erweist sich die Steuerungsanwendung als sehr flexibel: Sie nutzen sie nicht nur auf dem Raspberry Pi selbst, sondern per VNC auch auf entfernten Maschinen im LAN. Mit dem Paket von Dresden Elektronik sparen Sie so nicht nur Energie, sondern bauen auch ohne hohe Einstandskosten eine leistungsfähige Heimautomation auf. (*csi*)



7 Mithilfe der Zeitsteuerung automatisieren Sie die Steuerung der einzelnen Geräte.

Dateien zum Artikel herunterladen unter
www.linux-user.de/dl/48568

Weitere Infos und interessante Links
www.linux-user.de/qr/48568

COMPUTEC
marquard group

Ein Unternehmen der MARQUARD MEDIA GROUP AG
Verleger: Jürg Marquard

Redaktion/Verlag	Redaktionsanschrift: Redaktion LinuxUser Putzbrunner Straße 71 81739 München Telefon: (0911) 2872-110 E-Mail: redaktion@linux-user.de Web: www.linux-user.de	Verlagsanschrift: Computec Media GmbH Dr. -Mack-Straße 83 90762 Fürth Telefon: (0911) 2872-100
Geschäftsführer	Christian Müller, Rainer Rosenbusch	
Chefredakteur, Brand/Editorial Director	Jörg Luther (jlu, v. i. S. d. P.), joerg.luther@computec.de	
Redaktion	Uli Bantle (uba), ulrich.bantle@computec.de Thomas Leichtenstern (tle), thomas.leichtenstern@computec.de Carina Schipper (csi), carina.schipper@computec.de	
Linux-Community	Jörg Luther, joerg.luther@computec.de	
Datenträger	Thomas Leichtenstern (tle), cdredaktion@linux-user.de	
Ständige Mitarbeiter	Erik Bärwaldt, Hans-Georg Eßer, Peter Kreußel, Claudia Meindl, Hartmut Noack, Tim Schürmann, Anna Simon, Daniel Tibi, Ferdinand Thommes, Uwe Vollbracht	
Titel & Layout	Sebastian Bienert, Titelmotiv: ndul / Les Cunliffe, beide 123RF.com Bildnachweis: 123RF, Freeimages und andere	
Sprachlektorat	Astrid Hillmer-Bruer	
Produktion, Vertrieb, Abonnement	Martin Closmann (Ltg.), martin.closmann@computec.de Uwe Hönig, uwe.hoenig@computec.de	
Anzeigen	Verantwortlich für den Anzeigenteil: Bernhard Nusser Es gilt die Anzeigenpreisliste vom 01.01.2022.	
Mediaberatung D/A/CH	Bernhard Nusser, bernhard.nusser@computec.de Tel.: (0911) 2872-254, Fax: (0911) 2872-241	
Mediaberatung UK/USA	Brian Osborn, bosborn@linuxnewmedia.com	
New Business	Viktor Eippert (Project Manager)	
E-Commerce & Affiliate	Daniel Waadt (Head of E-Commerce & Affiliate), Veronika Maucher, Andreas Szedlak, Frank Stöwer	
Abo	Die Abwicklung (Rechnungsstellung, Zahlungsabwicklung und Versand) erfolgt über unser Partnerunternehmen: DPV Deutscher Pressevertrieb GmbH Leserservice Computec 20080 Hamburg Deutschland	
Einzelhefte und Abo- Bestellung	http://shop.computec.de	
Leserservice Deutschland	Ihre Ansprechpartner für Reklamationen und Ersatzbestellungen E-Mail: computec@dpv.de Tel.: (0911) 99 39 90 98 Fax: (01805) 861 80 02* (* 0,14 €/min via Festnetz, max. 0,42 €/min via Mobilnetz)	
Österreich, Schweiz	E-Mail: computec@dpv.de	
und weitere Länder	Tel.: +49 911 99399098 Fax: +49 1805 8618002	
Supportzeiten	Montag 07:00 – 20:00 Uhr, Dienstag – Freitag: 07:30 – 20:00 Uhr, Samstag 09:00 – 14:00 Uhr	
Pressevertrieb	DMV Der Medienvertrieb GmbH & Co. KG Meßberg 1, 20086 Hamburg http://www.dermedienvertrieb.de	
Druck	EDS Zrínyi Zrt., Nádas utca 8, 2600 Vác, Ungarn	
ISSN	1615-4444	

marquard group

Deutschland:

4PLAYERS, AREAMOBILE, BUFFED, GAMESWORLD, GAMESZONE, GOLEM, LINUX-COMMUNITY, LINUX-MAGAZIN, LINUXUSER, N-ZONE, GAMES AKTUELL, PC GAMES, PC GAMES HARDWARE, PC GAMES MMORE, PLAY 4, RASPBERRY PI GEEK, VIDEOGAMESZONE

Marquard Media Hungary:

JOY, JOY-NAPOK, INSTYLE, SHOPPIEGO, APA, ÉVA, GYEREKLÉLEK, FAMIILY.HU, RUNNER`S WORLD

ABONNEMENT

Mini-Abo (3 Ausgaben)	Deutschland	Österreich	Ausland
No-Media-Ausgabe [1]	14,90 €	14,90 €	14,90 €
DVD-Ausgabe	18,90 €	18,90 €	18,90 €
Jahres-Abo (12 Ausgaben)	**Deutschland**	**Österreich**	**Ausland**
No-Media-Ausgabe [1]	76,00 €	84,00 €	91,00 €
DVD-Ausgabe	97,00 €	105,00 €	112,00 €
Jahres-DVD zum Abo [2]	6,70 €	6,70 €	6,70 €
Preise Digital	**Deutschland**	**Österreich**	**Ausland**
Heft-PDF Einzelausgaben Digital	6,99 €	6,99 €	6,99 €
Digital-Abo (12 Ausgaben)	69,99 €	69,99 €	69,99 €
Kombi Digital + Print (No-Media-Ausgabe, 12 Ausgaben)	88,00 €	96,00 €	103,00 €
Kombi Digital + Print (DVD-Ausgabe, 12 Ausgaben)	109,00 €	117,00 €	124,00 €

(1) Die No-Media-Ausgabe erhalten Sie ausschließlich in unserem Webshop unter http://shop.computec.de, die Auslieferung erfolgt versandkostenfrei.

(2) Nur erhältlich in Verbindung mit einem Jahresabonnement der Printausgabe von LinuxUser.

Internet	http://www.linux-user.de
News und Archiv	http://www.linux-community.de
Facebook	http://www.facebook.com/linuxuser.de

Schüler- und Studentenermäßigung: 20 Prozent gegen Vorlage eines Schülerausweises oder einer aktuellen Immatrikulationsbescheinigung. Der aktuelle Nachweis ist bei Verlängerung neu zu erbringen. Andere Abo-Formen, Ermäßigungen im Ausland etc. auf Anfrage. Adressänderungen bitte umgehend beim Kundenservice mitteilen, da Nachsendeaufträge bei der Post nicht für Zeitschriften gelten.

Rechtliche Informationen

LinuxUser Community Edition

LinuxUser gibt es auch als Community Edition: Dabei handelt es sich um eine rund 30-seitige PDF-Datei mit ausgewählten Artikeln aus der aktuellen Ausgabe, die parallel zur Veröffentlichung des gedruckten Hefts erscheint.

Die kostenlose Community-Edition steht unter einer Creative-Commons-Lizenz, die es erlaubt, „das Werk zu vervielfältigen, zu verbreiten und öffentlich zugänglich machen". Sie dürfen die LinuxUser Community-Edition also beliebig kopieren, gedruckt oder als Datei an Freunde und Bekannte weitergeben, auf Ihre Website stellen – oder was immer ihnen sonst dazu einfällt. Lediglich bearbeiten, verändern oder kommerziell nutzen dürfen Sie sie nicht. Darum bitten wir Sie im Sinn des „fair use". Weitere Informationen finden Sie unter: http://linux-user.de/CE

Probleme mit den Datenträgern

Falls es bei der Nutzung der Heft-DVDs zu Problemen kommt, die auf einen defekten Datenträger schließen lassen, dann schicken Sie bitte eine E-Mail mit einer genauen Fehlerbeschreibung an die Adresse computec@dpv.de. Wir senden Ihnen dann umgehend kostenfrei einen Ersatzdatenträger zu.

Vorschau auf 03/2023

Die nächste Ausgabe erscheint am 16.02.2023

Handliche Desktop-Tools

In der nächsten Ausgabe sehen wir uns grafische Werkzeuge an, die lästige Alltagsaufgaben erleichtern. Der Text-Expander Espanso beispielsweise ersetzt Textkürzel durch individuelle Textbausteine, auf Wunsch sogar anwendungsspezifisch. Das wieselflinke Fsearch spürt Dateien und deren Inhalte sehr viel schneller auf als jedes CLI-Tool, versteht dabei aber auch reguläre Ausdrücke. Converseen, ein Qt-Frontend für ImageMagick, macht die Stapelverarbeitung Hunderter Bilder zum Kinderspiel. Mit dem praktischen Metadata Cleaner lassen sich die in Fotos und Dokumenten versteckten Infos anzeigen und rückstandsfrei entfernen.

Digitaler Zettelkasten

Werkzeuge zum Verwalten von Notizen am PC können meist viel mehr als der herkömmliche Zettelkasten oder Notizblock. Mit der Evernote-Alternative Joplin synchronisieren und verwalten Sie Ihre Merkzettel auch über mehrere Geräte hinweg. Wir haben uns angesehen, was die Notizanwendung sonst noch so alles leistet.

Smartphone im Griff

Die Wartung des Betriebssystems auf Android-Smartphones hat so ihre Tücken. Mit der Distribution mAid, einem spezialisierten Manjaro-Derivat, verlieren Firmware-Updates und Datenübertragungen ihre Schrecken. Welche Hersteller dabei unterstützt werden und welche Werkzeuge mit an Bord sind, klärt unser Test.

Die Redaktion behält sich vor, Themen zu ändern oder zu streichen.

Heft als DVD-Edition

- 108 Seiten Tests und Workshops zu Soft- und Hardware
- 2 DVDs mit Top-Distributionen sowie der Software zu den Artikeln. Mit bis zu 18 GByte Software das Komplettpaket, das Unmengen an Downloads spart

Heft als No-Media-Edition

- Preisgünstige Heftvariante ohne Datenträger für Leser mit Breitband-Internet-Anschluss
- Artikelumfang identisch mit der DVD-Edition: 108 Seiten Tests und Workshops zu aktueller Soft- und Hardware

Community-Edition-PDF

- Über 30 Seiten ausgewählte Artikel und Inhaltsverzeichnis als PDF-Datei
- Unter CC-Lizenz: Frei kopieren und beliebig weiter verteilen
- Jeden Monat kostenlos per E-Mail oder zum Download

DVD-Edition (9,99 Euro) oder No-Media-Edition (7,99 Euro) Einfach und bequem versandkostenfrei bestellen unter:

http://www.linux-user.de/bestellen

Jederzeit gratis herunterladen unter:

http://www.linux-user.de/CE

Neues auf der Heft-DVD

SparkyLinux 6.5 MinimalGUI i686 Non-PAE

SparkyLinux MinimalGUI erweist sich besonders für Nutzer betagter 32-Bit-PCs als interessant. Als Unterbau dienen Debian Stable und Testing. Dank GUI-Tools gestattet es Sparky auch Nutzern ohne tiefergehende Linux-Kenntnisse, das System individuell anzupassen. Die Distribution bringt nur ein Minimum an Anwendungssoftware mit, bietet dafür aber prall gefüllte Repositories mit einem reichhaltigen Angebot auch jenseits des Debian-Fundus. So stehen allein sieben verschiedene Office-Suiten zum Einsatz bereit. Einen ausführlichen Artikel zu SparkyLinux lesen Sie ab Seite 6 in dieser Ausgabe. Sie starten die Distribution von Seite B der DVD. Das zugehörige ISO-Image finden Sie im Verzeichnis `isos/`.

Puppy Linux 22.12 mit minimalen Ansprüchen

Das minimalistische Puppy Linux 22.12 alias „S15Pup“ basiert auf Slackware 15.0 und konzentriert sich auf das Nötigste. Das macht es zum Leichtgewicht, das sich auch für alte PCs eignet. Es entstand vollständig aus Slackware-Paketen, als Window-Manager kommt JWM 2.4.3 zum Einsatz. Die 300 MByte kleine Distribution benötigt als Minimalvoraussetzungen eine 233-MHz-CPU, 128 MByte Hauptspeicher sowie 512 MByte freien Plattenplatz zur Installation. Sie starten Puppy von Seite A (64 Bit) und B (32 Bit) der DVD. Die ISO-Images der 32- und 64-Bit-Version finden Sie auf der jeweiligen Seite im Verzeichnis `isos/`.

XeroLinux 2022.12 mit aktuellem KDE Plasma

Die auf Arch Linux basierende Distribution setzt in Sachen Desktop auf KDE Plasma. Die neueste Version setzt auf den Calamares-Installer, bringt verschiedene Verbesserungen und Optimierungen unter der Haube und unterstützt von der Community erstellte AUR-Recipes sowie Flatpak-Pakete. Den Kernel aktualisierte das Projekt auf Version 6.0.12, das Qt-Framework auf 5.15.7. KDE Plasma ist in Version 5.26.4 an Bord, KDE Frameworks liegt einschließlich aller Pakete in Version 5.101 vor. Die KDE-Gear-Tools wurden auf 22.12 aktualisiert. Sie starten die Distribution von Seite B der DVD. Das zugehörige ISO-Image finden Sie im Verzeichnis `isos/`.

Kali Linux 2022.04 geht auf Nummer sicher

Die Distribution für Sicherheitsexperten und Penetration-Tester erweitert das Werkzeugangebot, aktualisiert Gnome auf Version 43 und bringt KDE Plasma auf Version 5.26. Zudem gibt es jetzt ein Quick-Setting-Panel in angepasster Optik. Verfügbar sind erstmals das Python-Skript `Bloodhound.py` für Bloodhound, die Active-Directory-Tools Ldapdomaindump und Certipy, der Userspace-Treiber `hak5-wifi-coconut` für USB-WLAN-Geräte, PEASS-ng zur Privilege Escalation sowie das grafische Reverse-Engineering-Werkzeug Rizin-Cutter. Sie starten die Live-Distribution von Seite A der DVD. Das zugehörige ISO-Image finden Sie im Verzeichnis `isos/`. (*tle*)