c't

DIGITAL SOUVERÄN

Wie Sie die Kontrolle über Ihre Daten gewinnen

Cloud-Projekte zum Selbsthosten

Dienste selber betreiben: Foto-Speicher bis Sync-Server
Open-Source-Alternativen zu Cloud-Diensten

Admin-Wissen für die private Cloud

Handwerkszeug für Selbsthoster
Server-Administration · Virtualisierung
Zugriff von außen

Einstieg in Nextcloud

Marktübersicht DSGVO-konformer Nextcloud-Hoster
Praxisanleitung: Nextcloud-Server und -Clients einrichten

€ 14,90
CH CHF 27.90
AT € 16,40
LUX € 17,10

Raus aus der US-Cloud

Was das Problem mit Microsoft & Co. ist und warum Sie umsteigen sollten
Kontrolle über Daten zurückgewinnen · Europäische Alternativen zu US-Diensten

4 195957 614908 03

Digitale Souveränität

Für uns seit über 20 Jahren mehr als nur ein Buzzword.

Ob Cloud-Infrastruktur, Arbeitsplatz oder Desktop-Umgebung: Wir unterstützen Sie dabei, Ihre IT vollständig selbstbestimmt & zukunftssicher zu gestalten.

Souveräner Cloud Stack – mit OpenStack

Mit OpenStack realisieren Sie private oder öffentliche Clouds – ohne Vendor Lock-in, mit voller Datenhoheit und maximaler Flexibilität. Inklusive Container-, Datenbank-, Identitäts- & Server-Management.
Im Einsatz bei: Thüringer Landesrechenzentrum (TLRZ)

Souveräner Arbeitsplatz – mit openDesk

openDesk bietet einen transparenten, anpassbaren & sicheren Arbeitsplatz – optimiert für die Anforderungen von Verwaltung & Unternehmen.
Im Einsatz bei: Zentrum für Digitale Souveränität (ZenDiS)

Souveräner Desktop – mit Linux & zentralem Client-Management

Unsere Linux-Clients mit zentralem Management bieten hohe Leistungsfähigkeit, Sicherheit, Wartbarkeit & volle Kontrolle.

B1 SYSTEMS

B1 Systems GmbH – Ihr Linux-Partner

Linux/Open Source Consulting, Training, Managed Service & Support

www.b1-systems.de · info@b1-systems.de

Editorial

Liebe Leserin, lieber Leser,

da schmeckt US-Präsident Trump die Arbeit des Internationalen Strafgerichtshofs (IStGH) nicht und er verhängt deshalb Sanktionen. Die Folge: Karim Ahmad Khan, Chefankläger des IStGH, kann auf sein E-Mail-Konto nicht zugreifen. Denn die Mailkonten des IStGH verwaltet Microsoft und der Konzern sperrte, wohl ob der Sanktionen, kurzerhand Khans E-Mail-Konto. Schon unpraktisch, wenn man als internationale Institution zum Schutz des Völkerrechts auf einen US-Konzern als Dienstleister angewiesen ist.

Das Beispiel verdeutlicht die Abhängigkeit von Firmen, Institutionen, Behörden, ja ganzen Nationen von den großen Tech-Konzernen in den Vereinigten Staaten. Und Trump hat wiederholt deutlich gemacht, dass er es nicht scheut, die noch vorhandene Vormachtstellung der USA als Druckmittel einzusetzen. Wie man angesichts eines solchen Gebarens etwa als Medienkonzern ganze Produktionsabläufe und die gesamte Kommunikation auf die Microsoft-Cloud verlagern kann, ist mir unverständlich.

Seit Trump erneut im Weißen Haus sitzt, haben die Diskussionen zu „digitaler Souveränität“ wieder Hochkonjunktur – zu Recht, wie ich finde. Es gibt Wege dahin: einfach selbst machen oder Dienstleister in Europa nutzen und darauf achten, dass es keinen Vendor-Lock-in gibt, also keine unauflösbare Abhängigkeit von einem Hersteller. Viele gute Open-Source-Lösungen stehen dafür bereit.

Als Privatperson ist man von politischen Sanktionen meist nicht betroffen. Aber auch hier ist die Abhängigkeit von Apple, Microsoft, Google und Meta sowie von vielen kleineren Firmen problematisch: Schlagartig kann ein Anbieter sein Geschäftsmodell ändern, Preise drastisch erhöhen oder gar Dienste komplett einstampfen. Hinzu kommt die penetrante Neugier der Konzerne.

Wie Sie sich selbst aus der Abhängigkeit befreien und wieder souverän über Ihre Daten und Dienste verfügen, zeigen wir Ihnen in diesem Heft anhand zahlreicher Beispiele. Angefangen von alternativen Suchmaschinen über eine Open-Source-Fotocloud bis hin zur eigenen Nextcloud als universeller Kollaborationsplattform für die Familie, den Verein oder die Firma. Wir geben Ihnen Tipps, was Sie beim Selbsthosten beachten sollten, und blicken auf politische Versuche, Deutschland und Europa digital souverän zu machen.

Viel Spaß beim Lesen und Umsetzen!

Keywan Tonekaboni

Inhalt

RAUS AUS DEN US-CLOUDS

Spätestens seit der zweiten Amtszeit von Donald Trump ist es eine gute Idee, möglichst unabhängig von US-Cloud-Diensten zu sein. Wir werfen einen Blick auf Alternativen und darauf, wie sich die öffentliche Hand aus dem Würgegriff der Konzerne windet und dabei mitunter verzettelt.

ADMIN-WISSEN FÜR DIE PRIVATE CLOUD

Wer einen Bogen um US-Dienste machen möchte und sich auch nicht auf europäische Dienstleister verlassen will, muss selbst ran: Wir vermitteln das nötige Grundwissen und stellen einige nützliche Helfer als Basis für die private Cloud vor.

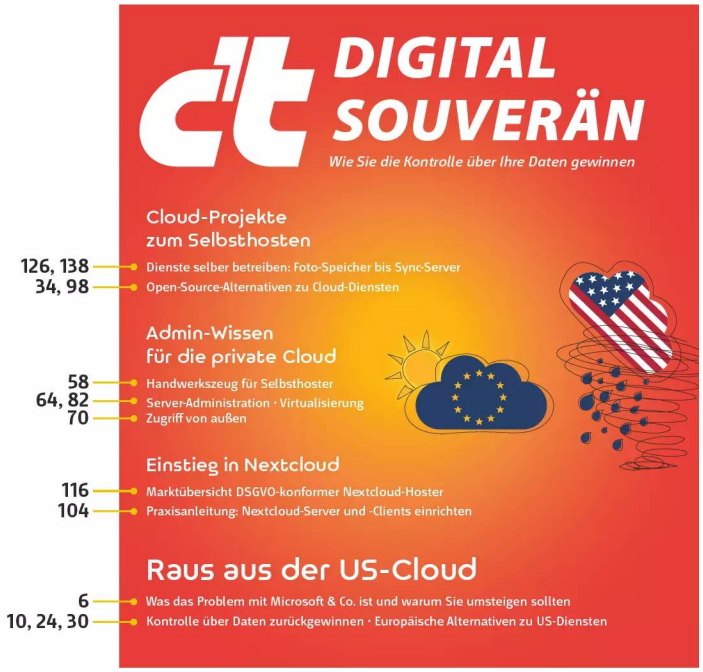
EINSTIEG IN DIE EIGENE CLOUD

Die Open-Source-Software Nextcloud ist auf dem besten Weg, zum Gattungsbegriff für private Clouds zu werden: Sie ist vielseitig erweiterbar und erfüllt die meisten Anforderungen, die Nutzer von Cloud-Diensten stellen. Wir helfen bei der Inbetriebnahme.

CLOUD-PROJEKTE ZUM SELBSTHOSTEN

Für gängige Mietdienste gibt es attraktive Alternativen – wir zeigen einige Beispiele: Immich hilft, die eigene Fotosammlung zu verwalten. Dawarich visualisiert komfortabel, wo Sie sich aufhalten. BASPi synchronisiert Ihre Dateien und liefert ein Backupziel ohne Cloud.

ZUM HEFT



Gründe für den Cloud-Ausstieg

Bild: KI, Collage c't

Vielen bluten schon die Ohren beim täglichen Trump-Tratsch in den Medien. Doch Wegschauen und Hoffen sind eher schlechte Optionen: Der US-Präsident stärkt die Macht der Tech-Riesen, die Interessen europäischer Kunden kümmern dabei niemanden. Wir lassen die Argumente Revue passieren, die für mehr digitale Souveränität und eine Abkehr von US-Clouds sprechen.

Von **Peter Siering**

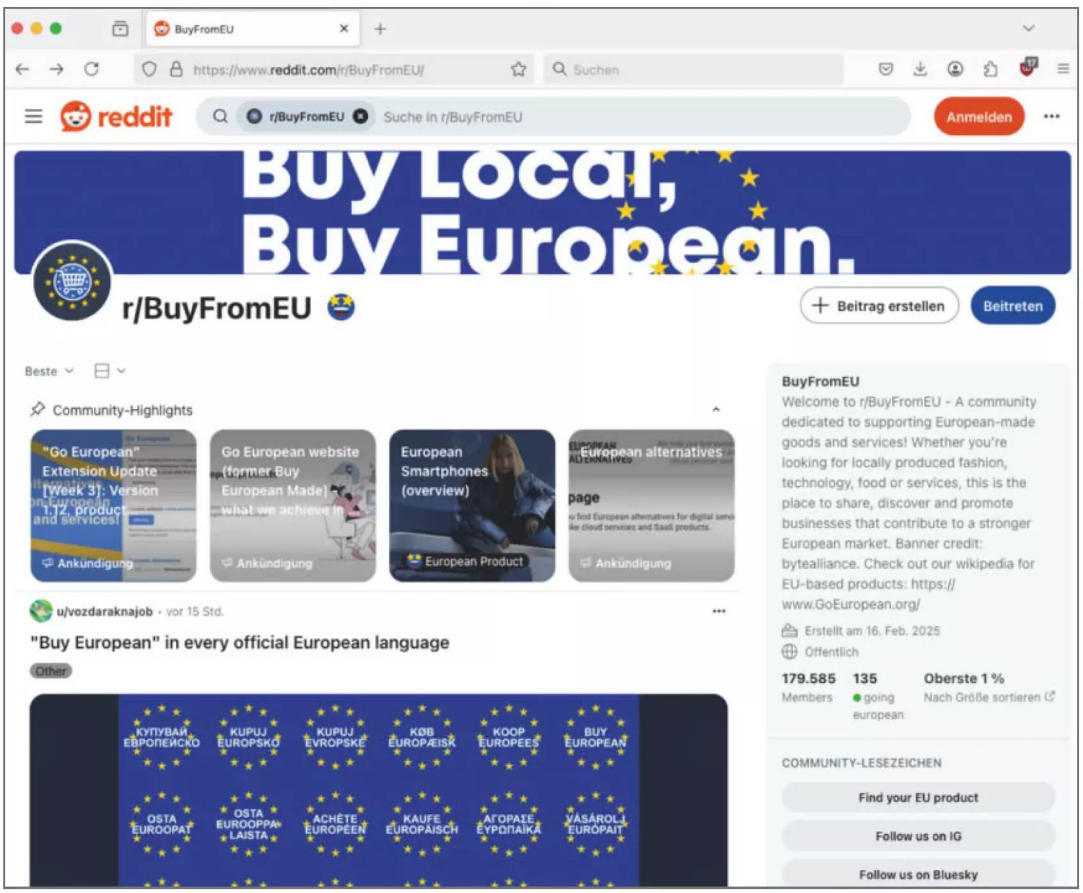
Firmen zwingt das EU-Recht dazu, aber auch für Verbraucher wird es immer wichtiger, die eigene digitale Existenz möglichst unabhängig von US-Clouds und -Unternehmen und somit von US-Interessen zu gestalten. Dieser Artikel fasst die wichtigsten Gründe dafür zusammen. Im folgenden finden Sie dann Tipps, um die dominierenden Dienste durch europäische Alternativen zu ersetzen. Der letzte Artikel dieses Schwerpunkts widmet sich den rechtlichen Aspekten.

Mancher der nun folgenden Hinweise könnte generell Nutzer von Clouddiensten zum Nachdenken bringen, egal ob sie nun von Unternehmen betrieben werden, die in den USA oder anderswo angesiedelt sind. Das ist gut so, denn gerade ungeduldige Datenflüchtlinge aus der US-Hegemonie laufen sonst Gefahr, kaum besseren Alternativen blind in die Arme zu rennen.

Was ist (US-)Cloud?

Cloud (Computing) ist erst mal nur ein technischer Begriff und meint mehr als den Zugriff auf Dateien: Es werden Informationen auf vernetzten Computern verarbeitet, die irgendwo im Internet stehen. Dabei ist es egal, ob diese Computer eher simple, kombinierbare Funktionen wie Datenbanken oder Rechenkapazität bereitstellen, komplexe Anwendungen wie Office im Browser anbieten oder einen einzelnen Dienst wie WhatsApp realisieren, einen Staubsaugroboter leiten oder die Kochhilfe mit Rezepten füttern.

Für die Beurteilung, ob es sich um eine US-Cloud oder einen US-Dienst handelt oder nicht, spielt dabei weniger der Standort der Computer eine Rolle, sondern der Sitz der Firma, die dieses Angebot betreibt. Residiert die in den USA, kann man sicher von einem US-Angebot sprechen. Der Betreiber ist gemäß US



Es ist eine Vorlage für einen Scherz von „Der Postillon“: Auf einer US-Plattform diskutiert „Europa“, wie man sich am besten aus der Trump-Zone begibt.

Cloud Act verpflichtet, den US-Behörden den Zugriff auf gespeicherte Daten unabhängig von deren Aufenthaltsort zu gewähren, was der Artikel auf Seite 24 näher aufdröselt. Dieser Durchgriff ist der Hauptgrund, die Trump-Zone zu verlassen.

Leider ist es heutzutage wenig offensichtlich, ob digitale Angebote ohne US-Cloudtechnik auskommen. Der Betreiber einer Chatplattform könnte zwar in Europa seinen Sitz haben, aber die nötige Rechenleistung in einer US-Cloud einkaufen. Das hieße dann, dass auch die US-Behörden Zugriff auf die dort verarbeiteten Daten erhalten könnten, indem sie den US-Cloudbetreiber in die Pflicht nehmen. Man muss also genau hinsehen.

Was schützt Daten?

Essenziell für die Inanspruchnahme von Clouddiensten ist heute Transportverschlüsselung. Die schützt alle Daten, die zwischen dem Kunden und dem Dienstleister über öffentliche Netze fließen. Niemand außer den Kommunikationspartnern kann somit mitlesen, auch nicht in einem WLAN ohne Verschlüsselung. Wie der Dienstleister die Daten allerdings speichert oder weiterleitet, steht auf einem anderen Blatt. Ohne weitere Maßnahmen landen und liegen sie dort im Klartext.

Deswegen ist Ende-zu-Ende-Verschlüsselung erstrebenswert: Ein Dienst, über den Nutzer sicher Nachrichten austauschen können, muss gewährleisten, dass nur ebendiese Nutzer jeweils an ihrem Ende die Daten entschlüsseln können. Die Achillesferse dabei sind die verwendeten Schlüssel. Die müssen die Kommunikationspartner austauschen. Wenn das nicht über einen separaten Kanal passiert, sondern der Dienst selbst dabei aktiv vermittelt, besteht die Gefahr, dass er den Abgleich manipuliert und sich dazwischensetzt.

Wer bei der Nutzung von Clouddiensten auf Nummer sicher gehen will, dass die dort abgelegten Daten nicht von Dritten abgesammelt werden können, sollte die Schlüssel niemals aus der Hand geben – also nur verschlüsselte Daten an die Dienste übermitteln. Sollen die Daten allerdings in der Cloud weiterverarbeitet werden, und sei es auch nur von einem Web-Viewer oder -Editor dargestellt werden, dann brauchen diese Dienste den Schlüssel. Wie schnell staatliche Organe hier übergriffig werden, zeigte sich im Februar in Großbritannien: Dort verlangte die Regierung von Apple, die Ende-zu-Ende-Verschlüsselung für deren Bürger zu deaktivieren. Cloud bleibt immer Vertrauenssache.

Chip-Hersteller und Cloudbetreiber versuchen mit hochkomplexen Techniken wie Trust Domain Extensions in Prozessoren auch Firmen die Cloud schmackhaft zu machen. Sie versprechen, die Daten der Kunden (auch untereinander) zu schützen. Der Aufwand, den sie für diese Confidential Computing genannte Technik und das Regelwerk treiben müssen, ist erheblich, teuer und allenfalls eine seltene Ausnahme und nicht der Standard in Cloudumgebungen. Das gilt in ähnlicher Weise auch für Techniken, die sich in den Datenstrom von Clouddiensten einmischen und die Daten schützen sollen – viel Aufwand und Technik, deren Standhalten fraglich bleibt.

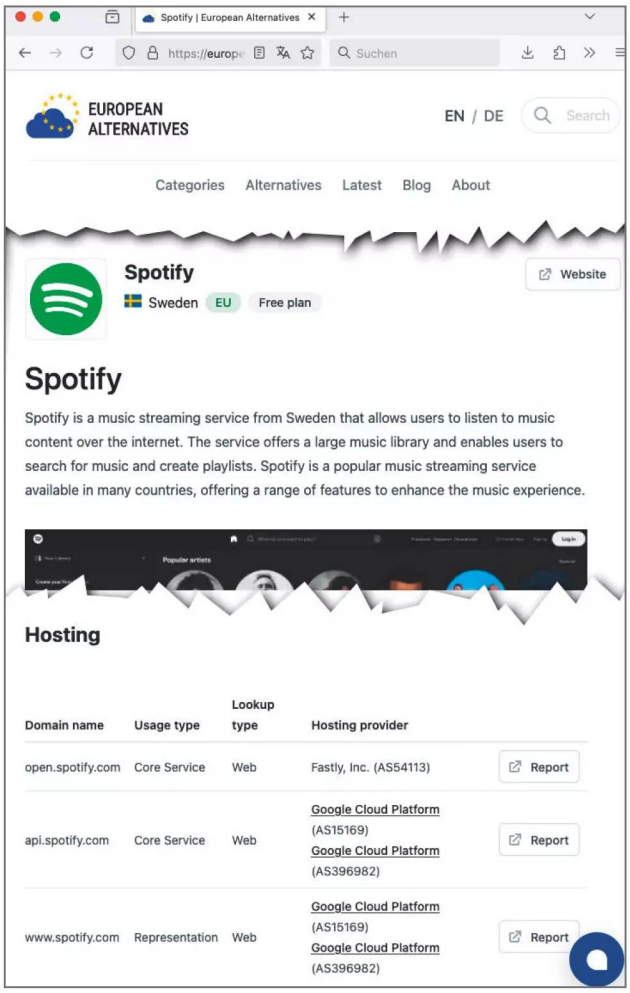
Was ist das Geschäft?

Das Geschäftsmodell gängiger Clouddienste, besonders der Gratisdienste, ist das Gewinnen von Daten. Sie sammeln Informationen, die sie über ihre Nutzer finden können: Wofür sie sich interessieren, wo sie sich aufhalten, welche Apps und Dienste sie verwenden, was sie einkaufen und wann sie besonders aktiv sind. Aus diesen Krümeln bilden Dienstleister Zielgruppen, die aufgrund der Datenfülle erstaunlich detailliert sind und von Datenbrokern weltweit gehandelt werden.

Oft steht nicht mal Cloud am Angebot dran, sondern der Nutzer erhält vermeintlich nur ein kostenloses Mailkonto, Dateispeicher zur Synchronisation von Dateien und Fotos, Zugang zu einem Forum oder Ähnliches. Über die Bewegungsdaten hinaus liefert er mit seinen Daten dem Anbieter nun weiteren Kontext. Dass solche Clouds auch die Daten analysieren, ist längst bekannt. Nur so sind beispielsweise deaktivierte Konten bei vermeintlich bedenklichen Inhalten erklärbar. Wer sich tatsächlich die Nutzungsbedingungen zu Gemüte führt, lernt das dort auch.

Während in Europa dank Datenschutzgrundverordnung (DSGVO) enge Grenzen für die Weitergabe und Analyse von Daten gelten, können Unternehmen in den USA viel freier agieren. Dennoch räumen viele den Nutzern freiwillig einen gewissen Spielraum ein, was den Umgang mit den Daten angeht: Wer Windows selbst einrichtet, kennt den Satz von Fragen, der dann abgespult wird. Aber: Wohltäter sind die Dienste nicht, ihr Geschäftsinteresse sind nun mal die Daten der Nutzer, die vermeintlich ein kostenfreies Angebot erhalten.

Zahlende Kunden sind von dieser Art Datenabfluss üblicherweise nicht oder nicht so stark betroffen. Aber auch sie sind Gefahren ausgesetzt: Bleiben



Websites, um nach europäischen Alternativen für IT und mehr zu recherchieren, haben Hochkonjunktur. European Alternatives von Constantin Graf nennt für jeden Dienst unter „Hosting" auch Details zur Netzwerkanbindung – die kann Überraschungen bergen.

Websites und Diskussionen zu europäischen Alternativen
ct.de/wk7w

die Preise stabil? Wird das Angebot umgebaut, etwa zu einem Abomodell? Was passiert, wenn das Unternehmen verkauft wird? Werden vielleicht Zölle fällig? Greift die US-Regierung ein? Untersagt sie womöglich die Bereitstellung von Diensten für unliebsame Ausländer? Nutzt sie Technik als Machtinstrument?

Gerade diese Unsicherheit macht klar: Wer Clouddienste nutzt, benötigt eine Exit-Strategie. Genau die fällt aber oft schwer. Je nach Beschaffenheit gelingt die Emigration der Daten aus den Cloudsilos nur schlecht. Was kann man schon mit den JSON- oder Textdaten einer Chatlösung anfangen, in der sich über Jahre das Team-Know-how gesammelt hat? Viele Clouddienste sind eine Einbahnstraße. Für bewährte Kommunikationsmethoden wie E-Mail gibt es wenigstens Archivierhilfen und -pflichten.

Was geht?

Mit dem Wissen um die Risiken gibt es keinen Grund, Clouddienste zu verteufeln. Die großen Clouds stellen weltweit verteilt Rechenleistung bereit. Sie werden von Admin-Teams rund um die Uhr das ganze Jahr betreut. Je nach dort gebuchten Diensten müssen sich die Kunden nicht um Wartungsaufgaben kümmern. Trotz aller Zuverlässigkeitsversprechen der Anbieter sollte man aber im Hinterkopf behalten, dass auch bei den Profis Dinge schiefgehen.

In einer großen Cloud sind die Auswirkungen dann umso drastischer, wie im Fall des bei Microsoft abhandengekommenen Masterkeys. Mitte 2023 fielen bei einer amerikanischen Regierungsbehörde verdächtige Mailzugriffe auf. Offenbar hatten Angreifer aus China sich mit einem entwendeten Signaturschlüssel selbst Zugangs-Token für Exchange ausstellen können. Zu der These, dass der Masterkey ein Generalschlüssel für die ganze Azure Cloud gewesen sei, hat sich Microsoft nie final geäußert.

Und: Elementare Teile der für den Betrieb des Internets notwendigen Dienste hängen derzeit von Systemen ab, die in den USA betrieben werden. Das gilt für die DNS Root Server, die die Wurzel der Namensauflösung bilden. Es betrifft aber vor allem die unverzichtbaren Zertifikatsketten, mit denen Kommunikation im Netz abgesichert wird. Die meisten Zertifikate, die den Ausgangspunkt dieser Sicherheit bilden, liegen bei US-Unternehmen. Auch deshalb ist Confidential Computing in der heutigen Zeit ein Trugbild.

Die Appelle für mehr digitale Souveränität erreichen mit Schlachtrufen wie „Unplug Trump" oder „Buy European" eine größere Dringlichkeit. Entsprechend geben daran anknüpfende Diskussionen und Webseiten (siehe ct.de/wk7w) viele nützliche Impulse, um Wege aus US-Clouddiensten und der Abhängigkeit von US-amerikanischen Unternehmen zu finden. Solche Tipps sind jedoch schnell überholt, etwa durch Firmenfusionen. Auch unser folgender Blick auf Alternativen kann deshalb nur ein Schnappschuss sein. (ps) c't

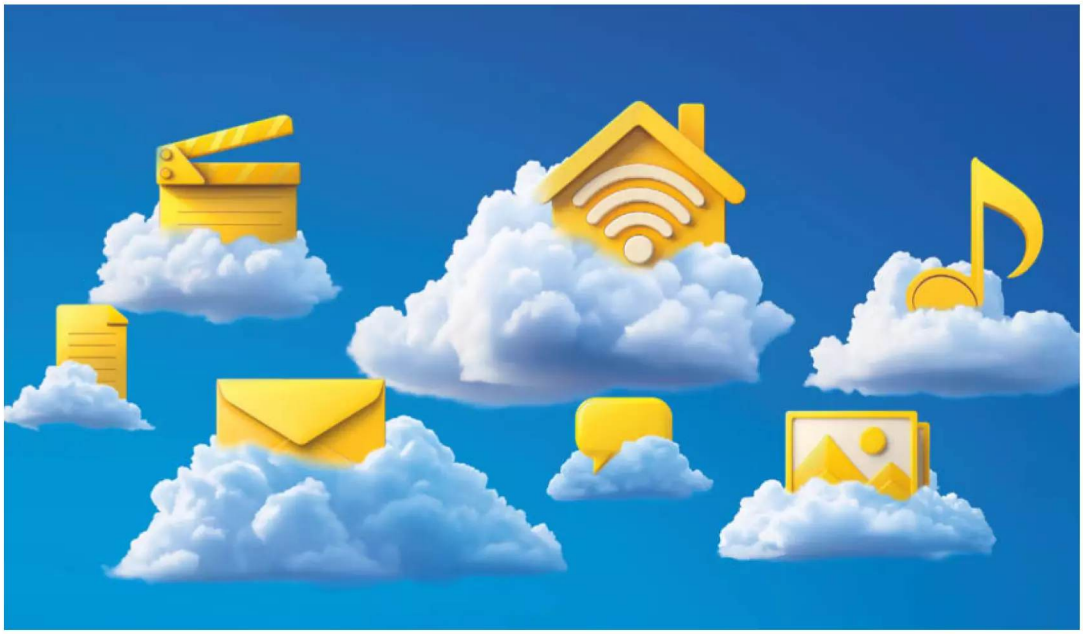


Bild: KI, Collage c't

Alternativen zu US-Clouddiensten

Clouddienste sind praktisch, dort abgelegte Daten überall verfügbar. Ihre Nutzung hinterlässt allerdings Spuren, die die Betreiber nur allzu gern verwerten. Die Unternehmen sitzen oft in den USA, und ihre Chefs haben bereitwillig für den neuen Präsidenten gespendet. Kuscheln sie nur oder werden sie kuschen? Egal. Wir zeigen, wie Sie unabhängiger von deren Treiben werden und Ihre Daten zurückerobern.

Von **Peter Siering**

Bei allen Vorteilen von Clouddiensten sollte man nicht übersehen, wie sehr sie unsere Welt durchsetzen. Sie sind mit der modernen Gesellschaft verwachsen wie das Pilzgeflecht mit den Wurzeln der Bäume. Sie breiten sich immens aus und sind oft unsichtbar.

Die erste Geige dabei spielen die Hyperscaler der US-Konzerne Amazon (AWS), Alphabet (Google Cloud) und Microsoft (Azure). Andere Unternehmen, etwa Smart-Home-Anbieter, mieten sich dort ein, um keine eigene Infrastruktur betreiben zu müssen. So liefern sie die eigenen Kunden indirekt den großen US-Anbietern aus.

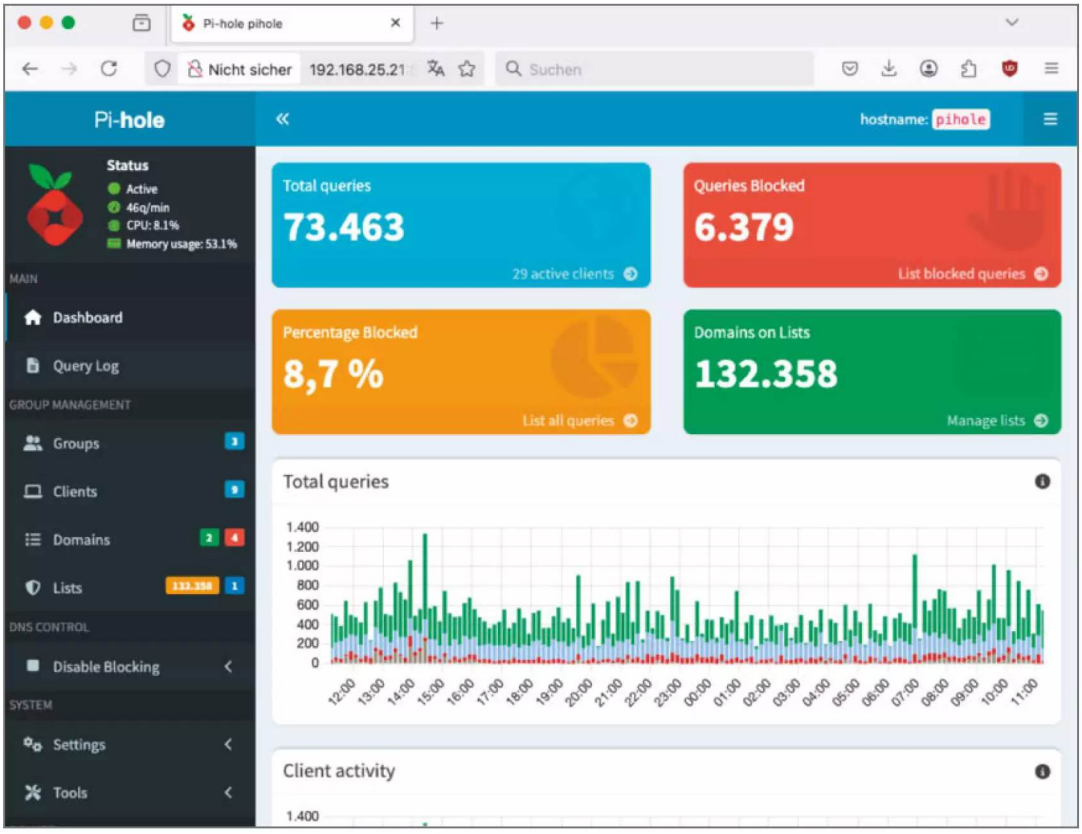
Das heißt, je unbedarfter man digitale Dienste nutzt, desto wahrscheinlicher bekommt man es mit diesen US-Anbietern zu tun – direkt oder indirekt.

Deswegen: Augen auf und Berührungspunkte minimieren. Die folgenden Tipps helfen dabei – und motivieren im Zweifel auch dazu, digitale Partner bewusst auszuwählen.

Spuren minimieren

Kein Dienst verrät mehr über Aktivitäten im Internet als das Domain Name System (DNS). Denn bevor etwa ein Browser den Server heise.de oder ein Mailclient den eingestellten Mailserver kontaktieren kann, muss er erst mal dessen IP-Adresse mittels DNS erfragen. Diese Anfragen an einen **DNS-Resolver** sind meist unverschlüsselt. Sie sind eine Datenspur, die Datensammlern das Leben sehr einfach macht.

Prüfen Sie, dass Sie hierfür nicht irgendwann einen Server eines US-Anbieters eingestellt haben. Wenn Sie zum Beispiel 8.8.8.8 als DNS-Resolver konfiguriert haben, erfährt Google sämtliche DNS-Anfragen. Nehmen Sie stattdessen einen datenschutzfreundlichen DNS-Resolver, der in Europa steht, ein paar Beispiele: quad9, DNS.SB, DNS0.EU und Digitalcourage. Tragen Sie den so ein, dass DNS-Anfragen verschlüsselt erfolgen. So minimieren Sie Ihre Datenspuren zusätzlich.



Um den Datenabfluss in US-Clouds zu minimieren, kann man schon bei grundlegenden Diensten beginnen: Nutzen Sie nur DNS-Resolver außerhalb des Einflussbereichs der großen US-Techkonzerne, lassen Sie einen DNS-Filter automatisiert Tracker und Werbelieferanten aussortieren und verwenden Sie einen Browser, dessen Hersteller Adblocker nicht aussperrt.

Eine weitere effektive Methode, Datensammlern das Leben schwer zu machen, ist ein **DNS-Filter**: Der konsultiert Listen, auf denen fleißige Helfer die Namen von Trackern, Werbenetzwerken und anderen unerwünschten Diensten sammeln. Taucht deren Name auf, erhält der anfragende DNS-Client eine Antwort, die eine Kontaktaufnahme zum Anbieter verhindert. Mit einem solchen DNS-Filter erwischen Sie viele auch unsichtbar agierende Tracker, etwa in Apps auf dem Mobiltelefon.

DNS-Filter sind bei einigen DNS-Dienst- und VPN-Anbietern Teil des Angebots. Sie können einen solchen Filter aber ebenso in Eigenregie betreiben: Pi-hole und AdGuard Home sind populäre, kostenlos nutzbare Lösungen, die sich auf einem NAS, Heimserver oder Raspberry Pi, AdGuard Home sogar auf einigen Routern direkt einrichten lassen.

Wenn Sie den Filter selbst betreiben, können Sie einfacher in den Logs nachvollziehen, was ein Gerät tut, und individuell anpassen, was es tun darf und was nicht. Der Vollständigkeit halber sei erwähnt: Natürlich sollte auch ein solcher lokaler Filter selbst nur einen DNS-Resolver befragen, der die oben genannten Regeln erfüllt. Einige schlagen die Filterprogramme direkt vor.

Und: Auf mobil genutzten Geräten, etwa im Mobilfunknetz oder in fremden WLANs wirken diese Maßnahmen nur, wenn Sie diese auch dort umsetzen. Das fällt am leichtesten, indem Sie auf diesen Geräten stets eine VPN-Verbindung zu Ihrem lokalen Netz unterhalten.

Ungestört surfen

Ein DNS-Filter ist schon recht wirksam, um einen guten Teil unerwünschter Anfragen zu tilgen. Allerdings ist sein Wirken nicht perfekt. Einen höheren Wirkungsgrad beim Surfen legen im Webbrowser aktivierte **Werbeblocker** an den Tag. Einer der besten ist das kostenlos als Browsererweiterung erhältliche uBlock Origin. Leider arbeiten Browserhersteller daran, solche Techniken zu schwächen [1].

Deswegen ist es eine zusätzliche Überlegung wert, ob Sie von Chrome oder einer der Betriebssystem-**Browser**-Beigaben wie Edge oder Safari auf Alternativen ausweichen, die mehr Privatsphäre versprechen. Firefox ist schon eine gute Wahl, hat in den vergangenen Wochen aber das Versprechen aus seiner FAQ getilgt, niemals persönliche Daten der Nutzer zu verkaufen. Vielleicht ist ein Fork wie LibreWolf, das gleich uBlock Origin mitbringt und keine Telemetriedaten nach Hause funkt, für Sie einen Versuch wert? Oder Sie probieren Vivaldi aus, der allerdings als Basis das von Google entwickelte Chromium verwendet?

Es wäre witzlos, wenn Sie Ihre DNS-Spuren verwischen und Tracker ausfiltern, aber stets weiter Google oder Bing konsultieren, wenn Sie etwas suchen – im schlechtesten Fall auch noch, während Sie dort mit Ihrem Benutzerkonto angemeldet sind. Die Suchmaschinenbetreiber schürfen mit den Anfragen das Datengold, um ihre Nutzer direkt an ihre Anzeigenkunden zu verticken. DNS-Filter und Adblocker dämmen diese Flut ein, aber viel schlägt dennoch in die Suchergebnisse durch.

Hier setzen Charity-**Suchmaschinen** wie Ecosia an. Sie reicht Suchanfragen an Google oder Bing durch, nicht jedoch die Daten des Nutzers, und tut nach eigenen Angaben Gutes mit den Anzeigenerlösen. Ecosia spendet 80 Prozent seiner Erlöse für Baumpflanzungen und Klimaschutz. Good Search versucht sich an einer ethisch ausgerichteten Suchmaschine, die keine Werbung anzeigt und nicht die Absicht hat, jemals Gewinne zu erzielen. Jüngst haben die Betreiber ein Abomodell für die Nutzer eingeführt, um die Betriebskosten zu finanzieren.

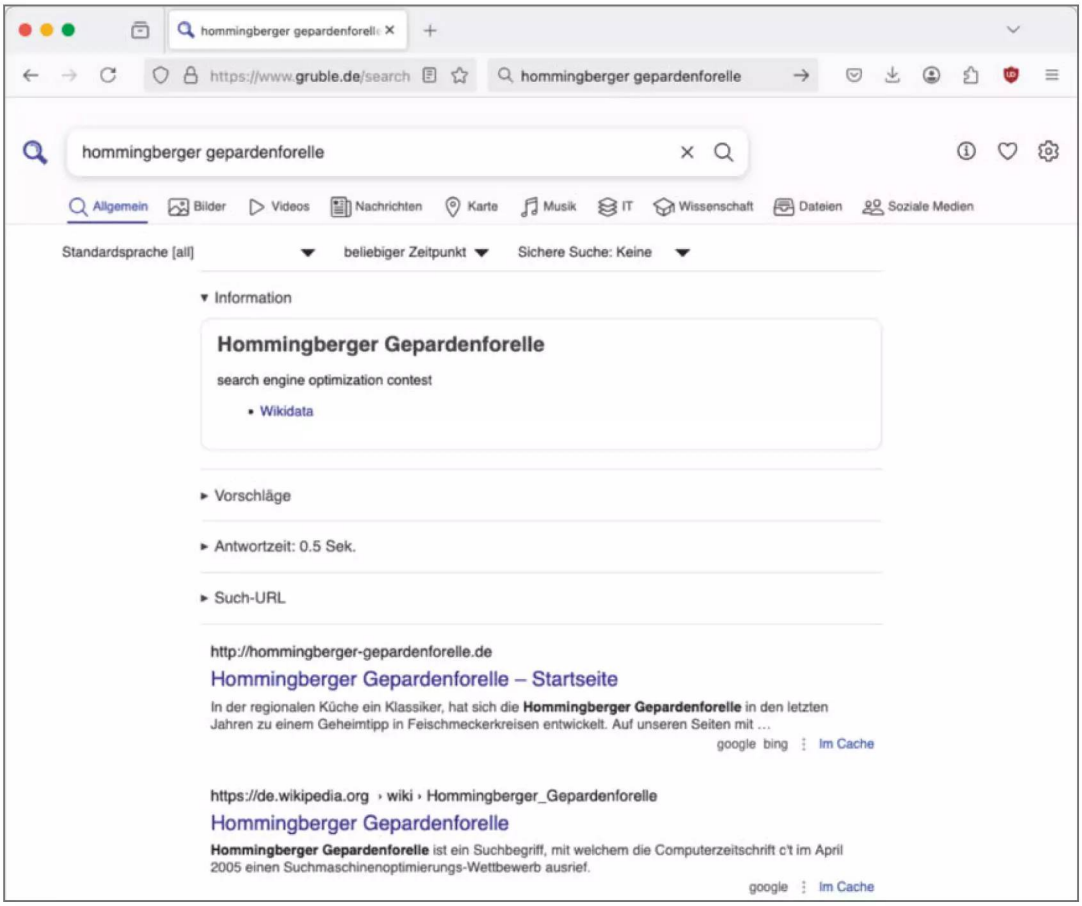
Unabhängig suchen

Ein ähnliches Geschäftsmodell verfolgt inzwischen die deutsche Suchmaschinenalternative metaGer. Kostenlose Nutzung für alle konnte der Verein nicht mehr finanzieren, über den Erwerb von Token steht die Suchmaschine aber Interessierten weiter offen. Neben Werbefreiheit, Trackingverzicht und Privatsphärenschutz macht die Technik das Angebot interessant: Open-Source-Software kombiniert die Ergebnisse aus mehreren Suchindexen, unter anderem Brave und Bing.

Mit SearXNG bietet sich eine weitere Meta-Suchmaschine an, die aus Open-Source-Software besteht. Sie ist aus inzwischen eingestellten Projekten hervorgegangen. Es gibt weltweit etliche frei zugängliche, laufende Instanzen. Wer interessiert ist, kann mit vergleichsweise geringem Aufwand eine eigene Instanz aufsetzen. SearXNG wirkt als Filter zwischen den Suchenden und den befragten Suchmaschinen.

Startpage, das in den Niederlanden seinen Sitz unterhält, aber Teil eines börsenorientierten US-Unternehmens ist, funktioniert ähnlich wie SearXNG als Vermittler zwischen Benutzer und Google-Suche. Es anonymisiert die Ergebnisse, filtert kontextbezogene Anzeigen und KI-Zusammenfassungen aus. Falls Sie sich wundern, warum das viel empfohlene

Ersatz für die populären Suchmaschinen, die unter direktem Einfluss eines US-Techkonzerns stehen, lässt sich auftreiben. Oft stützt sich der Ersatz aber auf den Index ebendieser Firmen. Die „Suchvermittler" versprechen immerhin, die Nutzerdaten nicht an den Indexbetreiber abzuführen. Wie lange solche kostenlosen Angebote bestehen können, ist fraglich. Die deutsche Metasuchmaschine metaGer kann sich nur noch zahlende Kunden leisten.



DuckDuckGo hier nicht auftaucht: Die Firma hat ihren Sitz in den USA.

Wenn Sie eine alternative Suchmaschine favorisieren, lässt sie sich als Standard in gängige Browser eintragen. Das kann manchmal etwas tüftelich sein. Bei Firefox gelingt es etwa über Add-ons oder per GUI, indem Sie das Suchfeld in die Symbolleiste bringen. Dort erscheint dann nach einem manuellen Aufruf der Website, sofern sie sich als Suchmaschine zu erkennen gibt, ein dezentes grünes Pluszeichen zum Ergänzen der Suchmaschinenliste. Anschließend lässt sich der Neuankömmling dann als Standard setzen.

Was Suchmaschinen wie SearXNG und Startpage vormachen, sich nämlich als Stellvertreter vor andere Dienste zu setzen und damit den Datenabfluss des Nutzers zu reduzieren, haben findige Entwickler auch auf viele andere Dienste übertragen. Es gibt mit LibRedirect sogar eine Browsererweiterung. Wenn sie aktiv ist, leitet sie den Browser automatisch zu einem anderen Server um, der die gewünschten Inhalte datenschutzfreundlich über eine vereinfachte Weboberfläche ausliefert, ähnlich wie ein Proxy. Bei denen lässt aber oft die Usability zu wünschen übrig.

Der Nutzer landet mit LibRedirect beispielsweise nicht bei YouTube, sondern einem weniger datensammelwütigen Proxy für das Videoportal, etwa Invidious. Diese „Proxies" sind zum einen Open-Source-Projekte, oft existieren aber öffentlich betriebene Instanzen derselben. Auf die leitet LibRedirect weiter. Achtung: Womöglich geraten Sie

dabei an Betreiber, die sich nicht der hehren Idee der Datensparsamkeit verpflichtet fühlen.

Daten befreien

Ein **E-Mail**-Postfach enthält oft sensible Daten. Darin findet sich Persönliches, aber vor allem Hinweise auf Beziehungen zu anderen Personen, Geschäften, Vereinen et cetera. Fast jeder dürfte dort auch kompromittierende Dinge aufheben, etwa Kommunikation über Dritte, die niemals in deren Hand geraten sollte. Und: Will jemand Ihre digitale Identität übernehmen, ist Ihr E-Mail-Konto der Universalschlüssel für Passwort-Resets und andere Arten der Informationserschleichung.

Um die E-Mail den großen US-Cloudprovidern zu entreißen, braucht es einen passenden Anbieter: Es gibt in Europa zahlreiche E-Mail-Dienstleister. Was man bekommt, hängt unmittelbar davon ab, was man zu zahlen bereit ist. Bei Diensten wie GMX, Freenet und so weiter geht es gratis, wenn man sich von Werbeanbietern tracken lässt. Premiumpakete, die pro Monat wenige Euro kosten, halten den Kunden zumindest einen Teil der Tracker vom Leib. Viele Internetprovider schenken ihren Kunden auch ein E-Mail-Postfach, das etwa die Telekom nur gegen Aufpreis werbefrei hält.

Hosting-Anbieter, die Webserver vermieten, bieten ebenfalls oft E-Mail-Postfächer an. Eine Domain gehört dann meist zum Paket dazu. Das ist für Firmen die interessantere Variante, weil solche Angebote dann auch mit mehr Rechtssicherheit glänzen und einen Auftragsverarbeitungsvertrag beinhalten. So hat man gleich etwas für die Datenschutzaufsichtsbehörde in der Hand, sollte sie einen Nachweis einfordern.

Die Königsklasse der E-Mail-Hoster hat sich auf Datenschutz spezialisiert, wie die Berliner Mailbox.org, Posteo und Tuta aus Hannover oder die Schweizer Proton. Bei einigen kann man anonym E-Mail-Adressen erhalten, wenn man Bargeld im Umschlag schickt. Das ist die Alternative zu übergriffigen E-Mail-Anbietern, die mitunter Mobilfunknummer und Ausweiskopie fordern – was nach aktueller Rechtslage für E-Mail-Anbieter nicht vorgeschrieben ist. Die Anbieter veröffentlichen Transparenzberichte und nennen so die Anfragen staatlicher Organe. Proton verspricht, dass betroffene Kunden von jeder Intervention erfahren.

Wenn ein passender Anbieter gefunden ist, braucht es etwas Zeit und die richtigen Werkzeuge für den Umstieg. Mit vielen Mailprogrammen kann man zwei E-Mail-Konten gleichzeitig einrichten und auf diese Weise die E-Mails per Drag & Drop vom alten Anbieter zum neuen kopieren – dazu müssen beide lediglich das gängige IMAP4 als Protokoll für den Zugriff auf die Daten gestatten. Für schwierige Fälle hilft eine Zwischenstation in Form eines lokalen Ordners, spezieller Software wie MailStore Home oder das komplexe imapsync von Gilles Lamiral auf der Kommandozeile. Viele Tipps haben wir in [2] zusammengetragen.

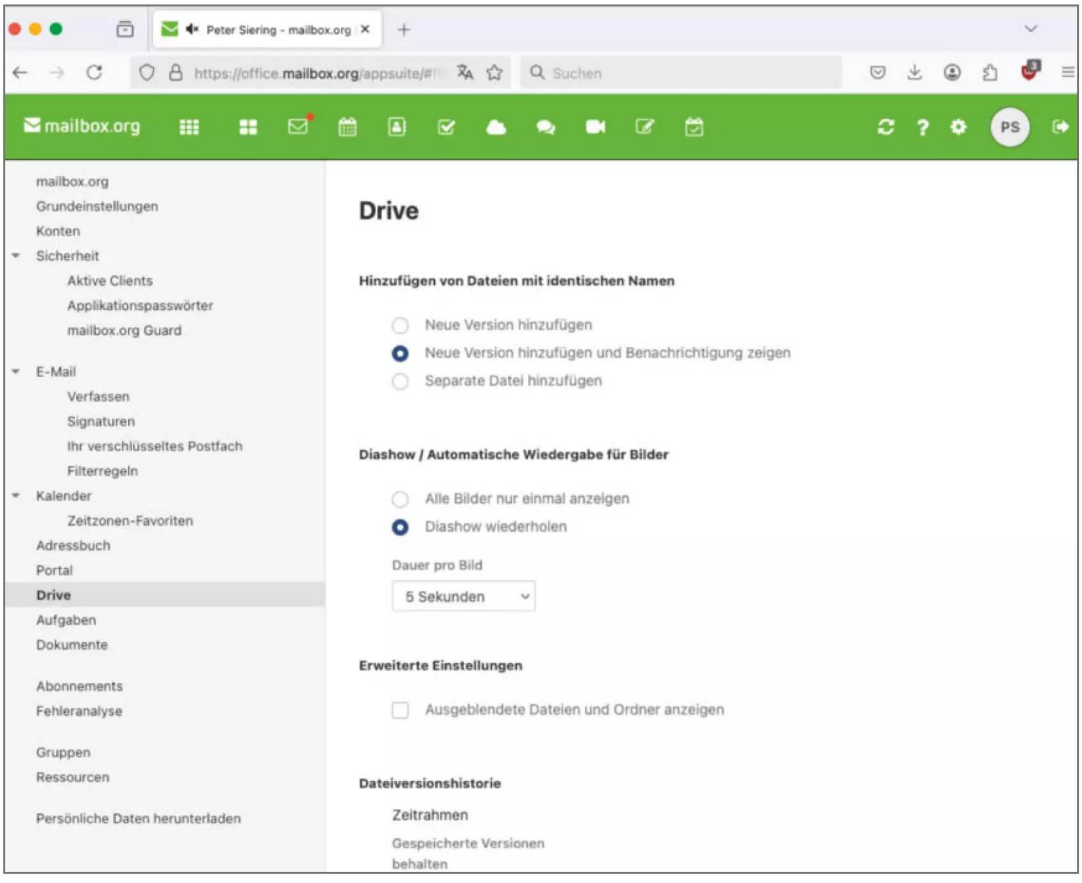
Dateien verschieben

Um **Kalender**- und **Adressbuch**daten aus einem Clouddienst herauszuholen, liegen oft die bereits erwähnten Mailhoster als Ziel nahe. Üblicherweise stecken dort Kalender und Adressbuch mit im Paket. Für den Export der Daten aus dem bisherigen Silo bieten sich die Dateiformate ICS und LDIFF an (verwandt mit den Zugriffsprotokollen Cal- und CardDAV). Dieses Format können die meisten Alternativen direkt importieren. Sie sollten dabei auf Details achten, gern missraten Serientermine und mitunter kommt es zu Zeitzonendifferenzen. Gegebenenfalls heißt es dann, in den Textdateien der Exporte Hand anzulegen.

Dienste wie OneDrive, Dropbox und Google Drive **synchronisieren Dateien** zwischen Rechnern und Mobilgeräten über eine zentrale Cloudablage per Sync-Software. Das ist ungemein praktisch, um Fotos automatisch wegzusichern oder wenn man auf mehreren Geräten arbeitet und sich nicht ständig einen Kopf darüber machen will, dass man auch Zugriff auf die aktuelle Fassung einer Datei hat.

Hilfreich ist auch der Versionsverlauf, über den sich alte Versionen einer Datei wiederherstellen lassen. Hinzu kommen Funktionen, um Dateien aus eigenem Bestand per Link mit anderen zu teilen – die brauchen für den Zugriff zumeist nicht mal ein Konto beim jeweiligen Dienst. Mehr und mehr werden auch Online-Bearbeitungsfunktionen Teil der neuen Dateiablagen: Google Drive nutzt dazu die eigenen **Online-Office**-Alternativen Google Docs et cetera. Dropbox greift auf die Programme der Microsoft-Office-Familie zurück. Microsoft OneDrive nutzt ebendiese. Auch einige der Mailhoster bieten die Onlinebearbeitung von Office-Dateien.

Mit Nextcloud gibt es eine Open-Source-Alternative für die Dateisynchronisierung und den -austausch. Open Source heißt aber nicht, dass man die selbst betreiben und womöglich übersetzen muss. Es haben sich inzwischen Dienstleister darauf spe-

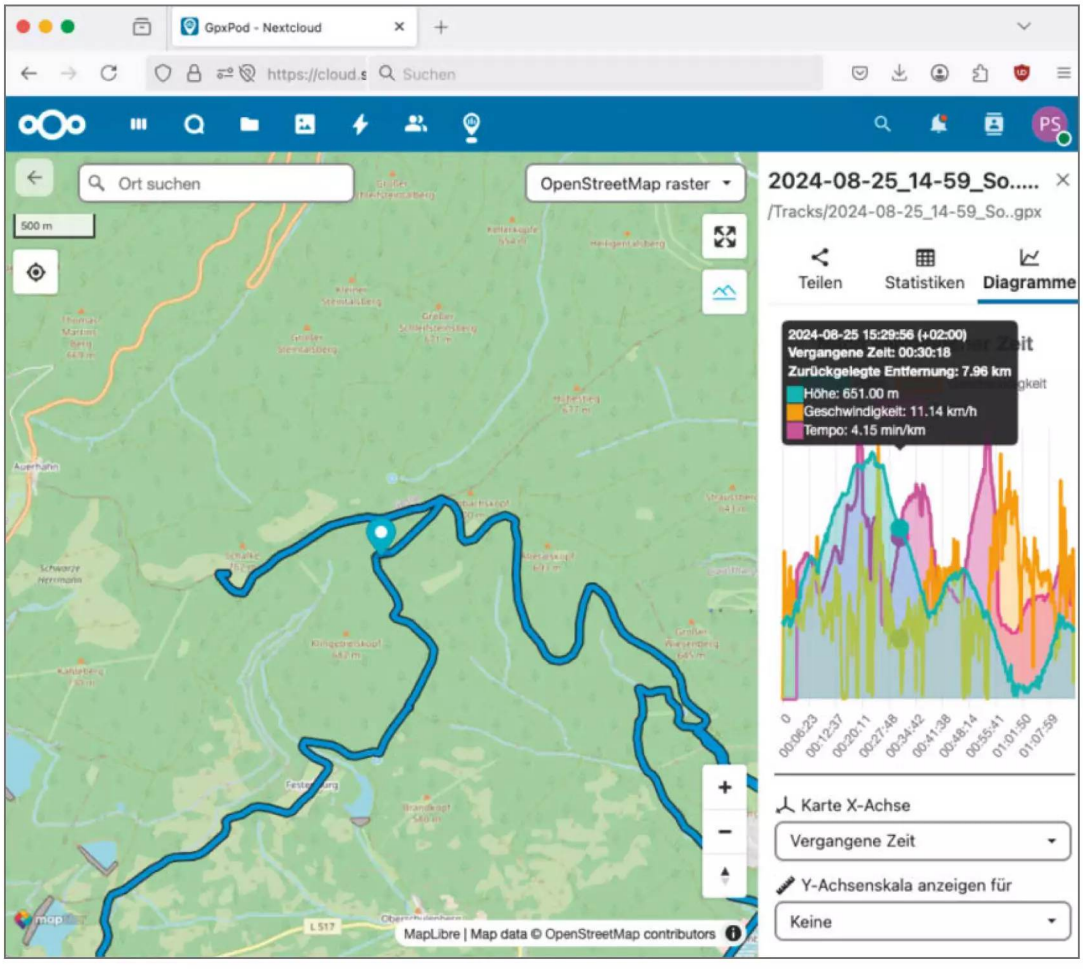


Maildienste wie mailbox.org kosten ein paar Euro pro Monat, dafür dealen sie nicht mit den Daten ihrer Kunden und widerstehen Auskunftsbegehren übergriffiger Behörden. Oft gehören zum Paket auch ein Kalender und ein Adressbuch, mitunter auch die Freigabe und Bearbeitung von Dateien. Die Anbieter unterscheiden sich im Funktionsumfang, etwa der Nutzung eigener Domains und den Anstrengungen, die gespeicherten Daten sicher zu verschlüsseln.

zialisiert, Nextcloud schlüsselfertig anzubieten (siehe S. 116). Bei vielen Hosting-Providern finden sich vorkonfigurierte Instanzen oder einfache Bausätze, um mit der eigenen Nextcloud zu starten. Sogar die Telekom bietet ihren Kunden eigene kleine, kostenlose Instanzen, die sich gegen Aufpreis aufwerten lassen.

Mit Nextcloud funktioniert ebenfalls das gemeinsame Arbeiten an Office-Dokumenten, wenn Collabora Online oder OnlyOffice als Erweiterungen installiert sind. Das ist nicht in jeder Nextcloud-Instanz der Fall und bei einigen Hosting-Angeboten mitunter sogar vom Betreiber ausgeschlossen worden. Auch einige Mailhoster bieten eine Dateisynchronisation in ihren Mailpaketen als Extra an.

Es gibt keinen verbreiteten Standard zur Synchronisation von Dateien, auf denen die Lösungen aufbauen können. Das heißt, es braucht jeweils die passende Software respektive App auf den Geräten. Ein Umzug von einem auf einen anderen Dienst heißt entsprechend, die Dateien auf einem der zum Sync verwendeten Geräte so zu kopieren, dass die neue Sync-Software sie zu fassen bekommt. Alte Versionsinformationen gehen dabei über die Wupper.



Nextcloud ist der Tausendsassa unter den Alternativen für US-Clouddienste und -anwendungen: Viele Hoster verkaufen Mietinstanzen, es eignet sich aber ebenso gut fürs Selbsthosten. Über in Nextcloud installierbare Apps erlernt es viele Disziplinen über Dateisynchronisation, Kalender und Adressbuch hinaus, etwa Videokonferenzen und die gemeinsame Arbeit an Office-Dokumenten. Und Nextcloud meistert Aufgaben, die auf den ersten Blick nicht gerade naheliegen, wie das Teilen von Outdoor-Aktivitäten.

In den Empfehlungen zur US-Cloudflucht finden sich noch andere Angebote, allerdings oft mit Haken: Die Software Seafile stammt von einer chinesischen Firma – ein Ausschlusskriterium mindestens für besorgte Nutzer. Bei der Schweizer pCloud, einem Cloudspeicherdienst, der lebenslange Abonnements zum Pauschalpreis anbietet, mehren sich Zweifel an den Hintergründen des Unternehmens.

Risiken verteilen

Mit dem **Kartendienst** Maps und gratis einsehbaren Luftbildern hat Google eine begrüßenswerte Entwicklung eingeleitet. Inzwischen trieft aber die Darstellung vor Werbeeinträgen. Dark Patterns beim Konfigurieren eines Google-Kontos tragen dazu bei, dass die Nutzer mehr Daten bei Google lassen, als ihnen lieb sein kann.

Die Spitze der Spionererei war der Standortverlauf (später „Zeitachse“), der sich bei Ermittlungsbehörden hoher Beliebtheit erfreute und inzwischen nicht mehr in der Cloud landet. Kurzum: Wenn Sie den Dienst unbedingt nutzen sollten, tun Sie das auf jeden Fall, ohne sich bei Google anzumelden.

Alternativen gibt es zuhauf: Here Maps ist ein europäisches Unternehmen, in das viele Autohersteller investiert haben. Sehr detaillierte Daten liefert das OpenStreetMap-Projekt, das auch in vielen Apps inzwischen die Basis für Karten bildet. Die von einer Community erarbeitete Datenbasis ist mittlerweile so gut, dass sie auch zur **Navigation** taugt. Was allerdings fehlt, sind Daten über den Verkehrsfluss.

Skeptisch sollten Sie bei Apps sein, die Geoinformationen mit Outdoor-Aktivitäten verknüpfen. Oft stecken trotz OpenStreetMaps-Basis doch US-Unternehmen dahinter, zum Beispiel Strava. Nach dem Social-Media-Prinzip werden Communities aufgebaut und Sie als Nutzer liefern bereitwillig Vitaldaten während des Trainings ab. Das öffnet missbräuchlicher Nutzung Tür und Tor.

Als App empfiehlt sich heute OsmAnd Maps. Die Open-Source-App ist in der Grundausstattung schon sehr nützlich und lässt sich durch In-App-Käufe auch noch erweitern. Sie kann Kartendaten herunterladen, funktioniert also auch offline.

Wer seinen eigenen Standort lokal als Aktivitätsverlauf aufzeichnen möchte, kann dazu ebenfalls die App hernehmen. Optional gibt es einen eigenen Clouddienst. Aufgrund der vielen Möglichkeiten muss man sich an mancher Stelle etwas Zeit zum Reinfuchsen gönnen. Auch mit einer selbst gehosteten Open-Source-Lösung lässt sich ein cloudfreier Standortverlauf aufbauen (siehe S. 132).

08/15-**Smart-Home**-Geräte, wie sie beim Discounter auf dem Grabbeltisch liegen, lassen sich oft nur über dubiose Apps in Betrieb nehmen und nutzen. Wenig besser sind Markengeräte, die von der gleichen Krankheit befallen sind: Ohne App geht nichts. Die App braucht ein Gegenstück, und das ist in der Regel ein Clouddienst.

Wo diese Clouddienste beheimatet sind, kann der Benutzer selbst kaum ermitteln. Der Herstellername ist kein zuverlässiger Hinweis. Nicht einmal die bei einem DNS-Filter (siehe oben) angefragten Namen liefern aussagekräftige Hinweise. Oft gehören die laut IP-Adresse angesprochenen Server nämlich zu einem US-Hyperscaler wie Amazon oder Google. Manchmal kann man an deren Namen den Serverstandort erkennen – aber es bleiben ja US-Unternehmen.

Idealerweise erlaubt ein smartes Gerät die Nutzung über herstellerunabhängige oder offene Protokolle wie ZigBee, Matter oder MQTT. Dann ist es aus gängigen Smart-Home-Zentralen verwendbar und auf keinen Clouddienst angewiesen. Alternativen sind geschlossene Systeme, die ohne Internetanbindung auskommen. Achten Sie darauf, dass das sowohl für die Konfiguration als auch für den Betrieb gilt.

In manchen Fällen können Sie auf den Geräten auch alternative Firmware installieren, um sie vom Cloudzwang zu befreien, etwa die Tasmota-Firmware für die verbreiteten Tuya-Geräte oder Valetudo für viele Saugroboter.

Konten kastrieren

Manche Unabhängigkeit ist trügerisch. Der beliebte Community Store für Home Assistant (HACS), eine Oberfläche, um komfortabel Erweiterungen zu installieren und zu aktualisieren, verwendet unter der Haube GitHub – einen Dienst, den Microsoft für Entwickler betreibt. Die Home-Assistant-Schöpfer nutzen hier der Einfachheit halber APIs, die GitHub anbietet. Das fällt wohl den wenigsten Nutzern im Eifer des Gefechts auf.

Apple, Google und Microsoft erwecken schon bei der Neukonfiguration den Eindruck, dass ihre Geräte oder Betriebssysteme ohne ein **Online-Konto** bei ihnen kaum sinnvoll nutzbar sind. Oft trügt der Anschein. Widerstehen Sie an dieser Stelle. Lediglich bei Windows 11 Home müssen Sie inzwischen einigen Aufwand treiben, um den Kontozwang zu überwinden.

Sie werden während der Nutzung der Geräte später auch wieder darauf hingewiesen, dass ein solches Konto notwendig sein kann. Nehmen Sie dieses Angebot nur an, wenn es sich für Ihre Nutzungsszenarien nicht vermeiden lässt. Ein Beispiel: Apple-Geräte erlauben ohne Anmeldung im AppStore nicht die Installation von Software (iOS) oder erhalten automatisiert keine Updates (macOS).

Bei Android-Geräten hingegen können Sie zu alternativen App-Stores wie F-Droid oder dem Aurora Store greifen, um Apps ohne Google-Konto zu beziehen und aktuell zu halten.

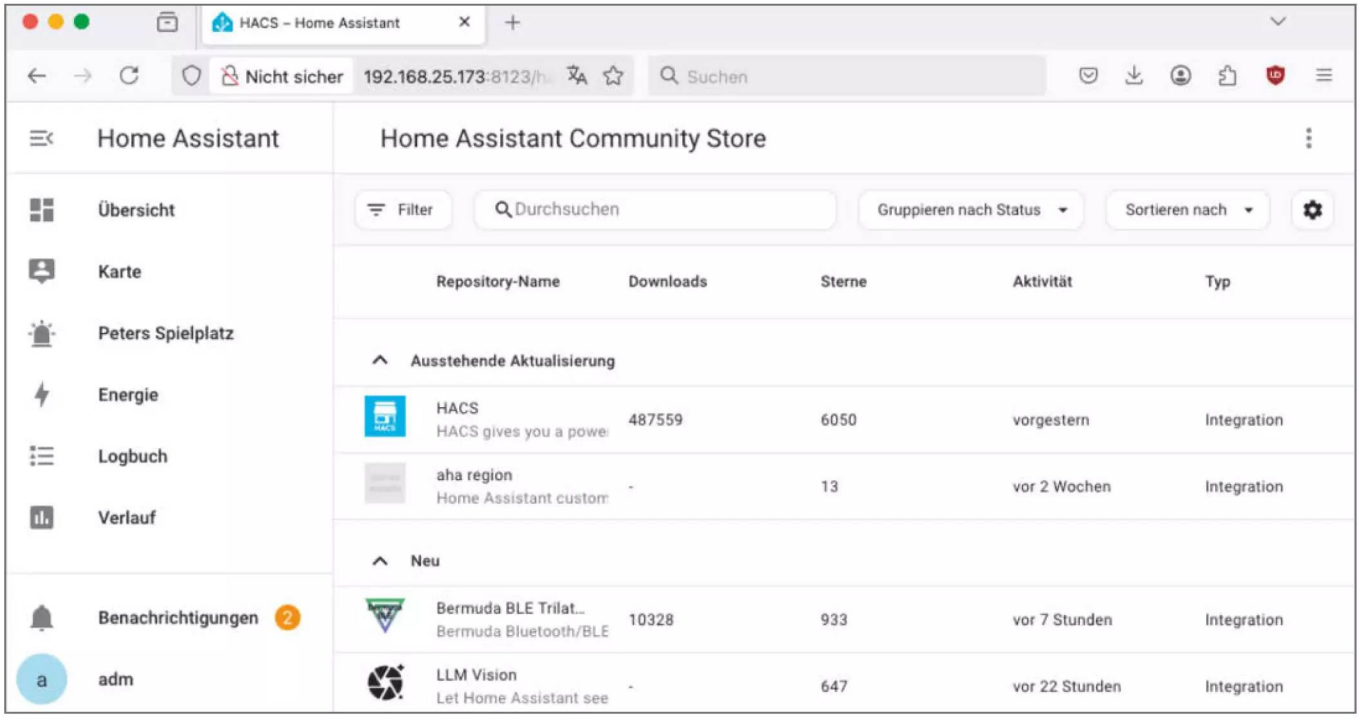
Überlegen Sie sich, welchem Konto Sie welche Daten anvertrauen. Wenn Sie E-Mail und Dateisynchronisation über ein und dasselbe Konto laufen lassen, kann das verzwickt werden: Sperrt der Anbieter das Konto, weil er in den Dateien Dinge gesehen haben will, die den Nutzungsbedingungen widersprechen, dann fehlt ihnen mit der E-Mail womöglich gleich Ihr Hauptkommunikationsweg.

Gratiskonten sind wie der kostenlose Kaffee in der Spielhalle: Wirkt nett, dient aber ausschließlich dem Ziel, Ihnen Geld abzuknöpfen. Irgendwann reicht das Freispeicherkontingent nicht mehr und Sie zahlen für mehr. Gleichzeitig sind Ihre persönlichen Daten die erste Rate: Der Anbieter erfährt Ihre Nutzungsgewohnheiten und Vorlieben.

Dezentral werden

Mit den großen **Social-Media**-Plattformen machen die Technik-Bros Stimmung weltweit. Künstliche Intelligenz und russische Botfarmen tun das Übrige,

Kostenlose Konten, wie sie Windows hartnäckig dem Kunden bei der Ersteinrichtung andrehen will, haben ihren Preis. Der Kunde zahlt mindestens mit seinen Daten.



Oft heißt es, genau hinsehen: Der Komfort im Community Store für Home Assistant (HACS) stellt sich erst ein, wenn man eine Anmeldung bei GitHub toleriert – schwupps, unterläuft man die eigenen Vorsätze, das smarte Heim nicht an US-Clouds zu koppeln.

um das gesellschaftliche Klima zu vergiften. Obendrein sammeln die Apps für die Plattformen munter Daten. Wenn es nicht ohne Social Media geht: Probieren Sie doch mal das Fediverse aus.

Das sind unabhängige, über ein Standardprotokoll (ActivityPub) miteinander verbundene Systeme. Hier kann kein Digitaldespot die Kontrolle übernehmen. Was Sie sehen und was nicht, entscheiden Sie selbst. Mit dem Betrieb eines eigenen Mastodon-Servers können Sie sich sogar aktiv daran beteiligen.

Die Idee, unabhängige Instanzen eines Diensts miteinander in den Austausch zu bringen, ist nicht auf Mastodon beschränkt: Pixelfed verwendet ebenfalls das ActivityPub-Protokoll, um eine Instagram-Alternative auf die Beine zu stellen, die vor allem für Fotofans interessant ist. Mit Radicle gibt es sogar ein Projekt, das versucht, die Software-Entwicklung per Git in der Art von GitHub & Co. zu dezentralisieren. Das Matrix-Protokoll gestattet ähnliche Ansätze.

Unabhängigkeit stärken

Unabhängigkeit von den Interessen eines Herstellers erhalten Sie nur, indem Sie konsequent auf **Open-Source**-Software setzen. Das kann im Kleinen mit alternativen Apps beginnen, etwa für Office [6]. Doch wirklich unabhängig werden Sie, wenn Sie bereit sind, auch das **Betriebssystem** zu ersetzen.

Computer nahezu jeder Couleur lassen sich heute mit einer Linux-Distribution aus der Herstellerhand befreien. Bei ganz modernen Systemen kann es unter Umständen etwas schwieriger sein [3]. Dass man für Linux die Software selbst übersetzen und ständig auf der Kommandozeile hantieren muss, stimmt längst nicht mehr. Selbst unbedarfte Computernutzer kommen gut klar.

Linux-Nutzer werden nicht von irgendwelchen Vorgaben eines Herstellers gegängelt, der ihnen zweifelhafte Funktionen wie Onlinekonten als Vorteil verkauft. Sie sind unbeobachtet und haben einen viel größeren Entscheidungsspielraum. Sollte mal etwas nicht auf Anhieb funktionieren, finden sie viele Hilfestellungen, und jede selbst gefundene Lösung lässt sie digital deutlich souveräner werden.

Was für viele Computer gilt, lässt sich auch auf Android-**Smartphones** übertragen. Für die Pixel-Familie gibt es mit GrapheneOS ein rundes, Google-freies Betriebssystem. Es erlaubt anders als andere sogenannte Custom-ROMs weiterhin Dienste aus dem Google-Play-Store zu verwenden, hegt sie aber in eine Sandbox ein und macht sie über einen Mini-App-Store zugänglich.

Was mit GrapheneOS für die Pixel-Reihe klappt, ist für andere Android-Telefone derzeit leider eher ein Thema für Bastler. Mike Kuketz hat in seinem Blog in einer Custom-ROM-Serie alternative Firmware analysiert und kommt immer wieder zu dem Schluss, dass in manchen immer noch viel Google drinsteckt und oft die Sicherheit leidet [4].

Für Apple-Mobilgeräte gibt es kein alternatives Betriebssystem, weder als proprietäre Lösung noch auf Basis von Open Source. Etliche Apps werden aber sehr wohl mit dieser Grundhaltung entwickelt. Wie das Beispiel OsmAnd Maps (siehe oben) zeigt, müssen sie sich keineswegs vor kommerziellen Angeboten verstecken, ganz im Gegenteil.

Wie auch schon einzelne Open-Source-Apps zeigen, ist der Ansatz, gemeinschaftlich an solchen Projekten zu arbeiten, zum einen erfolgreich, zum anderen erfreulich für die Mitwirkenden – egal, ob als Entwickler, Handbuchautor, Supporter in Foren oder nur Spender. Geben und Nehmen in einer Gemeinschaft trägt weiter als Konsum und steigert unser aller Souveränität.

Monopole meiden

Das Bonmot „Es ist noch niemand gefeuert worden, weil er bei IBM gekauft hat“ könnte man heute verdrehen zu „Es ist noch niemand gefeuert worden, weil er US-Clouddienste eingekauft hat“. Anders ist der anhaltende Run von Firmen auf Microsofts Cloudangebote in der jetzigen Zeit kaum zu verstehen.

Gern bemühen die Fürsprecher dieser Verantwortungsdelegation, dass die Bedrohungs- und Gesetzeslage Unternehmen keine Chance ließe und man in die Cloud wechseln müsse, um die Risiken zu minimieren. In den Gesetzen steht davon nichts, sondern nur, dass Firmen IT-Systeme nach dem Stand der Technik betreiben müssen. Das scheuen Unternehmen offenbar.

Was sie dafür erhalten haben: Sie verwalten Ihre Nutzer in einem Verzeichnisdienst, den derzeit nahezu ausschließlich Microsoft bereitstellt (**Active Directory**) und der alle daran anknüpfenden Dienste zusammenhält, also Kommunikation (Teams), Business-Software (Office und angehängte Verarbeitung) sowie E-Mail und Kalender (**Exchange**). Das alles liegt dann in der Cloud eines US-Unternehmens.

Es ist praktisch unmöglich, einzelne Dienste dort herauszunehmen und in andere Hände zu geben: Der Komfort leidet. Die Daten lassen sich nur schwer migrieren. Alternativen sind nicht entwickelt worden. Und: Die Nutzer meutern. Wer bereits in der Schule

Excel und Word eingetrichtert bekommt, wird sich freiwillig kaum mit Alternativen befassen – Nerds ausgenommen.

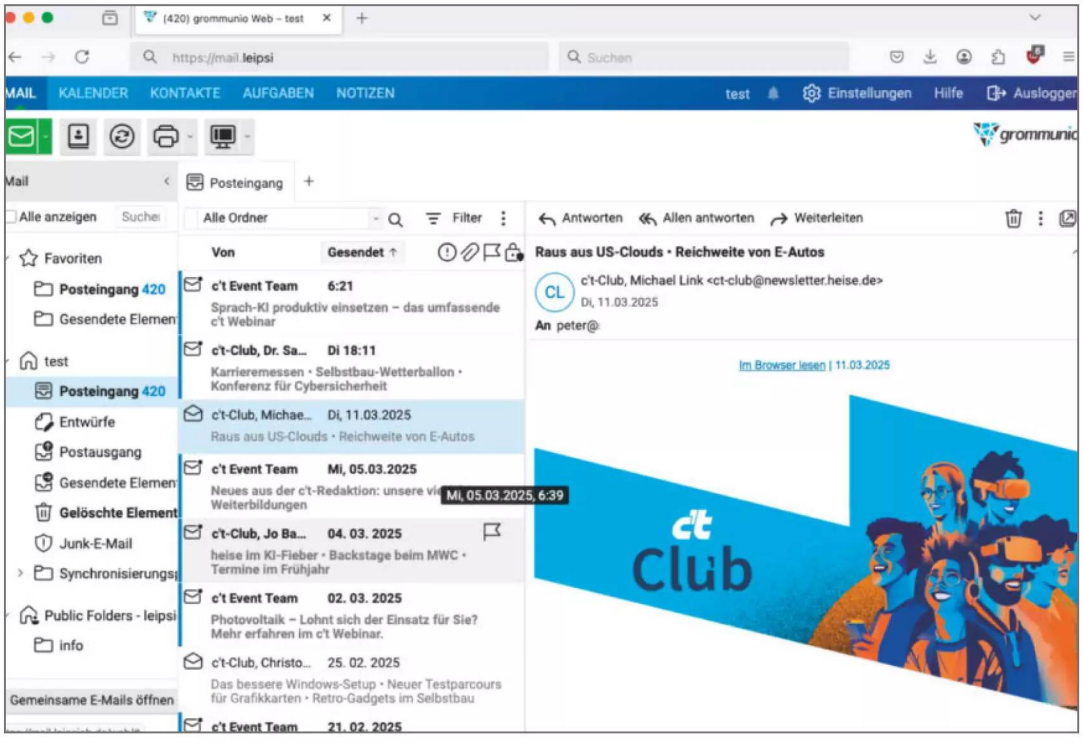
Die öffentliche Hand in Europa scheint immerhin erkannt zu haben, dass im Open-Source-Ansatz ein Weg zu mehr digitaler Souveränität und raus aus den US-Clouds führt. Sie hat jedenfalls Geld in allerhand Projekte wie openDesk, Phoenix-Suite, Gaia-X und das Zentrum für Digitale Souveränität gesteckt.

Doch inzwischen mehrt sich Kritik von Firmen, die schon lange Zeit im Open-Source-Umfeld Geld verdienen und die Entwicklung der Software vorantreiben, dass Trittbrettfahrer ihre Projekte zu Dumpingpreisen auf den Markt bringen, ohne etwas beizutragen. Das Nehmen funktioniert schon, das Geben müssen einige Akteure offenbar noch lernen (siehe S. 50).

Konsequent sein

Für den Weg raus aus der US-Cloudabhängigkeit gilt: Wer suchet, der findet. Viele der erwähnten Alternativen lassen sich in Eigenregie betreiben. Die hat aber einen Preis: Es genügt nicht, Installation und Konfiguration zu meistern. Fortan gilt es, sich um regelmäßige Updates zu kümmern, damit Sicherheitslücken geschlossen und Patches dafür installierbar bleiben.

Die wenigsten Alternativen muss man indes selbst betreiben. Für nahezu alles finden sich Dienstleister, die das gegen einen oft kleinen Obolus übernehmen. Besonders bei E-Mail dürfte das für die meisten US-Cloudabtrünnigen ohnehin der beste Weg sein. Einen E-Mail-Server vollständig selbst zu unterhalten verursacht hohen Aufwand.



Es wachsen neue Alternativen heran, die Microsofts Groupware- und E-Mail-Server Exchange ablösen wollen – das erspart manchem vielleicht den für Exchange obligatorisch scheinenden Umzug in die Microsoft-Cloud. Doch bislang können weder alte Versuche noch neue Anläufe das Original vollumfänglich ersetzen.

Open Telekom Cloud

Connecting your world.

WHAT A WONDERFUL CLOUD THIS COULD BE

Sie suchen eine souveräne Cloud aus Europa – ohne Kompromisse bei Leistung und Funktionen?

Sie haben sie gefunden: Mit der Open Telekom Cloud.

ALS FÜHRENDE EUROPÄISCHE PUBLIC CLOUD* BIETET SIE IHNEN:

✓ **UMFANGREICHES ANGEBOT INKLUSIVE KI:**
Direkter Zugriff auf mehr als 60 Services inklusive virtueller Maschinen, Container, Serverless-Funktionen und KI-Tools.

✓ **DIGITALE SOUVERÄNITÄT ALS STANDARD:**
Volle Kontrolle über Daten und Infrastruktur dank eines Open-Source-basierten Leistungsumfangs ohne Vendor-Lock-in-Effekte.

✓ **ZERTIFIZIERTE SICHERHEIT UND COMPLIANCE:**
DSGVO-Konformität, weitreichende Zertifizierungen und die Erfüllung branchenspezifischer Bestimmungen für regulierte Märkte.

* The Forrester Wave™: Public Cloud Platforms In Europe, Q3 2024

UND DAS ALLES MIT DER EXPERTISE UND ZUVERLÄSSIGKEIT DER DEUTSCHEN TELEKOM.

Jetzt entdecken und kostenfrei testen:

Souverän. Flexibel. Persönlich.

SOUNDS GOOD FOR EUROPE.

Alternativen für US-Clouddienste: Empfehlungen

Anwendung	US-Dienst	Alternative	Bemerkung
Adressbuch	Google, iCloud	Nextcloud, div. Mailhoster (siehe E-Mail)	
Chatserver	Slack	Nextcloud, Mattermost, Matrix	
Dateisynchronisation	Dropbox, Google Drive, OneDrive , iCloud	Nextcloud, Strato/IONOS HiDrive, div. Mailhoster (siehe E-Mail)	im Selbstbau Software wie Syncthing
E-Mail	Outlook, Google Mail, AOL, Yahoo ...	Posteo, mailbox.org, ProtonMail, Tuta, div. Hoster	einige Angebote mit Extras wie Adressbuch, Kalender, Dateisync sowie Teilen und Bearbeiten von Office-Dokumenten
Groupware	Exchange	Grommunio, Kopano Cloud, Open-Xchange	decken nicht den vollen Funktionsumfang ab
Foto-Speicher	Google Photo, iCloud	Immich	oft hilft hierbei auch Dateisynchronisation
Hyperscaler	AWS, Azure, Google Cloud	StackIT, div. Hoster	Alternativen setzen meist auf Kubernetes oder OpenStack
Kalender	Google Calendar, iCloud	Nextcloud, Mailhoster (siehe E-Mail)	
Kartendienste	Google Maps, Bing Maps	Here, OpenStreetMap	
KI	ChatGPT, Claude	Mistral	diverse Hoster bieten nicht US-KI als Service an
Messenger	WhatsApp	Threema, Element (Matrix), XMPP (Jabber)	
Musikstreaming	Apple Music	Spotify, Deezer, Qobuz, SoundCloud	Spotify: Gründer hat zur Trump-Amtseinführung gespendet
Notizen	OneNote	Joplin, Obsidian	
Office Online	M365	Nextcloud	Nextcloud greift auf OnlyOffice oder Collabora Online zurück; div. Mailhoster haben ähnliche Funktionen
Smart Home	Apple Home, Google Home	Home Assistant, HomeBridge, OpenHab, ioBroker, Domoticz	alle zum Selbsthosten und geeignet, um vorhandene Komponenten zu integrieren
Social Media	X, Facebook, Instagram, Reddit, LinkedIn, YouTube	Mastodon, Pixelfed, Lemmy, Quodari, Xing, PeerTube	
Spiele	Steam	gog.com	DRM-freier Spielekauf
Suchmaschinen	Google, Bing	Ecosia, Good Search, SearXNG, Qwant, metaGer, Startpage	
Versionsverwaltung	GitHub	Codeberg, Radicle, Forgejo	
Videokonferenzen	Teams, Zoom, Google Talk	Nextcloud, Jitsi Meet, BigBlueButton, OpenTalk	meist weniger starke Integration von E-Mail, Office & Co.
Videostreaming	Netflix, Amazon Prime, Disney, Paramount+, Apple-TV	Filmfriend, Sooner, Mubi, Joyn, RTL+, Mediatheken des öffentlich-rechtlichen Rundfunks	

Konsequent sein heißt aber auch: auf Annehmlichkeiten verzichten. Es gibt Versuche, alternative Sprachassistenten zu schaffen. Doch mit dem Komfort der gängigen Cloudwanzen von Amazon, Apple und Google kann bisher keiner mithalten. Vielleicht lässt sich manches „Problem“ eben ohne Cloud nicht lösen? Gerade hat Amazon erklärt, dass Alexa die Cloud zukünftig immer mitlauschen lässt ...

Gerade letzteres Beispiel zeigt, wie schnell sich die Bedingungen für Produkte ändern, die ohnehin schon von Clouddiensten abhängen. Die Kunden können ihr Missfallen nur bekunden, indem sie das Produkt außer Betrieb nehmen – in den ursprünglich versprochenen Grenzen lässt es sich schließlich nicht mehr nutzen.

Das führt zum letzten Punkt unserer Betrachtungen: Was tun, wenn Sie Alternativen für (US-)Clouddienste gefunden, für gut befunden und Ihre Daten dorthin migriert haben? Das letzte Kapitel kann Arbeit machen: Löschen von Daten ist meist nicht vorgesehen, es bleibt nur, das Konto zu killen.

Wie aufwendig das Löschen von Konten ist und wie es gelingt, dazu trägt Lukas Müller seit 2020 auf seiner Website [5] justdeleteaccount.com Informationen zusammen: Fast 800 Einträge, die Hälfte der Konten sei leicht zu schließen, über 200 schwer und 100 Konten lassen sich nach seiner Erkenntnis überhaupt nicht tilgen. Vielleicht schauen Sie dort vorbei, bevor Sie Ihre Daten der nächsten US-Cloud anvertrauen? (ps) c't

Literatur

[1] Jo Bager, Die Schirmherren, Google gibt neue Spielregeln für Werbung und Werbeblocker vor, c't 5/2024, S. 52

[2] Stefan Wischner, Sicherungsverwahrung, Mails sichern, archivieren und migrieren, c't 3/2025, S. 28

[3] Keywan Tonekaboni, Pinguin auf fremden Welten, Linux auf Notebook-Exoten installieren, c't 7/2025, S. 56

[4] Mike Kuketz, Mach dich digital unabhängig von Trump und Big Tech: https://www.kuketz-blog.de/unplugtrump-mach-dich-digital-unabhaengig-von-trump-und-big-tech/

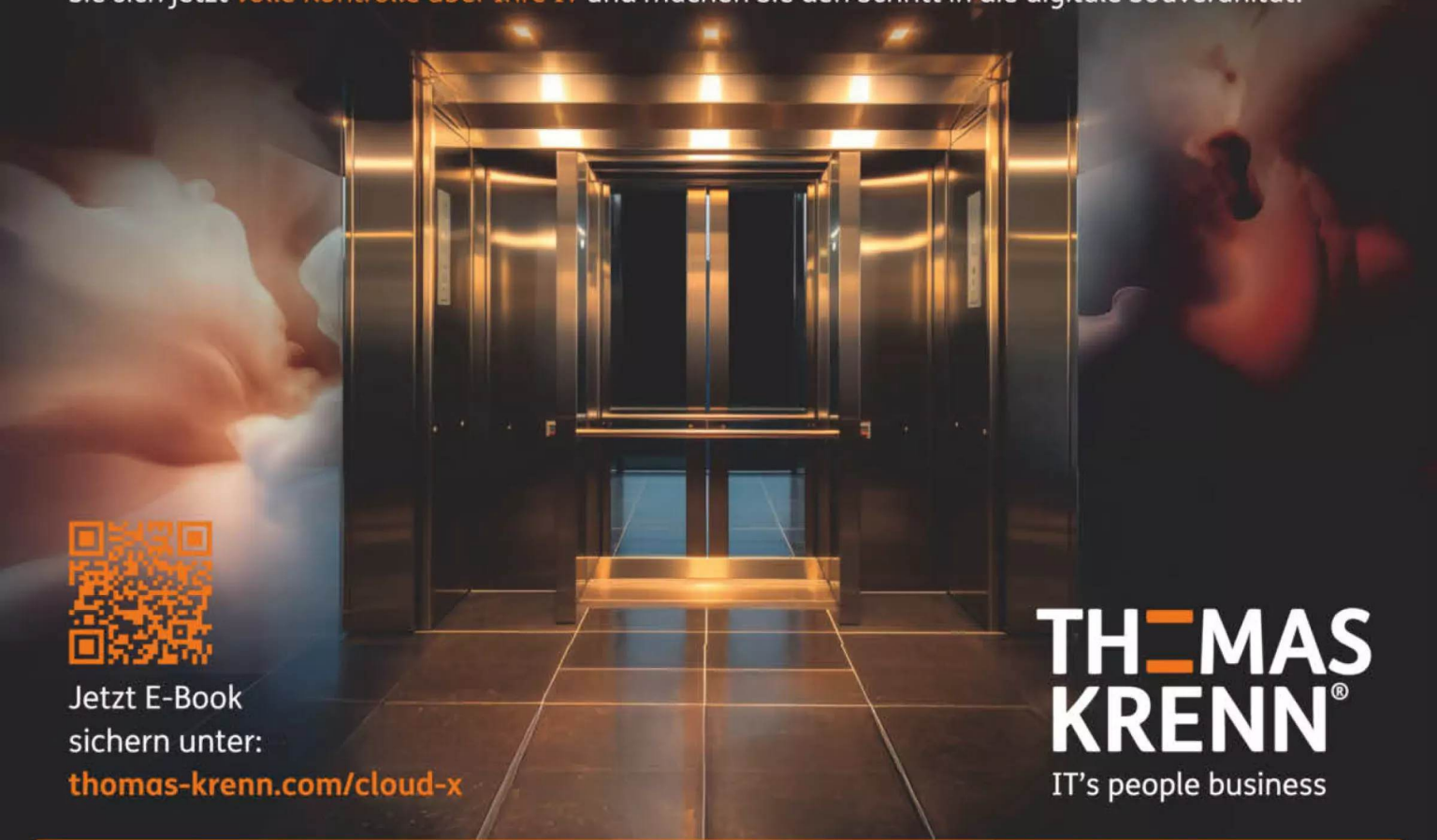
[5] Lukas Müller, Löschhilfen für Online-Konten: https://www.justdeleteaccount.com

[6] Stefan Wischner, Office ohne Microsoft, Fünf Alternativen zu Microsoft Office im Vergleich. c't 8/2025, S. 118

Endstation Cloud?

Zeit für digitale Souveränität!

Zuverlässige Technik, sicherer Zugriff auf Ihre Unternehmensdaten? Was Cloud-Lösungen nicht leisten können, erreichen Sie mit einer eigenen IT-Infrastruktur. Unsere Experten finden die optimale Hardware- und Software-Ausstattung für die Anforderungen Ihres Unternehmens – und helfen Ihnen beim Ausstieg aus unsicheren und unzuverlässigen Cloud-Umgebungen. Sichern Sie sich jetzt volle Kontrolle über Ihre IT und machen Sie den Schritt in die digitale Souveränität!



Jetzt E-Book sichern unter:
thomas-krenn.com/cloud-x

THOMAS KRENN®
IT's people business

Bild: KI, Collage c't

US-Clouds trotz aller Bedenken

Faktisch ist offensichtlich, dass Daten von EU-Bürgern in den USA nicht vor Behörden- und Providerzugriff geschützt sind. Mit welchen juristischen Verrenkungen die EU Transfers dennoch als DSGVO-konform auslegt, wirkt teils abenteuerlich.

Von **Holger Bleich**

So hatte sich Michael McGrath seinen Start sicher nicht vorgestellt: Gerade mal drei Monate im Amt, musste der Ire als EU-Kommissar für Demokratie, Justiz und Verbraucherschutz inmitten der transatlantischen Krise in die Höhle des Löwen reisen. Er traf sich in Washington, D.C. mit US-Tech-Lobbyisten, darunter diejenigen von Meta, Apple und Amazon. Viel sei es um die Datenschutz-Grundverordnung (DSGVO) gegangen, ließ er durchblicken. Es dürften keine angenehmen Gespräche gewesen sein.

Im März 2025 kam McGrath außerdem mit Beth Williams zusammen, „einem Mitglied“ des Privacy and Civil Liberties Oversight Board (PCLOB), schrieb er auf X. Man habe das „volle Engagement für die Umsetzung des EU-US-Datenschutzrahmens“ erörtert. Dieses Statement geriet unfreiwillig komisch, denn was McGrath seinen Followern vorenthielt, ist, dass Williams derzeit als einziges Mitglied des Boards fungiert. Alle anderen hatte US-Präsident Donald Trump bereits Ende Januar fristlos gefeuert, weil sie der demokratischen Partei angehören.

Das angeblich unabhängige PCLOB ist damit momentan (zum Redaktionsschluss Ende Juli 2025) nicht handlungs- und beschlussfähig. Genau das verunsichert viele europäische Unternehmen sehr,

die Daten in US-Clouds speichern und verarbeiten. Ihnen könnte Trump mit seinem Handeln und einer Unterschrift die Rechtsgrundlage für ihre Datentransfers entziehen.

Diese Grundlage beruht auf einem sogenannten Angemessenheitsbeschluss, den die EU-Kommission im Juli 2023 gemäß Art. 45 DSGVO verabschiedet hat. Darin bestätigt sie, dass die USA als „Drittland" ein der DSGVO vergleichbares Datenschutzniveau bietet und Transfers personenbezogener Daten in US-Clouds rechtlich okay sind. Die einzige Bedingung: Das verarbeitende US-Unternehmen muss sich dem „EU-US Trans-Atlantic Data Privacy Framework" (TADPF) unterwerfen und jährlich hierzu selbst zertifizieren.

Heilende Biden-Verordnung

Dem Angemessenheitsbeschluss vorausgegangen waren lange Verhandlungen der EU-Kommission mit der US-Regierung unter dem Präsidenten Joe Biden. Dieser musste sicherstellen, dass der Zugriff auf Daten von EU-Bürgern durch US-Behörden auf das „Notwendige" und „Verhältnismäßige" eingeschränkt wird. Bereits zweimal waren zuvor derartige Zusicherungen gescheitert, weshalb auch die zwei vorherigen Angemessenheitsbeschlüsse der EU-Kommission („Safe Harbour" und „Privacy Shield") durch Klagen des österreichischen Datenschutzaktivisten Max Schrems vom Europäischen Gerichtshof (EuGH) gekippt wurden.

Im Oktober 2022 etablierte Joe Biden deshalb ein neues Regime: Er rief das oben erwähnte Gremium PCLOB ins Leben. Es soll das Verhalten von US-Geheimdiensten daraufhin überwachen, dass es dem EU-Datenschutzniveau nicht zuwiderläuft. Ein Civil Liberties Protection Officer (CLPO) soll intern die Aktivitäten der US-Inlandsgeheimdienste überwachen und Beschwerden von EU-Bürgern annehmen. Außerdem erfand die Biden-Regierung den „Data Protection Review Court" (DPRC), der diese Beschwerden unabhängig in zweiter Instanz prüfen soll. Dass dieses Pseudogericht tatsächlich unabhängig agiert, ziehen Bürgerrechtler allerdings seit dessen Bestehen in Zweifel.

Was sie aber – an vorderster Front Max Schrems – vor allem kritisieren, ist die Form, in der Biden damals seine Zusicherungen gab. Der US-Präsident änderte keine Gesetze, sondern erließ lediglich eine Verordnung, also eine der mittlerweile berüchtigten Executive Orders (EO), die von seinem Nachfolger von einem Tag auf den anderen gekippt werden können. EO 14086 definiert viele Mechanismen, auf denen der EU-Angemessenheitsbeschluss fußt. Mit der Quasi-Ausschaltung des PCLOB hat Trump nun den ersten Fuß abgesägt. Wahrscheinlich ist, dass

Bild: EU-Kommission

EU-Kommissar Michael McGrath (rechts) traf sich Mitte März in Washington, D.C. mit Beth Williams, dem letzten verbliebenen Mitglied des Privacy and Civil Liberties Oversight Board (PCLOB).

er noch in der ersten Jahreshälfte die gesamte EO 14086 annulliert.

Kein Plan B in Sicht

Auf dieses Worst-Case-Szenario scheint die EU-Kommission nicht vorbereitet zu sein. De facto entfiele mit EO 14086 die Grundlage für den Angemessenheitsbeschluss, er müsste ebenfalls umgehend fallen. Das EU-Parlament, genauer gesagt der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE), will die Kommission dahin bringen, den Beschluss zumindest infrage zu stellen.

Was hätte es für konkrete Folgen, wenn der auf dem TADPF beruhende Angemessenheitsbeschluss wegfiele? Sowohl EU-Unternehmen als auch US-Konzerne, die auf dessen Basis Daten von EU-Bürgern von ihrer EU-Niederlassung in die USA transferieren, könnten sich nicht mehr darauf berufen. Dies beträfe also auch Meta, Google, Amazon, Apple, Microsoft und X. Sie müssten wie zuletzt vor dem TADPF die Transfers rechtlich wieder auf die wackeligen sogenannten Standardvertragsklauseln zwischen Verantwortlichem und Auftragnehmer (aus der Not reformierte Musterverträge der EU-Kommission) nach Art. 46 DSGVO stützen, inklusive jeder Menge Compliance-Aufwand und Unsicherheiten.

Allerdings sei erwähnt, dass EU-Datenschutz-Aufsichtsbehörden deren Einsatz niemals ernsthaft kritisiert haben. In Deutschland ist keine einzige Anordnung oder ernsthafte Sanktion einzig aufgrund illegaler US-Datentransfers bekannt, seitdem die DSGVO im Mai 2018 wirksam geworden war. Behörden und Unternehmen müssen folglich eher damit rechnen, dass es unbequemer wird, als dass es ihnen in näherer Zukunft ernsthaft an den Kragen geht.

All diese Probleme existieren, weil US-amerikanische Gesetze sowohl den Geheimdiensten als auch Strafverfolgungsbehörden Zugriff auf personenbezogene Daten ohne ausreichende Widerspruchsmöglichkeiten gewähren. Dies macht es für die EU so kompliziert, den Transfer dieser Daten auf US-Server zu legitimieren, selbst wenn diese auf EU-Gebiet stehen.

Behördenermächtigungen

Konkret geht es um den Electronic Communications Privacy Act (ECPA) aus dem Jahr 1986 und den Foreign Intelligence Surveillance Act (FISA) aus dem Jahr 1978. Der FISA ermächtigt US-Nachrichtendienste ohne individuelle Genehmigung einer Maßnahme, Telekommunikation im Ausland abzuschnorcheln sowie Personen zu überwachen, die in den USA wohnen. Dies geschieht insbesondere bei US-Tech-Unternehmen, wie spätestens die Snowden-Enthüllungen offenbart haben. Sie zeigten, dass Daten von EU-Bürgern, die auf US-Servern gespeichert sind, jederzeit im Zugriff von US-Behörden liegen.

Einen Teil des ECPA stellt der Stored Communications Act (SCA) dar. Um diesen gab es während der ersten Trump-Regierung 2017 Streit, weil Microsoft sich geweigert hatte, auf SCA-Grundlage in Irland gespeicherte Daten von EU-Bürgern an US-amerikanische Strafverfolgungsbehörden herauszugeben. In der Folge ergänzte die Trump-Regierung 2018 den SCA um den Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Er bestimmt seitdem, dass US-Cloudanbieter personenbezogene Daten auch dann herausgeben müssen, wenn sich diese außerhalb des US-Territoriums befinden, also beispielsweise auf Microsoft-Servern in der EU.

Von den Gesetzen machen die US-Behörden umfangreich Gebrauch, wie die Transparenzreports der US-Konzerne belegen. Deshalb gleicht es für die EU-Kommission der Quadratur des Kreises, eine DSGVO-konforme Angemessenheit zu bescheinigen, obwohl sie eindeutig nicht existiert. Da hilft eigentlich weder eine Selbstzertifizierung der Anbieter noch eine aus der Not geborene Beschwerdeinstanz wie der PCLOB.

De facto gingen die rechtlichen Maßnahmen stets an der Realität vorbei. Sie sollen den Datentransfer ermöglichen, weil daran viele Milliarden US-Dollar Umsatz der Tech-Branche hängen. Auf der Strecke bleibt die Glaubwürdigkeit. Denn in Wahrheit wissen auch alle Juristen, die sich mit der Thematik befassen, dass tatsächlicher Zugriffsschutz von EU-Daten in den USA nur mit Ende-zu-Ende-Verschlüsselung möglich ist. Diese würde aber verhindern, dass die Daten in den Clouds verarbeitet werden. Sie würde Projekte verteuern und außerdem dem Interesse der Konzerne zuwiderlaufen, die mit der Auswertung der Daten Geld verdienen.

Automatisierte Inhaltekontrolle

Doch nicht nur wegen des Profits drückt man seitens der EU mindestens ein Auge zu: Clouddienste, die personenbezogene Daten von Konsumenten speichern, sollen sogar ausdrücklich diese Inhalte einsehen und überprüfen. Es geht um verbotenes Material, vornehmlich Bilder und Videos, und hier ins-

besondere um Darstellungen von Kindesmissbrauch (Child Sexual Abuse Material, CSAM). Anbieter wie Meta, Microsoft und Google scannen abgelegte Inhalte wie Mails und Fotos automatisiert und schlagen Alarm, wenn sie vermeintlich oder tatsächlich fündig werden.

Sie alle kooperieren dazu mit dem US-amerikanischen National Center for Missing & Exploited Children (NCMEC), an das sie ihre Funde inklusive Angaben zum Datenbesitzer weiterleiten. Das NCMEC erhielt den jüngsten veröffentlichten Zahlen zufolge allein 2023 36,2 Millionen derartige Hinweise von Providern. Mit fast 29 Millionen (Facebook, Instagram und WhatsApp) liegt Meta ganz vorn, Google gab rund 1,5 Millionen Hinweise, Microsoft immerhin noch knapp 140.000.

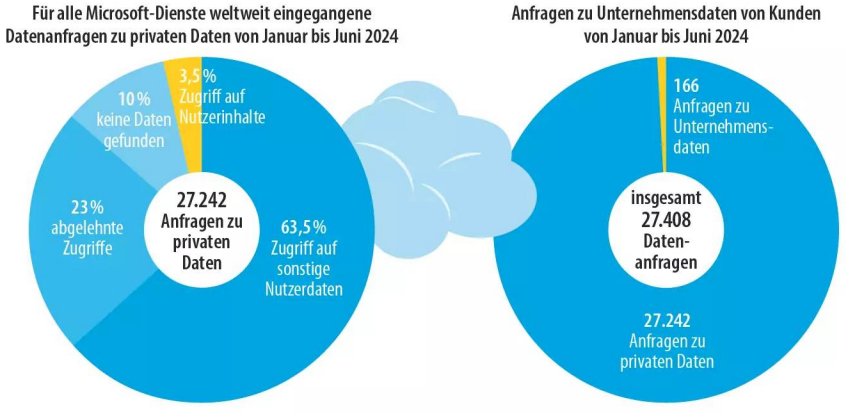
Wie die automatisierten Inhalte-Scans funktionieren und welche Techniken zum Einsatz kommen, haben wir ausführlich in c't 2/2022 geschildert [1]. Damals berichteten wir außerdem beispielhaft über den Fall eines Microsoft-Kunden, der wegen eines falsch positiven Treffers ins Visier von Microsoft und der Strafverfolgung geriet und sein Konto inklusive bezahlter Inhalte für immer verlor. Viele derartige Fälle sind bislang nicht bekannt, allerdings bedeuten sie im Einzelfall viel Ärger, bis hin zur Zerstörung der Existenz.

Diese Kollateralschäden geschehen, weil die persönlichen Kundendaten entweder gar nicht oder nur mit einem Generalschlüssel vor Zugriff geschützt werden. Das ist zwar generell so gar nicht im Sinne der DSGVO, doch die EU-Kommission hat sich hierfür eine Ausnahme von den Datenschutzregeln ausgedacht. Um CSAM-Material auf ihren Servern aufzuspüren, dürfen alle Cloudanbieter, auch die europäischen, freiwillig automatisiert die Inhalte der Nutzer durchsuchen. Dies besagt eine vorübergehende EU-Verordnung (2024/1307).

Allerdings läuft diese Verordnung 2026 aus. Es besteht also Handlungsbedarf. Derzeit will ein Teil der Mitgliedsstaaten sie entfristen und dahingehend verschärfen, dass Provider verpflichtend sogar in verschlüsselte Inhalte schauen müssen. Dieses strittige Vorhaben läuft unter dem verkürzenden Begriff „Chatkontrolle“. Wie sich die neue deutsche Bundesregierung zu dem Vorhaben positioniert, war bis zum Redaktionsschluss dieser Ausgabe

Behördenzugriffe auf die Microsoft-Cloud

Laut Microsoft gab es im ersten Halbjahr 2024 weltweit rund 27.000 versuchte Abfragen von Privatkundendaten bei Clouddiensten wie Outlook.com und OneDrive. MS-365-Unternehmensdaten stehen offensichtlich weniger im Fokus der Strafermittler.



Quelle: Microsoft

noch unklar. Fest steht, dass die neue dänische Ratspräsidentschaft es in der zweiten Jahreshälfte 2025 vorantreiben will.

Löchrige EU-Datengrenze

Derweil wird sich die EU noch mit dem eigentlichen Elefanten im Raum beschäftigen müssen. Microsoft ist mit seinen vielen Services rund um das Cloud-Paket Microsoft 365 zu einem faktisch unverzichtbaren Bestandteil europäischer Kommunikationsinfrastruktur geworden. Nähme man deutschen Unternehmen und Behörden diese Infrastruktur von einem Tag auf den anderen weg – die Gefahr wäre groß, dass der Staat in einen Blackout steuert.

Dabei haben inzwischen viele Aufsichtsbehörden bestätigt, dass der Einsatz von Microsoft 365 in der EU kaum DSGVO-konform möglich ist. Zum einen reichen die Zusicherungen des Konzerns nicht, zum anderen liegen viele Kundendaten nun einmal auf Servern im US-Zugriff. Im Dauerkonflikt mit den EU-Datenschutzbehörden versucht der Konzern aus Redmond permanent, die Wogen zu glätten.

Am 27. Februar verkündete Microsoft, sein mehrjähriges Projekt der „EU-Datengrenze“ (EU Boundary) für die Cloud abgeschlossen zu haben. EU-Kunden „aus dem privatwirtschaftlichen und öffentlichen Sektor können ihre Kundendaten und pseudonymisierten personenbezogenen Daten für die zentralen Cloud-Dienste von Microsoft – einschließlich Microsoft 365, Dynamics 365, Power Platform und der meisten Azure-Dienste – innerhalb der EU- und EFTA-Regionen speichern und verarbeiten“. Auch vom CLOUD Act sollen diese Daten verschont sein.

Kritiker monieren, dass die Datengrenze bislang löchrig und damit unwirksam sei. In der Tat gestattet sich Microsoft USA selbst „Remotezugriff auf in der EU-Datengrenze gespeicherte und verarbeitete Daten“ in Einzelfällen. „Wenn eine solche Datenübertragung erforderlich ist, verwendet Microsoft die modernste Verschlüsselung, um Kundendaten, pseudonymisierte personenbezogene Daten und Professional Services-Daten im Ruhezustand und während der Übertragung zu schützen“, heißt es in einem Blogbeitrag.

Man könnte nun einwenden, dass Microsoft auf das lukrative Cloud-Business mit Unternehmen in der EU angewiesen ist und einen Teufel tun wird, Kundendaten an US-Behörden herauszugeben und damit Vertrauen zu zerstören. Dieser Einwand beruht aber auf der Annahme, dass sich die Gesetze in den USA nicht verändern sowie dass Unternehmen, Regierung und Justiz sich stets an geltendes Recht halten. Nichts davon beschreibt die Situation, die im Frühjahr 2025 in den Vereinigten Staaten vorliegt. (hob) c't

Literatur

[1] Ludwig Gundermann, Andrea Trinkwalder, Zwischen Schutz und Überwachung, Wie Content-Scanner im Netz nach Missbrauchsbildern fahnden, c't 2/2022, S. 50

Tipps zum Verlassen der Trump-Zone

Rund um den europäischen Exodus aus den US-Clouds stellen sich viele Fragen, angefangen beim Sinn der Aktion und ihrer praktischen Machbarkeit bis zu Alternativen für einzelne Dienste. Wir liefern einige häufig erbetene Antworten.

Von **Peter Siering**

In der Falle?

? Wie erkenne ich denn eindeutig, dass ein Gerät oder Dienst die US-Cloud verwendet?

! Oft hilft ein wenig Detektivarbeit: Finden Sie heraus, welche DNS-Anfragen beim Benutzen anfallen, zum Beispiel über einen DNS-Filter wie Pi-hole. Wenn Sie keine Möglichkeit haben, in den Netzwerkverkehr zu schauen, hilft vielleicht eine alternative Quelle: Wenn es für das Gerät Plug-ins oder Erweiterungen für gängige Smart-Home-Lösungen auf Open-Source-Basis gibt, liefert die vielleicht Hinweise, etwa die Anpassung für Ihr E-Auto in Home Assistant. Im Quelltext sollten Sie in den URLs Hostnamen finden, die Dienste ansprechen.

Aus den Namen können Sie die angesprochenen IP-Adressen ermitteln. Zum Beispiel über die Netzwerk-Tools auf heise online finden Sie für den Namen „www.myvolkswagen.net“ heraus, dass dieser zu einer Adresse bei Akamai aufgelöst wird. Das ist ein US-Anbieter für Clouddienste und DDoS-Schutz. Es ist sehr gängig, dass Unternehmen solche Dienstleister vor ihr Angebot spannen – oft bedeutet das auch, dass TLS-gesicherte Verbindungen dort aufgebrochen werden (können).

Oftmals führt die erste Namenabfrage nicht auf die richtige Fährte. Stecken Sie in einem zweiten Anlauf versuchsweise die für den Namen ermittelte IP-Adresse in eine Suche nach dem zugehörigen Hostnamen. Oft weist der auf den eigentlichen Betreiber hin. So finden Sie zum Beispiel heraus, dass die Hosts hinter „my.shelly.cloud“ auf Servern bei Google liegen: Die umgedrehte Suche liefert Hostnamen der Domain „googleusercontent.com“.

Wenn das Internet ohne US-Technik und -dienste nicht läuft, wozu der ganze Zinnober?

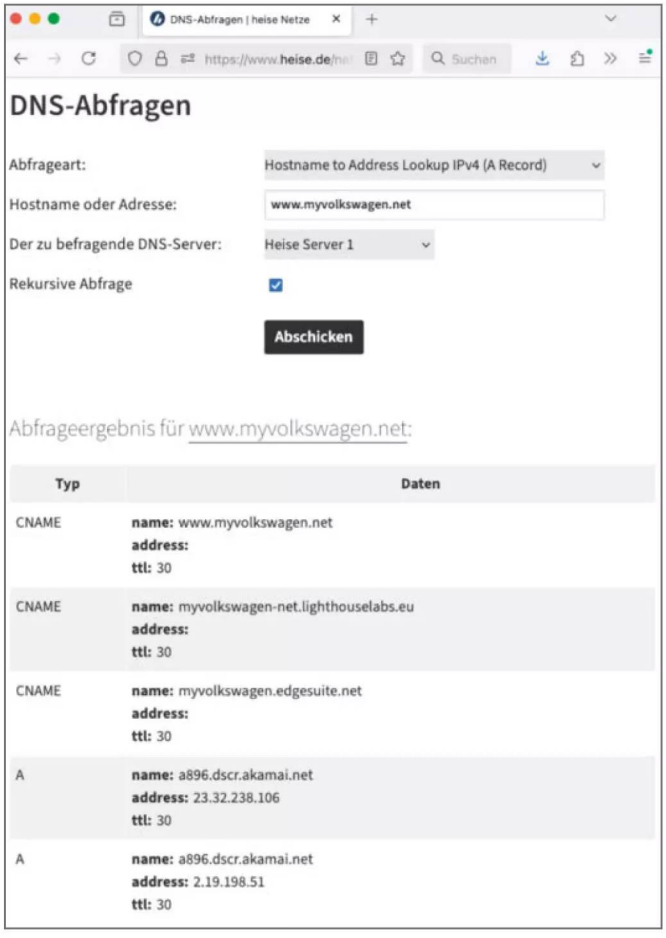
! In der Tat ist es Stand heute schwierig, vollständig auf US-Clouddienste und -Technik zu verzichten. Aber vieles geht eben doch gut ohne: Serverdienste für Groupware, Mail und Dateiaustausch lassen sich auf eigener, vor Ort betriebener Hardware (on-premises) verwenden, selbst wenn das Internet weg ist – es muss ja nicht unbedingt ein durchdrehender Präsident sein: Ein Bagger in der Nachbarschaft genügt schon.

Immer wieder lese ich, dass US-Cloudprovider für Unternehmen preislich und vom Funktionsumfang konkurrenzlos sind und die EU-Anbieter chancenlos sind. Wie realistisch ist es, Amazon, Google und Microsoft wirklich den Rücken zu kehren?

! Der Mythos hält sich hartnäckig, aber gerade die großen Cloudprovider sind keineswegs die günstigsten. Wer für seine privaten Projekte, den Verein oder ein kleines oder mittelgroßes Unternehmen nach Speicherplatz und Mietservern sucht, kommt bei deutschen und europäischen Anbietern oft viel günstiger weg. Ganz nebenbei erspart man

sich bei der Konfiguration viel Arbeit, weil die Oberflächen nach unserer Erfahrung deutlich aufgeräumter sind als die von Azure & Co.

Schwierig wird der Umzug, wenn man auf spezialisierte APIs angewiesen ist, die die Cloudprovider ebenfalls anbieten – zum Beispiel für künstliche Intelligenz, Spracherkennung oder Übersetzung. Auch für solche gibt es EU-Anbieter, aber der Umzug ist immer mit Programmieraufwand verbunden. Generell ist es stets eine Überlegung wert, nicht vorgefertigte Dienste einzukaufen, sondern lieber ganze Server zu mieten. So können Sie die Pauschalangebote für Datenvolumina, oft Flatrates, mitnehmen, statt für jedes GByte teuer blechen zu müssen.



Eine simple Möglichkeit, um herauszufinden, ob ein Gerät oder Dienst auf US-Clouds angewiesen ist, stellen DNS-Anfragen dar. Erst ermittelt man die IP-Adresse des benutzten Servers und lässt dann die für diese Adresse hinterlegten Namen feststellen. Der Name ist oft nicht identisch und mitunter ein Hinweis auf gängige Cloudserver bei Amazon, Google oder Microsoft.

Eigener Server

? Für das Selbsthosting fehlt mir technischer Background, obendrein ist es mir zu viel Verantwortung, gibt es das auch als betreutes Wohnen?

! Für nahezu jede Alternative zu US-Clouddiensten finden Sie Anbieter, die Ihnen das Hosting abnehmen. Die Produkte rangieren dabei vom nackten Rohbau, etwa einem realen oder virtuellen Server für wenige Euro, bis hin zur vollständig eingerichteten Villa mit Butler, der Updates einspielt und Backups zieht. Je mehr im Paket ist, desto weiter müssen Sie die Börse öffnen.

Eine Empfehlung für den Anbieter ist schwierig: Wenn Sie heute schon eine eigene Domain besitzen und zufrieden sind, schauen Sie am einfachsten, was der bisherige Dienstleister im Portfolio hat. Anbieter von Webspace liefern oft Konfigurationsassistenten für die gängigen Anwendungen wie Nextcloud, WordPress und so weiter. Auf diese Weise installierte Dienste erhalten meist auch automatisiert Updates.

Es gibt auch Hoster und kleinere Systemhäuser, die gängige Anwendungspakete über eine Weboberfläche auf Containerbasis gegen Entgelt bereitstellen. Die finden Sie am einfachsten über Empfehlungen im Umfeld der Software, für die Sie Hostingmöglichkeiten suchen. Constantin Grafs Website zur Suche nach europäischen Alternativen liefert auch eine Liste von Hosting-Anbietern (Link via ct.de/w34u).

Solche Listen bergen mitunter Überraschungen, so nennt Nextcloud die Telekom als Partner. Bei genauerem Hinsehen stellt sich heraus: Jeder Telekom-Kunde hat schon eine kleine Nextcloud-Instanz im Paket, die ist zwar rosa statt blau und erlaubt nur Grundfunktionen. Doch vielleicht genügt das schon? Ähnliches erlebt man auch bei Mailprovidern, so nutzt mailbox.org für seine Dienste Open-Xchange. Genügt fürs Selbsthosting ein Raspi daheim oder muss ich irgendwo einen Server mieten?

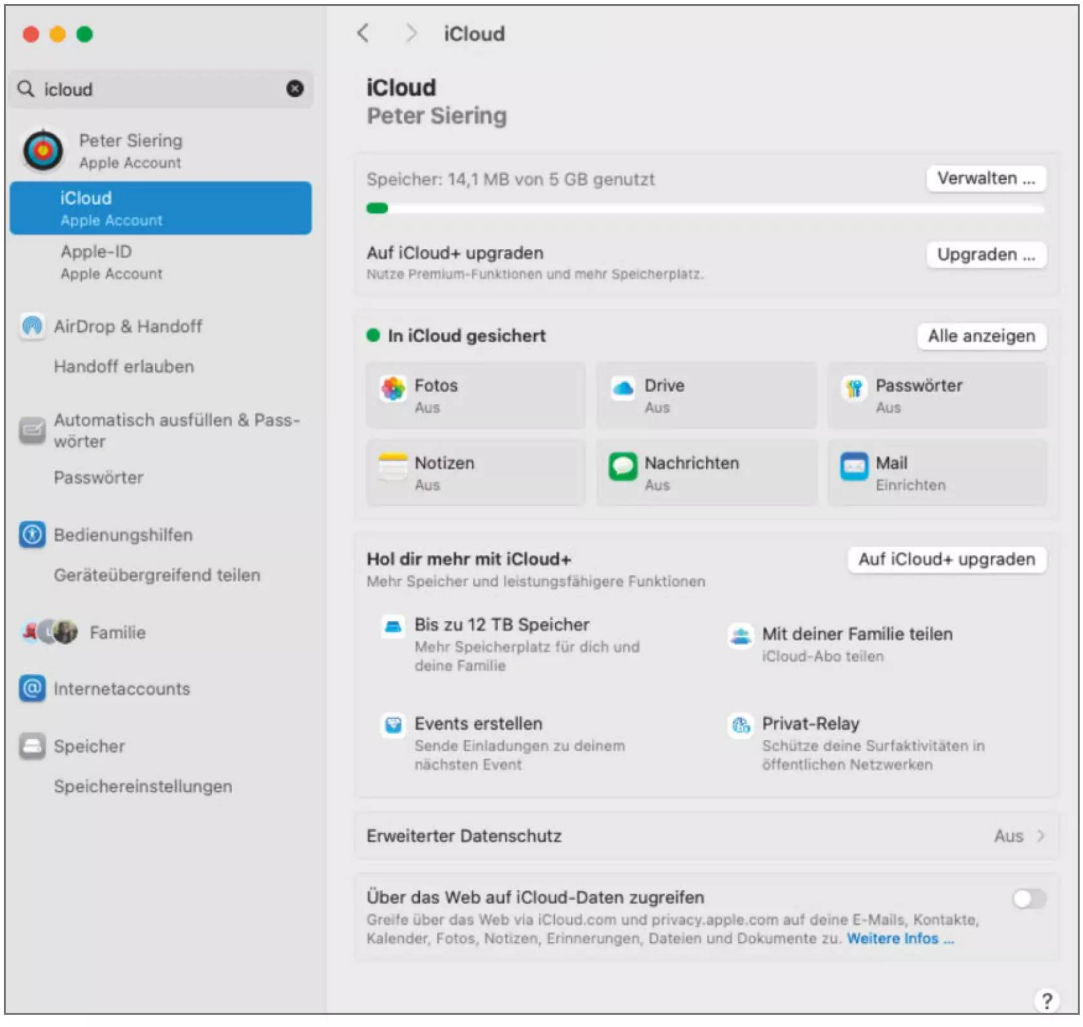
! Das kommt sehr darauf an, was Sie vorhaben. Für kleinere Aufgaben ist ein Raspi ausreichend. Wenn Sie einen ganzen Verein mit vielen Mitgliedern beglücken wollen, sollten Sie besser auf einen (virtuellen) Server bei einem Hoster zurückgreifen.

Das erleichtert im Vorfeld einiges: Sie müssen sich nicht mit Portweiterleitungen im Router herumschlagen, kriegen üblicherweise auch gleich eine Domain im Paket und müssen sich nicht mit irgendwelchen dynamischen DNS-Diensten befassen. Obendrein bremsen Zugriffe von außen den heimischen Internetanschluss dann nicht aus.

Ferner läuft so ein virtueller Server, der monatlich nur wenige Euro kostet, meist deutlich zuverlässiger. Er ist tendenziell nicht von Staubsaugern, fliegenden Sicherungen und versterbenden SD-Karten bedroht. Andererseits legen Sie dabei Ihre Daten auf fremde Festplatten. Wenn Sie vermeiden wollen, dass eventuelle Nachmieter noch Daten finden, empfiehlt es sich, die Datenpartition der physischen Datenträger eines Mietservers zu verschlüsseln. Profis hinterlassen den zum Entsperren nötigen Schlüssel nicht auf dem Server.

Messenger

? Ich habe Signal in der Aufstellung der Alternativen für Messenger-Dienste vermisst. Warum fehlt es?



Apple-Nutzer können in den Systemeinstellungen die meisten iCloud-Dienste abdrehen. Dort erkennen sie auch auf den ersten Blick, welche Daten dort schon gelandet sind. Ganz ohne iCloud lassen sich Apple-Geräte aber nicht sinnvoll verwenden.

Wir haben abwägen müssen, was wir empfehlen und was nicht. Die Signal-Foundation, die Apps und Protokoll entwickelt, hat ihren Sitz in den USA. Damit unterliegt sie der dortigen Gesetzgebung. Der Dienst baut auf Servern auf, die in den großen US-Clouds stehen oder deren Dienste nutzen – hier hat eine durchdrehende Regierung einen starken Hebel, um den Dienst außer Betrieb zu nehmen.

Der Betrieb eigener Server ist zwar technisch möglich, aber erlaubt nur den Aufbau eines geschlossenen Systems und keinen Austausch mit der jetzigen Signal-Nutzergemeinde. Das sprach für uns gegen eine Nennung als Alternative zu US-Diensten. Signals Software und Technik ist von vielen kompetenten Stellen geprüft und für sicher befunden worden. Viele Regierungsorganisationen empfehlen Signal unter anderem deswegen. Auch Journalisten schätzen den Messenger für vertrauliche Kommunikation.

Wie komme ich bei WhatsApp raus, wenn es doch für viele heute so selbstverständlich wie ein Anruf ist?

Ein guter Anfang wäre es, den Dienst nur noch für die Kommunikation zu nutzen, die sonst abreißen würde, etwa für die Kindergarten-, Haus- oder Vereinsgruppen. Der Tipp, auf ein WhatsApp-Business-Konto auszuweichen, das mit einer Festnetznummer funktioniert und nur noch mit einem speziellen Gerät, etwa einem Alt-Handy verwendet wird, scheint langfristig nicht praktikabel – obwohl dies im Netz immer wieder empfohlen wird. Vollnerds können in ihrem eigenen Chatserver eine Brücke zu WhatsApp einbauen.

Liste europäischer Hoster
ct.de/w34u

Apple ohne iCloud

Welche Optionen habe ich als Apple-Nutzer, ohne iCloud zurechtzukommen?

Sie können beim Konfigurieren eines macOS- oder iOS-Geräts hartnäckig vermeiden, eine Apple-ID anzugeben. Ganz ohne geht es langfristig dennoch nicht: Für den Bezug von Apps aus dem Apple-Store braucht es die ID und auch für Updates in macOS, wenn deren Installation mit Komfort ablaufen soll. Ansonsten erlaubt Apple es aber, die Nutzung der iCloud-Dienste weitgehend auszuschlagen. Ob das gelungen ist, können Sie jederzeit in den Systemeinstellungen überprüfen.

Der Verzicht bedeutet nicht, dass ein Apple-Gerät dadurch unbenutzbar wird. Die Anwendungen für Kalender und Adressbücher sprechen die offenen Protokolle CalDAV und CardDAV. So können Sie zum Beispiel die Daten vieler Groupware-Server komfortabel mit den Apple-Anwendungen nutzen. Das Gleiche gilt auch für die Mail-Anwendung, die via IMAP4 und SMTP mit allen gängigen Mailanbietern zusammenarbeitet.

Apples iOS-Apps sprechen darüber hinaus ActiveSync für den Zugriff auf Mail, Kalender und Adressbuch. Das ist eine ältere und oft in Groupware-Lösungen vorgesehene Protokollspielart, die Microsoft für Exchange geschaffen hat. Der Vorteil: Geräte müssen Änderungen nicht aktiv abfragen, sondern erhalten sie per Push. macOS spricht nicht ActiveSync, sondern verwendet Exchange Web Services (EWS) als Zugriffsprotokoll. (ps) c't

Bild: KI, Collage c't

Schleswig-Holstein will wechseln

Während viele Bundesländer weiter auf den Softwareriesen Microsoft setzen und sogar trotz aller Bedenken dessen Cloud nutzen wollen, schlägt Schleswig-Holstein einen eigenen Weg ein. LibreOffice, Open-Xchange und Nextcloud sollen im Norden Kosten senken und Unabhängigkeit garantieren. Eine Bestandsaufnahme vor Ort.

Von **Keywan Tonekaboni und Christian Wölbert**

Spätestens seit der ersten Amtszeit von US-Präsident Trump geistert der Begriff „Digitale Souveränität“ durch die Debatten. Obwohl bekannt ist, in welchem hohen Maß die öffentliche Verwaltung in Deutschland von Microsofts Produkten abhängig ist, passiert kaum etwas, um diesen Umstand zu ändern. Mehrere Bundesländer wie etwa Bayern planen, die Public-Cloud-Dienste von Microsoft zu nutzen, trotz Bedenken nicht nur von Datenschützern. Hinzu kommen die hohen Kosten. Im Jahr 2023 blätterte der Bund fast 200 Millionen Euro allein für Microsoft-Lizenzen hin. Und die diskutierte

Alternative Delos Cloud, für die im vergangenen Sommer Noch-Bundeskanzler Olaf Scholz warb, ist nicht nur noch teurer, sondern zudem lediglich ein von SAP bereitgestelltes Angebot von Microsofts Clouddiensten.

Nicht so Schleswig-Holstein. Das kleine Bundesland aus dem Norden verfolgt seit Jahren einen Sonderweg – und die hohen Lizenzkosten sind einer der Gründe. In einem ersten Schritt soll LibreOffice in der Landesverwaltung Microsoft Office ablösen. Gleichzeitig ist der Wechsel von Exchange zur freien Alternative Open-Xchange geplant. Und am Ende des Weges ist gar der Umstieg von Windows auf Linux anvisiert.

Diese Open-Source-Strategie verkündete der damalige Umwelt- und Digitalminister Jan Philipp Albrecht (Grüne) im Jahr 2020 [1]. Mittlerweile ist die Staatskanzlei für das Thema Digitalisierung zuständig. Dort treibt nun der CDU-Minister Dirk Schrödter den Umstieg voran (siehe Kasten auf S. 42 f.). Mit einem Kabinettsbeschluss im April 2024 leitete die Kieler Landesregierung einen schrittweisen Wechsel ein.

Plus eins für Open Source

Der Plan für den digital souveränen IT-Arbeitsplatz in der Landesverwaltung sieht sechs „Säulen“ vor, welche die Landesregierung mit unterschiedlichen Geschwindigkeiten abarbeiten will:

- Umstieg auf LibreOffice
- Wechsel von Exchange/Outlook zu Open-Xchange/Thunderbird sowie von Sharepoint zu Nextcloud
- Umstieg auf Linux
- Ablösung von Microsoft Active Directory durch Univention Corporate Server (UCS)
- Prüfung der Interoperabilität spezieller Verwaltungsprogramme mit LibreOffice und Linux (Bestandsaufnahme Fachverfahren)
- Open-Source-Telefonie-Lösung

Viele dieser Projekte sind derzeit in der Vorbereitungs- oder Pilotphase. Fortgeschritten ist hingegen die Umstellung der Office-Software: LibreOffice ist laut Landesregierung bereits auf allen knapp 30.000 IT-Arbeitsplätzen der Verwaltung installiert. Bis Oktober 2025 sollen 70 Prozent dieser IT-Arbeitsplätze dann Microsoft Office los sein. Denn zu diesem Zeitpunkt laufen die aktuell genutzten Microsoft-Office-Lizenzen aus und Kiel will möglichst wenige davon verlängern. Damit fällt auch Outlook weg, weswegen seit vergangenem Jahr gut 2500 Postfächer pro Woche von Microsofts Groupware- und Mailserver zu Open-Xchange migriert werden. Der Parallelbetrieb von Exchange und Open-Xchange soll ebenfalls bis Oktober 2025 enden. Als Outlook-Ersatz für Mails, Kalender und Kontakte gibt es die Open-Xchange-Weboberfläche und den E-Mail-Client Thunderbird.

Einen hundertprozentigen Umstieg zu LibreOffice strebt die Landesregierung zunächst nicht an, sie wird also auch nach Oktober zumindest in einzelnen Behörden oder Abteilungen Microsoft Office nutzen.

Minister Schrödter begründet das vor allem mit zwei Herausforderungen: Erstens gebe es Bereiche, deren spezielle Verwaltungssoftware („Fachverfahren“) aktuell nur mit Microsoft-Anwendungen wie Word zusammenspielen. Ein Beispiel ist etwa, wenn ein Sachbearbeiter ein Antwortschreiben verfassen will, wozu das Fachverfahren aus dem Datensatz eine Vorlage für das Office-Programm erzeugt. „Da müssen wir mit den Herstellern der Fachverfahren sprechen und das tun wir auch“, sagt Schrödter. In manchen Fällen enthielten die Anwendungen bereits Schnittstellen für LibreOffice, diese müssten nur aktiviert werden. In anderen Fällen müssten sie erst noch entwickelt werden.

Schrödter glaubt, dass die Unternehmen solche Extrawünsche nicht einfach aussitzen werden. „Die Digitalministerkonferenz hat beschlossen, dass das Open-Document-Format künftig bundesweit das Standardformat ist. Wer die Zeichen der Zeit erkennt, wird sehr schnell darauf reagieren.“ In manchen Fällen entwickelt Schleswig-Holstein die Fachverfahren auch gemeinsam mit anderen Bundesländern und muss sich mit diesen verständigen. „Da sind wir im Dialog und ich bin mir sicher, dass alle Länder früher oder später die Zeichen der Zeit erkennen“, sagt Schrödter. „Es ist schon viel Bewegung zu erkennen.“

Und zweitens gebe es Behörden und Abteilungen, die intensiv mit externen Stellen kommunizieren, die nicht mit bestimmten Dokumenten im Open-Document-Format umgehen können. In der Praxis hapert es laut Sven Thomsen, Chief Information Officer (CIO) von Schleswig-Holstein, vor allem bei älteren Dokumenten, etwa wenn sie von Word 95 zu Office Open XML (DOCX) konvertiert wurden oder wo andere Software fehlerhaft eingebettete Objekte (OLE) in der Office-Datei gespeichert hat. Mit den LibreOffice-Entwicklern arbeite man zusammen, um diese Problemfälle zu analysieren und zu beheben. „Zwar ist nicht alles reibungsfrei, aber die normale

Zusammenarbeit zwischen Microsoft-Office-Anwendern und jenen, die LibreOffice verwenden, ist grundsätzlich gut machbar“, betont Thomsen. Die Staatskanzlei nutze schon länger LibreOffice und habe meistens keine Probleme beim Austausch. Zentral bereitgestellte Vorlagen seien schon umgestellt. Für von Nutzern individuell erstellte Vorlagen gibt es einen Migrationsservice, der die Dateien überarbeitet.

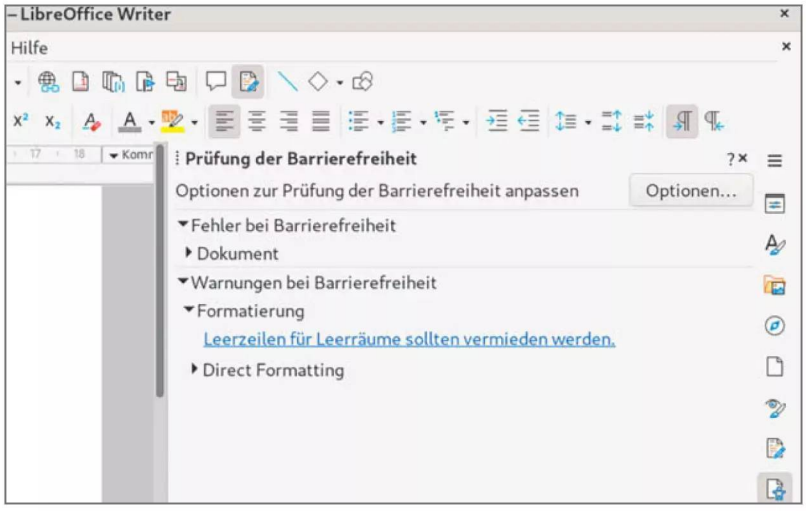
Manchmal ist die Inkompatibilität sogar ein Segen, zumindest aus Sicherheitsgründen. „Wenn mit Visual Basic Script in Excel programmiert wurde, sind wir verloren“, sagt CIO Thomsen, um gleich zu ergänzen: „Was aber grundsätzlich nicht schlimm ist, weil das ohnehin aufhören muss.“ Bei der Bestandsaufnahme kam aber auch zutage, dass einige Abteilungen die Datenbankverwaltungssoftware Microsoft Access einsetzen. Solche „Individualentwicklungen“ seien nicht gewünscht, erklärt Thomsen, insbesondere nicht für produktionskritische Prozesse und in proprietärer Software. Statt einer Access-ähnlichen Software würden die Daten in einer PostgreSQL-Datenbank neu aufgesetzt, mit einer Low-Code-Plattform als Bedienoberfläche.

Herausforderung Change Management

In den meisten Ministerien sei der Umstieg technisch problemlos, sagt Minister Schrödter: „Dort macht man im Wesentlichen Verwaltungsarbeit, die nicht immer mit dem Einsatz von Fachverfahren einhergehen.“ Herausfordernd sei aber auch dort das „Change Management“: „Die Menschen müssen sich auf die neuen Anwendungen einstellen.“ Die Landesregierung könne das von ihren Mitarbeitern aber durchaus erwarten, findet der Staatskanzlei-Chef. „In ihrem privaten Umfeld gehen sie auch mit technischen Neuerungen um.“ Wichtig sei es, die Motivation gut zu erklären. Zudem unterstütze man nicht nur durch Dokumentationen und Videos, sondern auch mit Schulungen vor Ort. „Wir haben inzwischen 250 Schulungen für jeweils 12 bis 15 Mitarbeitende durchgeführt“, betont Schrödter. „Außerdem stellen

Bild: Staatskanzlei Schleswig-Holstein

Der „digital souveräne IT-Arbeitsplatz“ umfasst sechs Teilbereiche, von Office über Telefonie bis zum Betriebssystem. Während der Umstieg auf LibreOffice im vollen Gang ist, gibt es für Linux noch keinen Termin.



Verbesserungen an Open-Source-Software, die Schleswig-Holstein in Auftrag gibt, wie der Barrierefreiheitsassistent in LibreOffice, sind für die Allgemeinheit verfügbar.

wir den Ressorts Einführungsmanagerinnen und -manager zur Seite".

Die Gewerkschaft Verdi berichtet hingegen, dass der Umstieg auf LibreOffice bei großen Behörden wie dem Landesbetrieb Straßenbau und Verkehr sowie dem Landesbetrieb Küstenschutz zu viel Unmut führe. Die Softwaremigration erhöhe die Arbeitsbelastung der Beschäftigten enorm, sagte Sabine Kaiser, Landesfachbereichsleiterin für öffentliche und private Dienstleistungen, im Gespräch mit c't. „In manchen Bereichen müssen Tabellen jetzt doppelt geführt werden, weil der Verzicht auf Excel noch nicht möglich ist." Außerdem reiche das Angebot an Schulungsplätzen bei weitem nicht aus, Beschäftigte würden bei Problemen häufig bloß auf Videos verwiesen. „Insgesamt lautet unser Eindruck, dass die Staatskanzlei das auf Biegen und Brechen durchzieht, ohne die Beschäftigten ausreichend mitzunehmen", sagte Kaiser. Die Beschäftigten sähen die Unabhängigkeit von Microsoft aber auch als sinnvolles Ziel an, „wenn es denn funktioniert".

Aus Sicht des Beamtenbunds dbb ist vor allem die Integration der Open-Source-Anwendungen in Fachverfahren eine große Herausforderung. „Wir befürchten durchaus, dass es Praxisprobleme geben wird, auch mit Blick auf den Zeitplan", sagte der Landesvorsitzende Kai Tellkamp auf Anfrage. Kritisch sieht der dbb zudem, dass Schleswig-Holstein einen Alleingang wagt und nicht auf eine „koordinierte Gesamtlösung" für alle Bundesländer setzt. „Insellösungen bedeuten gerade bei Digitalisierungsprojekten häufig Effizienzverluste", so Tellkamp. Grundsätzlich sei die digitale Souveränität aber ein „richtiges Ziel".

Der Widerstand in der Belegschaft war einer der Gründe, warum der Umstieg der Stadt München auf Linux so schnell rückabgewickelt wurde. In Schleswig-Holstein will man in der Kommunikation nicht den Wechsel von Microsoft zu Open Source in den Vordergrund stellen, sondern den Nutzen für die Anwender betonen. So wurde in der Landesverwaltung Microsoft Sharepoint bisher lediglich als schlichte Dateiablage genutzt. Abgelöst wird es durch Nextcloud samt Collabora Online Office, eine Variante von LibreOffice im Webbrowser, womit nun das gleichzeitige Bearbeiten von Dokumenten möglich ist. „Wir hatten das als kleines Feature gedacht", sagt CIO Thomsen. „Die Anwender sehen darin aber eine deutliche Erleichterung in der täglichen Arbeit." Die Umstellung auf Nextcloud ist nicht mit der Frist im Herbst 2025 verbunden, aber der Rollout läuft schon. Die Nextcloud sei absichtlich nicht nur auf die notwendigen Features reduziert, sondern offen gestaltet. Funktionen wie Formulare oder Kanban-Board (Deck) sind in der angebotenen Nextcloud-Instanz aktiv. Das soll Mitarbeitern die Freiheit geben, ihre Zusammenarbeit in unterschiedlichen Formen zu organisieren.

Keine neuen Abhängigkeiten

Die Umstellung koordiniert ein kleines Team in der Staatskanzlei. Mit der Umsetzung ist der IT-Dienstleister Dataport beauftragt, eine Anstalt öffentlichen Rechts, an der Schleswig-Holstein neben weiteren vorwiegend norddeutschen Bundesländern beteiligt ist. Zu Dataport hat das Land einen Großteil der IT-Tätigkeiten ausgelagert. Der Dienstleister betreibt die Serverinstanzen in einem geschlossenen Verwaltungsintranet. Das Projektteam arbeitet aber auch direkt mit den Herstellern zusammen, also etwa mit Open-Xchange oder Firmen aus dem LibreOffice-Umfeld, wenn es um fachliche Fragen geht. Für die betriebliche Umsetzung ist aber Dataport der Ansprechpartner und verantwortlich.

Das nördlichste Bundesland will Abhängigkeiten von Microsoft nicht ablösen durch neue Abhängigkeiten von anderen Anbietern. Bei der Auswahl neuer Software sei nicht nur wichtig, dass diese Open Source ist, sondern auch, dass es eine aktive

„Wenn mich ein Microsoft-Dokument erreicht, gebe ich es zurück“

Im Interview mit c’t erklärt Digitalisierungsminister Dirk Schrödter (CDU), warum die Landesregierung von Schleswig-Holstein von Microsoft auf Open-Source-Software wie LibreOffice und auf Linux umsteigt.

c’t: Herr Minister, Schleswig-Holstein ist das einzige Bundesland, das von Microsoft Office auf LibreOffice umsteigt. Sind Sie der Geisterfahrer oder sind es die anderen 15 Bundesländer?

Dirk Schrödter: Wir sind kein Geisterfahrer, sondern ein Pionier, der digitale Souveränität voranbringt. Es muss immer einen geben, der vorangeht. Und in dieser Rolle fühlen wir uns pudelwohl.

c’t: Der Umstieg auf Open-Source-Software war ursprünglich eine Forderung der Grünen, mit denen Sie in Schleswig-Holstein gemeinsam regieren. Wie haben die Grünen es geschafft, Sie zu überzeugen?

Schrödter: Bei unseren ersten Koalitionsverhandlungen 2017 stand die Frage der wirtschaftlichen Abhängigkeit von Softwareanbietern im Vordergrund. In den vergangenen Jahren hat sich dann gezeigt, dass wir auch aus strategischen Gründen digital unabhängiger werden müssen. Auch, weil wir gesehen haben, wie abhängig wir im Bereich der Energieversorgung waren und was das für einen Staat bedeutet. Digitale Souveränität ist aber mindestens so wichtig wie Energiesouveränität und deshalb ist es folgerichtig, den Weg zu gehen. Das ist dann auch wieder die DNA meiner CDU. Bei den Verhandlungen über den zweiten Koalitionsvertrag 2022 habe ich mich sehr intensiv mit diesen Fragen auseinandergesetzt und ich bin von unserem Weg persönlich überzeugt.

c’t: Was meinen Sie mit strategischen Gründen? Haben Sie ernsthaft die Sorge, dass Donald Trump Microsoft anweist, europäische Behörden lahmzulegen?

Schrödter: Wir müssen uns anhören, wie in den USA zum Beispiel über Grönland, den Panama-Kanal oder Kanada gesprochen wird. Die Datengesetzgebung der USA wirkt bereits jetzt extraterritorial auf die Daten, die in Europa verarbeitet werden. Und wir wissen nicht, wie in Zukunft damit umgegangen wird. Spätestens jetzt müssen wir daraus unsere Schlüsse ziehen. Das heißt, wir müssen Herr über unsere Datenhaltung sein und auf IT-Prozesse Einfluss nehmen können. Das erreichen wir nur, wenn wir uns aus Abhängigkeiten lösen durch offene Standards, den Einsatz von Open Source und eine vielfältige Anbieterlandschaft.

c’t: Sie haben sich das Ziel gesetzt, dass LibreOffice bis Oktober auf 70 Prozent der IT-Arbeitsplätze der Landesverwaltung die alleinige Office-Software ist. Arbeiten Sie selbst auch mit LibreOffice?

Schrödter: Ja, klar. Das ist für mich selbstverständlich und ich habe das von Anfang an gemacht. Als Führungskraft habe ich da auch eine besondere Verantwortung. Ich lebe unsere Beschlüsse. Und ich nehme grundsätzlich keine Vorlage mehr an, die nicht im Open-Document-Format gehalten ist. Wenn mich doch noch zufällig ein Microsoft-Dokument erreicht, gebe ich es zurück und sage, bitte einmal anders. Hier in der Staatskanzlei ist LibreOffice seit unserem Beschluss im letzten Jahr der Standard und wir werden nun Microsoft Office Schritt für Schritt deinstallieren.

Community in Europa gibt, sagt Thomsen. Das bedeutet, dass der Code nicht einzig von einem Hersteller stammt, sondern dieser auch offen dafür ist, dass andere Leute mit an der Software programmieren und Patches oder Zuarbeiten von diesen in den Upstream-Code aufgenommen werden. „Wir wollen immer Bestandteil einer größeren Community sein, was die Entwicklung, aber auch was die Nutzung angeht und deshalb keine isolierten Lösungen aufbauen“, betont Thomsen. Gerade im Umfeld von LibreOffice gibt es neben Collabora verschiedene weitere IT-Dienstleister. So hat das Land einen Auftrag vergeben, um die Barrierefreiheit von LibreOffice zu verbessern und den Barrierefreiheitsassistenten weiterzuentwickeln.

Da bleibt die Frage, warum das vom bundesweiten Zentrum für digitale Souveränität (ZenDiS) vorangetriebene Open-Source-Online-Office-Paket open-

c't: Wie sieht es in den anderen Ministerien und Landesbehörden aus? Können Sie diese notfalls anweisen, Microsoft Office zu deinstallieren?

Schrödter: Wir haben einen Kabinettsbeschluss und die Landesregierung setzt diese Beschlüsse um. Es gibt Bereiche, in denen der Umstieg schwieriger ist, zum Beispiel weil Microsoft Office tief mit speziellen Anwendungen der Verwaltung, den Fachverfahren, verwoben ist oder bei der länderübergreifenden Zusammenarbeit. Gerade die Verankerung von MS Office in Fachverfahren zeigt ja unsere Abhängigkeit, aus der wir uns befreien müssen. In den genannten Fällen brauchen wir möglicherweise einen etwas längeren Übergangszeitraum, deshalb das 70-Prozent-Ziel. Aber, ich denke, dieses Ziel werden wir bis Oktober erreichen. Dazu gehört auch der Umstieg von Microsoft Exchange und Outlook auf Open-Xchange und Thunderbird und von SharePoint auf Nextcloud.

c't: Mit welchen Kosten rechnen Sie für den Umstieg und wie viel sparen Sie auf der anderen Seite ein?

Schrödter: Obwohl unser Vorgehen auch wirtschaftlich ist, ist dies nicht der primäre Grund. Für uns steht unsere digitale Souveränität im Vordergrund. Aber klar, wir blenden Kostenfragen nicht aus. Für die nächsten zehn Jahre werden wir im Bereich der Office-Anwendungen Umstellungskosten von rund 6,5 Millionen Euro haben. Das liegt deutlich unter dem, was wir an Lizenzkosten hätten im selben Zeitraum. Der Umstieg ist also klar wirtschaftlich.

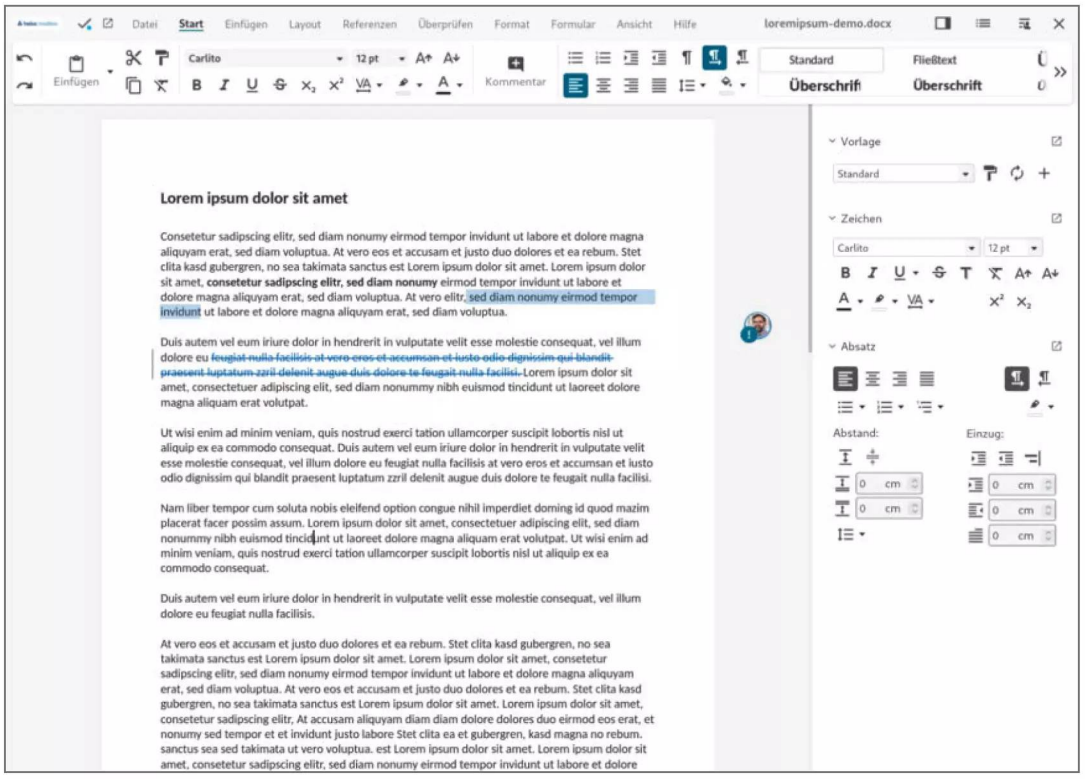
c't: Andere Bundesländer wie Bayern und Niedersachsen steigen von Microsofts klassischem On-Premise-Office auf Clouddienste wie Teams um und erhöhen damit die Abhängigkeit von Microsoft eher noch, statt sie zu verringern. Was sagen Sie Ihren Kollegen in diesen Bundesländern?

Minister mit Open-Source-Stickern auf dem Notebook: Staatskanzleichef Dirk Schrödter treibt in Schleswig-Holstein den Wechsel auf LibreOffice, Nextcloud, Open-XChange & Co. voran.

Schrödter: Ich erkläre ihnen die Vorzüge von digitaler Souveränität. Und ich sage: Macht euch über die langfristigen Konsequenzen Gedanken. Wenn man Herr über seine Datenhaltung sein will, geht das nicht mit einer Strategie, mit der man sich an einen einzelnen Anbieter kettet.

Desk in den Plänen der Kieler Regierung bislang nur eine Nebenrolle spielt. Dabei besteht openDesk ebenfalls aus Collabora Online Office, Nextcloud und Open-Xchange und ist sogar aus einem Dataport-Projekt namens Phoenix hervorgegangen. Dass openDesk nicht der Standard für alle Arbeitsplätze wird, begründet Schrödter damit, dass Schleswig-Holstein den Umstieg auf Open Source schon lange vor der Gründung des ZenDiS vorbereitet habe. „Wir sind viel schneller als die Kollegen, weil wir viel früher angefangen haben. Und wir wollen unsere Schnelligkeit beibehalten."

Stattdessen soll openDesk vor allem als Backup für Notfallarbeitsplätze eingesetzt werden, also zum Beispiel im Fall einer Cyberattacke. Thomsen nennt zudem praktische Gründe: Man wolle sich darauf konzentrieren, komponentengestützt, also Stück für Stück, zu migrieren, statt alles auf einmal. Wichtig



Statt auf Microsoft 365 setzt die Landesregierung auf Collabora Online Office, was in der von Schleswig-Holstein genutzten Nextcloud-Instanz integriert ist.

sei, dass man bis Oktober einen Großteil der Lizenzen nicht mehr benötigt. Die bei openDesk vorhandene Integration zwischen Open-Xchange, Nextcloud und anderen Komponenten stehe jetzt nicht im Vordergrund und sei relativ einfach nachzuziehen.

Festzuhalten ist, dass openDesk außerdem eine rein webgestützte Lösung ist, während Schleswig-Holstein mit LibreOffice und Thunderbird zumindest teilweise weiterhin klassische Desktopanwendungen nutzt.

Windows 11 statt Linux

Und Linux? Die Desktoprechner bleiben zunächst bei Microsofts Betriebssystem. Schleswig-Holstein plant die Anschaffung von Lizenzen für Windows 11. Trotzdem erkundet man schon jetzt, wie ein Arbeitsplatz mit einem Linux-Desktop aussehen könnte, und der Pilotbetrieb soll noch dieses Jahr starten. Beim Besuch in der Staatskanzlei präsentierte CIO Thomsen den c't-Redakteuren einen KDE Plasma Desktop. Für die nächsten Jahre sei bewusst die Entscheidung auf KDE Plasma gefallen. Denn KDE bietet eine aktive, europäische Community und die Bedienoberfläche mit Taskleiste und Startmenü ähnelt jener von Windows, was den Umstieg erleichtert. Auf eine Distribution habe man sich bisher nicht festgelegt; klar ist nur, dass es ein gemanagtes Enterprise-Linux sein soll, welches Dataport betreiben soll.

Fazit

Schleswig-Holstein geht seinen Sonderweg konsequent. Die Frage bleibt, ob es gelingt, die Beschäftigten mitzunehmen und die Landesregierung die versprochenen Einsparungen tatsächlich erzielen kann. Selbst wenn es sich finanziell nicht rechnen sollte, politisch ist die Unabhängigkeit womöglich essenziell. Der Anfang von Präsident Trumps zweiter Amtszeit zeigt, dass digitale Souveränität wichtiger denn je ist. (ktn/cwo) c't

Literatur

[1] Niklas Dierking und Christian Wölbert, „Mehr Flexibilität, mehr Souveränität, mehr Sicherheit“, Schleswig-Holsteins Digitalminister Jan Philipp Albrecht über den Wechsel zu Open Source, c't 23/2021, S. 34

Open-Source-Strategie und Hintergründe

ct.de/w5v1

// heise devSec()

Die Konferenz für sichere Softwareentwicklung

30. September und 1. Oktober 2025 Regensburg

Aus dem Programm:

- Software nachhaltig sicher entwickeln – ein Praxisbericht
- Software-Supply-Chain-Security: Mehr als nur Dependency-Management
- LLMs im Secure Dev Lifecycle
- Cyber Resilience Act – Cheatsheet für Entwickler
- Fünf Scanner, drei Dashboards, null Überblick? Zeit für eine ASPM-Lösung?
- Protectors of the Realm: Wie man einen Keycloak sicher hält

Jetzt Tickets sichern!

heise-devsec.de

Workshops zu sicherer Legacy-Software sowie OAuth 2.0 & Open ID Connect

Veranstalter: heise Security, iX Magazin für professionelle IT, dpunkt.verlag

Platin-Sponsor: SignPath

Gold-Sponsoren: BlueFlag Security, CONTRAST SECURITY

Silber-Sponsoren: INNOQ, mgm mgm security partners

Bronze-Sponsoren: KRONES.digital, Plus.line

Bild: KI, Collage c't

Digitale Souveränität in Mitteleuropa

Die Schweiz testet Open-Source-Software aus Deutschland, Dänemarks Digitalministerium wechselt zu Libre Office, und Deutschland, Frankreich und die Niederlande entwickeln gemeinsam Software für Behörden: Donald Trump treibt europäische Regierungen zu Microsoft-Alternativen.

Von **Falk Steiner und Christian Wölbert**

Mit der Kaltstellung der Ukraine, der Annäherung an Russland und mit seiner Zollpolitik hat US-Präsident Donald Trump die Europäer aufgeschreckt – und die Diskussion um digitale Souveränität befeuert. Die Risiken der Abhängigkeit von amerikanischen Tech-Konzernen sind auf der politischen Agenda plötzlich nach oben gerückt; nicht nur in Berlin, sondern auch in anderen europäischen Hauptstädten.

Die Diskussion hat viele Facetten, denn US-Konzerne wie Microsoft, AWS, Google, Oracle, Broadcom oder OpenAI dominieren in zahlreichen Bereichen der IT, von Hardware über Clouddienste bis hin zu Betriebssystemen und (KI-)Anwendungen. In einzelnen Segmenten haben allerdings auch chinesische Anbieter wie Lenovo und Huawei eine starke Stellung, genau wie die Europäer selbst, zum Beispiel mit ASML oder SAP.

Eine IT-Welt ohne Abhängigkeiten von Dritten wäre nicht förderlich für Produktivität und Wohlstand und ohnehin unrealistisch, schließlich ist in kaum einer Firma das gesamte Know-how für die immer komplexer werdenden Produkte vorhanden. Doch besonders die Abhängigkeit von Microsofts Software und Clouddiensten beunruhigt viele europäische Politiker. Sollte der Konzern sich aufgrund von Anordnungen der US-Regierung gezwungen sehen, Clouddienste wie 365 abzuschalten, wären die Auswirkungen drastisch: Ministerien und Behörden mit 365-Abo könnten von jetzt auf gleich nicht einmal mehr chatten oder mailen. Sollte Microsoft keine Sicherheitsupdates mehr liefern, gerieten früher oder später alle Nutzer von Windows und den „on premise“ (also auf Kundenhardware statt in der Cloud) laufenden Varianten von Office und Exchange in Schwierigkeiten.

Microsofts Plan, Office künftig nur noch in der Cloud anzubieten, setzt die Europäer zusätzlich unter Druck. Und der Wechsel zu anderen Anbietern wird unter anderem dadurch erschwert, dass Verwaltungsanwendungen wie E-Akte-Programme mit Microsoft Office verwoben sind.

Im Folgenden konzentrieren wir uns deshalb auf die Frage, wie einige europäische Länder ihre Abhängigkeit von Microsoft reduzieren wollen. Einen Überblick über umfassendere europäische Initiativen für digitale Souveränität wie EuroStack gibt der Kasten „EuroStack & Co.: Neue europäische Initiativen für digitale Souveränität“ (auf S. 52).

Niederlande planen strengere Cloud-Regeln

Zu den europäischen Regierungen, die intensiv Microsoft-Clouddienste nutzen, gehört die der Niederlande. Nachlesen lässt sich das in einem Bericht des niederländischen Rechnungshofs vom Januar. Demnach erlaubte das Innenministerium im Jahr 2022 den Regierungsbehörden die Nutzung von Public-Cloud-Diensten. Der staatliche IT-Dienstleister SSC-ICT, der 57.000 IT-Arbeitsplätze in Ministerien und Behörden betreut, schloss mit Microsoft einen Vertrag über die Nutzung des Online-Office-Pakets 365. Laut dem Bericht des Rechnungshofs wird dieses mittlerweile „beinahe von der gesamten Zentralregierung“ genutzt.

Hingegen nutzen die Ministerien der deutschen Bundesregierung in der Regel noch die On-Premise-Version von Office. Eine Ausnahme ist das Auswärtige Amt, das angekündigt hat, „im Rahmen der besonderen Erfordernisse der Auslands-IT“ Microsoft 365 einzuführen. Auch mindestens sechs Bundesländer, darunter Bayern und Niedersachsen, nutzen Microsofts Public-Cloud-Dienste oder planen das.

Frankreich, Deutschland und die Niederlande arbeiten gemeinsam am freien Editor Docs. Das Logo mit Baguette, Gouda und Brezel findet sich auf der GitHub-Seite des Projekts.

Die Bundesregierung setzt jedoch in erster Linie auf ein spezielles Projekt, nämlich auf eine Cloud der SAP-Tochterfirma Delos. Diese will in ihren Rechenzentren Microsoft 365 und weitere Clouddienste exklusiv für deutsche Behörden betreiben. Da SAP ein deutscher Konzern ist, haben US-Behörden juristisch gesehen keine direkte Zugriffsmöglichkeit. Technisch verspricht Delos ein relativ hohes Schutzniveau vor Spionage und Manipulation [1]. Und im Fall, dass Microsoft keine Updates mehr liefert, will das Unternehmen die Cloud zumindest für einige Monate weiter betreiben. Geht dieses Versprechen auf, wäre die Bundesregierung nicht so leicht erpressbar wie etwa die niederländische, die sich auf Microsofts Rechenzentren verlässt.

Doch mittlerweile rücken die Risiken der Microsoft-Cloud auch in den Niederlanden stärker in den Fokus. Die Regierung in Den Haag will ihre Richtlinie für den Einsatz von Clouddiensten überarbeiten. Die neuen Regeln würden „die Nutzung von Public-Cloud-Diensten einschränken“, kündigte das Innenministerium am 12. März auf eine Frage zweier Abgeordneter an. Die Aspekte der „digitalen Autonomie

und Sicherheit“ würden in der neuen Politik stärker berücksichtigt.

Außerdem beteiligen sich die Niederlande am Aufbau von Alternativen zu Microsoft Office und Teams: Im Dezember unterschrieb der niederländische Staats-CIO Art de Blaauw eine „Declaration of Intent“ über die Zusammenarbeit mit dem staatlichen deutschen Zentrum für digitale Souveränität (ZenDiS) sowie der Direction interministérielle du numérique (DINUM), der Digitalisierungseinheit der französischen Regierung. Dabei geht es um die Weiterentwicklung quelloffener Anwendungen für Behörden, aktuell vor allem für Produktivität und Kommunikation. Ein konkretes Produkt der deutsch-französischen Kooperation ist Docs, ein Online-Editor für kollaboratives Schreiben und Wissensmanagement. „Zurzeit nehmen wir die Niederlande an Bord“, heißt es auf der GitHub-Seite des Projekts. Docs ist mittlerweile auch Teil des deutschen Open-Source-Office-Pakets openDesk.

Dänemark: Vom US-Gehilfen zum Gegner

Auch im durchdigitalisierten Dänemark machte man sich bis vor Kurzem wenige Gedanken über die Abhängigkeit von Microsofts Clouddiensten. Das Land pflegte traditionell ein enges Verhältnis zu den USA. Das ging so weit, dass der dänische Auslandsnachrichtendienst der NSA von 2012 bis 2014 ermöglichte, einen Unterseekabel-Knotenpunkt anzuzapfen. Ziel dieser Abhöraktion waren laut Medienberichten Angela Merkel und weitere europäische Spitzenpolitiker.

Den Wechsel zu Microsoft 365 in der Public Cloud bereitet die dänische Regierung schon seit einigen Jahren vor. Mitte vorigen Jahres kam der staatliche IT-Dienstleister Statens IT in einer Datenschutzfolgeabschätzung zu dem Schluss, dass die Nutzung der Cloudanwendungen durch Behörden mit der DSGVO vereinbar ist. Zur Frage, wie viele Behörden bereits Microsoft 365 nutzen, gab das zuständige Finanzministerium auf Anfrage von c’t keine Auskunft.

Doch seit Donald Trumps Amtsantritt steht Dänemark plötzlich Kopf. Denn Trump will Grönland annektieren und bedroht das Königreich ganz offen. Man werde die Kontrolle über Grönland „auf die eine oder die andere Art und Weise“ übernehmen, sagte er im März vor dem US-Kongress. Seitdem gibt es auch in Dänemark eine Diskussion darüber, inwieweit das Land per Knopfdruck lahmgelegt werden könnte.

Dieses Risiko einer Totalabschaltung sei zwar gering, aber dennoch brauche Dänemark einen Plan B, sagte Jacob Herbst, Vorsitzender des dänischen Rates für Cybersicherheit und Technikchef der Sicherheitsfirma Dubex, im März gegenüber dem Sender TV 2. „Wenn die Amerikaner um 8 Uhr am Montagmorgen entscheiden, US-Clouddienste abzuschalten, dann wird Dänemark um 9 Uhr still stehen.“

Im Juni zog das Digitalministerium Konsequenzen: Es kündigte an, als erstes dänisches Ministerium von Microsoft Office zum quelloffenen Libre Office zu wechseln. Noch im Sommer soll die Hälfte der

Europäische Tech-Firmen profitieren vom „Trump-Effekt“

Seit dem Amtsantritt von Donald Trump verzeichnen viele europäische Cloudanbieter und Softwareentwickler einen plötzlichen Anstieg der Nachfrage, sowohl von Behörden als auch von Unternehmen. Ob auch eine Sofortmigration möglich sei, sei keine seltene Frage mehr, berichtet zum Beispiel Nextcloud-Gründer Frank Karlitschek im Gespräch mit c’t. Was früher mit monatelangen Abwägungsprozessen verbunden war, scheint nunmehr dringlich: Abhängigkeiten zu reduzieren, insbesondere von US-Anbietern.

Ähnliches berichtete der französische Anbieter OVHCloud: Nach dem Streit zwischen Trump und dem ukrainischen Präsidenten Selenskyj seien „signifikante Anfragen“ eingegangen, „auch aus DAX-Bereichen und dem öffentlichen Sektor“, sagte Deutschlandchef Falk Weinreich im Interview mit unserer Schwesterzeitschrift iX. Auch der deutsche Cloudanbieter Ionos meldete einen spürbaren Anstieg der Nachfrage.

Ob Europa seine Abhängigkeit von Microsoft, AWS & Co. aber tatsächlich signifikant reduziert, da ist sich Nextcloud-Chef Karlitschek trotz des großen Interesses nach dem Trump-Schock noch nicht sicher: „Die Frage bei der digitalen Souveränität ist, ob es nun vom Reden endlich ins Handeln übergeht.“

Angestellten des Ministeriums wechseln, bis zum Herbst der Rest. „Wir werden dem Ziel nicht näher kommen, wenn wir nicht starten“, sagte Digitalministerin Caroline Stage (Moderaterne) in einem Interview mit der Tageszeitung Politiken. Ob weitere dänische Ministerien dem Schritt folgen, war bis Redaktionsschluss offen.

Die Dänen müssen nicht weit reisen, um von den Erfahrungen anderer Behörden mit Libre Office zu profitieren: Das benachbarte Schleswig-Holstein ist das einzige deutsche Bundesland, das sich weitgehend von Microsoft Office verabschieden will (siehe S. 34). Bis Oktober 2025 soll auf 70 Prozent der IT-Arbeitsplätze der Landesverwaltung stattdessen Libre Office und Nextcloud genutzt werden. Vertreter dänischer Ministerien haben die Kieler Staatskanzlei bereits besucht und sich über das Projekt informiert, wie eine Sprecherin der Staatskanzlei auf Anfrage mitteilte. „Es wurde vereinbart, diesen Informationsaustausch fortzusetzen.“

> **»Wenn die Amerikaner um 8 Uhr am Montagmorgen entscheiden, US-Clouddienste abzuschalten, dann wird Dänemark um 9 Uhr still stehen.«**
>
> *Jacob Herbst, Vorsitzender des dänischen Rates für Cybersicherheit*

BOSS: Schweiz testet deutsches Office

Auch die Schweiz ist weit fortgeschritten auf dem Weg in Microsofts Public Cloud. Schon 2023 entschied die Berner Bundeskanzlei, Microsoft 365 in der Verwaltung einzuführen. Eine Alternative dazu gebe es nicht, da Microsoft seine On-Premise-Produkte nicht mehr weiterführe, führte die Bundeskanzlei damals aus. Mails und Kalenderdaten würden jedoch weiterhin in den Rechenzentren des Bundes gespeichert, außerdem dürften die Beamten keine vertraulichen Dokumente in der Microsoft-Cloud speichern.

Inzwischen seien 50 Prozent der 45.000 PC-Arbeitsplätze der Bundesverwaltung auf Microsoft 365 umgestellt, sagte ein Sprecher der Bundeskanzlei auf Anfrage von c’t. Bis Ende des Jahres folge der Rest. Trump ist für die Schweiz also kein Grund, die Migration abzubrechen.

Anders als Dänemark und die Niederlande haben die Eidgenossen allerdings schon zu Beginn der Microsoft-365-Einführung betont, dass sie ihre Abhängigkeit von Microsoft „mittel- bis langfristig“ reduzieren wollen: Im Rahmen einer Exit-Strategie prüfe man auch Open-Source-Alternativen, teilte die Bundeskanzlei 2023 mit. Das ähnelt den Äußerungen der deutschen Bundesregierung.

Welche Open-Source-Alternative die Schweiz konkret prüft, ist mittlerweile bekannt. Im Rahmen der Machbarkeitsstudie BOSS („Büroautomation mit Open-Source-Software“) pilotiert sie das vom deutschen ZenDiS mit Steuergeldern geschnürte Open-Source-Office-Paket openDesk. Dieses umfasst unter anderem Collabora Online, Open-Xchange, Nextcloud und Element [2].

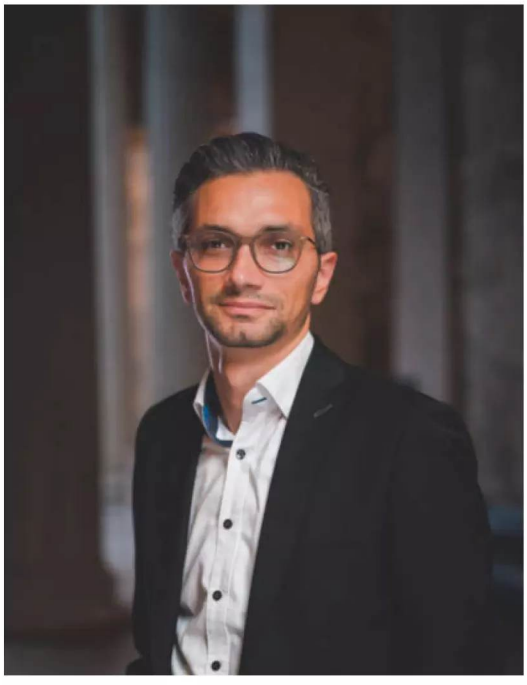
Man prüfe diese Anwendungen bis 2026 auf „Benutzerfreundlichkeit, Praxisnähe, Skalierbarkeit und Sicherheitsmerkmale“, erklärt die Bundeskanzlei auf ihrer Internetseite. Sie betont aber auch, dass sie nicht plant, Microsoft 365 durch BOSS zu ersetzen. Im Vordergrund stehe stattdessen die Eignung der Open-Source-Suite als Notfalllösung „unter Krisenbedingungen“ sowie als Werkzeug für die Bearbeitung sensibler Daten. Im Notfall stünde die Schweiz also immerhin nicht komplett nackt da.

Österreich: Bisher vor allem Absichtserklärungen

Wenige konkrete Informationen gibt es aus Österreich. Das Bundeskanzleramt ließ eine Anfrage von c’t zur Nutzung von Microsofts On-Premise-Produkten und Clouddiensten sowie eventuellen Alternativen unbeantwortet. Bekannt ist, dass Microsoft 365 im österreichischen Bildungssektor etabliert ist. Schon seit 2013 können Schulen im ganzen Land den Clouddienst über einen Vertrag des Bildungsministeriums nutzen.

Um Abhängigkeiten zu reduzieren, hat sich die seit März regierende Koalition aus ÖVP, SPÖ und Neos in ihrem Koalitionsvertrag vorgenommen, „in Abstimmung mit europäischen Partnern“ verstärkt auf Open-Source-Software zu setzen und digitale Souveränität bei Beschaffungen zu berücksichtigen. Konkretere Maßnahmen werden allerdings nicht erwähnt. Und auch über Pilotprojekte mit freien Office-Suiten für Behörden wie BOSS in der Schweiz oder openDesk in Deutschland ist aus Österreich nichts bekannt.

Ende März forderte der Grünen-Abgeordnete Süleyman Zorba die Wiener Regierung deshalb in einem Antrag auf, einen konkreten Zeitplan für Umsetzungsmaßnahmen zu erarbeiten und Fördermittel für Forschung und Entwicklung im Bereich Open-Source-Software bereitzustellen.



„In Österreich ist die Debatte über digitale Souveränität kaum vorhanden“, sagt Süleyman Zorba, Digitalpolitiker der österreichischen Grünen.

Die Energiekrise nach Beginn des Ukraine-Kriegs habe gezeigt, wie riskant starke Abhängigkeiten sind, argumentiert Zorba im Gespräch mit c't. „Österreich war abhängig von russischem Gas, und die Auswirkungen haben wir deutlich gespürt.“ Ihm gehe es nun allerdings nicht um Verbote bestimmter Software, sondern um den Aufbau von Alternativen, gemeinsam mit europäischen Partnern. „Ein Land wie Österreich kann das nicht allein stemmen.“

Der Digitalpolitiker macht sich jedoch keine großen Hoffnungen, dass die Bundesregierung seinem Antrag folgt. „In Österreich ist die Debatte über digitale Souveränität kaum vorhanden“, sagt er.

Frankreich: „La Suite Numérique“ als MS-Alternative

Auch die französische Regierung wollte auf Anfrage keine Details zur Nutzung von Microsofts Clouddiensten und On-Premise-Produkten durch Behörden verraten. „Aktuell nutzen viele Behörden proprietäre, kommerzielle Lösungen wie Microsoft Office“, erklärte eine Sprecherin der interministeriellen Digitalisierungsbehörde DINUM lediglich.

Doch das traditionell auf Souveränität bedachte Frankreich hat seinen Behörden schon 2021 relativ strenge Regeln für die Nutzung von Clouddiensten auferlegt. Die Daten französischer Bürger oder Unternehmen dürfen in der Regel nur mit Diensten verarbeitet werden, die immun gegen Nicht-EU-Gesetze sind und Anforderungen der französischen Cybersicherheitsbehörde erfüllen. Ausnahmen sind möglich, aber die DINUM betonte 2021, dass Microsoft 365 die Anforderungen nicht erfüllt. Der Clouddienst dürfte in französischen Behörden daher nicht die Regel sein, ähnlich wie in Deutschland auf Bundesebene.

Und genau wie Delos in Deutschland will auch ein französisches Unternehmen Microsofts Clouddienste für Behörden in speziellen Rechenzentren betreiben, um den Zugriff durch US-Behörden zu erschweren: Bleu, ein Joint Venture des Telekommunikationskonzerns Orange und des Beratungshauses Capgemini. Wie Delos arbeitet Bleu zurzeit daran, die Einhaltung der staatlichen Sicherheitsanforderungen nachzuweisen.

Seit der Coronapandemie entwickelt Frankreich zudem Open-Source-Anwendungen für Office-Aufgaben. Die 2021 offiziell vorgestellte Suite hieß zunächst SNAP und bestand aus dem Matrix-kompatiblen Messenger Tchap sowie Tools für Audio- und Videokonferenzen sowie einer Dateiablage mit integriertem Online-Office. 2022 taufte die DINUM das Paket in La Suite Numérique um. Diese umfasst mittlerweile auch Open-Source-Tools für Mail, Datenbanken und Tabellen sowie den Transfer großer Dateien. Der bereits erwähnte Editor Docs gehört ebenfalls dazu.

Ähnlich wie das ZenDiS in Deutschland verzahnt die DINUM die diversen Open-Source-Tools technisch miteinander und vereinheitlicht die Bedienoberfläche. Allerdings gehen die beiden Staaten dabei unterschiedlich vor: Das ZenDiS entwickelt die Software nicht selbst, sondern vergibt Entwicklungs- und Supportaufträge an die Hersteller der Software, etwa Nextcloud, Univention oder Open-Xchange. Die DINUM beschäftigt hingegen selbst viele Softwareentwickler und beauftragt Freelancer. „Die Reinternalisierung essenzieller digitaler Fähigkeiten ist ein Schwerpunkt der Digitalstrategie der französischen Regierung“, betonte die DINUM gegenüber c't.

Literatur

[1] Christian Wölbert, „Die Cloud ist unter unserer Kontrolle“, Interview: Wie „souverän“ ist die Delos-Cloud für die Verwaltung wirklich? c’t 4/2023, S. 38

[2] Kornelius Kindermann, Martin Gerhard Loschwitz, Bundes-Office-Suite: Was kann openDesk?, iX 1/2025, S. 110

Erwähnte Quellen

ct.de/wkxp

La Suite und openDesk warten noch auf den Durchbruch

Mit dieser Strategie hat die DINUM französische Open-Source-Entwicklerfirmen gegen sich aufgebracht. Deren Verband CNLL wirft der Regierung vor, den Unternehmen mit der mit Steuergeldern entwickelten Software unfaire Konkurrenz zu machen. „Die DINUM spielt gegen ihr eigenes Team“, heißt es in einer CNLL-Stellungnahme vom August 2024.

Auch der französische Rechnungshof sieht „La Suite Numérique“ kritisch. „Es ist zwar wünschenswert, dass der Staat bei Schwierigkeiten mit privaten Plattformen über eine souveräne Rückzugsmöglichkeit verfügt, aber die Ergebnisse entsprechen nicht den getätigten Investitionen“, heißt es in einem Bericht der Rechnungsprüfer aus dem Juli 2024. Die meisten Staatsbediensteten wüssten nichts von dem staatlichen Officepaket und die Nutzungszahlen mehrerer Tools seien rückläufig.

Wie viele französische Beamte inzwischen „La Suite“ anstelle von Microsoft Office nutzen, ist nicht bekannt. „Mehrere Behörden haben Tools der Suite Numérique eingeführt“, teilte die DINUM auf Anfrage lediglich mit. Tchap komme aktuell auf 230.000 Nutzer pro Monat. Die anderen Tools werden vermutlich weniger stark genutzt.

Im Vergleich zum deutschen openDesk scheint „La Suite“ jedenfalls eher günstig. Laut dem Bericht des Rechnungshofs investierte DINUM bis Ende 2023 rund 9,3 Millionen Euro in die Entwicklung, die jährlichen Wartungskosten werden mit 5 Millionen Euro beziffert. Aus Sicht der Pariser Rechnungsprüfer sind diese Kosten „erheblich“. Doch das deutsche Bundesinnenministerium investierte allein bis Mitte 2024 rund 35 Millionen Euro in die Entwicklung von openDesk, für die damals noch der norddeutsche IT-Dienstleister Dataport zuständig war.

Auch openDesk hat den Durchbruch noch nicht geschafft: Das ZenDiS verzeichnete im April zwar

EuroStack & Co.: Neue europäische Initiativen für digitale Souveränität

Mit Gaia-X wollten die deutsche und die französische Regierung schon 2019 die Wettbewerbsfähigkeit europäischer Cloudanbieter stärken. Das Projekt wird von einigen Unternehmen noch weiter vorangetrieben, es konzentriert sich aber mittlerweile auf spezielle Aspekte, etwa auf Datenräume für die Industrie. Größere Hoffnungen in Sachen „digitale Souveränität“ setzen Politik und Wirtschaft mittlerweile auf jüngere Initiativen. Dazu gehören zum Beispiel:

„Buy European“-Klauseln: Die Europäische Kommission will Ende des Jahres eine Reform des europäischen Vergaberechts vorstellen, das immer dann eingehalten werden muss, wenn staatliche Stellen in Europa etwas einkaufen wollen. Brüssel könnte darin eine Buy-European-Klausel verankern, also den Behörden vorschreiben, europäische Anbieter zu bevorzugen. „Durch ein Gebot für öffentliche Verwaltungen, mindestens die Hälfte ihrer digitalen Dienstleistungen, insbesondere Clouddienste, bei europäischen Anbietern zu beschaffen, könnten wir die Nachfrage generieren, die europäische Unternehmen für ihre Investitionssicherheit benötigen“, sagt Axel Voss, der für die CDU im Europaparlament sitzt. Auch die Grünen-Europaabgeordnete Alexandra Geese befürwortet eine solche Regel.

EuroStack: Die EuroStack-Initiative wurde unter anderem von der EU-Abgeordneten Alexandra Geese und den Wirtschaftswissenschaftlerinnen Cristina Caffara und Francesca Bria ins Leben gerufen. Sie fordern, dass die EU sich nicht darauf beschränkt, Tech-Konzerne zu regulieren, sondern einheimische Anbieter stärker fördert – mit Steuergeld, aber auch mit privatem Wagniskapital. Eine Studie von Bria und weiteren Autoren zeigt auf, auf welchen technischen Ebenen Europa von den USA und China abhängig ist und welche EU-Firmen bereits Alternativen bieten. Die neue Bundesregierung will laut Koalitionsvertrag die EuroStack-Initiative „stärken“.

EU OS: Auf der Webseite eu-os.eu konzipieren der Datenschutzexperte Robert Riemann und Mitstreiter ein PC-Betriebssystem für Nutzer im öffentlichen Sektor. Als Basis soll Fedora Linux dienen.

SECA: Die europäischen Cloudanbieter Aruba (Italien), Ionos (Deutschland) und Dynamo (Italien) arbeiten an einer offenen API-Spezifikation, die Kunden den Wechsel zwischen Cloudanbietern und den Betrieb von Multi-Cloud-Infrastrukturen erleichtern soll.

„70.000 Nutzende in allen Bundesländern“, doch die wenigsten davon dürften auf Microsoft Office verzichten. Und wenn man bedenkt, dass es im öffentlichen Dienst bundesweit mehrere Millionen PC-Arbeitsplätze gibt, wird klar, dass openDesk zurzeit noch ein zartes Pflänzchen ist. Und mittlerweile finanziert die Bundesregierung das Projekt nicht mehr so großzügig wie in den ersten Jahren, das ZenDiS muss sparen.

Das Ziel der Zusammenarbeit

Doch die Kooperation zwischen Deutschland, Frankreich und den Niederlanden sowie die Pilotierung von openDesk in der Schweiz zeigen: Europaweit steigt das Interesse an freien Office-Apps für Behörden. Und gemeinsam können die Europäer eher die Ressourcen zur Entwicklung wettbewerbsfähiger Software aufbringen als allein.

Das Ziel bestehe nicht darin, ein einheitliches europäisches Softwarepaket zu schnüren, sagt Alexander Smolianitski, Head of Open Source Products beim ZenDiS, im Gespräch mit c’t. „Es geht eher um Standards und Schnittstellen, die den Aufwand reduzieren, einzelne Anwendungen ein- oder auszubauen.“ So könne eine Produktlandschaft aus kompatiblen Tools entstehen. Nationen könnten bei Bedarf Apps voneinander übernehmen, aber auch ihre individuellen Bedürfnisse berücksichtigen.

Dass es um Open-Source-Software gehe, erleichtere die Zusammenarbeit enorm, betont Smolianitski: „Man muss gar nicht überlegen, ob andere den Code sehen dürfen, sondern man legt einfach zusammen los.“ (cwo) **c't**

WIR TEILEN KEIN HALBWISSEN.
WIR SCHAFFEN FACHWISSEN.

Webinar 16. September

Die Necromancer-Challenge: Lerne zu hacken

Sie lernen, wie Sie Server mit nmap abklopfen, Passwörter im Eiltempo mit Hydra knacken und Netzwerkverkehr mit Wireshark analysieren.

Webinar 9. Oktober

Elektroauto 2025

Lohnt sich der Umstieg aufs E-Auto derzeit – oder ist Abwarten die bessere Wahl? Das Webinar liefert fundierte Antworten und Orientierung.

Webinar 16. Oktober

Wärmepumpentechnik für Einsteiger

Wir erklären die Arbeitsweise der verschiedenen Wärmepumpen-Typen und liefern Anhaltspunkte für eine erste Machbarkeitsabschätzung in der eigenen Immobilie.

Webinar 6. November

Sprach-KI produktiv einsetzen

c't-Redakteure geben einen Überblick über die gängigen Sprachmodelle. Sie erläutern Kosten, Ressourcenbedarf und Einsatzmöglichkeiten.

Mehr anzeigen ▲

heise.de/ct/Events

Wie Behörden Open Source ausbeuten

Immer mehr Behörden setzen auf freie Software. Doch häufig beauftragen sie Dumpinganbieter, die dem Open-Source-Ökosystem schaden. Auch der Steuerzahler zahlt am Ende oft drauf.

Von **Christian Wölbert**

Man könnte meinen, in Deutschland herrschen goldene Zeiten für Open-Source-Entwicklerfirmen, wütet doch Donald Trump im Weißen Haus schlimmer denn je. Immer mehr Behörden erwägen deshalb, ihre Abhängigkeit von US-Konzernen wie Microsoft und Cisco zu verringern und auf Open-Source-Software umzusteigen.

Doch paradoxerweise profitieren die Unternehmen, die Open-Source-Software entwickeln, nur selten vom Trend zu „digitaler Souveränität“ im öffentlichen Sektor. Es komme immer wieder vor, dass Trittbrettfahrer ihre Software übernehmen und dann „mithilfe von Dumpingangeboten eine Ausschreibung gewinnen“, beklagte im Frühjahr 2025 die Open Source Business Alliance (OSBA), ein Verband von Open-Source-Firmen.

Den OSBA-Mitgliedern geht es dabei nicht nur um den entgangenen Umsatz. Die Dumpinganbieter

kalkulierten „häufig keinen ausreichenden Support und keine ausreichenden Aufwände für Weiterentwicklung, Pflege oder Upstream-Veröffentlichung der Software ein“, warnt der Verband. Wenn die Projekte scheitern, müssten die etablierten Open-Source-Firmen das Problem ausbaden. Die Misserfolge schadeten dem „Ruf der gesamten Open-Source-Community“.

Das HessenConnect-Debakel

Manchmal werden die Entwicklerfirmen von den Trittbrettfahrern sogar mit „parasitären Supportfragen“ überhäuft, wie der Open-Source-Unternehmer Peer Heinlein es in einer Präsentation formuliert. Er spricht vom „Kuckuck im Bieterverfahren“, der die Software der Entwicklerfirmen zu einem „Kampfpreis unter den echten Herstellungskosten“ anbiete, ohne diese als Partner für Wartung, Weiterentwicklung oder Support zu beteiligen. Das sei zwar legal, widerspreche aber den Gepflogenheiten der Branche und gefährde letztlich die Existenz der Entwicklerfirmen und ihrer Software.

Eine Ursache des Problems liegt darin, dass viele Politiker sich zwar als Open-Source-Verfechter sehen, die Branche jedoch kaum kennen. Gegenüber der OSBA berichtete ein Open-Source-Hersteller anonym von einem bizarren Gespräch: „Vor anderthalb Jahren hat mir der CIO eines Bundeslandes zum Deal für die Videoarbeitsplätze mit unserer Software gratuliert und geschwärmt, dass er ein großer Open-Source-Verfechter sei. Ich wusste zuerst nicht, wovon er sprach, und dann stellte sich heraus, dass das Unternehmen xyz mit unserer Software eine Ausschreibung gewonnen hat.“

Doch bei dem Thema geht es nicht nur um die Interessen der Open-Source-Lobby. Auch die Steuerzahler sind am Ende oft die Dummen.

Beobachten ließ sich das zum Beispiel in Hessen. 2022 kündigte das Bundesland an, von Microsofts Skype for Business auf „Open-Source-Lösungen von Element/Matrix und Jitsi unter einer einheitlichen Oberfläche“ umzusteigen. Die Pressemitteilung las sich so, als sei an dem Projekt namens „HessenConnect 2.0“ auch die Element Software GmbH beteiligt. Das ist die deutsche Niederlassung der Firma, die Matrix-Software wie den Chatserver Synapse und die Element-Clients maßgeblich entwickelt.

Die Ausschreibung hatte jedoch die Telekom-Tochter T-Systems gewonnen. Diese arbeitete im Rahmen des Projektes nicht mit Element zusammen, sondern mit anderen Unternehmen. Die T-Systems und ihre Partner bedienten sich am Open-Source-Code und begannen mit der Entwicklung zahlreicher Zusatzfunktionen und Optimierungen, die das Land Hessen forderte. Spätestens am 1. Januar 2025 sollte HessenConnect 2.0 auf 35.000 IT-Arbeitsplätzen der hessischen Behörden eingeführt werden, denn zu diesem Zeitpunkt liefen die Skype-Lizenzen aus.

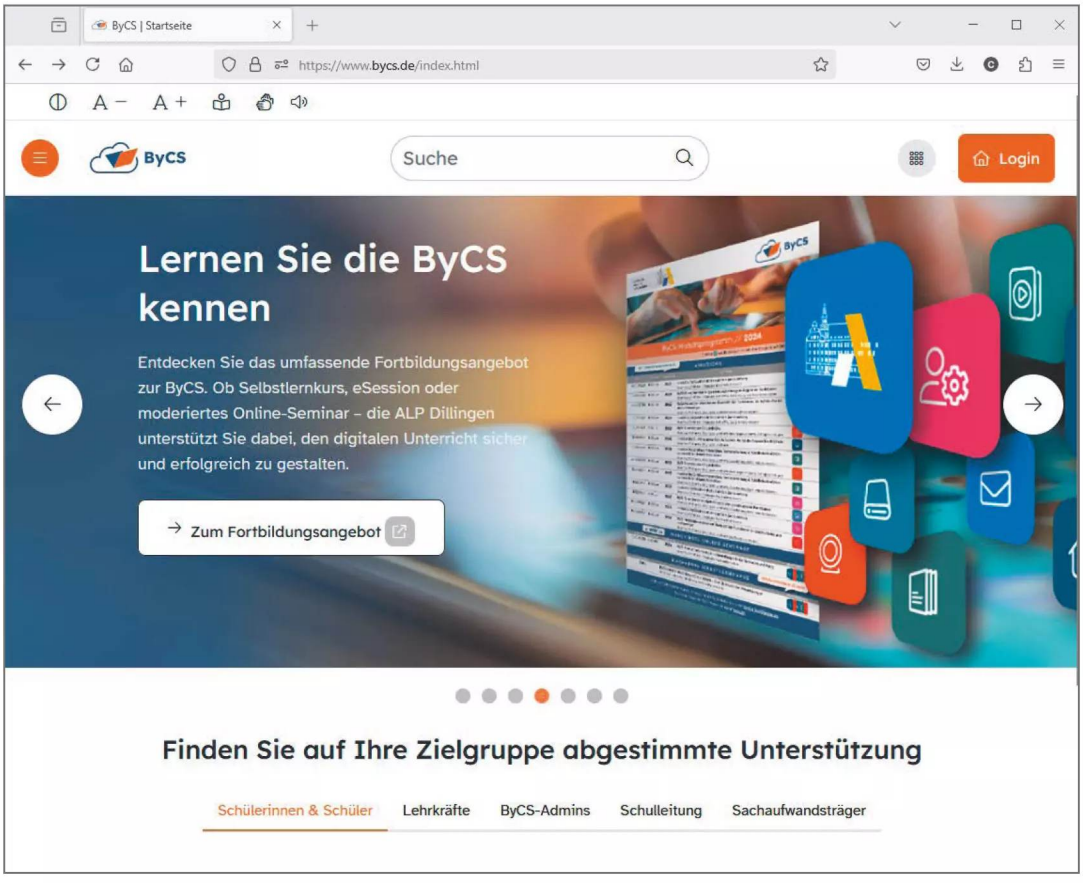
Doch kurz vor Weihnachten 2024 teilte das hessische Digitalministerium überraschend mit, HessenConnect 2.0 sei „zum aktuellen Zeitpunkt nicht einsatzbereit“. Daher führe man nun Webex von Cisco als „Übergangslösung“ ein. Auf Nachfrage von c’t erläuterte das Ministerium, T-Systems habe die Anforderung der Anwenderfreundlichkeit „nicht überzeugend und umfassend erfüllt“. T-Systems und einer der beteiligten Sub-Auftragnehmer wollten sich auf Anfrage von c’t nicht öffentlich zu dem Thema äußern.

Der Steuerzahler zahlt also nun doppelt: erstens für das HessenConnect-2.0-Projekt, zweitens für die ungeplanten Webex-Lizenzen. Und nicht nur das: Die zahlreichen Optimierungen, die die Telekom und ihre Subunternehmen entwickelt haben, flossen nicht „upstream“ in den Code der Element-Clients und der Serversoftware Synapse ein. Die Wahrscheinlichkeit ist deshalb groß, dass dieselben oder ähnliche Features im Auftrag anderer Behörden noch einmal entwickelt werden. Der Steuerzahler würde also auch für die Optimierungen doppelt zahlen.

Trittbrettfahrer als Sicherheitsrisiko

Ein ähnlicher Fall spielt in Bayern. Als das Bundesland eine Messenger-Anwendung für seine „BayernCloud Schule“ (ByCS) ausschrieb, setzte sich ein Tandem aus dem IT-Konzern Fujitsu und dem Koblenzer Unternehmen Sdui durch. Sdui übernahm den Quellcode der Element-Clients und des Synapse-Servers und entwickelte im Auftrag Bayerns Anpassungen. Die Quelltexte dieser Anpassungen wurden ebenfalls nicht der Matrix-Community übergeben.

Die Anpassungen seien „speziell auf die Bedürfnisse der bayerischen Schulen zugeschnitten“, eine Bereitstellung ergäbe deshalb „keinen konkreten Nutzen für Produkte außerhalb der ByCS“, rechtfertigte sich das bayerische Kultusministerium auf Anfrage. Diese Argumentation kann man hinterfragen, denn zu den Anpassungen gehörte laut Ministerium beispielsweise auch eine „PIN-Sperre für einzelne Räume zur Erhöhung der Sicherheit“.



Zur „BayernCloud Schule" gehört ein Messenger auf Matrix-Basis. Bayern nutzt allerdings eine seit Ende 2023 veraltete Version des Chatservers.

Sogar zu Sicherheitsrisiken kann die Trittbrettfahrerei führen. Denn wenn Dumpinganbieter bekannte Lücken nicht schnell genug schließen oder die Software ungeschickt konfigurieren, steigt die Gefahr von Datenlecks und Hackerangriffen.

Im Fall des bayerischen Schul-Messengers fällt auf, dass der dort verwendete Chatserver noch bei Redaktionsschluss auf Version 1.97.0 von Synapse basierte, die seit Dezember 2023 veraltet ist. Im Hauptzweig von Synapse hat Element seitdem zahlreiche Sicherheitslücken geschlossen, darunter zwei als schwerwiegend eingestufte.

Das Kultusministerium sieht dennoch kein Problem darin, die alte Version einzusetzen. Dies sei „Teil einer bewussten Strategie". Die Sicherheitslücken beträfen die bayerische Konfiguration nicht oder es seien keine Auswirkungen zu erwarten. Updates würden aber kontinuierlich evaluiert, obendrein habe das Landesamt für Sicherheit in der Informationstechnik das System getestet und freigegeben.

Bei Forks wie in Bayern oder Hessen gilt jedoch grundsätzlich: Je tiefgehender und umfangreicher die Anpassungen, desto aufwendiger wird es, Sicherheitspatches und andere Updates aus der Community einzubauen.

Patrick Alberts, der Produktchef der Entwicklerfirma Element, sorgt sich deshalb, dass die Strategie des Ministeriums „nicht nachhaltig ist und irgendwann zu einem Cybervorfall in den Schulen führen könnte". Darunter würde dann auch die Marke Ma-

trix leiden und „Open Source insgesamt als mal wieder nicht so sicher abgestempelt“, sagte er im Gespräch mit c’t.

Sdui antwortete auf die Frage von c’t nach konkreten Beispielen für Vertragsbeziehungen zu Open-Source-Herstellern nur ausweichend. Man gehe auf Anforderungen der Bundesländer ein und richte sich nach den entsprechenden öffentlichen Ausschreibungen, erklärte das Unternehmen.

Die c’t-Recherchen lösten wohl ein Umdenken in Bayern aus. Das Kultusministerium teilte mit, dass der beauftragte Dienstleister – gemeint ist Sdui – sich mit der Element Software GmbH in Gesprächen über eine mögliche Zusammenarbeit befinde. „Dies ist insbesondere aufgrund der Größe und Bedeutung des Projekts erforderlich, um langfristige Wartung und Weiterentwicklung zu gewährleisten.“ Sdui und Element zeigten sich auf Nachfrage beide zuversichtlich, aber bis Redaktionsschluss gab es keinen Abschluss.

OSBA-Forderungen:
ct.de/wr42

Sdui ist auch bei weiteren Ausschreibungen von Behörden zum Zug gekommen. Zum Beispiel stellt das Unternehmen für das Land Berlin eine Videokonferenzlösung auf Basis der Open-Source-Anwendung BigBlueButton bereit.

Die OSBA hofft nun, dass Behörden ihre Ausschreibungen künftig so gestalten, dass Dumpinganbieter nicht mehr im Vorteil sind. In einem Positionspapier (ct.de/wr42) schlägt der Verband Kriterien für die „nachhaltige Beschaffung von Open-Source-Software“ vor. Die Behörden sollen künftig zum Beispiel prüfen, ob der Anbieter eine Geschäftsbeziehung zum Softwarehersteller hat, ob er Änderungen an der Software im Sinne des Grundsatzes „Public Money, Public Code“ für die Allgemeinheit verfügbar macht und ob er einen hochwertigen Support leisten kann.

Manche Behörden setzen solche Kriterien bereits heute um. Als Positivbeispiel gilt in der Open-Source-Community etwa das Zentrum für digitale Souveränität (ZenDiS), das bei der Entwicklung seiner Web-Office-Suite mit Entwicklern wie Nextcloud, Univention und Open-X-Change zusammenarbeitet. Aber auch die Bundesländer Schleswig-Holstein und Thüringen werden von Entwicklern häufig als Positivbeispiele genannt. (cwo) c't

Portokasse für Open-Source-Tech

In der digitalen Infrastruktur steckt allerorts Open-Source-Software aus unzähligen Projekten. An der Finanzierung, die deren kontinuierliche Pflege und Weiterentwicklung sicherstellt, hapert es häufig. Seit Herbst 2022 verkleinert die Bundesrepublik diese Lücke, zunächst mit dem Sovereign Tech Fund, aus dem die Sovereign Tech Agency entstand.

Von **Keywan Tonekaboni**

Open-Source-Software hat sich zwar praktisch überall durchgesetzt. Doch Sicherheitslücken wie Heartbleed in OpenSSL, Log4Shell in Log4j oder der Angriff auf die xz-utils haben gezeigt, dass man quelloffene und freie Software auch pflegen muss. Daran beteiligen sich Nutzer, gemeint sind insbesondere Firmen und Institutionen, aber nur unzureichend. Hier setzte die vorherige Bundesregierung an und startete im Herbst 2022 den Sovereign Tech Fund (STF). Noch vor dem Bruch der Ampel-Koalition wurde dessen Arbeit in der neu gegründeten Sovereign Tech Agency verstetigt.

Doch zunächst ein Blick zurück auf den Anfang. Die Einrichtung des Sovereign Tech Fund kündigte Ende Dezember 2021 Franziska Brantner (Bündnis 90/Die Grünen), die damalige parlamentarische Staatssekretärin im Wirtschaftsministerium, per Tweet an. Das war kurz nach Bekanntwerden der Sicherheitslücke Log4Shell und auf das davon betroffene Projekt Log4j verwies Brantner. Um die „digitale Souveränität [und] Innovationskraft der deutschen Wirtschaft“ zu erhalten, sollen mit dem Sovereign Tech Fund „Open-Source Basistechnologien“ gefördert werden, begründete Brantner die

Initiative. Die ersten sieben Open-Source-Projekte der Pilotphase konnten im Oktober 2022 loslegen und deckten ganz unterschiedliche Bereiche ab: Curl, was neben dem gleichnamigen Kommandozeilen-Tool auch eine wichtige Bibliothek für Dateiübertragungen bereitstellt; RubyGems und Bundler, eine Paketverwaltung für Ruby-Programme; OpenSSH und OpenPGP, bei Letzterem die JavaScript- und Go-Implementierungen; das VPN-Protokoll WireGuard; aber auch OpenMLS (Ende-zu-Ende-Verschlüsselung von Nachrichten) sowie OpenBGPd, eine freie Implementierung des Routingprotokolls BGP.

Seitdem hat der Sovereign Tech Fund nach eigenen Angaben 60 Projekte unterstützt und in diese 23,5 Millionen Euro investiert. Insgesamt 195 „unterstützungswürdige Technologien" seien vom STF identifiziert und über 500 Anträge bisher eingereicht worden. Die Vielfalt der Projekte hat sich seit der Pilotphase noch vergrößert. Gefördert wurden und werden bekanntere Projekte wie Gnome, Samba oder Systemd ebenso wie welche für Spezialisten, etwa Yocto (Betriebssysteme für IoT-Geräte bauen) oder OpenBLAS (Bibliothek für lineare Algebra).

„Es geht um Tools, die andere Entwickler*innen nutzen, um selbst Software herzustellen oder zu ermöglichen", erklärt Powen Shiah, Kommunikationsmanager des STF, im Gespräch mit c't. „Unser Ziel ist die Stärkung des Open-Source-Ökosystems, auf das alle in der modernen Gesellschaft eigentlich angewiesen sind, auch wenn wir es nicht wissen."

Per X, früher Twitter, kündigte die grüne Staatssekretärin Brantner 2021 den Sovereign Tech Fund an.

Obwohl der Sovereign Tech Fund nachhaltige Förderung von digitalen Infrastrukturen und des Open-Source-Ökosystems fördert und explizit keine Innovationen, war er zunächst bei SPRIND angesiedelt, der Bundesagentur für Sprunginnovationen. Das hatte ganz pragmatische Gründe, denn der STF sollte möglichst schnell loslegen. Die SPRIND GmbH stellt die Strukturen wie Verwaltung und einen rechtlichen Rahmen bereit. Seit Herbst 2024 hat der STF mehr Eigenständigkeit bekommen, indem er in die eigens gegründete SPRIND-Tochtergesellschaft Sovereign Tech Agency (STA) ausgegliedert wurde. Unter dem Dach der Agency laufen neben dem eigentlichen STF noch das Bug-Resilience-Programm und weitere Projekte.

Push und Pull

Um Projekte für die Förderungen – genannt Investitionen – auszuwählen, arbeitet der STF mit zwei Ansätzen.

Projekte können sich bewerben, indem sie ein Online-Formular ausfüllen. Im Vergleich zu Anträgen für andere staatliche Programme beschränken sich die Fragen auf das Wesentliche. Antragsteller müssen übrigens nicht aus Deutschland kommen. Hingegen setzt der STF bei den geschätzten Kosten mindestens 50.000 Euro voraus, betreibt also keine Mikroförderung.

Um das Ziel zu erreichen, für die Allgemeinheit nützliche Basistechnologien zu stärken, verlässt sich der Sovereign Tech Fund nicht allein auf eingereichte Bewerbungen, sondern versucht auch von sich aus wichtige Komponenten und Projekte zu identifizieren. Das übernehmen Scouts, die dafür in der Open-Source-Community – etwa auf Konferenzen – unterwegs sind.

In beiden Fällen durchlaufen eingereichte oder identifizierte Kandidaten das gleiche Verfahren. Zunächst prüft eine weitere interne Stelle, ob sie die Voraussetzungen wie Relevanz, Verbreitung und Vulnerabilität erfüllen und ob es im Projekt die notwendige Expertise gibt.

Sind diese Voraussetzungen erfüllt, erarbeitet das Programmteam des STF gemeinsam mit den Projekten den Projektrahmen. „Das nennen wir Scoping", erläutert Kommunikations-Manager Powen Shiah. „Dieser Arbeitsplan beinhaltet dann Milestones, die dann im Dienstleistungsvertrag festgehalten werden." Der Projektplan wird anschließend noch von externen Experten begutachtet.

Das ganze Verfahren dauert, vom Zeitpunkt der Bewerbung bis ein Projekt beginnen kann, in der

Die Bauklötzchengrafik auf der Webseite des Sovereign Tech Funds spielt auf ein bekanntes xkcd-Comic an (siehe ct.de/wh42).

Regel gut sechs Monate. Die Projektvorhaben haben häufig eine Laufzeit von 12 bis 18 Monaten.

Unbürokratische Bürokratie

Während der Durchführungsphase sollen die Projekte sich auf die Umsetzung der vereinbarten Ziele konzentrieren. Berichte werden auch in Form von Links zu Pull-Requests akzeptiert. „Wir versuchen immer Komplexität zu internalisieren, damit wir nicht noch mehr Arbeit auf die schon überlasteten Open-Source-Maintainer abladen“, betont Powen Shiah.

Fragt man bei bisher finanzierten Projekten nach, bestätigen diese die unbürokratischen Abläufe. „Es hätte von deren Seite nicht besser sein können“, meint Tobias Bernard, der im Gnome-Projekt die Förderung durch das STF mitorganisiert hat. Das sieht auch Neal Walfield von Sequoia PGP so, einer modernen OpenPGP-Implementierung. „Der Sovereign Tech Fund hat uns bei der Umsetzung unseres Projekts relativ viel Freiheit gelassen“, betonte Walfield gegenüber c’t. „Sie vertrauten darauf, dass wir wissen, was das Beste für das Projekt ist. Das war sehr entspannend.“ Sequoia PGP erhielt zweimal eine Finanzierung vom STF, wobei sie im ersten Jahr übers Scouting ohne eigene Bewerbung angesprochen wurden.

Neben den allgemeinen Investitionen gibt es noch weitere Programme wie das Bug-Resilience-Programm. Dieses soll helfen, Schwachstellen in verbreiteten Open-Source-Komponenten zu identifizieren. Man zahle nicht nur für das bloße Finden von Fehlern, hebt Powen Shiah hervor, „sondern auch für die Fixes, weil das sonst einfach eine Last für die Projekte wäre und kein Gewinn.“ Für das Bug-Resilience-Programm arbeitet der STF mit der Plattform YesWeHack zusammen.

Relativ neu ist das „Fellowship für Maintainer*innen“, ein Stipendium für Projektleitungen von Open-Source-Software. Hier werden aktuell fünf Personen für ein Jahr auf freiberuflicher Basis bezahlt, um sich auf ihre Aufgabe als Maintainer zu konzentrieren. Eine weitere Person ist für den Zeitraum als „Maintainer*in-in-Residence“ bei der STF angestellt.

Strategie oder Feigenblatt?

All diese Programme kosten Geld. Die alte Ampel-Bundesregierung hatte schon geplant, das Budget für das kommende Jahr von 17 auf 15 Millionen Euro zu kürzen, aber in den Haushaltsverhandlungen wurden die Mittel dann sogar auf 19 Millionen Euro aufgestockt. Davon sollten zwei Millionen Euro auf das Bug-Resilience-Programm fallen. Das Ganze wurde Makulatur, als die Ampel-Koalition zerbrach und vor den vorgezogenen Neuwahlen für 2025 kein Haushalt mehr verabschiedet wurde. Zu Redaktionsschluss prangt auf der Webseite der Sovereign Tech Agency ein Hinweis, dass aufgrund der vorläufigen Haushaltsführung es zu längeren Entscheidungs-

phasen über Investitionen seitens des STF kommt. Die Arbeit gehe im kleinerem Rahmen weiter und der Planungshorizont sei derzeit kürzer, heißt es aus der Sovereign Tech Agency.

Die c't fragte damals in dem Zuge bei allen Bundestagsfraktionen um deren Einschätzung. Die Statements der Abgeordneten sind weiterhin aufschlussreich, auch wenn bis auf den CSU-Abgeordneten Reinhard Brandl alle anderen MdB mittlerweile nicht mehr dem aktuellen 21. Deutschen Bundestag angehören.

Der damalige digitalpolitische Sprecher der SPD-Bundestagsfraktion, Jens Zimmermann, sah darin ein „wichtiges Signal, dass wir auch in Zeiten begrenzter Haushaltsmittel den Sovereign Tech Fund weiter stärken". „Ich kenne kein Programm der Bundesregierung, das investierte Euros effektiver in IT-Sicherheit umwandelt als dieses", meinte die grüne Bundestagsabgeordnete Sabine Grützmacher.

Der FDP-Bundestagsabgeordnete Volker Redder, damals noch Obmann im Digitalausschuss, sagte, der STF sei zwar ein „essenzieller Beitrag [...] zur Stärkung der digitalen Souveränität und Cybersicherheit Deutschlands", war aber insgesamt zurückhaltender. Er plädierte für eine „initiierende Anschubhilfe", denn „staatliche Förderung darf keine dauerhafte Lösung sein."

Zustimmung in der Sache, aber Kritik am Vorgehen der Bundesregierung kam von der Abgeordneten Anke Domscheit-Berg, die da noch digitalpolitische Sprecherin von Die Linke im Bundestag war: Die Finanzierung des STF müsse „einerseits höher und langfristig gesichert werden."

CSU-Abgeordneter Brandl, damals ebenfalls Mitglied im Digitalausschuss, vermisste eine „aufeinander abgestimmte Open-Source-Politik". Hingegen habe die damalige Bundesregierung einen „Löwenanteil der Mittel zum Aufbau der digitalen Verwaltung für proprietäre Software außereuropäischer Hersteller" ausgegeben. Er plädierte außerdem für die Weiterentwicklung des Sovereign Tech Fund, um darüber auch Open-Source-KI zu fördern.

Die Kritik einer widersprüchlichen Open-Source-Strategie teilten damals auch Open-Source-Verbände. „Der Sovereign Tech Fund (STF) [...] gehört zweifelsohne zu den – wenn auch leider zahlenmäßig überschaubaren – erfolgreichen Open-Source-Vorhaben der Bundesregierung", meint Peter Ganten, Vorstandsvorsitzender der Open Source Business Alliance. Allerdings mahnt er auch: „Aus unserer Sicht sollte der STF in der öffentlichen Diskussion aber nicht als Feigenblatt dazu verwendet werden, über die mangelnde Geschwindigkeit bei der grundlegenden Open-Source-Transformation in der öffentlichen Verwaltung hinwegzutäuschen."

Doch wie sieht es aus, wo jetzt die Union in der aktuellen Bundesregierung die Federführung hat? Auf Nachfrage von c't lobte ein Sprecher des noch im Aufbau befindlichen neuen Bundesministeriums „für Digitales und Staatsmodernisierung" (BMDS) die Arbeit der Sovereign Tech Agency. „Sie hat sich innerhalb weniger Jahre zu einem national wie auch international viel beachteten Akteur des Open-Source-Ökosystems entwickelt", so der Sprecher des BMDS. „Die Sovereign Tech Agency wird ihre erfolgreiche Arbeit auch in der neuen Legislaturperiode fortsetzen." Bleibt abzuwarten, wie sich das nach der Sommerpause in den Haushaltsverhandlungen manifestiert.

Anscheinend sieht man aber mittlerweile die strategische Bedeutung. In dem Statement des Digitalministeriums gegenüber c't heißt es weiter: „Die Sovereign Tech Agency leistet einen wichtigen Beitrag zur Stärkung der digitalen Souveränität Deutschland und Europas." Die Sovereign Tech Agency solle ihre Erfahrungen als „Wegbereiter für die Förderung von offenen digitalen Basistechnologien [...] auch in das geplante European Digital Infrastructure Consortium (EDIC) im Bereich digitaler Gemeinschaftsgüter" einbringen. Das OpenForum Europe veröffentlichte erst kürzlich Machbarkeitsstudie zu einem EU Sovereign Tech Fund (EU-STF). Adriana Groh, Mitgründerin und CEO der Sovereign Tech Agency findet: „Die Studie zum EU-STF unterstreicht, was wir seit 2022 vertreten: schlanke, unabhängige und zielgerichtete Investitionsstrukturen stärken das Open-Source-Ökosystem wirkungsvoll und sichern die Basis für Innovation, Wettbewerbsfähigkeit und Resilienz." Man freue sich darauf, gemeinsam mit weiteren Mitgliedstaaten und Akteuren auf EU-Ebene daran zu arbeiten.

Dass kaum jemand den Sovereign Tech Fund grundsätzlich infrage stellt oder gar von der neuen Bundesregierung abgewickelt wird, zeigt, wie erfolgreich der STF agiert, wenn auch mit überschaubarem Budget. Von seiner Arbeit profitieren Unternehmen, aber auch andere staatliche Einrichtungen und die Zivilgesellschaft, die diese Komponenten für den Aufbau eigener digitaler Infrastruktur benötigen. Den Nutzen haben auch Akteure im europäischen Ausland erkannt, weshalb es Bestrebungen gibt, einen STF auch auf EU-Ebene zu installieren. Bleibt zu hoffen, dass sowohl im Bund als auch der EU das Unterfangen ausreichend finanziert wird. (ktn) c't

STF-Ankündigung und weitere Infos

ct.de/wh42

Das Self-Hosting-Kompendium

Bild: KI, Collage c't

Der Clouddienst nervt, wird immer teurer und Sie wollen endlich unabhängig werden? Das brauchen Sie, um Anwendungen von Webserver über Dateispeicher bis Hausautomation und Bildergalerie sicher zu Hause zu betreiben.

Von **Jan Mahn**

Self-Hosting ist digitale Selbstversorgung. Auf dem eigenen Raspberry Pi oder NAS sowie auf selbst betriebener oder gemieteter Serverhardware laufen problemlos Dateiablagen, Blogs, Chatserver, kollaborative Office-Suiten und vieles mehr. Damit versorgen Sie nicht nur sich selbst, sondern auch Ihre Familie oder gar ein kleines Büro oder einen Verein. Wer in der glücklichen Lage ist, einen wirklich breitbandigen Breitbandanschluss buchen zu dürfen, kann auch von unterwegs ruckelfrei auf die selbst betriebenen Dienste zugreifen.

Dennoch galt Self-Hosting lange als Hobby, an dem sich nur unbelehrbare Bastler und IT-Nostalgiker erfreuen konnten – alle anderen genossen in den vergangenen Jahren den Komfort, den fertige Angebote aus der Cloud versprachen: Software-as-a-Service, also von anderen verwaltete Rundumsorglos-Pakete. Doch spätestens seit die USA mit großem Tamtam an ihrem Status als verlässlicher Handelspartner sägen und sowohl Nutzer als auch Unternehmen darüber nachdenken, ob und wie man US-Schwergewichten entkommen kann, ist auch Self-Hosting als eine mögliche Strategie wieder im Trend. Mit Self-Hosting bezeichnen wir im Folgenden alle Formen von selbst betriebenen Diensten, die Sie unter eigener Kontrolle haben: Das kann auf Hardware sein, die Sie selbst besitzen, aber auch auf virtuellen oder physischen Maschinen, die Sie angemietet haben und die in einem Rechenzentrum stehen.

Haben Sie Ihre Familie überredet, die kommerziellen Clouddienste zu deaktivieren und Kontakte und Termine auf Ihrem Server abzulegen, wird Ihr Handy schlimmstenfalls auch nachts klingeln, wenn der Server Schluckauf hat.

Was hosten?

An Serversoftware, zumeist Open Source, die man selbst betreiben kann, mangelt es wahrlich nicht. Viele aktive und große Communities pflegen Projekte, die sich im Funktionsumfang nicht hinter kommerziellen Angeboten verstecken müssen. Nextcloud, die Dateiablage, die so viel mehr ist als eine schnöde Ablage, fällt zweifelsohne in diese Kategorie. Im nachfolgenden Kasten finden Sie eine Liste mit Software, deren Eigenbetrieb wir schon erfolgreich getestet haben und empfehlen können. Um konkrete Software soll es in dieser Artikelreihe jedoch nicht gehen, sondern um alles, was Sie für den sicheren und stabilen Betrieb sonst noch wissen müssen: von der Einrichtung der Internetverbindung bis zum Software-Unterbau und zur Security. Vor allem geht es um Entscheidungen. Denn vorm Selbsthosten gilt es einige davon zu treffen.

Worte der Warnung

Hic sunt dracones! Wenn Sie bis zu diesem Punkt gelesen haben, sind Sie womöglich fest entschlossen, einen Serverdienst auf heimischer Infrastruktur zu betreiben und aus dem Internet erreichbar zu machen. Das möchte Ihnen diese Artikelreihe keineswegs ausreden und Sie vielmehr mit dem nötigen Wissen für dieses Vorhaben ausstatten. Gleichzeitig ist aber eine Warnung angebracht: Damit Sie Dienste aus dem Internet ansprechen können, müssen Sie die Firewall Ihres Routers gezielt durchlöchern. Dieser digitale Schutzwall grenzt Ihr heimisches Netz in der Standardeinstellung vom Internet ab und lässt alle Anfragen von außen kategorisch abprallen.

Mit der bewussten Entscheidung, die Tür einen Spalt weit zu öffnen, werden Sie zum Serverbetreiber im weltweiten Internet. Dass sich dort nicht nur freundlich gesinnte Surfer herumtreiben, sollte sich allgemein herumgesprochen haben. Das bedeutet kein unkalkulierbares Risiko und Panik wäre unangebracht. Leichtfertig sollten Sie jedoch niemals Dienste im Internet veröffentlichen. Sichere Passwörter, am besten Zweifaktorauthentifizierung, sind genauso Pflicht wie die stets aktuelle Version Ihrer Software: Updates nicht einzuspielen, ist als Admin keine Option. Aber keine Angst: Für die automatische Pflege Ihrer Server gibt es probate Hilfsmittel, die wir im Artikel ab Seite 64 vorstellen.

Ab Seite 70 widmen wir uns dann verschiedenen Strategien, wie Sie das Tor zur Außenwelt gezielt öffnen und verschlüsselte Verbindungen von unterwegs auf ihre selbstverwalteten Dienste herstellen. Für Fortgeschrittene, die mehrere Standorte betreiben, eigene Domains einsetzen oder einen ganzen Zoo an Diensten veröffentlichen, empfehlen wir den weiterführenden Artikel ab Seite 78.

Unsere abschließende Warnung betrifft weniger technische als vielmehr zwischenmenschliche Probleme: Sobald Sie nicht mehr alleiniger Nutzer Ihres Servers sind, die Nextcloud beispielsweise Freunden und Verwandten bereitstellen, sind Sie verantwortlich für den reibungslosen Betrieb. Haben Sie Ihre Familie überredet, die kommerziellen Clouddienste zu deaktivieren und Kontakte und Termine auf Ihrem Server abzulegen, wird Ihr Handy schlimmstenfalls auch nachts klingeln, wenn der Server Schluckauf hat. Bevor Sie anderen digitales Obdach gewähren,

sammeln Sie erste Erfahrungen mit sich selbst als einzigem Nutzer.

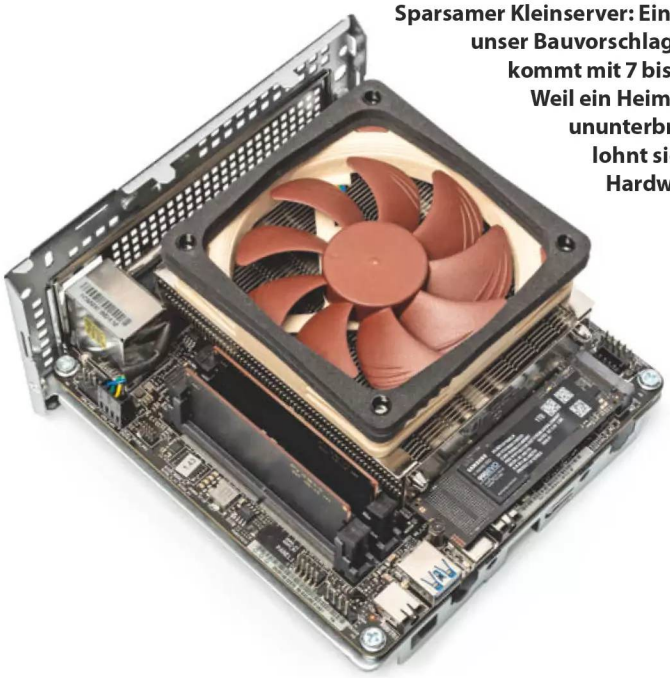
Welches Gerät?

Nach dieser Vorrede ist es Zeit für etwas Hardwarekunde für angehende Serverbetreiber. Die gute Nachricht: Server kann jeder Computer sein, der dauerhaft über das Netzwerk erreichbar ist und einen Serverdienst, zum Beispiel einen Webserver, ausführt. Technisch gesehen könnte jeder ausgemusterte Desktop-PC und jedes Notebook als Server laufen. Empfehlenswert ist das jedoch nicht, weil Self-Hosting damit schnell unwirtschaftlich wird. Schuld ist der Energiebedarf: Ein Monat hat im Schnitt 730 Stunden, schon ein Rechner mit 50 Watt Leistung genehmigt sich im Dauerbetrieb 36,5 Kilowattstunden Strom über diesen Zeitraum. Bei einem realistischen Einkaufspreis von 30 Cent sind das bereits saftige 11 Euro Stromkosten im Monat.

Weil die Stromaufnahme ein entscheidender Faktor für die Wirtschaftlichkeit des Heimbetriebs ist, sind vor allem Mini- und Einplatinencomputer beliebte Hardwareplattformen für zu Hause. Allen voran der Raspi mit seinem genügsamen ARM-Prozessor: Beim aktuellen Raspberry Pi 5 mit 16 GByte RAM maßen wir im Leerlauf eine Leistung von 2,95 Watt, was etwa 2 Kilowattstunden Strom im Monat entspricht. Soll der Heimserver auch große Datenmengen speichern, also zum Beispiel die Foto-, Film- oder Dokumentensammlung beherbergen, ist oft ein NAS das Mittel der Wahl. Wie hoch die Stromkosten im Monat sind, hängt maßgeblich von der Festplattenbestückung ab.

Zwischen Raspberry Pi und Desktop-PC liegen in Sachen Strombedarf die Mini-PCs. In Ausgabe 17/2024 haben wir einen Bauvorschlag vorgestellt, der mit 7 bis 10 Watt auskommt und nicht nur als Desktop-PC, sondern auch als Heimserver dienen kann [1]. Die monatlichen Stromkosten liegen bei bis zu 2,20 Euro – die Anschaffungskosten bei 600 Euro. Die müssen Sie für die Kalkulation auf eine realistische Nutzungszeit umlegen. Eine weitere Option: gebrauchte Thin Clients, die man schon ab 90 Euro ergattern und mit einer SSD ausrüsten kann.

Wer bereit ist, sich von der engen Definition des Self-Hostings im Sinne von „eigene Hardware, eigener Strom“ zu verabschieden, kann darüber nachdenken, virtuelle Maschinen bei einem Hoster zu mieten. Die bekommt man, gerade im Vergleich zu den oben genannten Hardware- und Stromkosten, erstaunlich günstig. Eine solche Miet-VM enthält nur ein nacktes Server-Betriebssystem, auf dem es genauso viel zu entscheiden, konfigurieren und pflegen gibt wie auf eigener Hardware. Volle Kontrolle, aber auch die volle Verantwortung.



Sparsamer Kleinserver: Ein Mini-PC wie unser Bauvorschlag mit Ryzen 5 kommt mit 7 bis 10 Watt aus. Weil ein Heimserver meist ununterbrochen läuft, lohnt sich sparsame Hardware über die Laufzeit.

Wenn virtuelle Mietserver für Sie infrage kommen, finden Sie am Ende dieses Abschnittes in der Tabelle exemplarisch Angebote bei deutschen und europäischen Hostern. Sobald Sie Strom- und Hardwarekosten für eigene Server gegenrechnen, werden Sie schnell feststellen, dass sich solche Angebote durchaus lohnen können.

Leichter fällt die Entscheidung für eigene Hardware, sobald Sie diese auch für Aufgaben einsetzen, für die sie in den eigenen vier Wänden stehen muss: Eine Smart-Home-Zentrale beispielsweise, die womöglich auch Funk-Sticks für Protokolle wie Zigbee ansteuert, oder das Backup-Ziel für die lokalen PCs sind zu Hause besser aufgehoben als irgendwo im Rechenzentrum.

Falls Sie die Kosten für Selbstbetrieb oder Mietserver jetzt vom Self-Hosting abschrecken, sollten Sie gegenrechnen, welche Abos bei Cloud-Anbietern Sie vielleicht perspektivisch sparen können.

Exemplarische Angebote bei deutschen Hostern			
Anbieter	**Produkt**	**Beschreibung**	**Preis pro Monat**
Hetzner	vServer CX22 mit 2 vCPU-Kernen und 4 GByte RAM	virtueller Server mit Linux	4,51 €
Hetzner	StorageBox 21 mit 5 TByte	Speicherplatz als Backup-Ziel oder Datenhalde	13 €
IONOS	VPS XS mit 1 vCPU-Kern und 1 GByte RAM	virtueller Server mit Linux	1 € (Einrichtung: einmalig 10 €)
Netcup	VPS 250 G11s mit 2 vCPU-Kernen und 2 GByte RAM	virtueller Server mit Linux	3,99 €

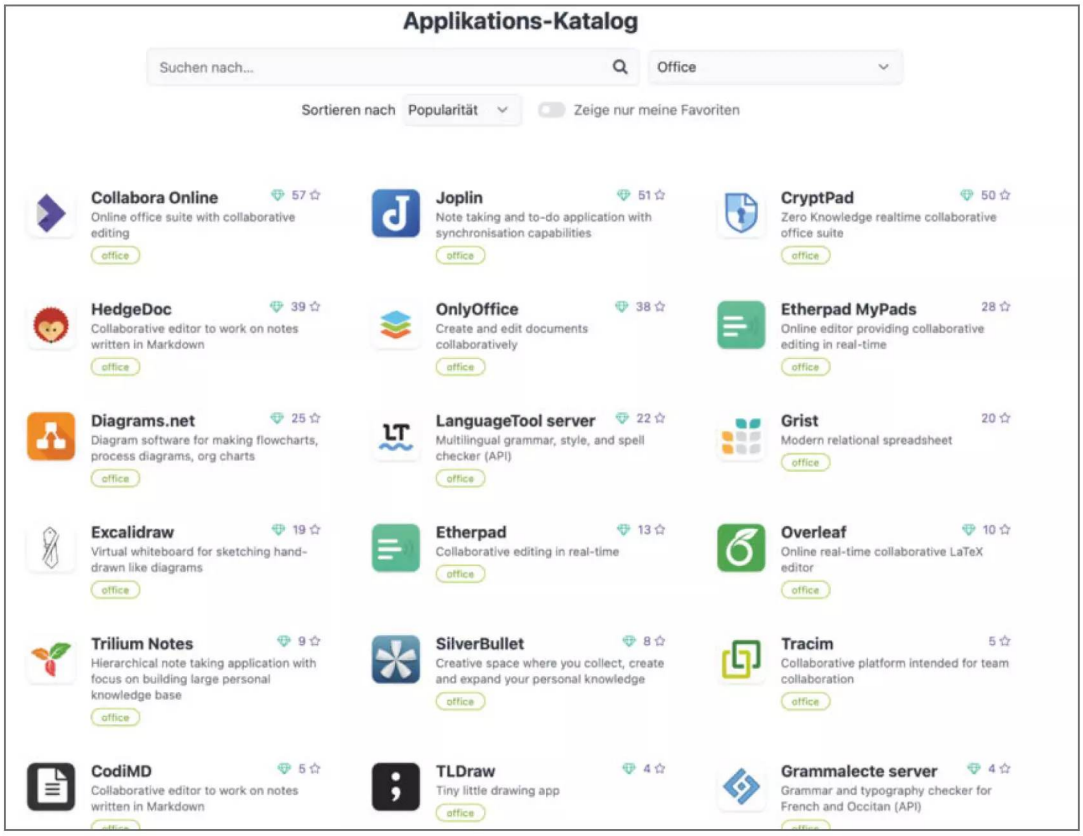
Softwareauswahl

Eng mit der Wahl der Hardware verbunden ist die Wahl des Serverbetriebssystems. Windows mag für Nutzer von Windows 10 oder 11 auf dem Desktop wie eine naheliegende Wahl erscheinen. Richtig ist: Es gibt von Microsoft eine Windows-Variante namens Windows Server. Erste Wahl für Self-Hosting ist Windows Server aber nicht. Seine Stärken spielt er aus, wenn er interne Serverdienste für ein Windows-Netzwerk (zum Beispiel Active Directory, Druck- und Dateiserver) bereitstellen soll, wie es in Firmennetzen üblich ist.

Unsere Empfehlung für Heimserver jeder Art ist klar Linux. Weil man das immer in Form einer Distribution installiert und nicht einfach den nackten Linux-Kernel herunterlädt, steht man direkt vor der nächsten Entscheidung: Distributionen gibt es viele und es lässt sich vortrefflich streiten, welche für Einsteiger ins Self-Hosting die beste ist. In jedem Fall bietet sich eine Distribution an, die es in einer Variante ohne grafische Oberfläche gibt. Einen grafischen Desktop brauchen Sie für den Serverbetrieb nicht, den sollten Sie sich sparen.

Für Neulinge empfiehlt sich aus unserer Sicht eine Distribution, die den Debian-Paketmanager Apt für die Installation eingebaut hat. Der große Vorteil: Die allermeisten Linux-Anleitungen, denen Sie begegnen werden, erklärt die Installation mindestens mit Apt und nur manchmal auch mit anderen Paketmanagern. Steigen Sie beispielsweise mit Ubuntu Server ohne grafische Oberfläche ein. Wenn Sie sich für einen Raspberry Pi als Hardware entscheiden, ist Raspberry Pi OS das gängigste Betriebssystem. Das ist ein Ableger von Debian und optimiert für den Betrieb auf dem ARM-Prozessor des Raspis.

Auf einem NAS stellt sich die Betriebssystemfrage auf den ersten Blick nicht, dort können Sie das (meist ebenfalls Linux-basierte) System nutzen, das der Hersteller sich dafür ausgedacht hat – wenn Sie sich nicht für eine Open-Source-Alternative wie TrueNAS entscheiden. Für ein NAS als Einsteigergerät



Es kann so einfach sein: Mit einem Unterbau wie YunoHost installieren Sie Serversoftware mit wenigen Klicks. Grundwissen über Linux und die Technik im Unterbau sollten Sie sich dennoch aneignen – spätestens bei Problemen werden Sie dafür dankbar sein.

spricht auf den ersten Blick, dass die Hersteller viele Alltagsaufgaben hinter grafischen Weboberflächen verstecken und Sie nicht am ersten Tag mit SSH und Kommandozeile hantieren müssen. Andererseits: Wie Sie ab Seite 64 lesen, gehört genau das zum Self-Hosting dazu, und spätestens bei Problemen ist solches Handwerkszeug essenziell.

Ein NAS kann man jedoch auch anders nutzen: als Gastgeber für virtuelle Maschinen, sofern die Hardware für Virtualisierung geeignet ist. Wenn Sie Serverdienste und reinen Dateispeicheralltag des NAS trennen wollen, aktivieren Sie im NAS-Betriebssystem die Virtualisierungsfunktion und richten eine VM mit einem Linux-Serversystem ein.

Einsteigerfreundliche grafische Oberflächen, die große Teile der Einrichtung verstecken, bekommen Sie auch abseits der NAS-Betriebssysteme zum Beispiel mit Systemen wie YunoHost oder Unraid (kostenpflichtig). Wie bei den NAS gilt: Spätestens bei schwerwiegenden Problemen sind Sie dankbar, wenn Sie sich von Anfang an mit Kommandozeile und technischem Unterbau vertraut gemacht haben.

Loslegen

Die beste Zeit, um mit dem Self-Hosting loszulegen, ist jetzt! Nie zuvor war es so leicht wie heute. Software muss heute, Technik wie Containerisierung sei Dank, nicht mehr zu Fuß installiert und verdrahtet werden. Hat man sich einmal eingerichtet, läuft ein neuer Dienst in wenigen Minuten.

Die wichtigsten Zutaten haben Sie vermutlich bereits: einen Internetanschluss und irgendwas, das als Linux-Server herhalten kann. Bevor Sie Ihr Abo bei Google und Dropbox kündigen können, gibt es zwar noch viel zu lernen, aber Sie öffnen mit dem ersten selbst betriebenen Dienst die Tür für ein vergnügliches Hobby. Wenn Sie Self-Hosting als solches sehen, müssen Sie den Bleistift für die Wirtschaftlichkeitsrechnung nicht allzu sehr spitzen. (jam) **c't**

Bild: KI, Collage c't

Werkzeugkunde für Server-Admins

Wer erstmals selbst Serverdienste betreiben will, muss sich früher oder später mit ungewohntem Handwerkszeug auseinandersetzen. Wir geben einen Überblick, damit Sie wissen, was auf Sie zukommt, und im Notfall keine unliebsamen Überraschungen erleben.

Von **Jan Mahn, Peter Siering und Sylvester Tremmel**

Ein verbreiteter Witz lautet: Es gibt keine Cloud, das sind nur die Computer von jemand anderem. Der Spruch enthält einen wahren Kern; mit einem eigenen Server sorgen Sie dafür, dass es wieder (oder erstmals?) Ihre eigenen Computer sind, auf denen Ihre Dienste laufen – oder zumindest Computer, die Sie kontrollieren. Aber obwohl Server auch bloß Computer sind, gibt es einige Unterschiede im Vergleich zu PCs oder Laptops, mit denen Sie sich vertraut machen sollten, wenn Sie unter die Selbst-Hoster gehen.

Kopflos auf der Kommandozeile

Der vielleicht wichtigste Unterschied: Server betreibt man meistens „headless“, also ohne Kopf. Damit ist

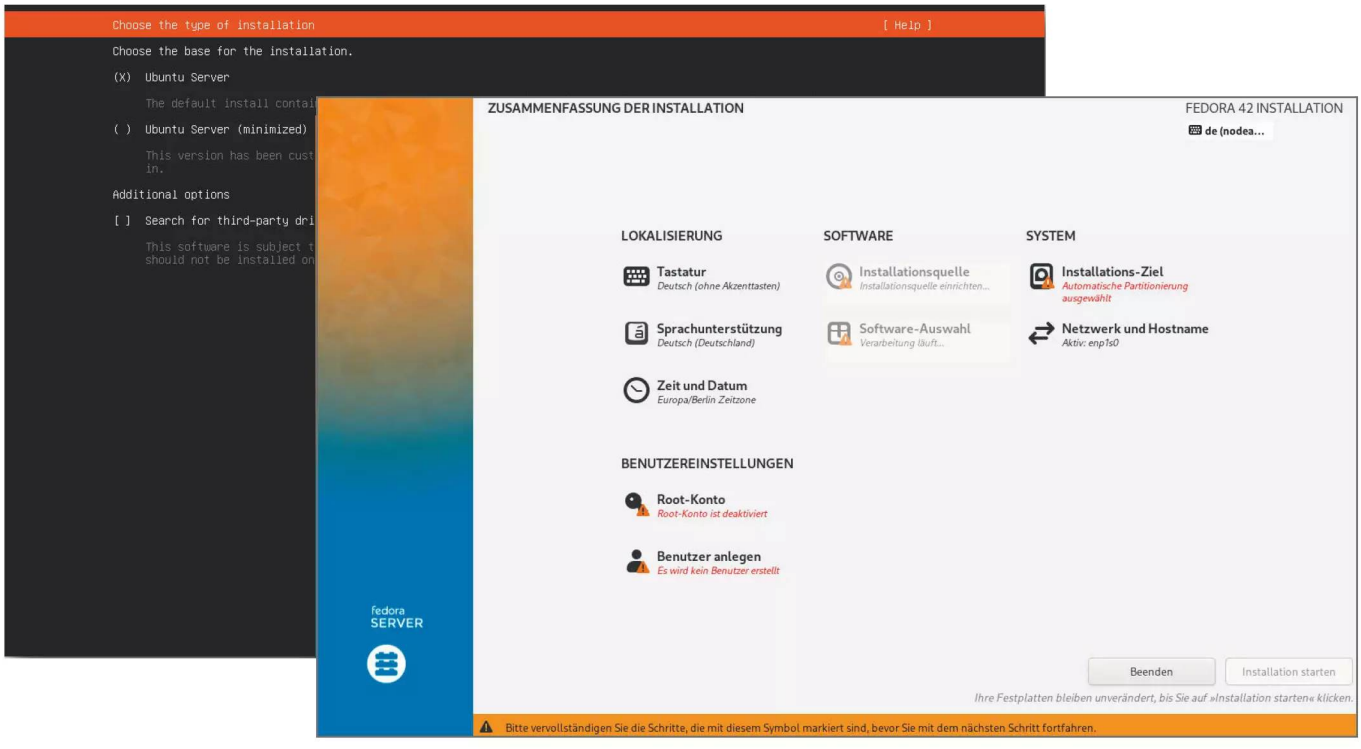
gemeint, dass in der Regel kein Monitor und keine Eingabegeräte an das System angeschlossen sind und dass auf ihm keine grafische Desktopumgebung installiert ist – schlicht, weil es keinen Grund dafür gibt. Auf einem rund laufenden Server arbeitet man nicht direkt und wenn ein Server mit Problemen kämpft, will man möglichst simple und direkte Zugriffsmethoden, die kaum in Mitleidenschaft gezogen werden können.

Bei Servern auf eine Desktopumgebung zu verzichten bedeutet keinesfalls, ganz allgemein grafische Oberflächen (GUIs) zu meiden. Typischerweise stellen Serverdienste Weboberflächen zur Verfügung, sodass man sie bequem und grafisch im Browser verwalten kann.

Es empfiehlt sich aber in jedem Fall, ein wenig Vertrauen zur (Linux-)Kommandozeile aufzubauen. Je nachdem, welches Server-Betriebssystem Sie wählen, werden Sie während oder nach der Installation ohnehin einige Schritte damit gehen müssen. Studieren Sie die Installations- und Post-Installations-Dokumentation des Betriebssystems aufmerksam. Es ist allemal besser, sich die Sache in Ruhe anzusehen, wenn man sich ohnehin in Neues einarbeitet, als erst dann in dieser Umgebung zu landen, wenn ein Server Probleme entwickelt und auch keine grafische Oberfläche mehr bereitstellen kann.

Es ist daher keine schlechte Idee, Server auch dann headless zu installieren, wenn man die Wahl hat. Viele Linux-Distributionen für Server kommen standardmäßig ohne grafische Oberfläche, etwa die von Ubuntu oder Fedora. Andere, wie Debian, fragen explizit nach und ansonsten gibt es in der Regel dedizierte Installationsimages ohne Desktop, etwa „Raspberry Pi OS Lite“, falls ein Raspi Ihr Server werden soll. Links zu allen im Text genannten Projekten finden Sie unter ct.de/wb9e.

Klassischerweise installiert man auf Linux-Systemen Software über eine Paketverwaltung wie apt, dnf oder dergleichen. So könnte man oft auch die



Die Server-Installation selbst mag textbasiert (im Bild Ubuntu) oder grafisch sein (Fedora), am Ende landet man meist auf der blanken Kommandozeile – und das ist auch gut so.

eigentlichen Dienste installieren, für deren Betrieb man einen Homeserver haben möchte, aber davon raten wir ab; unter anderem, weil man Probleme bekommt, wenn mehrere Dienste auf demselben Server miteinander inkompatible Voraussetzungen haben. Es ist zeitgemäßer, Dienste über Container bereitzustellen.

Über die Paketverwaltung sollten Sie daher nur Werkzeuge installieren, die zum Betrieb der Maschine unerlässlich sind – soweit die Betriebssysteminstallation sie nicht schon mitgebracht hat. Das trifft einmal auf die Containerlösung Ihrer Wahl zu (siehe unten), auf eventuell liebgewonnene Administrations- und Diagnosewerkzeuge und auf einen SSH-Server, in der Regel OpenSSH. Achten Sie darauf, regelmäßig (Sicherheits-)Updates für installierte Pakete einzuspielen; entweder manuell oder indem Sie `unattended-upgrades`(Ubuntu), `dnf-automatic` (Fedora) oder dergleichen installieren und einrichten.

Verlässliche Verbindung

SSH ist das Mittel der Wahl, um unter Linux (und auch vielen anderen Betriebssystemen) auf einen entfernten Server zuzugreifen: Per SSH kommen Sie auf jedes (Linux-)System. Auch viele NAS – die alle zur normalen Verwaltung ein Web-GUI mitbringen – erlauben den Zugriff per SSH; es lohnt sich, das Tool kennenzulernen.

Der Befehl `ssh max@example` bringt Sie auf die Kommandozeile des Servers `example` und meldet Sie dort mit dem Benutzernamen `max` an; `example` darf auch eine IP-Adresse sein. Auf dem Server muss dafür der erwähnte SSH-Server installiert sein (und laufen), auf dem PC, mit dem Sie sich Zugang verschaffen wollen, ein SSH-Client. Letzteren haben alle relevanten Betriebssysteme vorinstalliert, sogar Microsoft erbarmte sich und spendiert Windows seit Version 10 einen SSH-Client. Die langjährige Behelfslösung PuTTY brauchen Sie nicht mehr.

Standardmäßig müssen Sie das Passwort des Benutzerkontos kennen, mit dem Sie sich anmelden möchten. Das ist praktisch, weil SSH dann wie eine lokale Anmeldung am Server funktioniert, aber eher unsicher und daher nicht ratsam – insbesondere, wenn der Server auch aus dem Internet per SSH erreichbar sein soll. Besser ist die Anmeldung mit öffentlichen Schlüsseln („pubkey“), die das Erraten oder Durchprobieren von Zugangsdaten zuverlässig verhindern. Dabei hilft ein kleines, zusammen mit dem SSH-Client installiertes Skript: Der Aufruf `ssh-copy-id max@example` meldet sich per Passwort am Konto `max` des Servers `example` an und hinterlegt dort den öffentlichen Schlüssel Ihres SSH-Clients. Anschließend können Sie sich mit diesem Client als `max` auf dem Server anmelden, ohne Max' Passwort zu nutzen. Bei manchen Mietservern können Sie bereits während der Erstellung der VM über die Weboberfläche des Hosters Ihren öffentlichen Schlüssel hinterlegen.

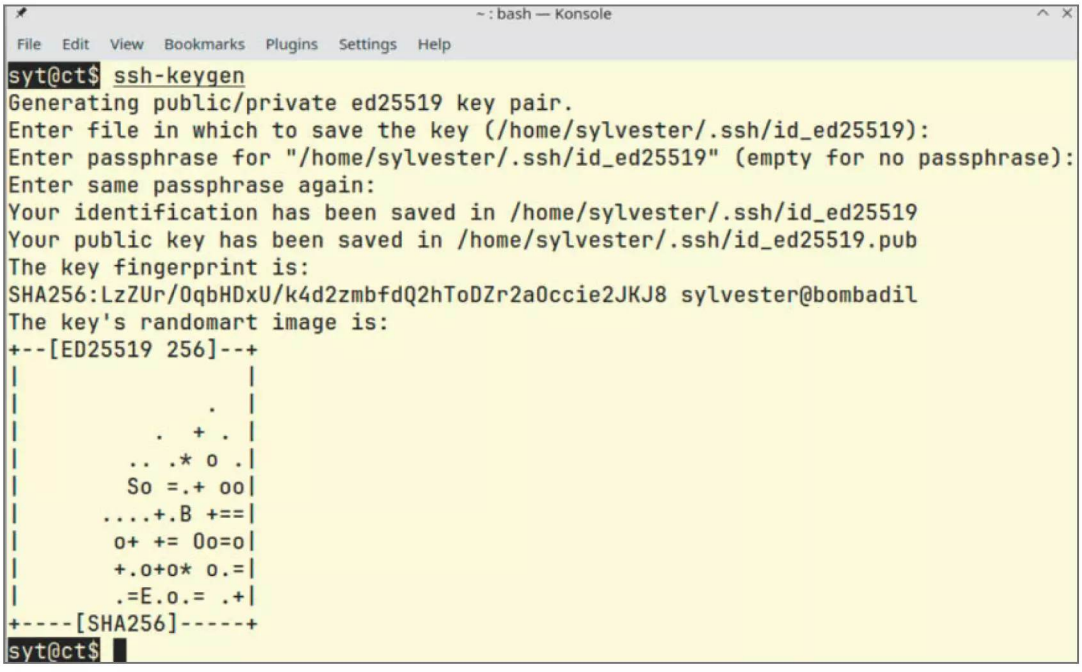
Falls Ihr Client noch kein SSH-Schlüsselpaar hat (und `ssh-copy-id` entsprechend meckert), hilft der Aufruf von `ssh-keygen`. Das Programm schlägt einen Speicherort für das Schlüsselpaar vor, den Sie übernehmen können, und fragt nach einer optionalen Passphrase. Es ist sehr empfehlenswert, SSH-Schlüssel damit zu schützen. Sobald die Anmeldung per Schlüssel klappt, sollten Sie in der Konfigurationsdatei des SSH-Servers die `PasswordAuthentication` abschalten.

Prüfen Sie jetzt, ob nach einem Reboot alles noch funktioniert. Wenn Ihr neuer Server ordentlich hochfährt, automatisch einen SSH-Server startet und Sie sich dort mit öffentlichem Schlüssel anmelden können, haben Sie im Grunde schon die halbe Miete. Fortan sind Bildschirm und Tastatur optional und Sie können die Maschine in jene Ecke packen, in der sie dauerhaft ihren Dienst verrichten soll. Für alle weitere Administration genügt die SSH-Verbindung.

SSH ermöglicht übrigens weit mehr, als sich auf entfernten Servern einzuloggen. Das Werkzeug taugt etwa auch als Proxy, um lokalen Traffic über den SSH-Server zu leiten oder umgekehrt. Bei der Administration hilft insbesondere das Begleitprogramm `scp`, das Dateien und Ordner via SSH überträgt, analog zum `cp`-Befehl. Der Wiki-Artikel von Ubuntuusers bietet eine deutschsprachige Übersicht über SSHs Fähigkeiten, die auch für andere Linux-Distributionen gilt (siehe ct.de/wb9e).

Alles schön abkapseln

Wie bereits erwähnt empfehlen wir, die eigentlichen Dienste Ihres Servers nicht über den Paketmanager zu installieren, sondern in Container zu sperren. So trennen Sie die Dienste sauber voneinander. Im Unterschied zu virtuellen Maschinen teilen sich alle Container den Kernel des Hosts. Das isoliert Dienste weniger streng, verbessert aber die Performance erheblich, sodass auch auf Kleincomputern wie Raspberry Pis Self-Hosting mit Containern Freude macht. Container sind die erste Wahl, um vertrauenswürdige Dienste auf einem Server zu vereinen, sie stellen aber keine adäquate Quarantäne für poten-



Ein SSH-Schlüsselpaar ist schnell erstellt und sichert Verbindungen besser als Passwörter.

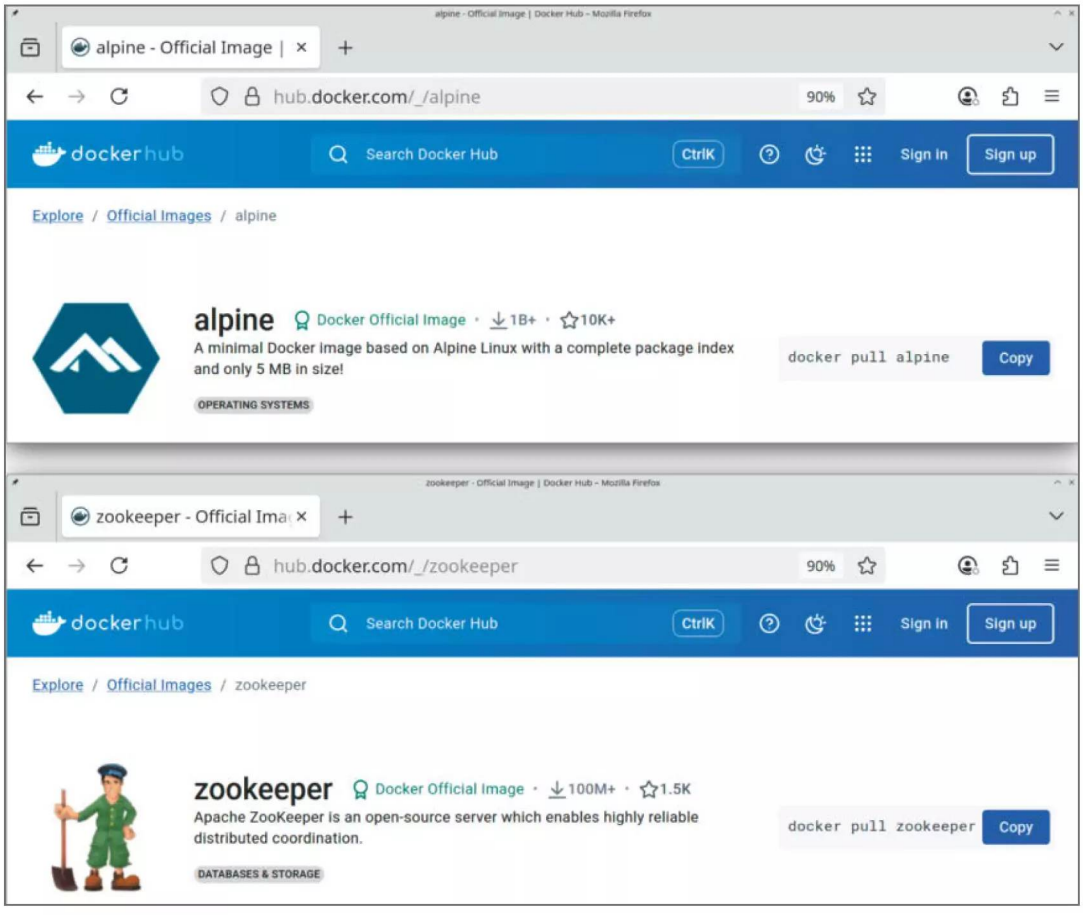
ziell bösartige Software dar! Die verbreitetste Container-Engine heißt Docker. Die Alternative nennt sich podman. Sie ist in der Benutzung sehr ähnlich und ebenfalls eine gute Wahl. Eine von beiden sollten Sie über die Paketverwaltung Ihres Betriebssystems installieren. Docker bietet für viele Linux-Distributionen auch eigene Repositories, die Pakete mit aktuelleren Versionen der Software bereitstellen. Details erklärt die jeweilige Dokumentation des Projekts (siehe ct.de/wb9e).

Mittlerweile kennen sehr viele Dienste die Option, sie als Docker-Images zu installieren; oft ist das sogar die empfohlene Variante. Idealerweise umfasst ein Container immer nur eine spezifische Komponente. Eine Anwendung, die beispielsweise aus einem Serverdienst und einer Datenbank (und eventuell weiteren Komponenten) besteht, dürfte sich also auf zwei (oder mehr) Container verteilen. Um so eine Sammlung von Containern zu starten, kann man eine Reihe von `docker`- oder `podman`-Befehlen absetzen. Die definieren über Umgebungsvariablen und Parameter, von welchen Images Container gestartet werden sollen, wie sie zu vernetzen sind, in welchen „Volumes“ sie Daten dauerhaft speichern können und so weiter.

Auf Dauer ist das mühsam. Legen Sie die Konfiguration der Container deswegen besser in Docker-Compose-Dateien fest. Das sind Konfigurationsdateien in der leicht lesbaren Beschreibungssprache YAML, die mehrere Container und ihr Zusammenspiel beschreiben. Die Installation von Diensten über Docker-Compose-Dateien erschöpft sich oft in dem simplen Dreischritt aus: Konfigurationsdatei(en) herunterladen, Dateien anpassen, `docker compose up -d` ausführen.

Wenn Sie selbst viel an den Konfigurationsdateien schrauben, hilft es, diese in einer Versionsverwaltung zu managen, typischerweise einem Git-Repository. So können Sie jeden Stand mit einem Kommentar versehen sichern und problemlos zu früheren Ständen zurückkehren.

Docker ist mittlerweile zu einem Ökosystem geworden, in dem Sie für praktisch alle Serverdienste passende Software finden dürften. Über 14 Millio-



Von A wie Alpine bis Z wie ZooKeeper: Im Docker Hub findet sich praktisch alles, was man hosten wollen könnte.

nen Images verzeichnet der Docker Hub, die größte sogenannte Registry, aus der sich Docker-Images beziehen lassen. Dazu gehören auch nützliche Helferlein, die Sie beim Verwalten Ihrer Container unterstützen und gleichzeitig selbst in Containern laufen.

Prominente Beispiele sind Portainer, ein Web-GUI, das den Betriebszustand Ihres Container-Zoos anzeigt und verwalten kann, oder watchtower, das alle auf dem Server laufenden Container automatisch aktualisiert. Letzteres gehört in jede produktiv genutzte Container-Umgebung, um das Einspielen von (Sicherheits-)Updates nicht manuell erledigen zu müssen. Leider ist die Weiterentwicklung von watchtower im originalen Repository eingeschlafen und findet stattdessen in verschiedenen Forks statt. Spätestens wenn Sie alle gewünschten Dienste als Docker-Container installiert und eingerichtet haben, sollten Sie wieder prüfen, ob auch nach einem Reboot alles noch funktioniert. Dann bedeutet auch ein versehentlich gezogenes Kabel oder ein kleiner Stromausfall nur, dass Ihre private Cloud kurz nicht erreichbar ist und danach alles wieder funktioniert – ohne dass Sie auch nur einen Finger krumm machen müssen.

Fehler finden

Doch trotz aller Sorgfalt werden eines Tages Fehler auftreten, sei es eine abstürzende Datenbank, eine vollgelaufene SSD oder ein fehlerhaftes Update, das den Betrieb lahmlegt. Wer seinen Server regelmäßig wartet und pflegt, muss im Falle solcher Ärgernisse

und Katastrophen oft weit weniger Zeit aufbringen als jemand, der seit Jahren keinen Blick mehr auf die Maschine geworfen hat.

Zur Pflege gehört mindestens ein regelmäßiger Blick in die Ereignisprotokolle. In kleinen Projekten reichen dafür die Bordwerkzeuge der Kommandozeile: `docker logs example` zeigt die Logs des Containers `example` an. Innerhalb eines Docker-Compose-Projekts können Sie mit `docker compose logs example` die Logs eines Dienstes `example` (wie Container in der Compose-Umgebung heißen) anzeigen. Der Parameter `--follow` zeigt neu eintreffende Nachrichten in Echtzeit an. Die Parameter `--since` und `--until` akzeptieren Timestamps (wie `2025-05-27T22:25:00`) und relative Zeitangaben (wie `3h` für 3 Stunden). Sie helfen, die Ausgabe auf Zeiträume einzuschränken, in denen Probleme auftraten.

Das zweite Werkzeug, das Sie kennen sollten, ist `journalctl`. Damit fragen Sie das Journal des verbreiteten Diensteverwalters systemd ab. In einer typischen Linux-Distribution finden Sie so alle Ereignisse und Probleme außerhalb der Container. Ohne weitere Parameter liefert das Werkzeug allerdings eine so umfassende wie detaillierte – und daher wenig hilfreiche – Liste, die mit den ältesten Einträgen beginnt. Mit dem Parameter `--reverse` drehen Sie die Reihenfolge um; mit `--boot` sehen Sie nur Nachrichten seit dem letzten Reboot und mit `--priority xyz` können Sie die Ausgabe auf Einträge einer gewissen Dringlichkeit beschränken. Ersetzen Sie dafür `xyz` durch eine der – absteigend dramatischen – Fehlerkategorien `emerg`, `alert`, `crit`, `err`, `warning`, `notice`, `info` und `debug`.

Machen Sie sich am besten direkt nach der Einrichtung Ihres Servers mit diesen Werkzeugen vertraut und verschaffen Sie sich ein Gefühl dafür, was Ihre Dienste und das Betriebssystem so in Friedenszeiten ins Log schreiben. Bei Weitem nicht jede Nachricht zeugt von einem ernsthaften Problem, das Sie zum Handeln zwingt. Sie sehen zum Beispiel auch fehlgeschlagene Anmeldungen, die automatische Scanner und böswillige Akteure regelmäßig verursachen. Daran müssen Sie sich gewöhnen: Sobald Ihr Dienst im Internet hängt, wird jemand versuchen, sich anzumelden oder den Server anderweitig zu behelligen.

Auf Nummer sicher

Daher sollten Sie Ihren Server auch nicht aus dem Internet erreichbar machen, bevor Sie ihn fertig eingerichtet haben – nicht einmal nur kurz! Bei einem System, das bei Ihnen zu Hause steht, reicht der Router als Schutz, solange Sie keine Portweiterleitungen mit dem Server als Ziel (etwa aus früheren Experimenten) eingerichtet haben. Bei Mietservern sollten Sie sicherstellen, dass sie per Firewall vernagelt sind; entweder mit der externen Firewall des Hostinganbieters oder mit einer internen, die Serverbetriebssysteme typischerweise mitbringen.

Erst wenn Sie das System wie gewünscht eingerichtet und alle Dienste fertig konfiguriert haben, können Sie überlegen, passende Löcher in Router oder Firewall zu bohren (siehe S. 70). Dafür müssen diese Dienste eine Authentifizierung bieten, damit nicht jeder dahergelaufene Bösewicht darin frei herumfuhrwerken kann, Sie müssen der Sicherheit des Dienstes und seiner Anmeldeoptionen vertrauen und Sie müssen selbige mit sicheren Zugangsdaten konfiguriert haben. Grundsätzlich müssen auch alle Konten auf dem Betriebssystem sichere Passwörter haben.

Dienste, die hier durchfallen und Ihnen nicht ausreichend sicher erscheinen, sollten Sie nicht direkt ins Internet hängen. Stattdessen können Sie Ihren Server nur per VPN erreichbar machen (siehe S. 70) oder die Dienste hinter einem Reverse-Proxy verstecken (siehe S. 78).

Bevor Ihr Server produktiv zum Einsatz kommt, sollten Sie sich außerdem über Backups Gedanken machen. Denn er kann nicht nur ein guter Bestandteil Ihrer Backupstrategie sein, Sie sollten ihn auch selbst gegen Katastrophen und katastrophale Fehler schützen. Bei Mietservern hilft möglicherweise ein Backup-Dienst des Hosting-Anbieters, der regelmäßig das gesamte System sichert und alte Kopien vorhält. Andernfalls müssen Sie selbst zu Backupprogrammen greifen, kommandozeilenbasierte Lösungen wie Borg, duplicity oder restic bieten sich an.

Überlegen Sie sorgfältig, was Sie sichern müssen. Container selbst sind typischerweise vergänglich, es reicht, die Konfigurationsdateien und besonders auch die Volumes zu sichern, in denen Ihre Dienste die eigentlichen Nutzdaten speichern. Die Docker-Dokumentation erklärt, wie Sie Inhalte der Volumes eines Containers ins Dateisystem des Servers extrahieren (siehe ct.de/wb9e). Dort können Sie sie dann mit dem Backupprogramm Ihrer Wahl erfassen. Überdies sollten Sie die (Konfigurations-)Daten des Servers selbst sichern. Die Details hängen vom gewählten Betriebssystem ab, aber typischerweise betrifft das die Verzeichnisse /etc, /home und /usr/local. Eine Liste der installierten Pakete zu sichern erspart im Fall der Fälle ebenfalls viel Frust. (syt) c't

Genannte Dokumentation und Projekte

ct.de/wb9e

Bild: KI, Collage c't

Dienste im Internet zugänglich machen

Sie möchten einen in Ihrem lokalen Netz konfigurierten Dienst unterwegs nutzen? Wir erklären Grundlagen, zeigen Methoden und helfen, Steine aus dem Weg zu räumen.

Von **Peter Siering**

Lokale Netzwerke hängen nicht direkt am Internet, sondern ein Router vermittelt, wenn dort stationierte Geräte Daten aus dem Internet abrufen. Er lässt dabei Verbindungen von innen nach außen durch. Anfragen, die ihn aus dem Internet erreichen, prallen hingegen ab. Das stellt sicher, dass Drucker, Dateifreigaben und andere Dienste nicht im Internet sichtbar und von dort aus erreichbar sind.

Wenn Sie allerdings zum Beispiel auf Ihren selbst gehosteten Kalender oder Ihre Fotosammlung unterwegs zugreifen wollen, gilt es, diesen Schutz gezielt zu überwinden. Maximalen Komfort erreichen Sie, wenn Sie dem Router erlauben, bestimmte Anfragen aus dem Internet ins interne Netz durchzureichen – man spricht von Weiterleitung oder Freigabe. Das ist nicht ohne Risiko: Der Dienst, der so erreichbar ist, muss widerstandsfähig und gewissenhaft abgesichert sein.

Wer dieses Risiko nicht eingehen will, kann sich mit einem VPN-Zugang ins lokale Netz helfen. Auf

vielen Routern lässt sich ein VPN-Server mit wenigen Handgriffen einrichten. Zugriff auf Ressourcen im lokalen Netz erhalten dann nur VPN-Clients, die sich vorher legitimieren. Dadurch werden sie logisch Teil des freigegebenen Netzes, genießen also dieselben Rechte wie lokal verbundene Geräte – auch das birgt Risiken. Das Folgende hilft, die Vor- und Nachteile zu verstehen und die Techniken Ihrem eigenen Bedarf anzupassen.

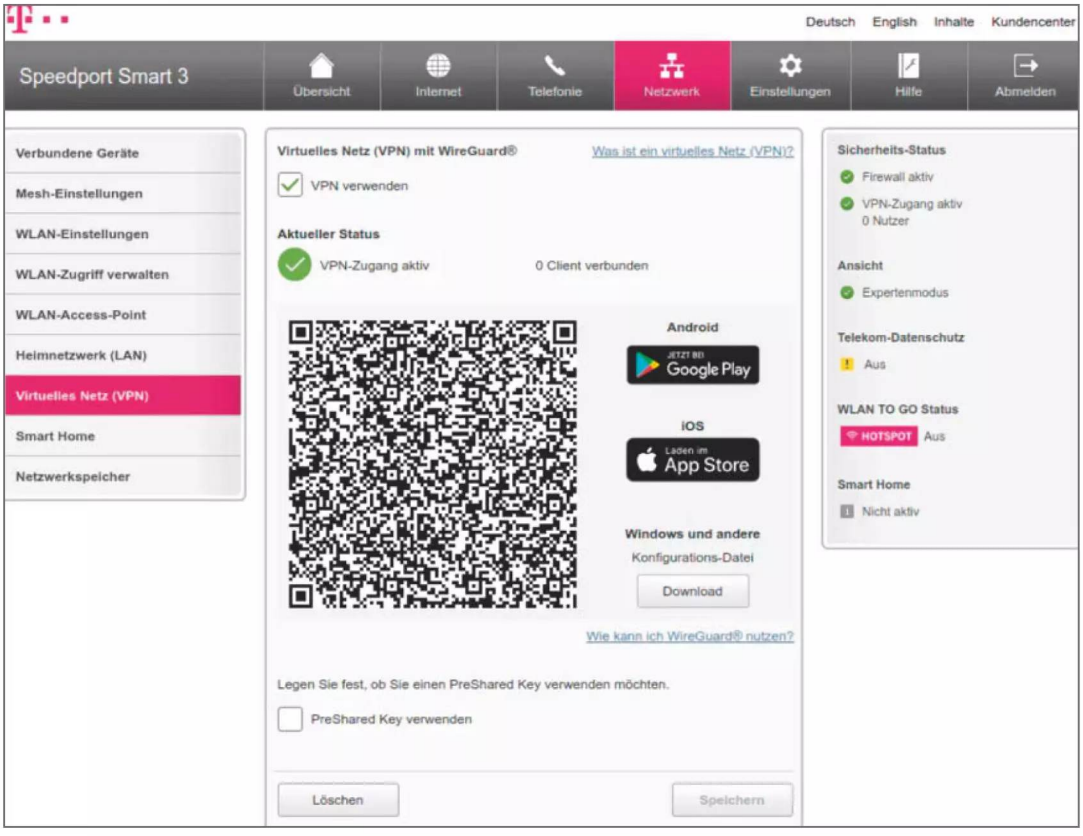
VPN oder was

Es ist mehr als eine Geschmacksfrage, ob VPN oder Freigaben besser geeignet sind: Wenn Sie Daten mit Dritten teilen wollen, etwa per Nextcloud, klappt das für Dienste hinter einem VPN-Zugang nur, wenn Sie allen Nextcloud-Nutzern VPN-Zugriff gewähren. Für solche Dienste eignet sich eine Weiterleitung durch den Router deshalb besser.

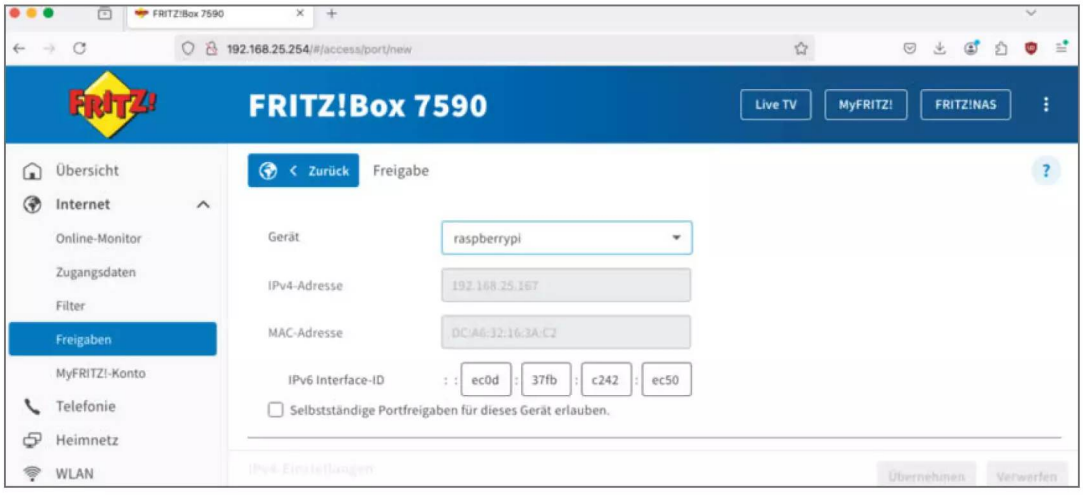
VPN-Zugänge funktionieren oft exklusiv. Das heißt, dass Sie sich beispielsweise zwischen Zugang zum eigenen, privaten Netz und einem VPN von Ihrem Arbeitgeber entscheiden müssen. Sie können zwischen den VPNs wechseln, aber nicht mit beiden gleichzeitig verbunden sein. Gleichzeitig aktive Split-VPN-Verbindungen sind anspruchsvoll und nicht alle Clients spielen mit. Weiterleitungen funktionieren gemeinhin in jedem Fall, ob eine VPN-Verbindung aktiv ist oder nicht.

Über die Weiterleitungen müssen Sie sich anfangs mehr Gedanken machen. Ein VPN oder Mesh-VPN ist dagegen schnell aufgesetzt. Wenn dann aber die Bedürfnisse wachsen, etwa weil einzelne Nutzer nur begrenzten Zugriff erhalten sollen oder im Mesh nur bestimmte Dienste zugänglich sein sollen, wächst hier der Aufwand im Nachhinein.

Unschlagbar ist ein VPN dann, wenn Sie administrativen Zugang zu Ihrem Netz aus der Ferne erhal-



Für die Erreichbarkeit der Dienste eines Single-Haushalts und zur Fernverwaltung praktisch: ein im Router aktivierter VPN-Zugang statt Portweiterleitungen.



In der Weboberfläche der Fritzbox beschreibt das Feld „IPv6 Interface ID“ den konstanten Teil der globalen IPv6-Adresse eines Gerätes. Es ist der Schlüssel für dauerhaft funktionstüchtige Portweiterleitungen.

ten wollen. Mit einem abgesicherten Zugang erreichen Sie dann alle Geräte. Das ist im Vergleich zur Freigabe von administrativen Oberflächen von NAS, Router & Co. auf jeden Fall die empfehlenswerte Alternative.

Wenn wir hier VPN schreiben, meinen wir WireGuard. Dafür sprechen viele Punkte: Die Serverkomponente für dieses VPN-Protokoll steckt heute in vielen Routern. Sie ist mit wenigen Klicks konfiguriert. Die Client-Software gibt es für alle Plattformen kostenlos. Eine ständige Verbindung vom Mobiltelefon bleibt ohne starke Auswirkung auf die Akkulaufzeit und übersteht auch Netzwerkwechsel. Dass ein Router WireGuard-Zugänge offen hält, lässt sich von außen nicht erkennen – das ist ein weiterer Unterschied zu Weiterleitungen.

Ports für Freigaben

Das Grundprinzip, wie Dienste im Netzwerk und im Internet erreichbar sind, ist einfach: Über IP-Adressen sprechen Clients die Server an, ähnlich einer Telefonnummer. Die Dienste lauschen an festgelegten Ports, zum Beispiel Port 80 und 443 für Zugriffe über das HTTP/HTTPS-Protokoll, über das Browser Webseiten abrufen. Als Nutzer hat man eher selten mit den Ports zu tun, Anwendungen wie ein Browser ergänzen sie meist von sich aus. Serverbetreiber müssen die Ports hingegen kennen.

In der Telefonanalogie entsprechen Ports einer Nebenstelle beziehungsweise Durchwahl. Soll ein Dienst hinter einem Router erreichbar sein, muss der Router Verbindungsanfragen für den jeweiligen Port annehmen und an den Server des Dienstes im internen Netz weiterleiten. Daher kommt auch der Name Portweiterleitung oder -Freigabe (das Folgende nutzt weiter den Begriff „Weiterleitung“, Router-GUIs bevorzugen oft „Freigabe“). Es gibt zwei Arten von Ports, solche für das Protokoll TCP und solche für UDP. Die meisten Anwendungen nutzen TCP.

Welche Ports für welchen Dienst notwendig sind, steht mindestens in dessen Dokumentation. Docker-Images beschreiben normalerweise detailliert, welche Ports für den enthaltenen Dienst relevant sind. Daran können Sie sich gut orientieren. Prüfen Sie aber doppelt, ob ein Port wirklich im Internet sichtbar sein muss. Der Datenaustausch zwischen Containern gelingt meist ohne.

Adressdeutungen

Zurück zu den IP-Adressen: Die Analogie der Telefonnummer passt nur teilweise. Viele Geräte haben nicht nur eine Adresse, sondern mehrere. Das kommt unter anderem daher, dass sie nicht nur eine IPv4-Adresse wie „193.99.144.80“ nutzen, sondern wegen deren Knappheit auch IPv6-Adressen wie „2a02:2e0:3fe:1001:302::“ (beide Adressen führen zu heise.de).

Sowohl bei IPv4 als auch bei IPv6 gibt es private Adressen, die für lokale Netze gedacht sind. Bei IPv4 sind dafür Adressen typisch, die mit „192.168.“ beginnen (es gibt aber noch weitere private Nummernblöcke). Bei IPv6 fangen solche Adressen in der Regel

mit „fc“, „fd“ und „fe“ an. Die privaten Adressen sind aus dem Internet nicht direkt ansprechbar. Nur global gültige IP-Adressen sind direkt erreichbar.

Im Fall von IPv4 erhält nur der Router eine solche global gültige Adresse. Er übersetzt für das interne Netz aus- und eingehende Pakete zwischen privaten und global gültigen Adressen; Network Address Translation (NAT) nennt sich dieses Vorgehen. Bei einer eingerichteten Portweiterleitung findet NAT nicht nur für Verbindungen von innen nach außen statt, sondern auch umgekehrt.

Im Fall von IPv6 erhalten auch die Geräte im internen Netz global gültige Adressen. Hier muss der Router also nicht übersetzen. Er fungiert üblicherweise nur als Filter und leitet IPv6-Verkehr erst an Geräte im internen Netz durch, wenn er explizit dazu aufgefordert wird. Das geschieht analog zu IPv4 oft ebenfalls durch eine Portweiterleitung, wobei die nur im Paketfilter eine entsprechende Weiterleitungsregel setzt und kein NAT aktiviert.

Üblicherweise ändern sich die global gültigen Adressen mit jedem neuen Aufbau einer Verbindung zum Internet durch den Router. Bei IPv4 betrifft das eine Adresse, bei IPv6 gleich mehrere: die des Routers und alle vom Router an Geräte im lokalen Netz verteilten IPv6-Adressen. Diese Adressen stammen üblicherweise aus einem von mehreren IPv6-Netzen, die ein Router während des Verbindungsaufbaus vom Internetanbieter zur freien Verfügung erhält. Jedes dieser Netze hat ein eigenes Präfix, das sind die ersten 64 Bit einer IPv6-Adresse.

v6-Tücken

IPv6 verkompliziert die Weiterleitung von Diensten obendrein dadurch, dass ein Gerät üblicherweise nicht nur eine IPv6-Adresse erhält, sondern mehrere. Das sind nicht nur private, sondern auch mehrere global gültige Adressen mit identischem Präfix, die sich unter anderem aus Datenschutzgründen

regelmäßig ändern, ohne dass es dafür einen externen Anlass wie einen Neuaufbau der Internetverbindung gäbe.

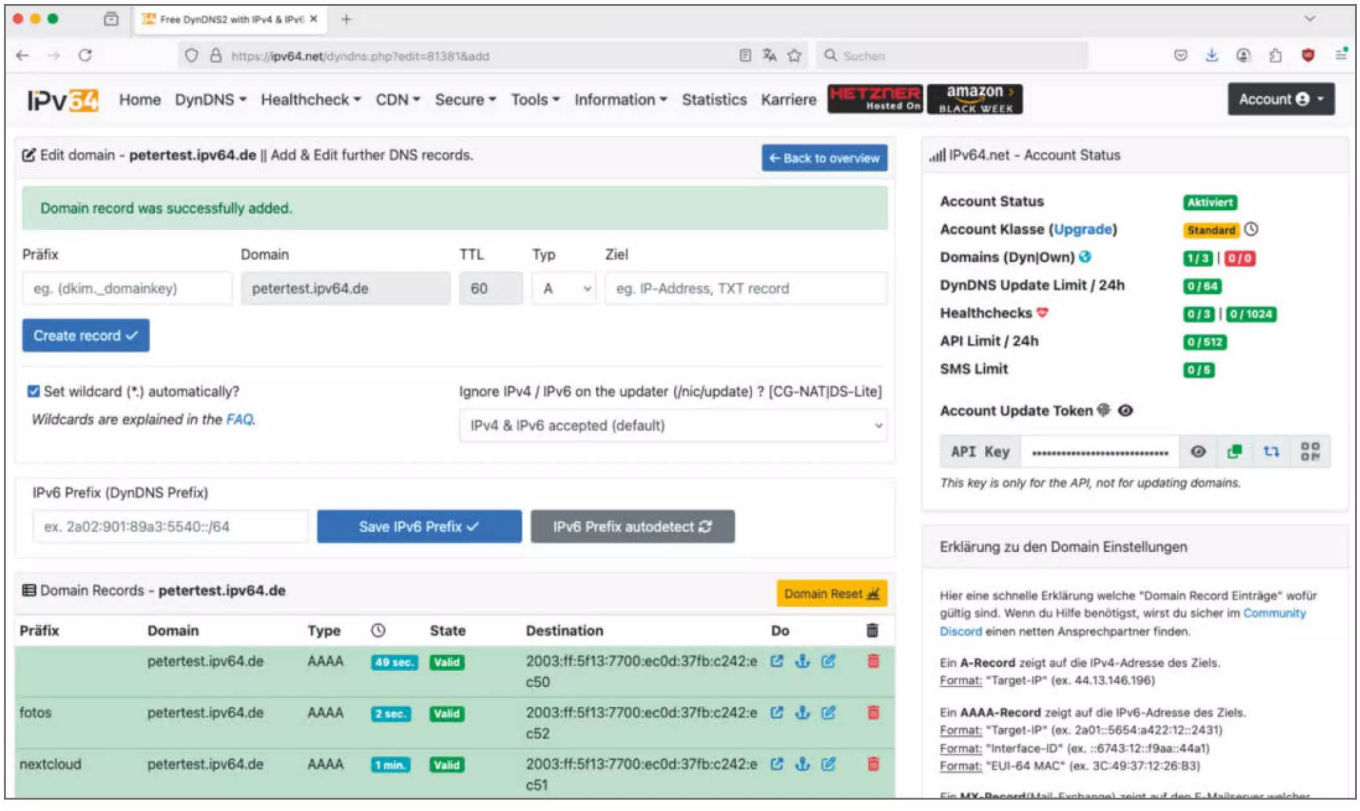
Die Kunst bei IPv6 besteht darin, für die Portweiterleitung die dauerhaft stabile globale Adresse zu identifizieren. Dabei kommt es nicht auf das Präfix an, also die ersten 64 Bit, sondern auf die hinteren 64 Bit, die Interface ID heißen. Unsere IPv6-FAQ (siehe ct.de/w22y) nennt für verschiedene Betriebssysteme die wesentlichen Handgriffe, um die richtige Interface-ID zu ermitteln. Diese müssen Sie in der Weboberfläche des Routers bei der Portweiterleitung eintragen.

Das alles ist eine stete Quelle für Frust, wenn diese Details nicht bekannt sind. Oft gelingt dann das Freigeben eines Dienstes, aber nach einiger Zeit ist er plötzlich nicht mehr erreichbar. Das passiert, wenn man die falsche IPv6-Adresse für die Portweiterleitung ausgesucht hat, und fällt womöglich erst auf, wenn ein Client eine IPv6-Verbindung versucht und erst nach einem deutlich spürbaren Timeout auf IPv4 zurückfällt. Ein zäher Verbindungsaufbau ist ein typisches Symptom.

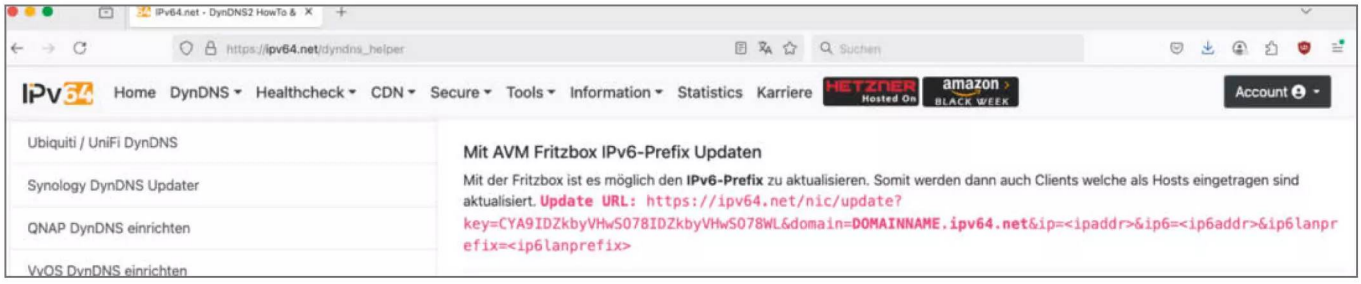
Namen statt Nummern

Mit IP-Adressen zu hantieren, ist mühsam und fehleranfällig, da sie sich bei Internetverbindungen für Heimanwender immer mal wieder ändern. Das passiert zwar seltener als früher, oft wochenlang nicht, aber auszuschließen ist es nicht. Und es passiert garantiert immer dann, wenn man es gerade nicht gebrauchen kann.

Nachdem sich die Adresse eines Diensts geändert hat, müsste man die Konfiguration aller Clients ändern, was wenig praktikabel ist. Die Lösung für die-



Wenn der DynDNS-Anbieter (hier ipv64.net) IPv6-Präfix-Updates erlaubt, so legt man die Namen für die einzelnen IPv6-Hosts dort in der Weboberfläche an.



Anbieter von DynDNS-Diensten dokumentieren ihr API – meist genügt eine speziell konstruierte URL mit Platzhaltern, um Zugangsdaten, IP-Adressen und Namen zu übertragen. Das Beispiel im Bild zeigt eine solche URL für ipv64.net mit den Parametern für ein IPv6-Präfix-Update.

ses Problem heißt dynamisches DNS (DynDNS). Ein DynDNS-Dienst versieht wechselnde IP-Adressen automatisiert mit immer gleichen Namen. Das könnte zum Beispiel „meinserver.dyndns.org“ sein.

Über ein schlichtes API kann ein Router, sobald er neue IP-Adressen erhalten hat, sie beim DynDNS-Dienst für einen vorher ausgewählten Namen hinterlegen. Dafür genügt es, sich bei einem DynDNS-Anbieter anzumelden und dort einen Domainnamen samt noch freiem Hostnamen auszusuchen. Die meisten Router-GUIs kennen einige DynDNS-Anbieter schon und fragen diese Daten passend ab. Oft ist es auch möglich, eine URL anzugeben, die das dokumentierte API anspricht.

AVM bietet für seine Router MyFritz an und stellt damit eine Alternative zu externen DynDNS-Anbietern dar – allerdings enden die Namen wenig einprägsam: „ccn2...77hmn.myfritz.net“. Hier hat es sich für Besitzer eigener Domains bewährt, die MyFritz-Namen dort in CNAME-Records abzulegen. Ein sprechender Name wie „meiner.example.com“ verweist dann auf die komplizierte, aber immer gleiche MyFritz-Adresse und diese wiederum auf die jeweils aktuelle IP-Adresse.

IPv6 verkompliziert auch DynDNS: Es genügt nicht, nur die IPv6-Adresse des Routers zu registrieren, weil bei IPv6 Geräte jeweils über ihre eigene IPv6-Adresse anzusprechen sind. Es gibt zwei Methoden, damit umzugehen: Die IPv6-Geräte führen selbst die DynDNS-Updates durch oder der Router übernimmt das stellvertretend. Dazu muss er die Geräte mit Portweiterleitungen und deren Namen kennen – so funktioniert letztlich MyFritz.

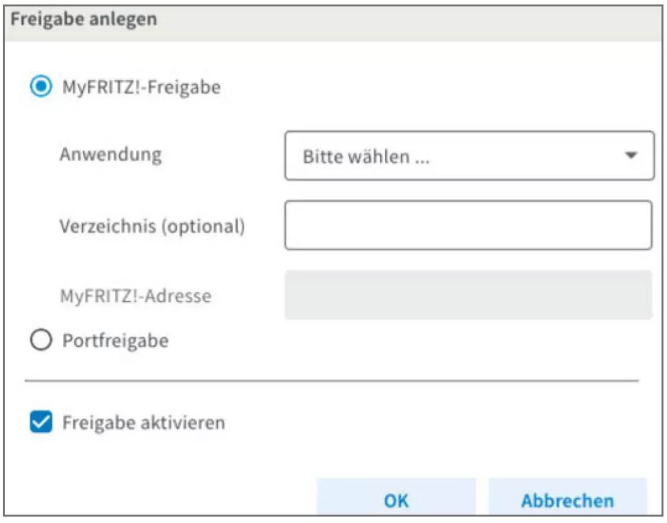
Die Alternative besteht darin, dass der Router dem DynDNS-Dienst nur das IPv6-Präfix mitteilt. Für

IPv6-Plädoyer

Angesichts der ganzen Detailprobleme, die IPv6 aufwirft, liegt die Idee nahe, es schlicht abzuschalten, um sich ihrer zu entledigen. Das ist aber nicht nur wenig zeitgemäß, vor allem tun angehende Admins gut daran, sich mit der Technik vertraut zu machen. Mancher hat vielleicht gar keine Wahl, wenn sein Provider ihm nur IPv6-Adressen gibt – kreative Lösungen dafür zeigt der Folgeartikel.

IPv6 bietet außerdem durchaus auch Vorteile: Anders als bei IPv4 können hinter einem Router mehrere Geräte Dienste auf demselben Port anbieten, weil sie jeweils eine eigene öffentliche IPv6-Adresse haben. Das geht dann ohne die Angabe von Non-Standard-Ports in jeder URL und ohne eine vermittelnde Instanz, wie sie der folgende Artikel vorstellt.

Unsere Empfehlung: Lernen Sie, wo die Besonderheiten von IPv6 liegen, und entscheiden Sie dann. So werden Sie jedenfalls nicht blauäugig in die typischen Probleme hineinlaufen, sondern wissen, mit welchem Fehlverhalten Sie rechnen müssen und wie Sie es in den Griff bekommen.



Fritzboxen kennen zwei Methoden, Portweiterleitungen einzurichten, traditionell als Portfreigabe und über MyFritz, was dann praktisch ist, wenn mehrere Clients mit IPv6-Adressen hinter dem Router Dienste freigeben sollen.

die einzelnen Hosts mit IPv6-Adressen muss man nun händisch beim Anbieter DNS-Einträge für IPv6 anlegen (sogenannte AAAA-Records). Bei einem Präfix-Update aktualisiert der Dienst dann nur die ersten 64 Bit der hinterlegten IPv6-Adressen.

Unterm Strich ist MyFritz die einfachste Lösung (wenn Sie denn eine Fritzbox als Router nutzen), besonders weil AVM Portweiterleitung und DynDNS kombiniert. Wenn nur ein Dienst überhaupt freigegeben werden soll und keine Fritzbox als Router arbeitet, bietet sich das Ausführen des DynDNS-Updaters auf dem Gerät selbst als praktischste Methode an.

Für weitergehende Ansprüche dürfte das Präfix-Update der passende Weg sein. DynDNS-Dienste, die nur auf einem Gerät im Netz laufen, etwa einem NAS, eignen sich in der Regel nur dafür, ihre eigenen Adressen mit einem Namen zu versehen, nicht aber die anderer Gerätekollegen im lokalen Netz.

Zertifikate

Egal welchen Dienst Sie ins Internet bringen, für die Zugriffe darauf ist Transportverschlüsselung obligatorisch. Die lässt sich mit selbst signierten Zertifikaten oder einer eigenen Zertifizierungsstelle herstellen, doch es ist viel einfacher, sich von Let's Encrypt ein kostenloses Zertifikat ausstellen zu lassen. Die halten derzeit 90 Tage und können regelmäßig automatisch erneuert werden.

Für Dienste, die auf dem HTTP-Protokoll aufbauen, ist das relativ einfach zu bewerkstelligen: Über das ACME-Protokoll („Automated Certificate Management Environment") kann ein kleines Programm – der ACME-Client – regelmäßig ein neues Zertifikat bestellen und einbauen. Per HTTP beweist es seine Berechtigung dazu, indem es den Webserver eine spezielle Datei ausliefern lässt. Ein gängiger ACME-Client für die Linux-Kommandozeile ist das Programm Certbot. Der folgende Artikel stellt alternative Methoden vor, per Reverse-Proxy die Zertifikatsbeschaffung automatisiert zu betreiben.

Keine Bange

Das Wichtigste zum Schluss: Lassen Sie sich von den vielen Details nicht Bange machen, sondern lernen Sie an der Praxis. Ein Raspi oder eine virtuelle Maschine (VM) mit einem Minimal-Linux genügt für erste Experimente. Damit laufen Sie dann auch nicht Gefahr, versehentlich die familieneigene Sammlung von Fotos und Videos frei verfügbar ins Internet zu packen.

Nach einigen Gehversuchen werden Sie in der Lage sein, erste Dienste eigenverantwortlich zu betreiben und zugänglich zu machen. Konkrete Inspiration liefern auch viele c't-Artikel dazu – einige nennt die Literatur. Wenn dann der Bedarf wächst und Sie weitere Dienste an den Start bringen möchten, liefert der Folgeartikel Inspiration. (ps) *ct*

IPv6-FAQ
ct.de/w22y

Bild: KI, Collage c't

Reverse-Proxy und (VPN-)Tunnel

Die Frage, wie man selbst gehostete Dienste sicher ins Netz bekommt, treibt die Self-Hosting-Community um wie keine andere. Lernen Sie einfache und fortgeschrittene Methoden kennen und entscheiden Sie für sich, welche am besten passt.

Von **Niklas Dierking**

Der erste Heimserver läuft, die ersten Dienste laufen auf dem Raspi oder Mini-PC und die ersten Nutzer greifen darauf zu. Nicht selten steigen dann irgendwann die Ansprüche: Spätestens, wenn mehrere Rechner oder VMs ins Spiel kommen oder Dienste für alle Nutzer auch ohne VPN aus dem Internet erreichbar sein sollen, lohnt es sich, eine Infrastruktur zu zimmern, die jederzeit leicht erweitert werden kann. Dabei helfen Reverse-Proxys, automatisches Management von TLS-Zertifikaten und (VPN-)Tunnellösungen.

Letztere ermöglichen auch das Self-Hosting, wenn der Internetanbieter Carrier-Grade-NAT (CG-NAT, CGN) oder Dual Stack Lite verwendet. CG-NAT wird genutzt, um knappe IPv4-Adressen zu sparen, indem Kunden IPv4-Adressen aus dem privaten Adressbereich zugeteilt werden. Ein zusätzliches Gateway zwischen dem Router und dem Netzbe-

treiber kümmert sich dann um die Adressübersetzung. Bei DS Lite bekommen Kunden eine öffentliche IPv6-Adresse und IPv4-Traffic wird in IPv6-Paketen gekapselt. Dadurch sind keine Portweiterleitungen zu Geräten im Heimnetz mit IPv4-Adresse möglich.

Schloss ist Pflicht

Wie Sie im vorigen Artikel gelesen haben, ist es obligatorisch, Dienste, die im Internet hängen, mit einer Transportverschlüsselung zu versehen. Brauchen Sie nur einen Automatismus, der ein TLS-Zertifikat beschafft und vor dem Ablauf austauscht, genügt das Kommandozeilenwerkzeug Certbot. Aber wenn Sie mehrere Dienste betreiben, sollten Sie einen Reverse-Proxy einspannen, der Anfragen aus dem Internet entgegennimmt und an den richtigen Dienst durchreicht sowie Zertifikate besorgt und erneuert. Bei den Self-Hostern in der c't-Redaktion ist Traefik dafür beliebt. Dieser Reverse-Proxy bietet sich an, wenn man eine Vielzahl von containerisierten Diensten betreibt, setzt aber etwas mehr Konfigurationsaufwand voraus.

Mit dem Nginx Proxy Manager gibt es eine besonders einsteigerfreundliche Lösung mit einer Weboberfläche, die YouTube-Kollege Jan-Keno Janssen bei c't 3003 erst kürzlich vorgestellt hat (siehe ct.de/wvkd). In diesem Artikel empfehlen wir Caddy, der ebenfalls leicht zu konfigurieren ist, dem wir aber aufgrund des größeren Entwicklerteams und regelmäßigeren Updates eine bessere Zukunftsfähigkeit zutrauen.

Für die automatisierte Beschaffung von Zertifikaten brauchen Sie eine eigene Domain. Eine günstige Domain bekommen Sie bei einem Registrar bereits für wenige Euro im Jahr. Mit der sogenannten HTTP-Challenge beweisen Sie einer Zertifizierungsstelle wie Let's Encrypt, dass Sie diese Domain kontrollieren, indem Ihr ACME-Client, in diesem Fall Caddy, ein Token im Verzeichnis `/.well-known/acme-challenge` des Webservers platziert. Sie müssen nur jeweils eine Weiterleitung zu TCP-Port 80 für die HTTP-Challenge und Port 443 für den Zugriff via HTTPS einrichten.

Wie der Proxy eingehende Anfragen zu Ihren selbst gehosteten Diensten routet, legen Sie im sogenannten Caddyfile fest. Wir gehen davon aus, dass Sie sowohl Caddy als auch den zu veröffentlichenden Webdienst als Docker-Container betreiben. Eine Beispielkonfiguration mit einem nginx-Container haben wir in einem GitHub-Repository hinterlegt. Praktisch: Teilen sich beide Container ein Docker-Netzwerk, können Sie den Container des Dienstes mit seinem Namen, in diesem Fall schlicht `nginx`, in der Konfigurationsdatei für Caddy ansprechen. Diese Datei heißt Caddyfile, ohne jegliche Dateiendung.

Um einen Dienst mit Transportverschlüsselung zu versehen und Anfragen an Port 80 des Containers durchzureichen, reicht schon der folgende Codeschnipsel im Caddyfile:

```
webserver.example.com {
    reverse_proxy nginx:80
}
```

Sie müssen lediglich die Domain webserver.example.com durch Ihre eigene Domain oder eine DynDNS-Domain ersetzen und den Namen des Containers und den Port anpassen. Wenn Sie eine Domain gekauft haben, nehmen Sie die DNS-Einträge für Subdomains in der Weboberfläche des Registrars oder Hosters vor.

Caddy kann auch Anfragen zu Diensten außerhalb des Docker-Netzwerks oder auf anderen Hosts durchreichen. Angenommen, Caddy und der nginx-Container laufen auf Ihrem Homeserver, aber es gibt noch eine weitere Anwendung auf einem Raspi mit der IP-Adresse 192.168.0.150, die auf Port 8080 lauscht. Ergänzen Sie bei Ihrem Registrar die entsprechenden Subdomains und fügen dann die Raspi-Anwendung und weitere Dienste einfach nach dem Vorbild des nginx-Eintrags zum Caddyfile hinzu:

```
app.example.com {
    reverse_proxy 192.168.0.150:8080
}
```

So wird der Reverse-Proxy Caddy zum alleinigen Schlüsselmeister und leitet alle angehenden Anfragen aus dem Internet, je nach angefragtem Namen entweder zum Webserver oder App oder zu weiteren möglichen Diensten in Ihrem Heimnetz weiter. Das funktioniert auch auf einem angemieteten Server, auf dem Sie mehrere Dienste gleichzeitig hosten. Denken Sie in diesem Fall daran, Port 80 und 443 für Caddy in einer etwaigen Firewall des Hosters zu öffnen. Betreiben Sie Caddy im Heimnetz, müssen Sie an Ihrem Router ebenfalls nur die Portweiterleitungen für Caddy konfigurieren.

Eierlegendes Wollmilch-VPN

Der aufgehende Stern am Homelab- und Self-Hosting-Himmel, wenn es darum geht, lokale Dienste ohne Portfreigaben am Router im Netz zu veröffent-

lichen, ist ein Open-Source-Projekt namens Pangolin. Pangolin nimmt Anfragen aus dem Internet entgegen und verteilt sie intern via WireGuard-VPN an den richtigen Dienst. Ein Aufruf der Subdomain home.example.com kann zum Raspi im Heimnetz führen, nas.example.com stattdessen zum NAS bei den Eltern. Es bietet die Vorteile proprietärer Tunnellösungen von Anbietern wie Cloudflare, ist vergleichsweise schnell und einfach eingerichtet und lässt sich selbst hosten. Dadurch sind Sie unabhängiger und im Unterschied zu einem Cloudflare-Tunnel gibt es keinen Anbieter, der prinzipiell den internen Traffic mitschnüffeln kann.

Die Entwickler haben Pangolin unter zwei Lizenzen, die AGPL-3 und die Fossorial Commercial License, gestellt. Letztere verbietet es unter anderem, den Dienst als Software-as-a-Service zu verhökern. Als Privatnutzer müssen Sie sich darum nicht scheren. Pangolin besteht aus mehreren Komponenten. Es gibt den gleichnamigen zentralen Server, der die Weboberfläche und das API bereitstellt und sich um Authentifizierung kümmert. Um das WireGuard-Schlüsselmanagement und um den Aufbau der verschlüsselten Verbindungen kümmert sich Gerbil. Traefik wird als Reverse-Proxy eingespannt und um eine Middleware namens Badger ergänzt, die als Türsteher unzulässige Anfragen an Pangolin zur Authentisierung weiterleitet.

Auf den Systemen, auf denen selbst gehostete Dienste laufen, die Sie später mit Pangolin veröffentlichen wollen, können Sie Pangolins WireGuard-Client namens Newt installieren. Pangolin nimmt aber prinzipiell auch herkömmliche WireGuard-Verbindungen an. Pangolin betreiben Sie am besten auf einem schmalen vServer, der nicht mehr als wenige Euro im Monat kostet. 1 vCPU und 1 GByte Arbeitsspeicher genügen bereits. Außerdem brauchen Sie eine eigene Domain.

Erstellen Sie einen Wildcard-DNS-Eintrag (*.example.com), der auf die IP-Adresse Ihres Pangolin-Servers zeigt, und öffnen Sie die TCP-Ports 80 für die Beschaffung von Zertifikaten, 443 für die Pangolin-Weboberfläche und Ihre Dienste sowie den UDP-Port 51820 für WireGuard. Das Pangolin-Projekt stellt einen praktischen, textbasierten Installer zur Verfügung, den Sie mit dem folgenden Befehl herunterladen und ausführbar machen:

```
wget -O installer ↵
↳"https://github.com/fosrl/pangolin/↵
↳releases/download/1.4.0/↵
↳installer_linux_$(uname -m | sed 's/↵
↳x86_64/amd64/;s/aarch64↵
↳/arm64/')" && chmod +x ./installer
```

Der Installer legt unter anderem die nötige Verzeichnisstruktur an und lädt dann die oben beschriebenen Pangolin-Komponenten als Docker-Images herunter. Docker wird ebenfalls installiert, wenn es bisher nicht vorhanden ist.

Schuppentier einrichten

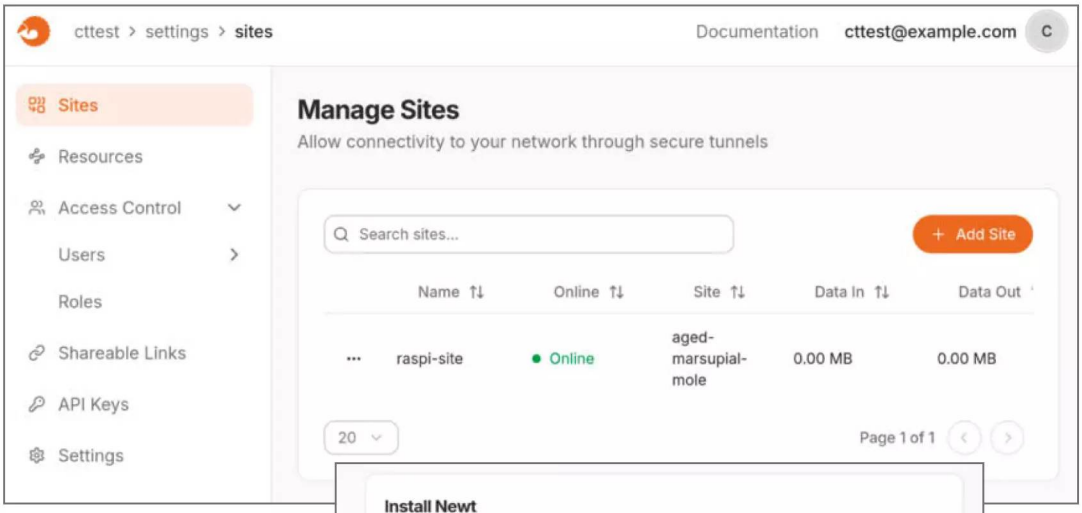
Sie starten den Installer mit dem Befehl `sudo ./installer`, der daraufhin einige Informationen abfragt. Zuerst müssen Sie Ihre Basisdomain eingeben (example.com). Anschließend braucht es eine Subdomain für die Pangolin-Weboberfläche, etwa pangolin.example.com. Danach tragen Sie Ihre E-Mail-Adresse für Let's Encrypt ein, die E-Mail-Adresse des Administrators und vergeben ein sicheres Passwort. Bei den restlichen Fragen können Sie jeweils die Vorauswahl (default) bestätigen. Wenn Pangolin Mails versenden soll, müssen Sie den Pangolin-Installer mit den Zugangsdaten für einen SMTP-Server füttern.

Nachdem die Installation abgeschlossen ist, können Sie sich in der Weboberfläche auf pangolin.example.com einloggen. Zunächst müssen Sie einen Namen und eine ID für Ihre Organisation vergeben. Erstellen Sie jetzt einen ersten Tunnel von einem System in Ihrem Heimnetz („Site“) zu Pangolin.

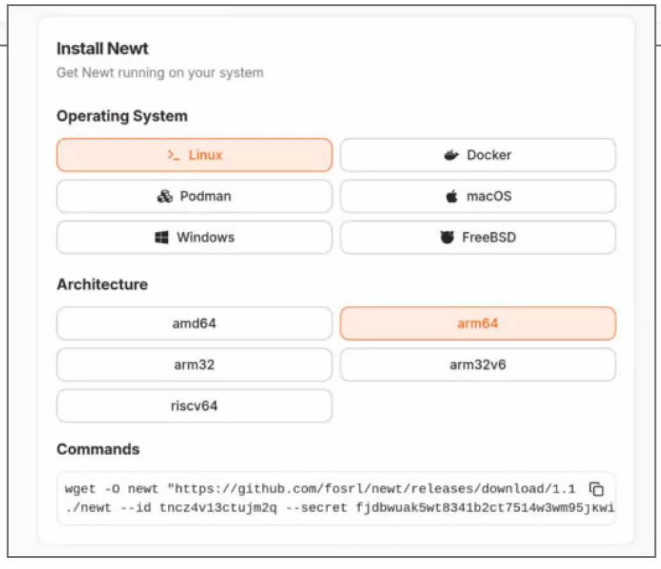
Dafür müssen Sie einen Namen vergeben und etwas nach unten scrollen, um das Betriebssystem und dessen Architektur anzugeben. Unser Beispieltunnel soll mittels Newt, dem Pangolin-Wireguard-Client, zu einem Raspberry Pi mit Docker führen, also wählen wir Docker und arm64 aus. Ganz unten auf der Seite zeigt Pangolin dann eine Docker-Compose-Vorlage an, in deren Umgebungsvariablen eine Newt-ID, der Pangolin-Endpunkt und ein Geheimnis für WireGuard stecken.

Legen Sie auf dem Zielsystem ein Verzeichnis für Newt an und kopieren die Konfiguration aus der Pangolin-Weboberfläche in eine docker-compose.yaml-Datei. Starten Sie dann den Container mit dem Befehl `docker compose up -d`. Nach kurzer Zeit sollte die Verbindung zustande kommen und Pangolin das System im Menü „Sites“ als „online“ auflisten. Um einen Dienst, der in Ihrem Heimnetz läuft, jetzt ins Internet zu hängen, müssen Sie in das Menü „Resources“ wechseln.

Für einen Webserver wählen Sie den „Resource-Type“ HTTPS, vergeben eine Subdomain wie web.



Auf einem Raspi im Heimnetz läuft der WireGuard-Client Newt und baut eine Verbindung zu Pangolin auf, das auf einem Mietserver läuft.



Wo soll's hingehen? In der Weboberfläche von Pangolin konfigurieren Sie Newt für das Zielsystem.

example.com und tragen für den Proxy die IP-Adresse und den Port des Dienstes unter „Target" ein. Voilà! Sie können den Dienst jetzt im Browser unter web.example.com erreichen.

Damit haben Sie die Kernfunktionen von Pangolin kennengelernt. Wer mag, ergänzt Pangolin um einen externen Identity Provider wie Keycloak oder Authentik oder vernagelt seine Dienste mit einer zusätzlichen Passwort- oder PIN-Abfrage. Alle Features in diesem Artikel zu erläutern, würde den Rahmen sprengen. Apropos vernageln: Sie sollten in Pangolin aber unbedingt die Zwei-Faktor-Authentifizierung aktivieren, denn es ist immerhin zugleich Tür und Türsteher zu Ihren selbst gehosteten Diensten.

GitHub-Repository mit Beispielen und Downloadlinks:
ct.de/wvkd

Fazit

Je nach Anzahl der selbst gehosteten Dienste oder Architektur Ihres Homelabs mag für Sie eine Portweiterleitung zu einem Reverse-Proxy wie Caddy, eine „klassische" VPN-Verbindung ins Heimnetz oder eine Allroundlösung wie Pangolin am besten passen. Aber auch raffinierte Software wie Pangolin entbindet Sie nicht von der Aufgabe, die Webdienste, die Sie hosten, aktuell zu halten und sicher zu konfigurieren. (ndi) c't

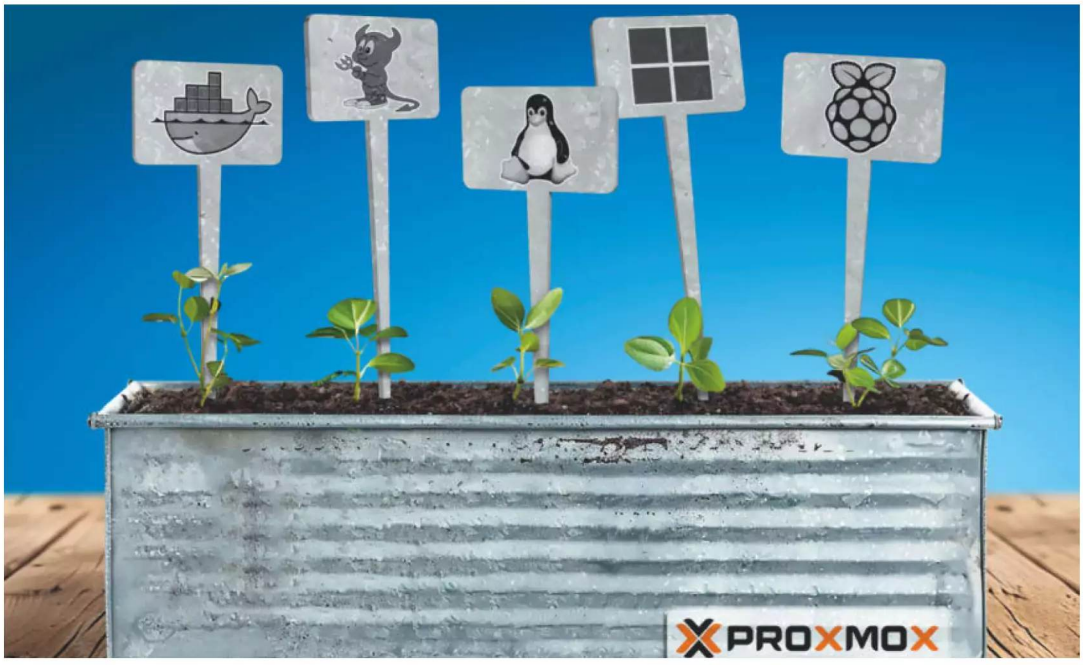


Bild: Collage c't

Ein Blick auf Proxmox VE

Proxmox VE ist eine auf Virtualisierung spezialisierte Linux-Distribution für Server. Sie ist interessant für Menschen, die virtuelle Maschinen nicht auf einem lärmenden Rechner unterm Schreibtisch betreiben wollen, sondern im Separee, Keller oder im Rechenzentrum. Es macht im Home Lab wie beim Hoster eine gute Figur und erweist sich in vielen Szenarien als kostengünstige VMware-ESXi-Alternative.

Von **Peter Siering**

Was Linux-Distributionen gern zugeschrieben wird, nämlich kryptisch zu sein, gilt für Proxmox VE nicht: Nach der Installation eröffnet dem Nutzer eine komfortable Weboberfläche die gesamte Welt der Virtualisierung: virtuelle Maschinen (VMs) einrichten, starten, stoppen, klonen, Snapshots anfertigen, Netzwerkdetails konfigurieren, Platten vergrößern, Backups ziehen, Proxmox-Updates installieren und vieles mehr.

Ebenfalls im Browser erhält man Zugriff auf die Konsolen der virtuellen Maschinen, etwa um eine darin ablaufende Betriebssysteminstallation zu bedienen. Dieser Tastatur-, Maus- und Bildschirmersatz genügt zum Bedienen. An den Komfort der Desktop-

Virtualisierung mit VMware Workstation, VirtualBox und Co. reicht es aber nicht ganz heran, weil es standardmäßig auf dem simplen VNC-Protokoll aufbaut.

Mit all diesen Mitteln lässt sich ein Mietserver beim Hoster prima aufteilen, etwa VMs an Freunde untervermieten oder produktive und experimentelle Arbeitslasten voneinander trennen. Selbst auf schwächeren Geräten, etwa einem aufgemotzten Thin Client läuft Proxmox anstandslos und ersetzt so den Raspi-Zoo und wuppt nebenbei die Arbeitslast des in die Jahre gekommenen Home-Servers.

Wie es geht

Beim Einrichten einer VM oder auch später lässt sich alternativ zu VNC ein anderes Verbindungsprotokoll der Konsole aktivieren: Spice. Mit einem Spice-Client und etwas vermittelnder Software kann man sich so komfortabel direkt auf die virtuelle Konsole einer VM aufschalten, ohne dafür auch nur die Proxmox-Weboberfläche aufrufen zu müssen; die dabei hilfreiche Software PVE VDI Client, die nicht von Proxmox selbst stammt, finden Sie via ct.de/w39z.

Bei der Art und Weise, wie Proxmox die virtuellen Festplatten der VMs verwaltet, weicht es von Desktop-Lösungen ab: Statt Dateien benutzt es standardmäßig logische Volumes, also Teilbereiche vorhandener Partitionen, die ein spezialisiertes Volume-Management verwaltet. Man muss sich darüber keine Gedanken machen, sollte das aber wissen.

Welche Art von Volume-Management Proxmox nutzt, lässt sich schon bei der Installation bestimmen: Die Proxmox-Entwickler haben als Alternative zum bewährten Logical Volume Managenent (LVM) auch ZFS eingebaut. Natürlich ist es möglich, auch später noch Speicher zu ergänzen. Man ist dabei nicht auf das bei der Installation ausgewählte Verfahren festgelegt; es ist im Vorfeld aber sinnvoll, sich mit der Auswahl zu befassen.

Für ZFS spricht: Es kennt inkrementelle Snapshots. Die verwendet Proxmox geschickt, um Änderungen an virtuellen Platten von einem Proxmox-Knoten auf einen anderen zu replizieren. Da nur geänderte Daten durch die Leitung wandern, ist das schnell und für alle interessant, die mehrere Proxmox-Rechner als Cluster-Knoten betreiben und VMs hin und herschieben wollen.

Proxmox baut auf der Virtualisierung im Linux-Kernel (KVM) auf. In diesem Kontext liest man auch immer wieder den Namen QEMU. Dieses ursprünglich als Systememulator gestartete Projekt hilft Virtualisierungssoftware häufig dabei, die nötige PC-Umgebung auf die Beine zu stellen, so auch Proxmox.

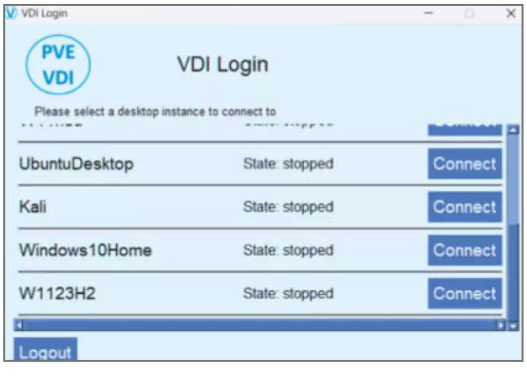
Was drin ist

Die Minimalausstattung für einen Proxmox-Knoten ist ein x86-PC mit nutzbaren Virtualisierungsfunktionen im Prozessor und eine SSD als Datenspeicher für Betriebssystem und die VMs; Magnetplatten taugen für Virtualisierung nicht, sie sind zu langsam. Ein Mini-PC oder mancher Thin Client genügt also vollkommen, je nach Arbeitslast und Inhalt der VMs natürlich.

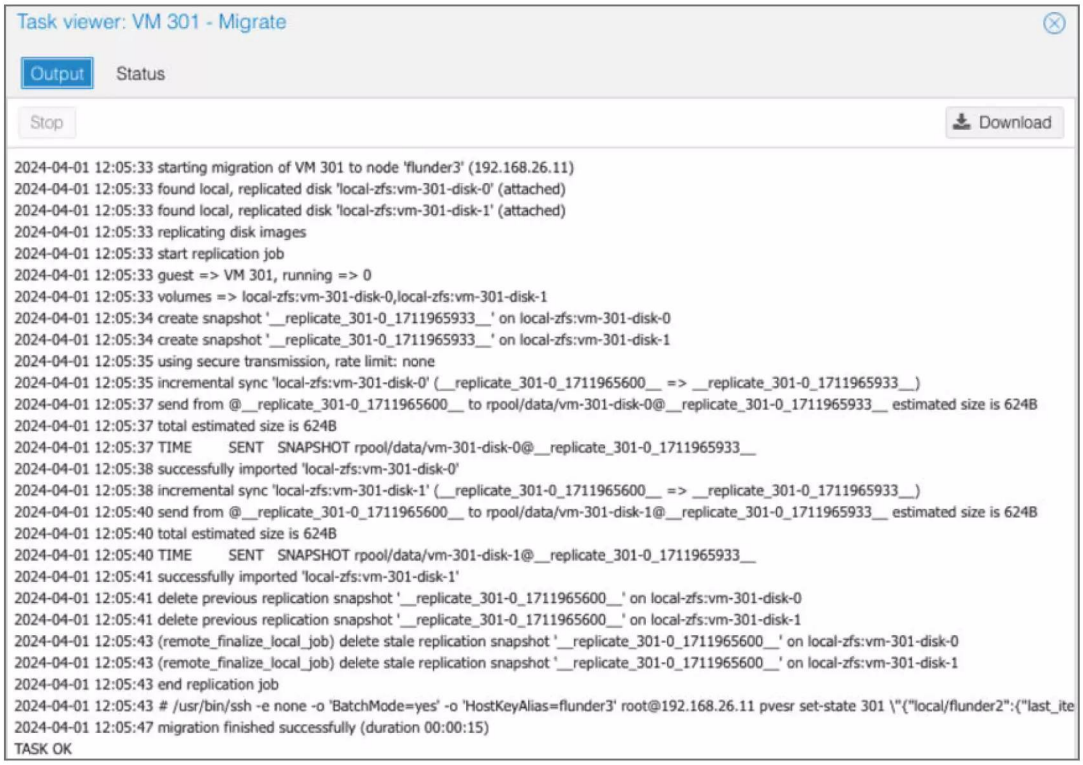
Unter der Haube von Proxmox steckt ein aufgebohrtes Debian. Der Hersteller erweitert es mit eigenem Kernel, unter anderem für den ZFS-Support, Erweiterungen zur Verwaltung der virtuellen Maschinen (qemu-Server genannt) und viele Zutaten, die erst im professionellen Einsatz interessant werden, wenn mehrere Proxmox-Knoten im Verbund auf ein gemeinsames Speichersystem zugreifen sollen oder gemeinsam ein solches bilden.

Grundsätzlich ist eine Installation auch aus einem bereits laufenden, aktuellen Debian-System heraus möglich. Das kann hilfreich sein, wenn Proxmox auf einen Mietserver gelangen soll, dort keine passenden Vorinstallationen angeboten werden und auch ein Anstöpseln eines USB-Sticks oder ISOs aus der Ferne nicht vorgesehen ist.

Dass Debian die Basis bildet, ist auch aus einem weiteren Grund wichtig zu erwähnen: Für Updates nutzt Proxmox die Debian-Paketverwaltung (APT). Deren Ausgaben und eventuelle Rückfragen bei der Paketinstallation versteckt es nicht hinter der Weboberfläche, sondern öffnet ein weiteres Browserfenster mit einer Textkonsole dafür. Hier muss der Nutzer eventuell Fragen beantworten und sieht den Fortschritt.



Etwas zusätzliche Software hilft, vom Desktop-PC oder Notebook die VMs fernzubedienen, ohne die Proxmox-Weboberfläche überhaupt aufrufen zu müssen.



Mit ZFS als Aufbewahrungsort und eingerichteter regelmäßiger Replikation schiebt Proxmox VMs binnen Sekunden von einem Cluster-Knoten auf einen anderen.

Die Update-Installation und Upgrades auf die nächste Proxmox-Version sind die einzigen Stellen, an dem auch Proxmox-Nutzer ohne Linux-Ambitionen eine Kommandozeile verwenden müssen. APT stellt dort Rückfragen, die mit der vorgegebenen Standardantwort meist passend beantwortet werden können. Die Proxmox-Entwickler helfen bei Upgrades zur nächsten Version vorbildlich: Es gibt ein Programm, das überprüft, ob alle Voraussetzungen überhaupt erfüllt sind, und mit Hinweisen dient, wie die gegebenenfalls herzustellen sind.

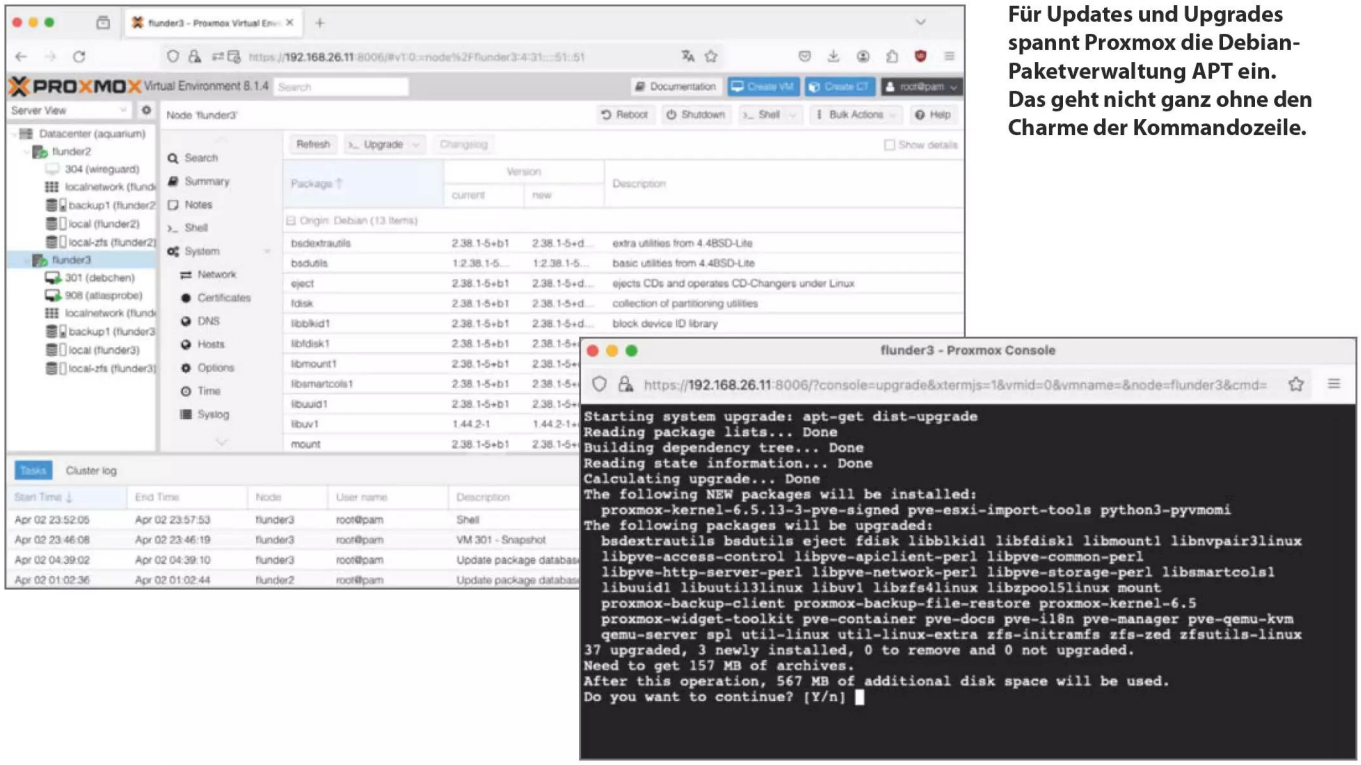
Mit jeder Proxmox-Version wachsen die Fähigkeiten des Produkts. Sämtliche Funktionen werden nur die wenigsten Nutzer brauchen. Ein paar Highlights: Die integrierte Nutzerverwaltung kennt Zweifaktorauthentifizierung und Rollen. Die ohnehin komfortable Netzwerkverwaltung, die mit VLANs und Bridges umgehen kann, ist zum vollwertigen SDN-Stack angewachsen (Software-defined Networking).

Schon immer kennt Proxmox nicht nur gekapselte virtuelle Maschinen, sondern erlaubt es auch, Container-Technik zu nutzen. Die Entwickler setzen dabei allerdings nicht auf Docker, sondern Linux Container (LXC), die technisch anders funktionieren (siehe S. 88).

Was entsteht

Proxmox macht bereits auf einem Minimal-PC eine gute Figur. Es kann dort VMs beherbergen, die zum Beispiel die im Haus verstreuten, fürs Smarthome zuständigen Raspis ersetzen. Über die Funktionen zum Hineinreichen von USB-Geräten des Wirts-PCs in die VMs kommen Docker-Container in einer VM bequem auch an Zigbee-Sticks heran. In der Proxmox-Oberfläche trägt man dazu nur die USB-IDs ein und die VM sieht das Gerät.

So bündelt Proxmox Dienste, die aus taktischen Gründen als separate Hosts eingerichtet sind, platz- und energiesparend in VMs: VPN-Server, Backup-Server, virtualisierte Ripe Atlas Probe, Freifunk-Offloader sowie Software-Firewall haben keine großen Ansprüche an Hauptspeicher. Denen genügen oft ein paar GByte oder sogar nur wenige 100 MByte RAM und etwas Plattenplatz.



Für Updates und Upgrades spannt Proxmox die Debian-Paketverwaltung APT ein. Das geht nicht ganz ohne den Charme der Kommandozeile.

Ebenso gut befeuert Proxmox fett ausgestattete Systeme, um darauf mehrere Windows-VMs zu betreiben, beispielsweise eine Testumgebung inklusive Active Directory. Egal, ob Linux oder Windows: Groupware, Maildienste, Software für die private Cloud, all das lässt sich in VMs auftrennen, sodass unterschiedliche Systemanforderungen, etwa für die Basisdistribution, nicht den Einsatz weiterer Rechner erfordern. Weitere VMs genügen.

Mit wachsenden Ansprüchen bietet Proxmox die Möglichkeit, mehrere Server zu Clustern zusammenzufassen. Es überträgt VMs, die man unter den Schutz des High-Availability-Modus stellt, automatisiert auf andere Knoten im Cluster. Live-Migration von VMs von einem auf einen anderen Knoten brauchen dann nicht zwangsläufig ein gemeinsam genutztes Speichersystem. Aber auch das kann Proxmox: Mit dem verteilten Speichersystem Ceph lässt es mehrere Knoten auf einen gemeinsamen Speicher blicken.

Was davon man wirklich braucht, hängt von den Ansprüchen ab. Wer nur sicherstellen will, keine VMs und darin enthaltene Daten zu verlieren, sollte sich in jedem Fall den Proxmox Backup Server ansehen. Der ist auch dann sehr nützlich, wenn man VMs nur gelegentlich bequem per Mausklick von einem auf einen anderen Server schieben möchte.

Erwähnte Downloads

ct.de/w39z

Wer dahintersteckt

Fast unglaublich ist, wie entspannt die Proxmox-Schöpfer ihr unter AGPLv3 gestelltes Produkt anbieten. Jeder darf die Virtualisierungsumgebung gratis nutzen. Wer die stärker qualitätsgesicherten Enterprise-Pakete verwenden möchte, die der Hersteller für produktiven Einsatz empfiehlt, kann dafür ein Community-Abo für 115 Euro pro Jahr und Sockel abschließen. Supportleistungen sind ab 355 Euro pro Jahr inbegriffen.

Der folgende Artikel taucht tiefer in die Welt von Proxmox ein und zeigt Wege auf, wie VMware-ESXi-Verstoßene ihre VMs recht bequem in die entspannte Proxmox-Welt retten können. Sollten Sie nur nach einer Alternative zur bisher verwendeten Desktop-Virtualisierung suchen: Sie werden längst nicht alles brauchen, was der Artikel zeigt. Aber das schadet auch nicht. (ps) c't

Für Nerds und Maker

shop.heise.de/highlights2024

Zubehör und Gadgets

Oxocard Artwork Creative Coding

Lernen Sie die Grundlagen der Computeranimation mit dem ESP32-Chip. Erzeuge beeindruckende visuelle Effekte wie in Spielen und Filmen dank leistungsfähiger Hardware.

Ideal für Einsteiger!

~~69,90 €~~

39,90 €

Oxocard Science Plus GOLD Edition

Hochwertige Computerplatine mit 8 Sensoren, 16 Werten, Experimentierplatine und offener Programmierschnittstelle zur Beobachtung und Änderung der Programme.

Im praktischen Kreditkartenformat!

119,90 €

c't 3003-Hipbag/Bauchtasche

Total praktisches c't 3003-Merch.
Dieses ultimative Fashion-Statement fällt garantiert überall auf und es passt jede Menge rein.
Mit Innentasche und verstellbarem Hüftgurt.

Sieht garantiert ghyle aus!

14,90 €

Cyber Clean Professional Reinigungsmasse

High-Tech-Masse entfernt 99,99% der Keime, reinigt strukturierte Oberflächen und Zwischenräume, ohne Feuchtigkeit abzugeben. Ideal für empfindliche Oberflächen und elektronische Geräte.

Für Hygiene und Wohlbefinden!

16,90 €

Nitrokey Passkey

Schützen Sie Ihre Accounts zuverlässig gegen Phishing und Passwort-Diebstahl mit sicherem, passwortlosem Login und Zweifaktor-Authentifizierung (2FA) durch WebAuthn/FIDO2. Praktisches USB-A Mini Format für den Schlüsselbund.

Qualität made in Germany!

34,90 €

AUCH ALS USB-A/C-VERSION

Nitrokey-Secure-Bundle C/C

Der Nitrokey 3A NFC ist ein starker Security Token für mobile Geräte. Der USB-C Daten Blocker schützt vor unerwünschter Datenübertragung. Inklusive c't-Security-Checklisten als PDF.

Schutz gegen Massenüberwachung und Hacker!

64,90 €

c't Jumbotasse „Kein Backup? Kein Mitleid!“

Unsere Tasse erinnert Ihre Kollegen an regelmäßige Updates. Jetzt mit 450 ml für mehr Kaffeegenuss.
Nie wieder Stress ungesicherter Daten:
Kein Backup? Kein Mitleid!

Natürlich spülmaschinengeeignet!

17,90 €

Messbecher „Wissenschaft“

Schluss mit Langeweile in der Küche! Auf diesem Messbecher stehen 14 nerdige Fun Facts. Fragen wie „Wie viel Platz nehmen 30.000 Reiskörner ein?“ werden beantwortet.

Aus hitzebeständigem Borosilikatglas!

19,90 €

Jetzt NEU

Neue Version 2025:

c't Desinfec't 2025

Ihr Rettungssystem bei Virenbefall

+

c't 12/2025 digital auf einem bootfähigen 32 GByte USB-Stick

- Bootbarer Hybrid-Stick USB-A/C mit 32 GByte
- Enthält das Antiviren-Tool der c't-Experten
- Mit digitaler c't 12 und Desinfec't-Anleitung

NEU

im heise shop!

shop.heise.de/ct-desinfect25

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise shop

Bild: Collage c't

Starten mit Proxmox VE

Proxmox Virtual Environment ist eine funktionsreiche und vielseitige Virtualisierungsumgebung, die man komfortabel über eine Weboberfläche administriert. Wir zeigen, wie Sie Proxmox aufsetzen, virtuelle Maschinen erstellen oder bestehende importieren und was man beachtet muss, um es produktiv zu nutzen.

Von **Niklas Dierking**

Wie lege ich mit Proxmox los?“, „Passt das zu unseren Anforderungen?“, „Wie ziehe ich die VMs um?“ dürften Fragen sein, die sich in jüngster Vergangenheit vom Familienadmin über den Homelabber bis zum technischen Leiter eines IT-Teams viele Nutzer gestellt haben dürften.

Die Open-Source-Virtualisierungsplattform Proxmox ist unter Interessierten schon lange kein Geheimtipp mehr, steht aber spätestens im Rampenlicht, seitdem Broadcom, der neue Eigner von VMware, die kostenlose Variante des vSphere Hypervisor (VMware ESXi) abgekündigt hat. Auch abseits von Heim-

und Testumgebungen fühlen sich Kunden von der Umstrukturierung der Lizenz- und Produktlandschaft gegängelt und sehen sich nach Alternativen um.

Der Wechsel zu Proxmox liegt nahe, denn die Virtualisierungsplattform ist etabliert und lässt, wenn es um Brot-und-Butter-Virtualisierung geht, wenig Wünsche offen. Einsatzgebiete und die dafür nötigen Hardwarekonfigurationen reichen von einer Handvoll VMs auf einem Mini-PC, um mal eine Linux-Distribution Probe zu fahren, bis zu VM-Flotten auf einem hyperkonvergenten Cluster im Rechenzentrum, der Hunderte Produktivsysteme ausführt.

c't-Redakteure nutzen die Virtualisierungsumgebung beispielsweise, um Malware in einer isolierten Windows-VM auf die Finger zu schauen oder betreiben einen Kubernetes-Cluster auf einem Verbund schlanker Linux-VMs. Proxmox schultert auch einen Teil der Heise-Infrastruktur, wie man unter ct.de/w5bh nachlesen kann. Wer beruflich mit Virtualisierungsumgebungen arbeitet, könnte bei Proxmox eine automatische Verteilung von VMs im Cluster, abhängig von der Last der einzelnen Knoten, und Support für Enterprise-Backups wie Veeam vermissen. Die meisten Nutzer dürften sich aber für Proxmox interessieren, um aus einem Computer mehrere zu machen und das in der Regel auf einer dafür abgestellten Maschine, die über das Netz administriert werden kann.

In diesem Artikel konzentrieren wir uns deswegen zunächst auf die Installation auf einem einzelnen Rechner. Wir führen durch die Weboberfläche und zeigen, wie Sie VMs erstellen, importieren und sichern. Das reicht, um sich mit der Virtualisierungsplattform vertraut zu machen. Wer Größeres vorhat, verdrahtet mehrere Proxmox-Knoten zu einem Cluster.

Proxmox installieren

Zunächst laden Sie ein Installationsmedium aus dem Downloadbereich der Proxmox-Website herunter und schreiben das mit einer Anwendung wie Etcher auf einen USB-Stick (alle Tools und Downloads finden Sie über ct.de/w5bh). Alternativ installieren Sie auf einem Debian-System Proxmox und dessen Kernel aus dem Proxmox-Repository. Das bietet sich beispielsweise an, wenn Sie Proxmox bei einem Cloudprovider aufsetzen wollen, der es nicht im Angebot hat.

Grundsätzlich hat Proxmox keine hohen Systemvoraussetzungen. Für Testzwecke reicht eine 64-Bit-CPU mit Intel-VT- oder AMD-V-Features, die auch im UEFI-BIOS aktiviert sein müssen, und 1 GByte Arbeitsspeicher. Wer mehrere VMs betreiben will, braucht mehr Arbeitsspeicher. Um Geräte wie eine Grafikkarte in eine VM zu reichen (PCIe-Passthrough), müssen CPU und Motherboard IOMMU-Remapping (I/O Memory Management Unit) beherrschen. VMs und Proxmox selbst profitieren von schnellem SSD-Massenspeicher. Für die Sicherung virtueller Maschinen empfiehlt sich ein zweiter Rechner, auf dem Sie Proxmox Backup Server installieren, aber dazu später mehr.

Schließen Sie Monitor, Maus und Tastatur an den Proxmox-Host an und verbinden Sie ihn mit einem Netzwerk, auf das Sie von einer weiteren Maschine Zugriff haben. Nach dem Start vom USB-Stick begrüßt Sie der grafische Installationsassistent. Akzeptieren Sie die Lizenzvereinbarungen und wählen dann ein Laufwerk für die Installation. Wenn Sie nur ein Laufwerk haben, das sowohl Proxmox selbst als auch VM- und Container-Images beherbergt, müssen Sie jetzt eine wegweisende Entscheidung treffen.

Der Installer beansprucht standardmäßig das gesamte Laufwerk und richtet es für den Linux-eigenen Logical Volume Manager (LVM) als physisches Volume ein. Das gliedert sich in die logischen Volumes root, swap und data. Die Root-Partition wird mit ext4 formatiert. Das data-Volume nutzt LVM-thin, um platzsparende Snapshots zu ermöglichen.

Diesen Weg empfehlen wir den meisten Nutzern, die Proxmox im Heimbetrieb einsetzen. Wer aus mehreren Proxmox-Knoten einen Cluster machen will, greift stattdessen zu ZFS. Das ist Voraussetzung für die sogenannte Storage Replication zwischen Proxmox-Knoten. Dabei werden Schnappschüsse der Gastsysteme auf weiteren Knoten vorgehalten. Das verkürzt die Migration einer VM von mehreren Minuten auf wenige Sekunden. Natürlich können Sie später auch weiteren Speicher hinzufügen und für ZFS einrichten. Beachten Sie, dass ZFS gern mehr RAM beansprucht. Die Proxmox-Entwickler raten mindestens zu 8 GByte.

Im nächsten Schritt müssen Sie Land, Zeitzone und Tastaturlayout angeben, wenn der Installer das nicht selbst ermitteln konnte. Anschließend vergeben Sie eine Mail-Adresse und ein Passwort für den Nutzer root, mit dem Sie sich standardmäßig in der Weboberfläche und via SSH anmelden. Der Installer sollte Proxmox eine IP-Adresse mittels DHCP besorgt haben. Falls nicht, dann passen Sie jetzt die Netzwerkkonfiguration an. Sie sollten dem Proxmox-Host in Ihrem Router eine feste IP-Adresse zuweisen oder reservieren. In dieser Anleitung

gehen wir davon aus, dass der Hostname Ihres Proxmox-Knoten „pve“ lautet.

Kontrollieren Sie im letzten Schritt die Zusammenfassung und starten dann die Installation. Nach einem Neustart zeigt Proxmox die URL seiner Weboberfläche an, beispielsweise https://192.168.1.90:8006.

Rufen Sie die Adresse im Browser von einem anderen Gerät im Netz auf, bestätigen Sie die Ausnahme für das selbst signierte Zertifikat und melden Sie sich dann als root an. Wenn die Seite nicht erreichbar ist, gibt es wahrscheinlich ein Problem mit Ihrer Netzwerkkonfiguration. Bei der Fehlersuche hilft ein Blick in /etc/network/interfaces und die Proxmox-Dokumentation (siehe ct.de/w5bh).

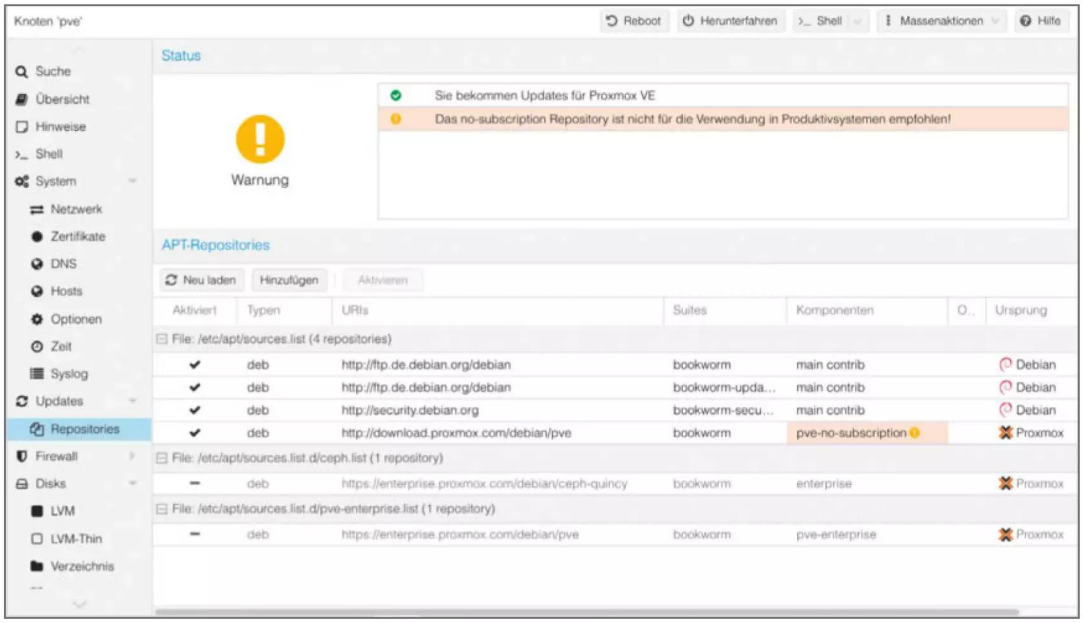
Weboberfläche

Die Weboberfläche von Proxmox setzt sich aus vier Bereichen zusammen. Über den Header am oberen Rand erstellen Sie Gastsysteme, nehmen persönliche Einstellungen vor und fahren den Knoten herunter. Am linken Rand finden Sie eine Baumansicht, die Proxmox „Ressource Tree“ nennt, mit allen Rechenressourcen. Die oberste Ebene darin ist das Rechenzentrum beziehungsweise der Cluster, sofern Sie einen eingerichtet haben. Auf der Ebene der Knoten werden deren Netzwerk, Storage-Pools, sowie VMs und Container gelistet. Zunächst besteht Ihr Rechenzentrum nur aus einem Knoten namens pve.

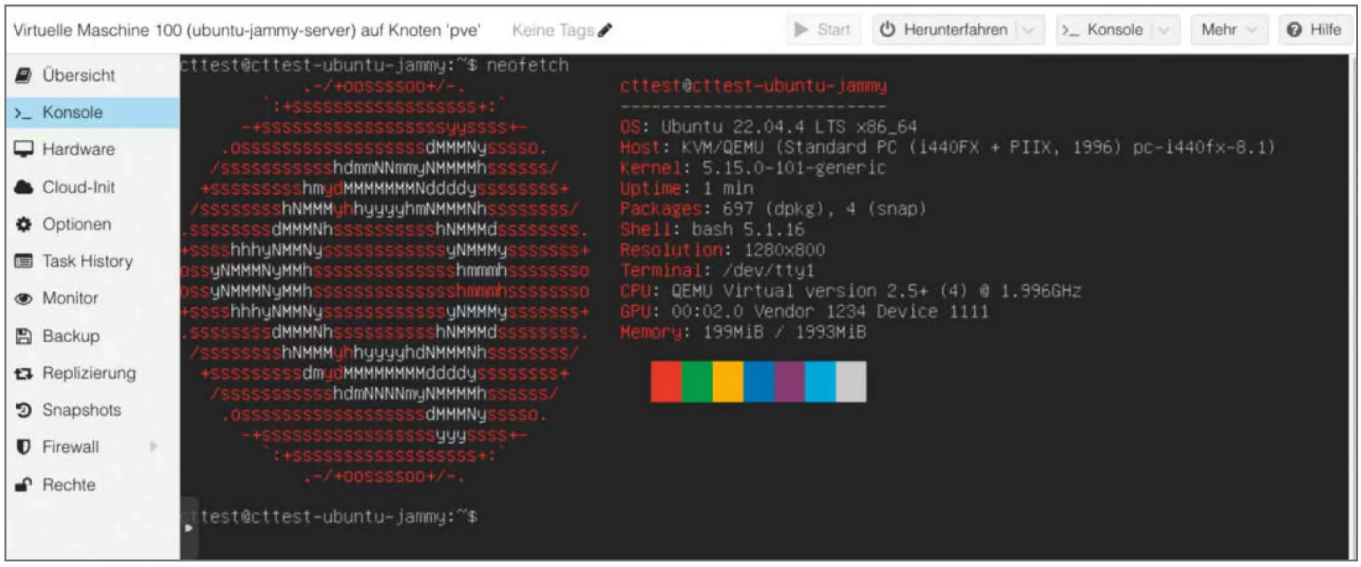
In der Mitte der Weboberfläche befindet sich ein dynamischer Bereich, der Informationen über die ausgewählten Objekte anzeigt. Das Log Panel am unteren Rand des Fensters listet laufende und abgeschlossene Tasks. Ein Task kann beispielsweise ein Backup oder der Neustart einer VM sein.

Proxmox warnt Sie nach der Anmeldung, dass Sie keine Subskription abgeschlossen haben. Durch diese Support-Abos, die in der günstigsten Variante „Community“ 115 Euro pro CPU-Sockel im Jahr kosten, kann Proxmox das Projekt weiter entwickeln und Sie bekommen Zugriff auf die Enterprise-Repositories. Die enthalten Pakete, die intensiver getestet wurden. Professionellen Support gibt es ab 355 Euro im Jahr.

Wenn Sie Proxmox ohne Support-Abo nutzen, müssen Sie die Enterprise- gegen die Community-Repositories tauschen, damit Sie Updates bekommen. Navigieren Sie auf der Ebene des Knotens in das Menü „Repositories“ unterhalb von „Updates“ und deaktivieren dort die Repositories „pve“ und „ceph-quincy“ von enterprise.proxmox.org. Klicken Sie danach auf die Schaltfläche „Hinzufügen“. Es



Proxmox ist erst mal kostenlos für Jedermann. Wer nicht für Enterprise-Repositories bezahlen will, die intensiver getestete Pakete enthalten, muss mit den Community-Repositories vorliebnehmen.



Standardmäßig stellt VNC in einem Fenster die Bildschirmausgaben einer virtuellen Maschine dar. Das funktioniert auch bei Betriebssystemen mit grafischer Oberfläche.

öffnet sich ein Fenster, in dem Proxmox erneut ein Support-Abo empfiehlt. Schließen Sie das Fenster nicht, sondern bestätigen Sie mit „Ok“. Danach fügen Sie das Repository „No-Subscription“ aus dem Dropdown-Menü hinzu.

Aktualisierungen für Proxmox VE spielen Sie über das Menü „Updates“ ein. Alle Funktionen, die in diesem Artikel anhand der Proxmox-Weboberfläche erklärt werden, haben eine Entsprechung auf der Kommandozeile (ct.de/w5bh).

Stauraum

Der Ressource Tree listet unterhalb des Knoten pve mindestens zwei lokale Storage-Pools, die unterschiedliche Aufgaben erfüllen. Wenn Sie sich bei der Installation für LVM entschieden haben, heißen sie „local“ und „local-lvm“. Proxmox verfügt über eine ganze Reihe von Storage-Plug-ins und unterscheidet Storage nach Datei- oder Blockebene (siehe ct.de/w5bh).

Der Storage local ist vom Typ „Verzeichnis“, operiert auf Dateiebene und ist für ISO-Images, Container-Templates und lokale Backups bestimmt. local-lvm ist hingegen ein Blockspeicher für die Laufwerke der virtuellen Maschinen und Container. Falls Sie sich für ZFS entschieden haben, finden Sie local und local-zfs, die auf Datei- und Blockebene operieren.

Über das Menü „Storage“ können Sie jederzeit weitere Datenspeicher, beispielsweise entfernte SMB-/CIFS- oder NFS-Freigaben, für Backups ergänzen.

Virtuelle Maschinen anlegen

Befördern Sie eine ISO-Datei in den Storage local, um sie als Installationsmedium für eine virtuelle Maschine zu nutzen. Die können Sie von Ihrem lokalen Rechner hochladen, von einer URL herunterladen oder mit `scp` in das Verzeichnis /var/lib/vz/template/iso schieben. Für erste Gehversuche bietet sich beispielsweise das schlanke Ubuntu Server 24.04 als Gastsystem an (siehe ct.de/w5bh).

Klicken Sie im Header auf die Schaltfläche „Erstelle VM“, öffnet sich ein Assistent, der Sie durch die Erstellung der virtuellen Maschine führt. Geben Sie der Maschine einen Namen, beispielsweise ubuntu-jammy-server, und eine VM ID. Die ID brauchen Sie unter anderem bei Backups oder wenn Sie mit den Kommandozeilenwerkzeugen von Proxmox an VMs herumdoktern. Am besten überlegen Sie sich früh ein Schema, nach dem Sie IDs vergeben, beispielsweise 300 bis 400 für Test-VMs und 800 bis

900 für den Produktivbetrieb. Im Reiter „OS“ legen Sie der VM die ISO-Datei aus dem Storage local ins virtuelle Laufwerk, die restlichen Einstellungen übernehmen Sie. Bei „System“ müssen Sie nichts anpassen.

Sie sollten nach Möglichkeit immer den Haken für den QEMU-Gastagenten setzen und den Helfer später auf dem Gastsystem installieren. Wie üppig Sie die VM mit CPU, Speicherplatz und Arbeitsspeicher versorgen, hängt von Ihrer Hardware und geplanten Workloads ab. Bei der Option CPU-Typ müssen Sie gewünschte Performance und Kompatibilität abwägen. Die Einstellung „host“, auch CPU-Passthrough genannt, ist performanter als eine generische CPU wie „x86-64-v2-AES“, kann aber zu Problemen führen, wenn Sie VMs in einem Cluster zwischen Knoten mit unterschiedlichen Prozessoren migrieren wollen. Im Reiter „Speicher“ legen Sie über die erweiterten Optionen zusätzlich zum maximalen Speicher auch eine minimale Speichermenge fest. Zum Schluss fasst der Assistent die Konfiguration der VM noch mal zusammen.

Markieren Sie die Ubuntu-VM im Ressource Tree und starten Sie sie. Mit einem Klick auf „Konsole“ öffnen Sie VNC (Virtual Network Computing), das als Fenster in die Maschine dient und Tastatureingaben durchreicht, wenn das Fenster den Fokus hat.

Nach der Installation von Gastsystemen sollten Sie den QEMU-Gastagenten nachrüsten. In Ubuntu installieren Sie dazu das Paket qemu-guest-agent:

```
sudo apt update
sudo apt install qemu-guest-agent
```

Je nach Distribution müssen Sie danach noch dafür sorgen, dass der Agent beim Systemstart anläuft:

```
sudo systemctl enable qemu-guest-agent
sudo systemctl start qemu-guest-agent
```

Bei einem Debian-Gastsystem können Sie sich diesen Schritt sparen. Danach zeigt Proxmox die IP-Adresse(n) der VM im Menü „Übersicht“. Außerdem fährt es VMs mit dem Gastagenten geordnet herunter und bereitet sie auf Backups und Snapshots vor.

Um nicht immer wieder den Installationsprozess, beispielsweise von Ubuntu Server, zu durchlaufen, können Sie VMs klonen oder Sie in Templates umwandeln, also Vorlagen. Proxmox unterscheidet zwischen vollständigen und verknüpften Klonen. Letztere sparen Speicherplatz, sind aber nicht Knoten-übergreifend möglich, weil sie Zugriff auf den lokalen Storage mit der virtuellen Festplatte brauchen. Die Proxmox-Dokumentation rät dazu, VM-Templates frei von Nutzerdaten und Geheimnissen zu halten (siehe ct.de/w5bh). Wie Sie Gastsysteme mit cloud-init vorkonfigurieren und verhindern, dass virtuelle Maschinen aus Templates die gleiche IP-Adresse wie die Vorlage bekommen, haben wir in [1] aufgeschrieben.

Windows-VMs

Im Assistenten zur Erstellung virtueller Maschinen müssen Sie im Reiter „OS“ für Windows-VMs den Typ „Microsoft Windows“ auswählen. Im Unterschied zu den meisten Linux-Distributionen, die Treiber für paravirtualisierte Geräte (VirtIO) mitbringen und automatisch laden, müssen Sie die bei Windows-VMs nachinstallieren.

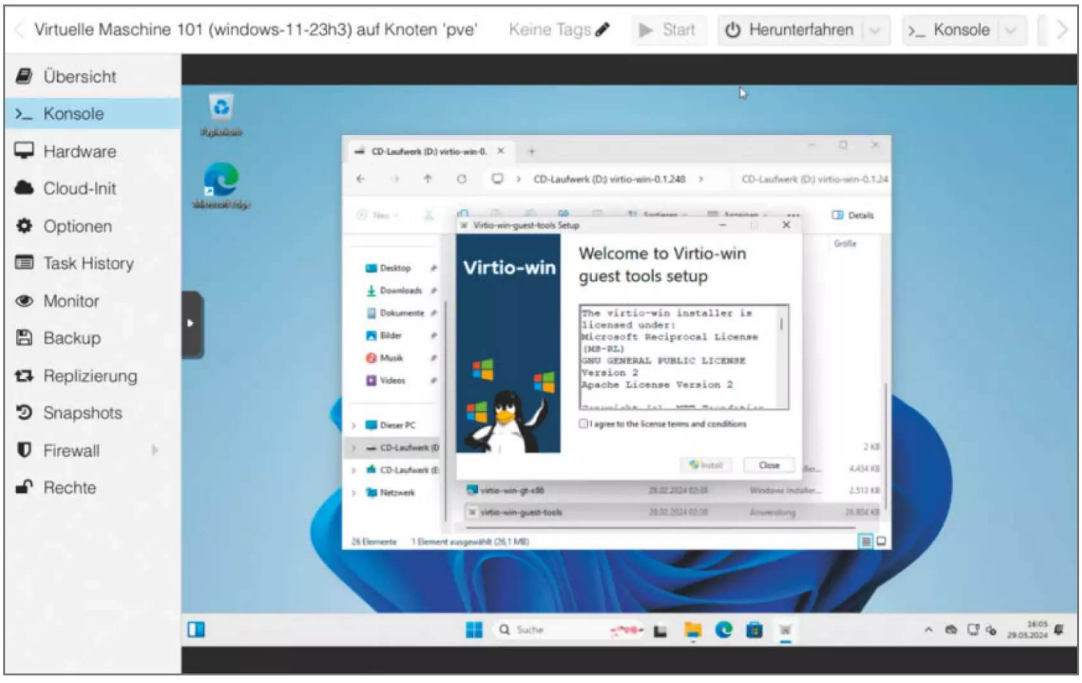
Das Fedora-Projekt stellt ein ISO-Image mit quelloffenen, signierten VirtIO-Treibern und dem QEMU-Gastagenten zur Verfügung (siehe ct.de/w5bh). Laden Sie die ISO-Datei in den local-Storage und reichen Sie sie an die virtuelle Maschine durch. Das können Sie beim Erstellen der VM direkt im Reiter „OS“ erledigen, indem Sie den Haken bei „Zusätzliches Laufwerk für VirtIO-Treiber hinzufügen“ setzen oder Sie holen das später im Menü „Hardware“ nach. Die Treiber- und Werkzeugsammlung installieren Sie dann in Windows.

Für Windows-11-VMs müssen Sie außerdem OVMF (UEFI) statt SeaBIOS auswählen sowie ein TPM (Trusted Platform Module) und ein EFI-Laufwerk hinzufügen. Achten Sie beim ersten Start darauf, dass die Installations-ISO die höchste Priorität in der Bootreihenfolge bekommt. Das erledigen Sie im Menü „Optionen“ unter „Bootreihenfolge“.

VMs von ESXi importieren

Um virtuelle Maschinen von einem VMware-ESXi-Host zu Proxmox zu migrieren, gibt es mehrere Methoden. Ihnen ist gemein, dass Sie vor dem Transfer Umzugskartons packen müssen, indem Sie eingehängte ISO-Dateien auswerfen, VMware-Gästetools deinstallieren und die VMs herunterfahren.

VMware stellt für Umzüge das Kommandozeilenwerkzeug `ovftool` zum Download bereit (siehe ct.de/w5bh), das man auch direkt auf dem Proxmox-Knoten ausführen kann. Dadurch spart man sich beispielsweise den Umweg über eine Netzwerkfreigabe. Für den Download mussten wir einen kostenlosen VMware-Account einrichten. Befördern Sie den



Für Windows 11 in Proxmox braucht es ein paar zusätzliche Handgriffe. Treiber für VirtIO bringt man über eine ISO-Datei in die virtuelle Maschine.

Installer via `scp` auf den Proxmox-Knoten. Dort machen Sie ihn ausführbar und installieren `ovftool`:

```
chmod +x ./VMware-ovftool-\
4.6.2-22220919-lin.x86_64.bundle

./VMware-ovftool-\
4.6.2-22220919-lin.x86_64.bundle
```

Mit dem folgenden Befehl fischen Sie virtuelle Maschinen als OVF-Paket aus dem ESXi-Datastore:

```
ovftool vi://root@192.168.1.10/vm \
/var/lib/vz/template/iso
```

Ersetzen Sie im obigen Befehl die IP-Adresse durch die Ihrer ESXI-Instanz und den Platzhalter „vm“ durch den Namen Ihrer virtuellen Maschine. Das Import-Verzeichnis können Sie frei wählen, unser Beispielaufruf nimmt das Standardverzeichnis für ISO-Dateien.

Navigieren Sie in das Importverzeichnis und importieren Sie die VM in Proxmox:

```
qm importovf 301 vm.ovf local-lvm
```

Ersetzen Sie die VM-ID 301 durch eine eigene VM ID und passen den Namen der OVF-Datei an. Außerdem müssen Sie einen Storage für die virtuelle Festplatte der VM festlegen, beispielsweise local-lvm. Die importierte Maschine taucht anschließend im Ressource Tree auf. Die OVF-Datei können Sie jetzt löschen.

Bevor Sie die VM das erste Mal starten, müssen Sie sie in Proxmox vorbereiten. Welche Arbeitsschritte anstehen, hängt davon ab, wie Sie die VM in ESXi konfiguriert hatten. Nach einem Transfer von Ubuntu Server 22.04 mussten wir die Firmware von SeaBIOS auf OVMF umstellen, eine EFI-Disk ergänzen, eine Netzwerkkarte (VirtIO) hinzufügen und den SCSI Controller auf VirtIO SCSI single umstellen.

Eine IP-Adresse via DHCP bekam die VM erst, nachdem wir in Ubuntu in der Datei /etc/netplan/00-installer-config.yaml das neue Netzwerkinterface namens enp0s19 eingetragen hatten. Sie sollten außerdem stets den QEMU-Gastagenten nachinstallieren und in der VM-Konfiguration das entsprechende Häkchen setzen.

Die Proxmox-Entwickler haben inzwischen auch einen Assistenten für die VM-Migration von ESXi in die Weboberfläche von Proxmox integriert. Für den

Virtualisierung light: Container

Neben VMs verfügt Proxmox mit Linux Containern (LXC) noch über eine zweite Methode der Virtualisierung. Anders als bei „ausgewachsenen" virtuellen Maschinen, wo jedes Betriebssystem einen eigenen Kernel ausführt und je nach Konfiguration auch Geräte emuliert werden müssen, teilen sich Container den Kernel mit dem Host. Das reduziert den Overhead und ermöglicht schnellere Startzeiten. Verwechseln Sie Linux Container aber nicht mit Docker- oder anderen OCI-Containern (Open Container Initiative).

In seiner Anfangszeit hat Docker auf LXC aufgebaut und beide nutzen auch heute die gleichen Kernel-Funktionen zur Containerisierung, erfüllen aber verschiedene Anwendungszwecke. Docker-Images sind bewusst schlank gehalten und darauf gestutzt, nur eine Anwendung im Container auszuführen, während Linux Container als Ersatz für ein komplettes System dienen. Deswegen unterscheidet man sie auch als Anwendungs- und Systemcontainer. In Linux Containern finden Sie alle Dienste und Anwendungen, die man von einem Linux-System erwartet.

Praktisch: Proxmox bringt eine große Vorauswahl an Container-Templates mit, die Sie über das Menü „Container-Templates" in den local-Storage laden können. Darunter sind viele populäre Linux-Distributionen und Images von turnkeylinux.org, in denen, ähnlich wie bei Docker-Containern, bereits eine Anwendung wie WordPress oder eine Datenbank wie PostgreSQL steckt.

Container erstellen Sie über die Schaltfläche „Erstelle CT" im Header. Durch den gemeinsam genutzten Kernel sind Container weniger isoliert vom Wirt als eine virtuelle Maschine. Damit ein kompromittierter Prozess keinen Schaden auf dem Host anrichten kann, sollten Sie nach Möglichkeit auf unprivilegierte Container setzen. Die biegen die User-ID 0 des root-Nutzers im Container auf die User-ID eines unprivilegierten Nutzers außerhalb des Containers um.

Container profitieren ebenso wie virtuelle Maschinen von Proxmox-Features wie Replizierung, Migration oder High Availability. Dabei greifen sie auf die gleichen Ressourcen zu, beispielsweise auf die Netzwerkkonfiguration. Aber Vorsicht: Docker sollten Sie nie direkt in Proxmox installieren. Stattdessen richten Sie eine virtuelle Maschine als Dockerhost ein.

müssen Sie im Menü „Storage" Ihren ESXi-Datastore einbinden, den Proxmox über das ESXi-API anzapft.

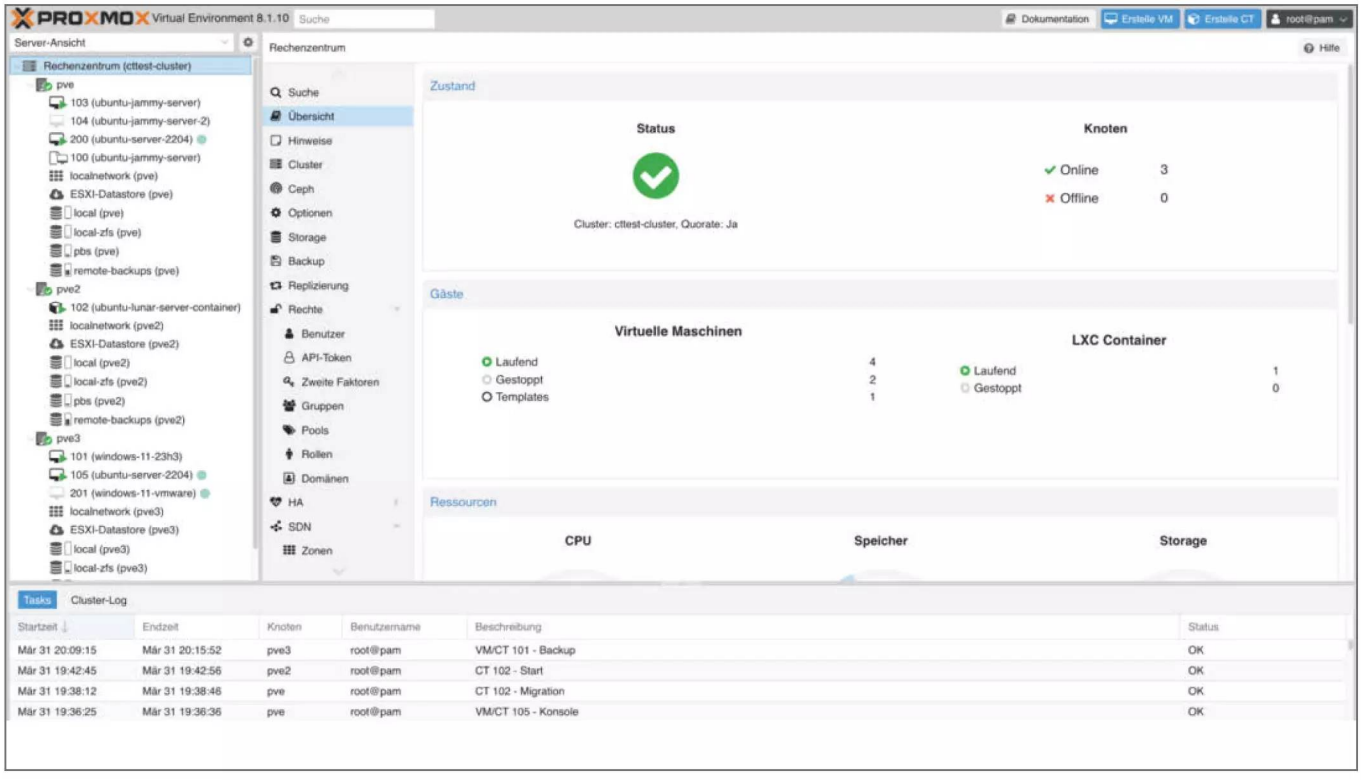
Danach markieren Sie die zu importierenden VMs in einer Liste. Sie sollten deren Konfiguration gründlich prüfen und eventuelle Fehler ausbügeln, bevor Sie den Transfer starten. Bei unserem Testlauf hat der Assistent einer Windows-11-VM beispielsweise vier CPU-Sockel angedichtet, obwohl es vier CPU-Kerne hätten sein müssen. Einige Nutzer berichten im Proxmox-Forum auch von Problemen mit Rate Limiting bei Massenimporten. In den erweiterten Hosteinstellungen von ESXi können Sie das Limit der gleichzeitigen Verbindungen erhöhen, indem Sie den Wert bei `Config.HostAgent.vmacore.soap.maxSessionCount` erhöhen oder eine 0 setzen, um Rate Limiting zu deaktivieren.

Für die Nachsorge gelten die gleichen Tipps wie beim herkömmlichen Import von VMs mit `ovftool`. Mehr Informationen dazu finden Sie in der Proxmox-Dokumentation und im Community-Forum (siehe ct.de/w5bh).

Proxmox-Cluster

In einer Produktivumgebung ist es sinnvoll, mehrere Proxmox-Knoten zu einem Cluster zusammenzufassen, um VMs herumzureichen. Die Konfigurationen der VMs speichert Proxmox dann im Cluster-Dateisystem pmxcfs und synchronisiert die Daten über das Cluster-Protokoll corosync. Damit das klappt, müssen die Knoten sich gegenseitig über die UDP-Ports 5405 bis 5412 für corosync und Port 22 für SSH erreichen können.

Für High Availability (HA), also den automatischen Transfer einer VM, wenn ein Knoten ausfällt, braucht es mindestens drei Knoten im Cluster, damit die sich auf ein gemeinsames Vorgehen einigen können. Es besteht aber die Möglichkeit, ein externes



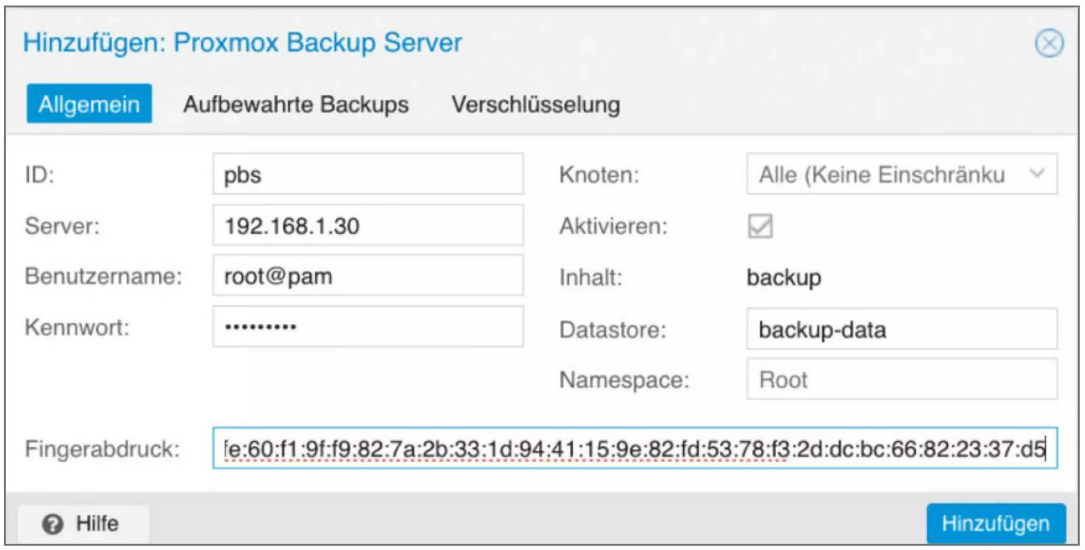
Ganz schön was los: Mehrere Proxmox-Knoten bilden einen Cluster, um VMs im High-Availability-Modus bei Problemen mit einem Knoten schnell umziehen zu können.

QDevice (Quorom Device) einzubinden, beispielsweise einen stimmberechtigten Raspberry Pi (siehe ct.de/w5bh). Weil corosync allergisch auf hohe Latenzen reagiert, sollten Sie den Cluster-Traffic im Idealfall über eine zweite Netzwerkkarte in einem separaten Netzwerk leiten.

In unserem Testlauf haben wir drei Proxmox-Knoten mit ZFS-Storage zu einem Cluster verdrahtet. Sie erstellen den Cluster über die Weboberfläche im gleichnamigen Menü auf der Ebene des Rechenzentrums. Prüfen Sie vorher, ob die IP-Adressen und Hostnamen aller Knoten passen, denn nach dem Beitritt zum Cluster können die nicht mehr geändert werden. Proxmox zeigt nach dem Erstellen des Clusters Informationen an, die Sie an die anderen Beitrittskandidaten im Menü „Cluster beitreten“ verfüttern.

Um einen verteilten Storage mit Ceph einzurichten, wird Netzwerkhardware aufwärts von Gigabit-Ethernet empfohlen. Um auch ohne Ceph Redundanz im Cluster zu gewährleisten, können Sie Schnappschüsse von VMs auf anderen Knoten vorhalten (ZFS-Replikation). Das verkürzt die Dauer der Migration zwischen zwei Knoten von mehreren Minuten auf wenige Sekunden. Navigieren Sie dazu in das Menü „Replizierung“. Hier legen Sie einen oder mehrere Zielknoten fest und konfigurieren ein Intervall, in dem Proxmox das Volume der VM synchronisiert. Nach der ersten vollständigen Synchronisation werden beim nächsten Mal nur die Änderungen am Datenstand, auch Delta genannt, übertragen.

Nur weil Ihr Cluster alle Voraussetzungen für den High-Availability-Modus erfüllt (siehe ct.de/w5bh), heißt das noch nicht, dass der Cluster Ressourcen automatisch migriert, sobald ein Knoten offline ist. Dafür müssen Sie die VMs oder Container unter den Schutz des High-Availability-Managers (`ha-manager`)



Nach der Installation bekommen Sie vom Proxmox Backup Storage nicht mehr viel mit. Er verhält sich wie ein weiterer Storage, den Sie als Ziel für Backups konfigurieren können, bietet aber viel mehr Funktionen.

stellen. Das geht über die Weboberfläche im Menü „HA“ auf der Ebene des Rechenzentrums, wo Sie auch einsehen können, ob ein funktionierendes Quorum besteht, der Cluster also beschlussfähig ist. Aktivieren Sie den HA-Modus über die Schaltfläche „Hinzufügen“ für alle Ressourcen, die Sie gegen Ausfall schützen wollen.

Je nach Workload und Zweck der VM kann es sinnvoll sein, den angestrebten Zustand, beispielsweise „started“ oder „stopped“, sowie die maximalen Versuche der Wiederbelebungen und Migrationen anzupassen.

Wer Proxmox professionell einsetzt, sollte bedenken, dass echte High-Availability auch entsprechende Hardware und Infrastruktur wie redundante Stromversorgung oder Failover-Netze braucht. Die meisten Heimanwender dürften mit einem Proxmox-Host und einer Backuplösung auskommen, aus der man VMs wiederherstellen kann.

Backups

Proxmox VE hat mit `vzdump` ein simples und solides Backup-Werkzeug an Bord, das Sie über die Weboberfläche oder die Kommandozeile konfigurieren können. Es funktioniert gut, erfasst aber alle Daten einer VM, erstellt also jedes Mal ein vollständiges Backup. Das mag für Setups mit wenigen oder kleineren virtuellen Maschinen gut funktionieren. Wenn man aber viele VMs betreibt oder gleichzeitig mehrere Backups vorhalten will, dürfte Speicherplatz irgendwann rar werden.

Ein beliebtes Ziel für vzdump-Backups sind SMB-/CIFS- oder NFS-Freigaben, zum Beispiel auf einem NAS. Binden Sie dafür die Netzwerkfreigabe im „Storage“-Menü als Ziel ein, indem Sie auf „Hinzufügen“ klicken. Bei einem NFS-Share müssen Sie einen Namen (ID) vergeben, die IP-Adresse des Servers und die exportierte Freigabe eintragen, beispielsweise /mnt/backups. Über das Dropdown-Menü „Inhalt“ markieren Sie die Freigabe als Ziel für „VZDump Backup Dateien“. Backup-Jobs, also wann von welcher Maschine Backups gezogen werden und wie lange sie vorgehalten werden, konfigurieren Sie im Menü „Backups“ in der Weboberfläche von Proxmox VE.

Proxmox unterscheidet für virtuelle Maschinen die Backup-Modi snapshot, suspend und stop: Letzterer vermeidet inkonsistente Daten, verursacht aber Downtime, weil die Maschine heruntergefahren und nach dem Backup neu gestartet werden muss. Der Modus snapshot funktioniert im laufenden Betrieb. Wenn der QEMU-Gastagent läuft, reduziert er das Risiko inkonsistenter Daten. Vom suspend-Modus raten die Entwickler ab. Er ist aus Kompatibilitätsgründen vorhanden.

Ein eigenständiger Proxmox Backup Server, den Sie auf einem weiteren Rechner installieren, bietet

mehr Funktionen als lokale oder NAS-Backups mit `vzdump`, beispielsweise platzsparende Deduplizierung, inkrementelle Backups oder die Wiederherstellung einzelner Dateien. Die ISO-Datei laden Sie kostenlos von der Proxmox-Website herunter.

Die Installation funktioniert so, wie Sie es bereits von Proxmox VE kennen, und auch der Backup Server bringt eine eigene Weboberfläche zur Administration mit. Als ersten Schritt können Sie wie bei Proxmox VE auf die Community-Repositories umsatteln.

Wenn sie nicht auf Profi-Features wie Tape-Archivierung angewiesen sind, müssen Sie in der Weboberfläche des Backup Servers nicht viel Zeit verbringen. Am einfachsten legen Sie mit Backups los, indem Sie den Datastore namens backup-data als Storage wie im Screenshot auf dieser Seite einbinden. Neben IP-Adresse, Benutzernamen und Passwort brauchen Sie dafür auch den Fingerprint des selbstsignierten TLS-Zertifikats. Den Fingerprint zeigt der Backup Server Ihnen im Dashboard an. Optional können Sie die Backups Client-seitig verschlüsseln lassen.

Backup Server verhalten sich passiv zu Ihrem Proxmox-Cluster: Sicherungen konfigurieren Sie pro VM im Menü „Backups“ in der Weboberfläche von Proxmox VE, das die Snapshots an den Backup Server schickt (Push-Betrieb). Die Funktion zur Wiederherstellung einzelner Dateien einer VM haben die Entwickler im Menü „Backup“ auf VM-Ebene versteckt. Die Schaltfläche für die Dateiwiederherstellung erscheint dort erst, nachdem Sie den Backup Server als Storage ausgewählt haben. Über den Dateibrowser können Sie auch Dateien auf Ihre lokale Maschine herunterladen.

Wer die Möglichkeiten des Proxmox Backup Server ausschöpfen will, sollte sich mit der umfangreichen Dokumentation vertraut machen. Das günstigste Support-Abo für den Proxmox Backup Servert ist mit 540 Euro deutlich teurer als Proxmox VE. Professionellen Support gibt es für ihn ab 1080 Euro im Jahr.

Fazit

Sie haben die wichtigsten Funktionen von Proxmox VE kennengelernt und können jetzt mit dem Virtualisieren loslegen. Wir ermutigen dazu, nach Herzenslust zu experimentieren, denn – das ist ja das Schöne an virtuellen Maschinen – Fehler lassen sich meistens schnell ungeschehen machen. Wenn Sie Fragen haben, die in Richtung „und wie mache ich XY bei meinem exotischen Anwendungsfall“ tendieren, dann sei Ihnen ein Besuch im Proxmox-Forum empfohlen. Dort tummeln sich eine sehr hilfsbereite Community und viele Proxmox-Entwickler, die Fragen beantworten. Wahrscheinlich hatte jemand anders das Problem schon vor Ihnen und Sie können von der Lösung profitieren. (ndi) c't

Literatur

[1] Niklas Dierking, Alles nach Plan, Infrastructure as Code mit Terraform und Proxmox, c't 16/2023, S. 136

Proxmox-Dokumentation, ISO mit VirtIO-Treibern und mehr:

ct.de/w5bh

Nextcloud: Wieso, weshalb, warum

Bild: Andreas Martini

Clouddienste versprechen Komfort: Geteilte Kalender, automatisch synchronisierte Dateien, gemeinsames Office, Todo-Listen sowie Notizen und alles verfügbar auf Desktop, Smartphone und Tablet. Niemand muss sich dafür zwangsläufig in die Fänge von Amazon, Apple, Google oder Microsoft begeben. Mit Nextcloud bleiben Sie Herr über die eigenen Daten.

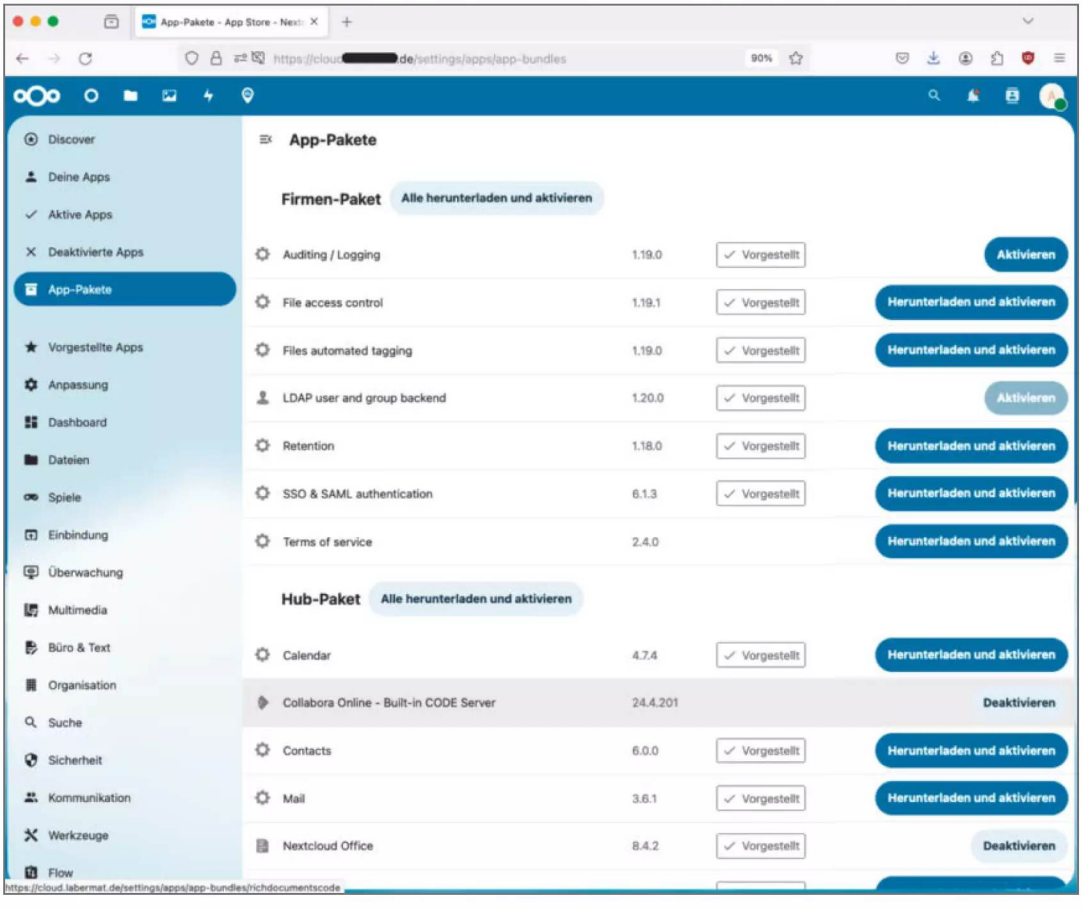
Von **Peter Siering**

Clouddienste selbst betreiben, das klingt kompliziert. Mit Nextcloud als Basis fällt das leicht. Die Daten bleiben dabei auf dem eigenen Server, dem NAS, einem Raspi oder liegen betreut beim Hoster Ihrer Wahl. Drei Wege führen zu den Daten: eine komfortable Weboberfläche, Standardschnittstellen wie CalDAV für Zugriffe auf Kalender sowie spezialisierte, Nextcloud-eigene Software auf Clients, etwa für die Synchronisation von Dateien.

Für die eigene Nextcloud spricht, dass niemand unerwartet reinredet. Die großen Cloudhoster scannen Inhalte und sperren schon mal den Zugang, wenn ihnen Bilder verdächtig vorkommen. Nutzer berichten dann immer wieder von üblen Erlebnissen und Misserfolgen, über den Support wieder Zugriff auf Ihre Daten zu erhalten. Neuerdings füttern die Anbieter auch ihre KI-Modelle mit den Daten ihrer Kunden. Mit Nextcloud können Sie alles selbst in die Hand nehmen.

Cloud mit Apps

Technisch steckt hinter Nextcloud zunächst ein klassischer LAMP-Stack: oft ein freies Betriebssystem wie Linux, ein Webserver wie Apache, eine Datenbank wie MySQL und PHP-Code, der auf den Dreien aufbaut. Entsprechend ist es denkbar, eine Nextcloud-Instanz auf gängigen Webhosting-Paketen einzurichten. Empfehlenswert ist das aber nur selten und



Eine Fülle von Apps erweitert Nextcloud. App-Pakete helfen, weil sie gängige Anwendungen bündeln und Abhängigkeiten kennen.

oft sogar in den Bedingungen der Anbieter explizit ausgeschlossen.

Die Software, die den Nextcloud-Kern bildet, sozusagen der Server, ist durch Apps vielseitig erweiterbar. Die Grundfunktionen bestehen vor allem aus Dateisynchronisation und Verwaltungsfunktionen. Soll eine Instanz zum Beispiel Adressbuch oder Kalender bereitstellen, so genügt es, mit wenigen Mausklicks in der Weboberfläche gewünschte Apps dafür hinzuzufügen. Je nach Installationsmethode sind diese beiden Apps oft schon installiert.

Anwendungen für Desktopbetriebssysteme ergänzen Nextcloud: Die zur Dateisynchronisation stellt wie etwa die für OneDrive oder DropBox sicher, dass Clients automatisch geänderte Dateien übertragen und empfangen. Das Ganze passiert nach einer einmaligen Konfiguration automatisch und weitgehend unaufgeregt.

So lässt sich mit einem Dateisatz sehr bequem auf mehreren Computern arbeiten, ohne sich Gedanken machen zu müssen, wie die Dateien dorthin gelangen. Der Nextcloud-Server hält nicht nur die aktuelle Version einer Datei vor, sondern auch ältere, in der Weboberfläche gezielt abrufbare Stände. Er dünnt die alten Versionen automatisch nach einem festen Schema aus.

Für Clients mit Mobilbetriebssystem gibt es nicht nur eine Nextcloud-App, sondern gleich mehrere. Sie kümmern sich separat beispielsweise um Dateien (und Fotos), Anbindung an die Chat- und Videotelefoniefunktionen (Talk) und die Kanbanboards (Deck). Andere Funktionen wie Kalender und Adressbuch sind über gängige Protokolle wie CalDAV und CardDAV zugänglich und benötigen keine separate App.

… mit Optionen

Um eine Nextcloud-Instanz einzurichten, taugt jeder Computer, auf dem ein Unix-artiges Betriebssystem läuft oder das zumindest Docker-Container mit Linux darin ausführen kann. Ein Raspberry Pi 3 genügt schon. Moderne NAS-Geräte eignen sich genauso. Fertige virtuelle Maschinen sind ebenfalls zu haben, die dann schlicht den nötigen Linux-Unterbau enthalten.

Mit dem Einrichten der Instanz ist es aber nicht getan: Damit sie sich sinnvoll nutzen lässt, muss sie auch erreichbar sein. Hinter einem Router müssen Sie sich als Betreiber darum kümmern, dass dessen Firewall per Portweiterleitung Zugriffe auf Port 443 durchlässt. Außerdem ist es heute zeitgemäß und für einige Installationsmethoden sogar unverzichtbar, eine Instanz mit einem Zertifikat zu versehen, sodass verschlüsselte Verbindungen möglich sind.

Für wen das alles böhmische Dörfer sind oder wer sich damit nicht im Detail selbst auseinandersetzen möchte, der findet inzwischen einige Hoster, die schlüsselfertige Nextcloud-Umgebungen vermieten und sich auch um die Zertifikate, Domain und Aktualisierung kümmern. Kunden starten direkt in die Verwaltung der eigenen Instanz. Unsere Marktübersicht auf Seite 116 vergleicht einige deutsche Anbieter.

Sollten Sie nur die Dateisynchronisation brauchen und auch keine großen Speicherplatzansprüche hegen, könnte es sein, dass Sie schon Zugriff auf eine Nextcloud haben, die nur anders heißt: Hinter der für Kunden der Telekom bis 15 GByte kostenlosen Magenta Cloud zum Beispiel steckt Nextcloud, allerdings abgespeckt und ohne Option, in der Instanz zusätzliche Apps installieren zu können.

Wenn eine Nextcloud-Instanz vielen Benutzern dienen soll, genügt wahrscheinlich der simple LAMP-Stack nicht mehr. Es werden Helfer nötig, die als Zwischenspeicher dienen, Optimierungen an der PHP-Umgebung vornehmen, die Office-Dienste als separaten Server betreiben und die Videotelefoniefunktionen mit Vermittlungsdiensten optimieren. Das alles klingt kompliziert, ist aber dank einer von Nextcloud selbst veröffentlichten All-in-one-Lösung recht einfach.

Seit Ende 2022 wird an Nextcloud-AIO entwickelt, und Nextcloud empfiehlt, Installationen damit vorzunehmen. Unter der Haube steckt Docker. Eine davor angeflanschte Oberfläche zur Administration und für Backups ist sehr nützlich. Einzig um die Zertifikatsbeschaffung muss sich der Betreiber selbst kümmern, erhält aber für alle gängigen Verfahren Tipps (etwa Traefik und Caddy). Unser Artikel auf Seite 104 liefert weitere Hilfestellungen.

… mit Macken

Was der Artikel bis hierher lax als Nextcloud bezeichnet, nennen seine Schöpfer Nextcloud Hub. Das ist kein separates Produkt, sondern der Versuch auszudrücken, dass die Software viele Funktionen dazu gewonnen hat, und seit Version 18 der offizielle Name. Eine wesentliche Erweiterung damals war die vollständige Integration von OnlyOffice, sodass Nutzer direkt in der Weboberfläche gleichzeitig Dokumente bearbeiten konnten.

Bis heute gehört aber die bittere Wahrheit dazu, dass diese Integration eher eine technische Machbarkeitsstudie darstellt als einen produktiv nutzbaren Ansatz: Um OnlyOffice zu aktivieren, fügt man einer Installation zwei Apps hinzu, den OnlyOffice Connector und den Community Document Server. Die spielen dann Hand in Hand beim Bearbeiten von Office-Dokumenten.

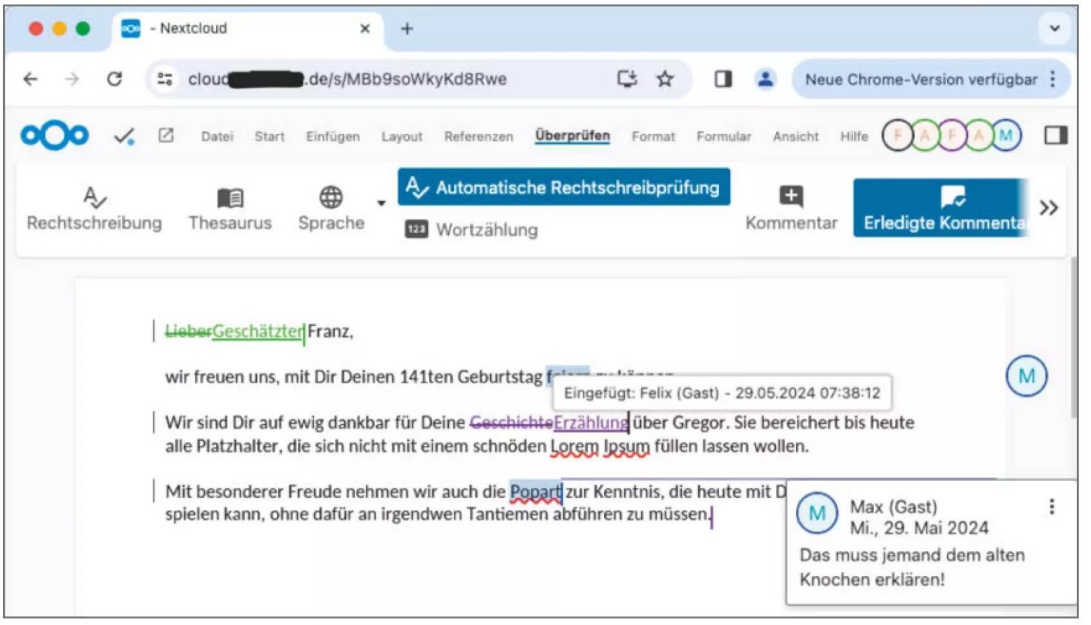
Die Implementierung des Community Document Server als App innerhalb von Nextcloud war ein geschickter Trick, weil das den Aufwand für den Betrieb eines separaten Serverdienstes spart. Aber: Seit vielen Jahren sichert diese Komponente die Eingaben eines Nutzers nicht automatisch, sodass andere Nutzer nur ein unbearbeitetes Dokument sehen. Nicht einmal der Versionsverlauf des Nutzers enthält Hinweise auf seine Bearbeitungen.

Als Workaround für solche Setups galt lange der Tipp, die Cache-Inhalte des Document Servers regelmäßig zu leeren; dann wurden die Daten im Verlauf und für andere Nutzer sichtbar. Im aktuellen Nextcloud aber ist genau dieser Aufruf kaputt (entsprechende Tickets mit detaillierten Hinweisen haben wir in ct.de/wyy7 verlinkt).

Bitter daran ist, dass der Fehler seit Jahren bekannt, aber bis heute nicht behoben ist. Und, was schwerer wiegt: Das ist kein Einzelfall, denn dokumentierte Fehler oder Eigenheiten von Nextcloud bleiben lang unbearbeitet. Viele Nutzer kennen das vermutlich aus eigener Anschauung: Auf der Suche nach einer Problemlösung stoßen sie auf ältere, offene Tickets, zum Glück oft mit Tipps aus der Community.

Ein kurzer Rückgriff zu Office in Nextcloud: Dass der Community Server für OnlyOffice nicht rund läuft, sagt nichts über die Office-Integration als solche aus. Der identische Ansatz für LibreOffice mit einem ebenfalls als App in Nextcloud ausgeführten Server (Collabora online – Built-in CODE Server) funktioniert inzwischen besser als der früher eingeführte für OnlyOffice.

Generelle Empfehlung für den produktiven Betrieb mit der Online-Bearbeitung von Office-Dokumenten: einen separaten Server nehmen, dann funktionieren beide Office-Varianten ohne Zipperlein. Und ein Tipp dazu zum Schluss: Wenn Office-Dokumente auch mit Mobilgeräten bearbeitet werden sollen, braucht OnlyOffice spezielle Lizenzen und eigene Apps. Deswegen und auch wegen der Probleme mit OnlyOffice favorisiert Nextcloud LibreOffice mit Collabora online und dem Built-in CODE Server.



Mit aktiver Office-Integration können mehrere Benutzer gleichzeitig an einem Dokument arbeiten, so wie das bei Google und Microsoft möglich ist. Im Hintergrund arbeiten dafür bei Nextcloud üblicherweise LibreOffice oder OnlyOffice. Es genügt übrigens ein Freigabelink dafür, die teilnehmenden Nutzer brauchen kein eigenes Konto auf der Nextcloud.

… mit Community

Die Schwierigkeiten bei der Office-Integration werfen die Frage auf, wer bei Nextcloud nach welchem Muster über die Entwicklung bestimmt. Dazu holen wir ein wenig aus: Die zentrale Figur hinter Nextcloud ist Frank Karlitschek. Er gründete 2010 Owncloud und entwickelte dort die Dateisynchronisation mit einem Team. Das Unternehmen finanzierten Investoren. Mit deren Einfluss auf freie Software haderte Karlitschek und verließ mit einigen Teammitgliedern Owncloud.

Mit Nextcloud startete Karlitschek ein neues Unternehmen, das fortan einen Fork von Owncloud entwickeln sollte. Es erzielt seine Einkünfte durch den Verkauf von Supportdienstleistungen, die Nextcloud dann zu einer Enterprise-Ausgabe aufwerten. So kann das neue Unternehmen frei vom Einfluss von Investoren entscheiden, wie Karlitschek es darstellt.

Seit der Gründung 2016 ist die Nextcloud-Belegschaft auf rund 100 Mitarbeiter gewachsen. Eine um Nextcloud entstandene Open-Source-Community arbeitet ebenfalls an der Entwicklung mit. Eine alles übergreifende Koordination der Aktivitäten scheint nicht stattzufinden, was immer mal wieder den zuvor geschilderten zähen Umgang mit offensichtlichen Fehlern wie bei OnlyOffice erklärt.

Mit dem Ausstieg Karlitscheks schwand zumindest hierzulande die Bedeutung von Owncloud zunehmend. Die Entwicklung der beiden Projekte ging unterschiedliche Wege. Heute liefern sie sich vor allem bei Großinstallationen einen Wettbewerb. Owncloud scheint bei Bildung und Wissenschaft beliebter zu sein, Nextcloud bei Politik und Verwaltung. Die aktivere Community hat definitiv Nextcloud.

Mit Opencloud schickte Anfang 2025 die Heinlein Gruppe eine weitere Alternative ins Rennen. Sie baut technisch auf der Vorarbeit von Owncloud auf und konzentriert sich, anders als Nextcloud, auf die zentralen Funktionen für die Zusammenarbeit: Dateisynchronisation, Datenorganisationshilfen für Teams und gemeinsames Arbeiten an Office-Dokumenten.

… mit Perspektiven

Bei allem Hin und Her und manch unbefriedigender Funktionseinschränkung ist Nextcloud eine ungemein nützliche Software und vom Funktionsumfang Owncloud deutlich überlegen. Insofern widmen sich auch die nachfolgenden Artikel der Welt von Nextcloud und den Möglichkeiten, diese auch denjenigen zugänglich zu machen, die nicht selbst Serverdienste aufsetzen wollen. (ps) c't

Erwähnte Tickets
ct.de/wyy7

21. Oktober

Sicher online bezahlen

Angriffe erkennen,
zielführend reagieren
und Verluste vermeiden

c't WEBINAR

Jetzt informieren:

heise-academy.de/webinare/sicher-online-bezahlen

Bild: Moritz Reichartz

Eine frische Nextcloud einrichten

Nextcloud nimmt Sie als Administrator mehr in die Verantwortung als gewöhnliche Cloudspeicher. Um Freude mit Ihrer Nextcloud zu haben, sollten Sie zunächst ein paar Pflichtübungen absolvieren. Dazu geben wir Starthilfe für frische Installationen vom Hoster und für die offizielle Installationsmethode.

Von **Niklas Dierking**

Für die meisten Nutzer dürfte eine verwaltete Nextcloud-Instanz bei einem Hoster der attraktivste Weg zur eigenen Cloud sein. Die Dienstleister liefern eine schlüsselfertige Installation und kümmern sich gegen einen monatlichen Obolus auch um Backups und Instandhaltung. Wenn Sie sich hier angesprochen fühlen, können Sie beim Abschnitt „Nextcloud öffne dich“ wieder einsteigen.

Wer hingegen alle Fäden selbst in der Hand halten will, ein paar Abstriche beim Komfort in Kauf nimmt und sich selbst um die Wartungsarbeiten kümmert, kann die Software auf einem Heim- oder Mietserver installieren, etwa um mehr Kontrolle über die eigenen Daten zu haben oder die Technik hinter dem Cloudspeicher zu verstehen. Voraussetzung: Linux- und Docker-Erfahrung sowie eine eigene Domain.

Cloudarchitektur

Um Nextcloud auf einem eigenen Server zu installieren, gibt es viele verschiedene Möglichkeiten: klassisch auf einem LAMP-Stack, über Spezialimages für den Raspberry Pi oder als VM-Appliance. Wir raten zum offiziellen Installationsweg mit Docker und dem sogenannten AIO-Container (All-In-One). Dabei fungiert ein von Nextcloud entwickelter Container (nextcloud-aio-mastercontainer) als Schaltzentrale, stellt eine Weboberfläche für Administrationsaufgaben bereit, legt verschlüsselte Backups an und automatisiert Updates.

Wir zeigen, wie Sie Nextcloud über die AIO-Methode auf einem angemieteten VPS (Virtual Private Server) mit Ubuntu Server 24.04 LTS und öffentlicher IPv4-Adresse installieren. Sie müssen außerdem einen A-Record bei Ihrem DNS-Provider setzen, beispielsweise nextcloud.example.com, der auf die IP-Adresse des Servers zeigt. Stellen Sie außerdem sicher, dass die TCP-Ports 80, 443 und 8080 des Servers nicht blockiert sind.

Eine Docker-Compose-Vorlage sowie eine Konfigurationsdatei (Caddyfile) für den Reverse-Proxy Caddy, der auch ein TLS-Zertifikat von Let's Encrypt besorgt, finden Sie in dem GitHub-Repository, das wir unter ct.de/wvtm verlinkt haben. Hinweise, wie Sie die Dateien anpassen müssen, und die Befehle zum Starten finden Sie in der Readme-Datei auf GitHub.

AIO-Weboberfläche

Nachdem Sie den Nextcloud-Mastercontainer und Reverse-Proxy gestartet haben, rufen Sie die AIO-Weboberfläche im Browser auf. Die URL lautet https://<IP-Adresse des Servers>:8080. Ihr Browser wird Sie warnen, dass es sich um ein selbst signiertes Zertifikat handelt und Sie müssen eine Ausnahme hinzufügen.

Die Weboberfläche des Mastercontainers zeigt Ihnen jetzt einmalig eine Passphrase für den AIO-Login an. Speichern Sie die an einem sicheren Ort, beispielsweise in einem Passwortmanager, und melden Sie sich danach mit der Passphrase an. Jetzt werden Sie vor die Wahl gestellt, ob Sie eine neue Nextcloud-Instanz einrichten wollen oder aus einem Backup eine bestehende Instanz wiederherstellen wollen.

Geben Sie die Domain für Ihre neue Instanz ein, beispielsweise nextcloud.example.com, und klicken dann auf „Submit domain". Im nächsten Schritt haben Sie die Möglichkeit, optionale Container in das Setup einzubinden. Einige der optionalen Container funktionieren nur auf x86-Systemen, verhindern die serverseitige Verschlüsslung oder erhöhen die Systemanforderungen. Vorausgewählt sind ein eigenständiger Document-Server für Collabora (Nextcloud Office), die Chat- und Videokonferenzsoftware Talk sowie Imaginary für die Web-Vorschau von PDF- und Bilddateien.

Wenn alles geklappt hat, zeigt das AIO-Webinterface jetzt oben auf der Seite Ihren initialen Benutzernamen „admin" sowie ein zufällig generiertes Passwort an. Klicken Sie auf die Schaltfläche „Open your Nextcloud" und melden sich mit diesem Passwort an. Falls Sie Ihre Instanz von einem der Provider beziehen, die wir uns im Artikel auf Seite 116 angesehen haben, bekommen Sie die URL Ihrer Nextcloud und die Zugangsdaten für den Administrator-Account via E-Mail oder im Kundenportal.

Nextcloud öffne dich

Beim ersten Login zeigt eine Animation eine Übersicht von Nextcloud-Features. Nextcloud bietet Ihnen auch sofort an, die Clients, beispielsweise für Mobilgeräte, herunterzuladen. Wir raten dazu, sich jedoch erst mal mit der Weboberfläche vertraut zu machen und Nextcloud zunächst zu konfigurieren. Wie Sie die Clients für Windows, macOS, Linux und mobile Systeme einrichten, erklären wir im Artikel ab Seite 110.

Danach begrüßt Sie die Nextcloud-App „Dashboard". Diese Übersicht informiert Nutzer nach dem Login über die neuesten Aktivitäten, beispielsweise Erwähnungen in Chats, freigegebene Dateien, neue Mails oder anstehende Termine.

Rundgang durch die Weboberfläche

Die Nextcloud-Bedienoberfläche gliedert sich in unterschiedliche Teilbereiche. Über den oberen Rand des Fensters navigieren Sie zu den Apps, die auf Ihrer Nextcloud-Instanz verfügbar sind. Herzstück der Nextcloud ist „Dateien", die Dateimanager-App. Am linken Rand des Fensters finden Sie Informationen zur gerade geöffneten App. Im Dateimanager sind das beispielsweise kürzlich verwendete Dateien oder Favoriten. In der Mitte des Fensters befindet sich ein dynamischer Bereich, der den Inhalt der aktuellen App anzeigt, in diesem Fall einige Beispieldateien. Oben rechts finden Sie die Suche, die Kontaktliste sowie die Einstellungen, die sich in „Persönliche Einstellungen" für den gerade angemeldeten

Account und „Verwaltungseinstellungen“ für die Nextcloud-Instanz gliedern – letztere sehen nur Administratoren.

Wer bin ich?

Auf einer frischen Installation sollten Ihre ersten Schritte Sie in die persönlichen Einstellungen des Administrator-Accounts führen. Im Menü „Persönliche Informationen“ können Sie von Ihrem vollen Namen bis zu Social-Media-Accounts jede Menge Informationen über sich preisgeben. Wichtig ist, dass Sie für jeden Nutzer eine E-Mail-Adresse angeben, damit Nextcloud weiß, wie es sie benachrichtigen kann, beispielsweise um das Passwort zurückzusetzen.

Wenn Sie Nextcloud von einem Hoster beziehen, sollte Ihre E-Mail-Adresse hier bereits hinterlegt sein, es schadet aber nicht, als Backup eine weitere Adresse anzugeben.

Grüner Haken?

Wenden Sie sich jetzt der Seite „Übersicht“ in den Verwaltungseinstellungen zu. Hier meldet die Weboberfläche Konfigurationsprobleme und verlinkt Einträge in der Dokumentation, die erklären, wie Sie die Probleme lösen.

Auf einer verwalteten Instanz von einem Hoster sollte Nextcloud hier nichts zu meckern haben und einen grünen Haken anzeigen. Wenn doch, dann melden Sie sich beim jeweiligen Support. Sie werden die Probleme in der Regel nicht selbst lösen.

Bei einer eigenhändigen Installation, zum Beispiel mittels Nextcloud-AIO, sieht das oft anders aus. Nextcloud beschwert sich darüber, dass keine Standard-Telefonregion festgelegt ist und keine E-Mails verschickt werden können.

Das erste Problem ist in einer AIO-Installation mit folgendem Befehl schnell behoben, der mit dem Nextcloud-Kommandozeilenwerkzeug `occ` die richtige Region in die Konfigurationsdatei schreibt:

```
docker exec --user ↵
↳www-data nextcloud-aio-nextcloud ↵
↳php occ config:system:set ↵
↳default_phone_region --value="DE"
```

Die Abkürzung `occ` steht für „Owncloud Console“, das an die gemeinsame Herkunft von Owncloud und Nextcloud erinnert. Bei den meisten Wehwehchen, die eine Installation plagen können, ist `occ` die Lösung. Wer selbst hostet, sollte sich unbedingt mit der Dokumentation vertraut machen (siehe ct.de/wvtm).

Im Menü „Grundeinstellungen“ bringen Sie Nextcloud bei, Mails zu verschicken. Es hat keinen eigenen Mail-Server an Bord, kann Mails also nur über einen externen Server versenden. Sie können auch ohne funktionierenden E-Mail-Versand leben, aber sobald mehrere Benutzer an Bord sind, nehmen Ihnen die automatisierten Mails viel Arbeit ab. Nutzer müssen dann beispielsweise nicht zum Telefonhörer greifen, wenn sie mal das Passwort vergessen haben, sondern können es selbst zurücksetzen.

Auch für Sie als Admin lohnen sich E-Mail-Benachrichtigungen, damit Nextcloud sie beispielsweise über Erfolg oder Scheitern terminierter Backups informiert; dazu später mehr.

Tragen Sie Absender, Hostnamen, Port und Zugangsdaten für einen externen SMTP-Server ein. Welchen Anbieter Sie dafür nutzen, bleibt Ihnen überlassen. Klicken Sie auf „E-Mail senden“, um eine Test-Mail zu schicken. Wenn die angekommen ist, können Sie anfangen, weitere Nutzer anzulegen.

Schluss mit Einsamkeit

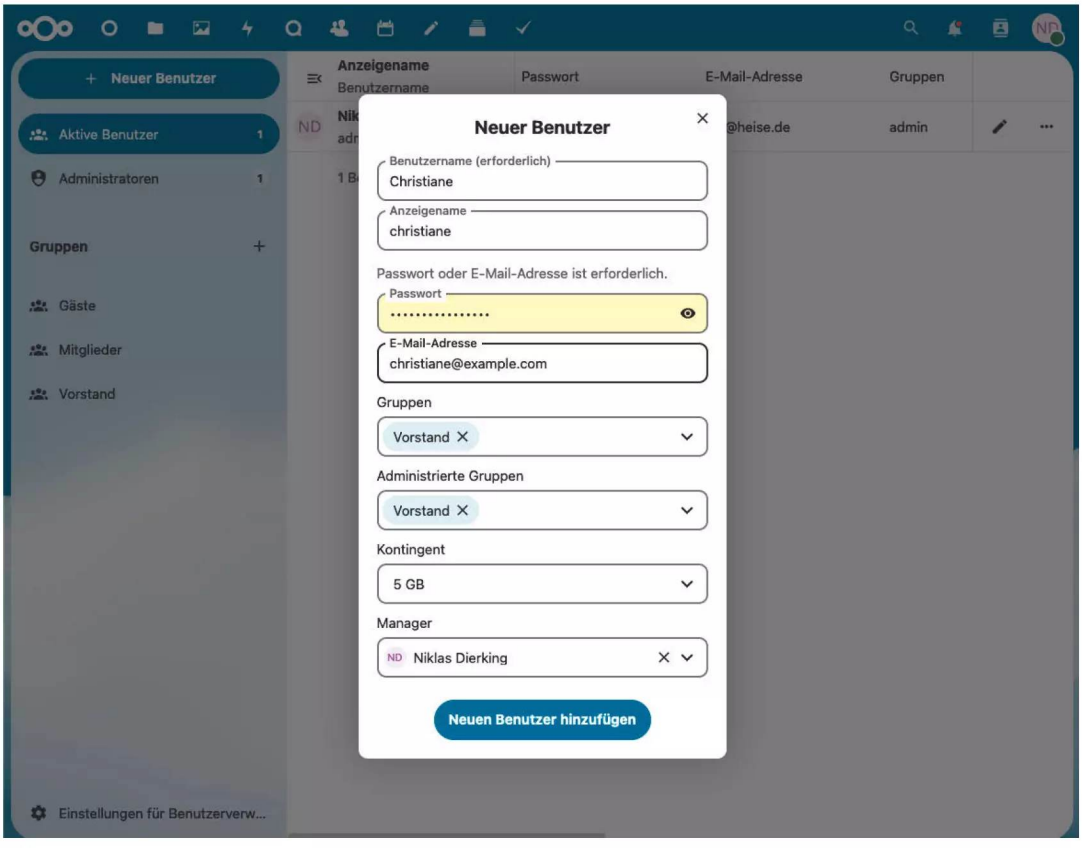
Eine Nextcloud ist praktisch, um persönlichen Dateien, Kalender und Kontakte zu synchronisieren, hat also schon für einen einzelnen Nutzer seine Daseinsberechtigung.

Um Familienmitglieder, Kollegen oder andere Taubenzüchter einzuladen, navigieren Sie ins Menü „Benutzer“. Abhängig davon, wie Sie die Nextcloud nutzen, kann es sich lohnen, zunächst einige Gruppen anzulegen, bevor Sie Benutzer einladen. In einem Verein könnten die beispielsweise „Vorstand“, „Mitglieder“ und „Gäste“ heißen.

Gruppen sind praktisch, weil es mit ihnen einfach ist, Dateien und Ordner schnell mit vielen Nutzern gleichzeitig zu teilen.

Klicken Sie jetzt auf „Neuer Benutzer“ und tragen Sie mindestens einen Benutzernamen und eine E-Mail-Adresse ein. Der eingeladene Benutzer bekommt eine Einladungsmail und kann dann ein eigenes Passwort festlegen. Wenn Sie Nextcloud ohne Mailversand betreiben, müssen Sie ein Passwort vorgeben.

Optional weisen Sie den neuen Benutzer einer Gruppe zu, lassen ihn selbst eine Gruppe administrieren, legen ein Speicherkontingent fest oder bestimmen einen anderen Nutzer als dessen „Manager“. Das markiert die Person als Vorgesetzten, stattet sie aber nicht mit Administratorrechten aus.



Als Administrator erstellen Sie Accounts für andere Benutzer, laden sie via Mail ein oder öffnen die Registrierung.

Wenn Sie einen Nutzer zur Gruppe „admin“ hinzufügen, bekommt er die gleichen Rechte wie Ihr Administrator-Account und kann beispielsweise Apps installieren und löschen. Vergeben Sie dieses Privileg nicht leichtfertig.

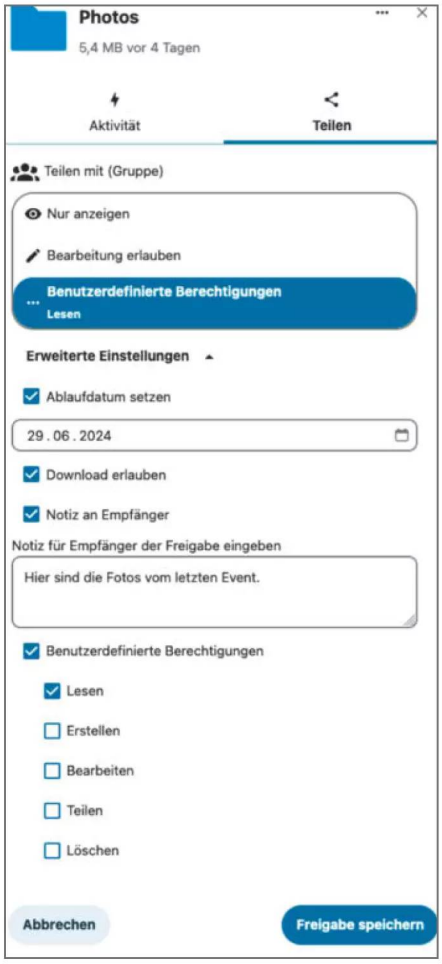
Wer ein umfangreiches Onboarding plant, sollte sich die Nextcloud-App „Registration“ ansehen, die es Nutzern ermöglicht, selbst ein Benutzerkonto anzulegen, das Sie im Anschluss als Administrator freischalten müssen. Die App setzt voraus, dass Ihre Installation Mails verschicken kann.

Deine, meine, unsere Dokumente

Grundsätzlich gilt: Alles, was nicht geteilt wurde, ist für andere Nutzer unsichtbar.

Um eine Datei in der Weboberfläche mit anderen Nutzern zu teilen, rufen Sie die App „Dateien“ auf. In der Übersicht finden Sie neben Dateien und Ordnern ein Personensymbol mit Pluszeichen. Das öffnet die Optionen zum Teilen. In dem Feld „Nach Freigabe-Empfängern suchen“ tragen Sie Benutzer oder Gruppen ein, denen Sie die Ressource zugänglich machen wollen. Sie haben dabei viele Möglichkeiten, den Zugriff durch das Setzen von Berechtigungen zu limitieren.

Außerdem können Sie leicht Dateien über Freigabelinks öffentlich machen, um sie mit Leuten zu teilen, die kein Benutzerkonto haben. Standardmäßig können die so geteilten Dateien nur gelesen werden, Schreibrechte räumen Sie in den erweiterten Einstellungen ein. Für sensible Daten ist es sinnvoll, ein Passwort zu vergeben, das Sie dem Empfänger auf einem anderen Kanal zukommen lassen. Bei installiertem Nextcloud-Client auf dem Desktop stehen die Freigabefunktionen auch im Kontextmenü der Dateiverwaltung bereit, etwa im Finder oder Explorer.



Wer darf welche Dateien wie lange ansehen, herunterladen oder bearbeiten? Bei der Dateifreigabe haben Sie die volle Kontrolle.

An dieser Stelle lohnt sich ein Hinweis auf die Nextcloud-App „Gruppenordner“, die Sie als Administrator aus dem App-store nachrüsten. Anschließend können Sie in den Verwaltungseinstellungen im Menü „Gruppenordner“ geteilte Ordner für alle Mitglieder einer Gruppe anlegen sowie ein Speicherkontingent und Berechtigungen festlegen. Die Gruppenordner werden dann allen Mitgliedern der Gruppe in der Dateiübersicht angezeigt und müssen nicht extra freigegeben werden.

Login absichern

Maßnahmen zum Schutz Ihres Accounts konfigurieren in den persönlichen Einstellungen im Menü „Sicherheit“.

Zusätzlich zum Passwort sollten Sie eine Form von 2FA (Zwei-Faktor-Authentifizierung), beispielsweise TOTP (Time-based one-time password), für Ihren Account konfigurieren. Dazu müssen Sie zunächst Backup-Codes generieren und speichern, die als Notfallschlüssel dienen, falls Sie keinen Zugriff mehr auf Ihren zweiten Faktor haben. Falls Sie mit Apps von Drittanbietern auf die Nextcloud zugreifen, müssen Sie für diese Clients ein App-Passwort festlegen.

Nextcloud bietet auch eine passwortlose Anmeldung nach dem FIDO2-Standard (WebAuthn) an, beispielsweise mit einem FIDO2-kompatiblen Hardwaresicherheitsschlüssel oder einem Passkey. Die Funktion heißt „mit einem Gerät anmelden“.

In den Verwaltungseinstellungen gibt es ebenfalls das Menü „Sicherheit“. Hier legen Sie Passwortregeln für Benutzer fest und können sie zur Zwei-Faktor-Authentifizierung verpflichten. Wenn Sie Ihre Instanz selbst hosten, gelten die üblichen Ratschläge: Verbieten Sie den SSH-Login mittels Passwort; nutzen Sie stattdessen SSH-Schlüssel. Halten Sie das Betriebssystem und Nextcloud(-Container) aktuell. Lassen Sie in Ihrer Firewall nur Zugriffe auf die Ports zu, die die Dienste wirklich benötigen.

Verschlüsselung

Nextcloud kann ein großer Schritt in Richtung Datenhoheit sein, der fällt aber kleiner aus, wenn man eine verwaltete Instanz von einem Provider anmietet, der prinzipiell Zugriff auf die eigenen Daten hat. Der Beschreibungstext der Option „Serverseitige Verschlüsselung“ im Menü „Sicherheit“ der Verwaltungseinstellungen suggeriert, dass hochgeladene Dateien verschlüsselt gespeichert werden und damit für einen etwaigen Hoster nicht lesbar sind.

Tatsächlich hält die Funktion weniger, als sie verspricht, denn so wie sie aktuell implementiert ist, liegt der Schlüssel im Datenverzeichnis von Nextcloud (siehe ct.de/wvtm). Ein Plus an Sicherheit gibt es dadurch nur, wenn Sie einen externen Datenspeicher, beispielsweise Google Drive, eingebunden haben.

Vorsicht: Hoster wie IONOS raten stark davon ab, die serverseitige Verschlüsselung zu aktivieren. Außerdem können Sie die Verschlüsselung nicht über die Weboberfläche wieder deaktivieren, son-

dern brauchen dafür das `occ`-Kommandozeilenwerkzeug. Machen Sie sich unbedingt mit der Dokumentation zur Serverseitigen Verschlüsselung vertraut (siehe ct.de/wvtm). Wenn Sie das Feature trotzdem aktivieren wollen, müssen Sie zunächst im App-Store „Default encryption module“ aktivieren. Andernfalls bleibt die Option im Menü „Sicherheit“ ausgegraut.

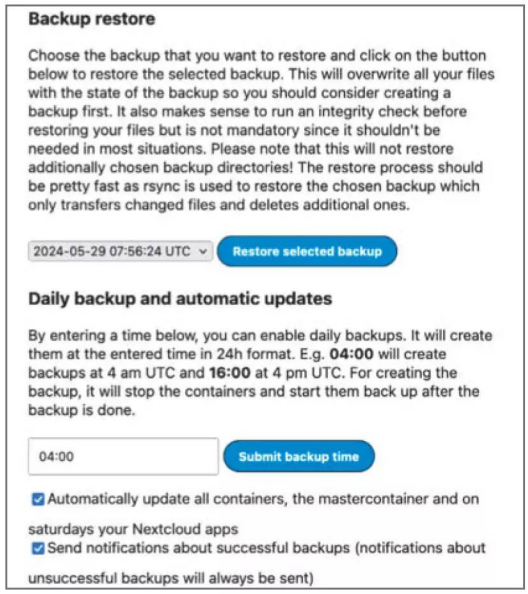
Nextcloud bietet für die Sync-Clients eine Ende-zu-Ende-Verschlüsselung an, wenn Sie die App „End-to-End Encryption“ installieren. Wir können die Funktion aber derzeit nicht für den Produktivbetrieb empfehlen. Beim Einrichten der Funktion stürzte ein Nextcloud-Client ab, bevor wir uns die Passphrase notieren konnten. Im Nextcloud-Appstore finden sich außerdem Berichte über Sync-Fehler und Datenverlust, beispielsweise nach einem Update der App.

Backups und automatische Updates

Wenn Sie sich dafür interessieren, Nextcloud von einem Hoster zu beziehen, dann achten Sie darauf, dass regelmäßige Backups sowie ein Mechanismus zur Wiederherstellung zum Angebot gehören. Die Backups verwalten Sie dann in der Regel im Kundenbereich Ihres Anbieters. Wenn Sie selbst hosten, müssen Sie sich zwar selbst darum kümmern, der Nextcloud-AIO-Container macht einem das aber inzwischen sehr leicht. Er integriert ein automatisches verschlüsseltes Backup mittels BorgBackup, das Sie in der AIO-Weboberfläche konfigurieren. Eine Einführung zu BorgBackup lesen Sie in [1].

Navigieren Sie sich über die Schaltfläche „Open Nextcloud AIO Interface“ im Menü „Übersicht“ in den Verwaltungseinstellungen zum AIO-Interface. Der direkte Login über https://<IP-Adresse des Servers>:8080 ist lahmgelegt, während die Nextcloud läuft. Geben Sie bei „Backup and restore“ ein Verzeichnis für das Backup an, beispielsweise /mnt/backup. Danach bekommen Sie die Passphrase angezeigt, die Sie benötigen, um die Backups wieder zu entschlüsseln. Speichern Sie die Passphrase an einem sicheren Ort.

Mit „Create Backup“ stoßen Sie das erste Backup an. Die Weboberfläche ist währenddessen nicht erreichbar und Dateisynchronisation ist auch nicht möglich. Planen Sie automatische Backups also zu einer Zeit, in der Sie mit wenigen Zugriffen rechnen. Es werden alle hochgeladenen Dateien, inklusive der Datenbank und Konfigurationsdaten gesichert. Falls Sie einen externen Datenspeicher eingebunden haben, wird der nicht mitberücksichtigt.



Das integrierte Backup-Feature der All-in-One-Variante ist nützlich, wenn man Nextcloud selbst hostet. Auf Wunsch folgen auf erfolgreiche Backups automatische Updates der Container und Apps.

Wenn das erste Backup erfolgreich erstellt wurde, können Sie anschließend ein tägliches automatisches Backup konfigurieren. Besonders praktisch: Nextcloud-AIO aktualisiert im Anschluss den gesamten Container-Verbund und einmal wöchentlich die installierten Nextcloud-Apps. Im Hintergrund spannt es dafür Watchtower ein (siehe ct.de/wvtm). Wie lange und wie viele Backups vorgehalten werden sollen, passen Sie bei Bedarf über Umgebungsvariablen in der Datei docker-compose.yaml an. Ein lokales Backup schützt nicht ausreichend vor Datenverlust und sollte durch Offsite-Backups ergänzt werden.

Ausblick

Ihre Nextcloud ist jetzt bereit, um sie mit anderen Nutzern zu teilen und Sie haben einige Fallstricke kennengelernt, die Sie vermeiden können. Im folgenden Artikel liegt der Fokus auf den Desktop- und Mobil-Clients, die für Windows, macOS, Linux sowie Android und iOS zur Verfügung stehen. (ndi) c't

Literatur

[1] Tim Schürmann, BorgBackup: Datenverlust ist zwecklos: Verlässliche Datensicherungen unter Linux, macOS und Unix, c't 8/2023, S. 166

Nextcloud-Dokumentation, GitHub-Repository mit Docker-Vorlage:
ct.de/wvtm

Bild: Moritz Reichartz

Nextcloud-Clients für Desktop und Mobil

Die eigene Nextcloud läuft, aber wie verheiratet man den Server mit Desktop-Rechner, Tablet und Smartphone? Die Clients brauchen ein paar Handgriffe, bis alles läuft, aber dann finden Daten automagisch in Ihre eigene Cloud.

Von **Niklas Dierking**

Um Dateien, Kalender und mehr auf verschiedenen Geräten synchron zu halten, steht eine Reihe von nützlichen Nextcloud-Clients für Desktop- und Mobilgeräte zur Verfügung. Sie sollten zunächst wissen, dass die Clients primär auf den Dateiaustausch im Hintergrund zugeschnitten sind. Auf Mobilgeräten unterscheidet das Nextcloud-Projekt zwischen der App „Nextcloud“ für die Dateisynchronisation und „Nextcloud Talk“ für Chat und Videokonferenzen.

Installer für die Windows- und macOS-Desktop-Clients laden Sie aus dem Downloadbereich der Nextcloud-Website herunter. Für Linux gibt es ein distributionsübergreifendes AppImage. Die Clients für Mobilgeräte laden Sie aus den jeweiligen App-Stores der Plattform oder über F-Droid herunter.

Desktop

Für die Installation des Clients unter Windows und macOS folgen Sie einfach den Anweisungen des Installers. Wenn Sie das AppImage unter Linux nutzen wollen, müssen Sie es erst ausführbar machen, beispielsweise indem Sie im Verzeichnis mit dem AppImage diesen Befehl im Terminal ausführen:

```
sudo chmod +x Nextcloud-3.16.6-x86_64
```

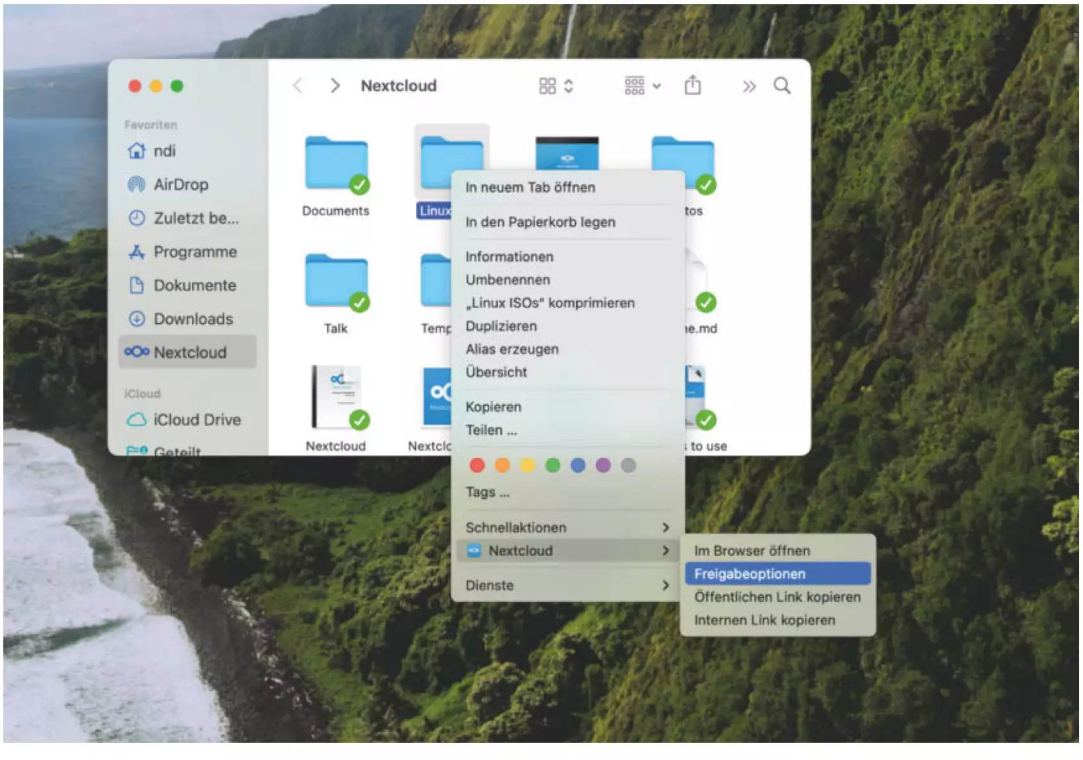
Achten Sie darauf, den korrekten Dateinamen anzugeben. In einigen Distributionen, beispielsweise in Ubuntu Desktop 24.04 LTS, brauchen Sie zusätzlich das Paket libfuse2:

```
sudo apt install libfuse2
```

Nach dem Start verdrahten Sie den Client, unabhängig vom Betriebssystem, mit Ihrem Server. Klicken Sie in dem Begrüßungsbildschirm auf „Anmelden“. Jetzt müssen Sie die vollständige URL Ihres Nextcloud-Servers eingeben, egal ob Sie Nextcloud anmieten oder selbst einen Server betreiben, beispielsweise https://nextcloud.example.com. Danach öffnet sich Ihr Browser und Sie müssen sich authentifizieren. Wenn Sie bereits im Browser angemeldet sind, klicken Sie dort direkt auf „Zugriff gewähren“.

Im Client erscheint zunächst das Menü „Nextcloud Konto hinzufügen“. Hier legen Sie einen Standardordner für Nextcloud fest. Der liegt gewöhnlich im Homeverzeichnis des Benutzers, wo er auch gut aufgehoben ist. Inhalte, die Sie darin ablegen, lädt er auf den Server hoch. In die umgekehrte Richtung können sie entscheiden, alle Daten vom Server zu synchronisieren oder nur einzelne Ordner zum Abgleich auszuwählen.

Unter macOS und Linux lädt der Client standardmäßig alle Dateien vom Server herunter, wenn Sie das entsprechende Häkchen für die Option nicht entfernen oder die zu synchronisierenden Elemente anderweitig begrenzen. Der Windows-Client kann



Im Finder und Explorer gibt es praktische Nextcloud-Funktionen. Unter Linux muss man etwas nachhelfen.

aber einen besonderen Trick, nämlich virtuelle Dateien als Vorschau anzeigen, anstatt sie lokal vorzuhalten. Das ist besonders praktisch, wenn wenig Speicherplatz auf dem Endgerät verfügbar ist. Der Client besorgt die Datei dann erst, wenn Sie geöffnet wird. Dateien, die andere Nextcloud-Nutzer mit Ihnen teilen, landen im Unterordner „Shared“.

Den Nextcloud-Client rufen Sie fortan über das Icon im Infobereich der Taskleiste beziehungsweise unter macOS über das Icon in der macOS-Menüleiste und in Linux über das Tray-Icon auf. Am Icon lesen Sie auch ab, ob Nextcloud gerade einen Sync ausführt. Ein Haken zeigt an, dass der Datenstand aktuell ist und es nichts zu tun gibt. Zwei Pfeile, die sich im Kreis jagen, bedeuten, es wird synchronisiert.

Wenn Sie die Anwendung öffnen, zeigt sie die Aktivitätenübersicht an, die sich in Systembenachrichtigungen, beispielsweise zu einem erfolgreichen Backup, und Sync-Benachrichtigungen aufteilen. Für letztere müssen Sie etwas runterscrollen. In der Menüleiste am oberen Rand des Fensters sehen Sie den gerade angemeldeten Nutzer. Sie können nachträglich auch weitere Nutzer von Ihrem Server oder anderen Nextcloud-Instanzen hinzufügen.

Integration in Dateimanager

Mit einem Klick auf die Schaltfläche mit dem Ordnersymbol springen Sie in das Nextcloud-Verzeichnis im Dateimanager. Synchronisierte Dateien markiert Nextcloud hier mit einem grünen Haken. Einen laufenden Sync erkennen Sie an einem blauen Symbol. Dateien, die andere Nutzer mit Ihnen geteilt haben, werden mit einem grünen Symbol versehen, das wie ein Gabelung aussieht.

Um Dateien mit anderen Nutzern oder öffentlich zu teilen, braucht es nicht unbedingt die Weboberfläche. Schneller geht es über das Nextcloud-Kontextmenü, das Sie mit einem Rechtsklick auf eine Datei oder einen Ordner aufrufen.

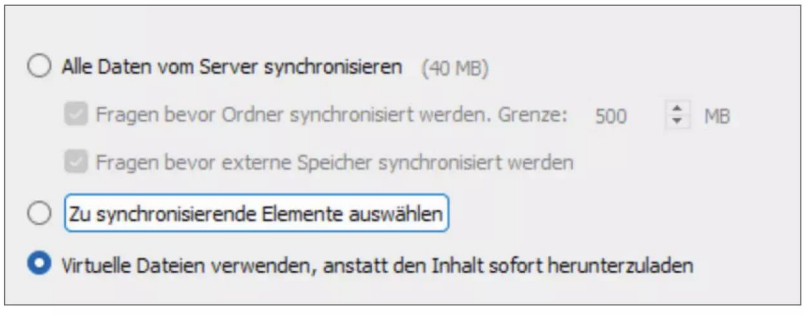
Unter Linux bietet das distributionsübergreifende AppImage keine Integration in den Dateimanager, weil es vom Rest des Systems isoliert ist. Bei einigen Linux-Distributionen können Sie den Client und die Integration auch über die offiziellen Paketquellen installieren. In Ubuntu Desktop erledigen Sie das mit dem Befehl `sudo apt install nextcloud-desktop nautilus-nextcloud`.

Wenn Sie den KDE Plasma Desktop nutzen, ersetzen Sie `nautilus-nextcloud` durch `dolphin-nextcloud`, um die Integration nachzurüsten.

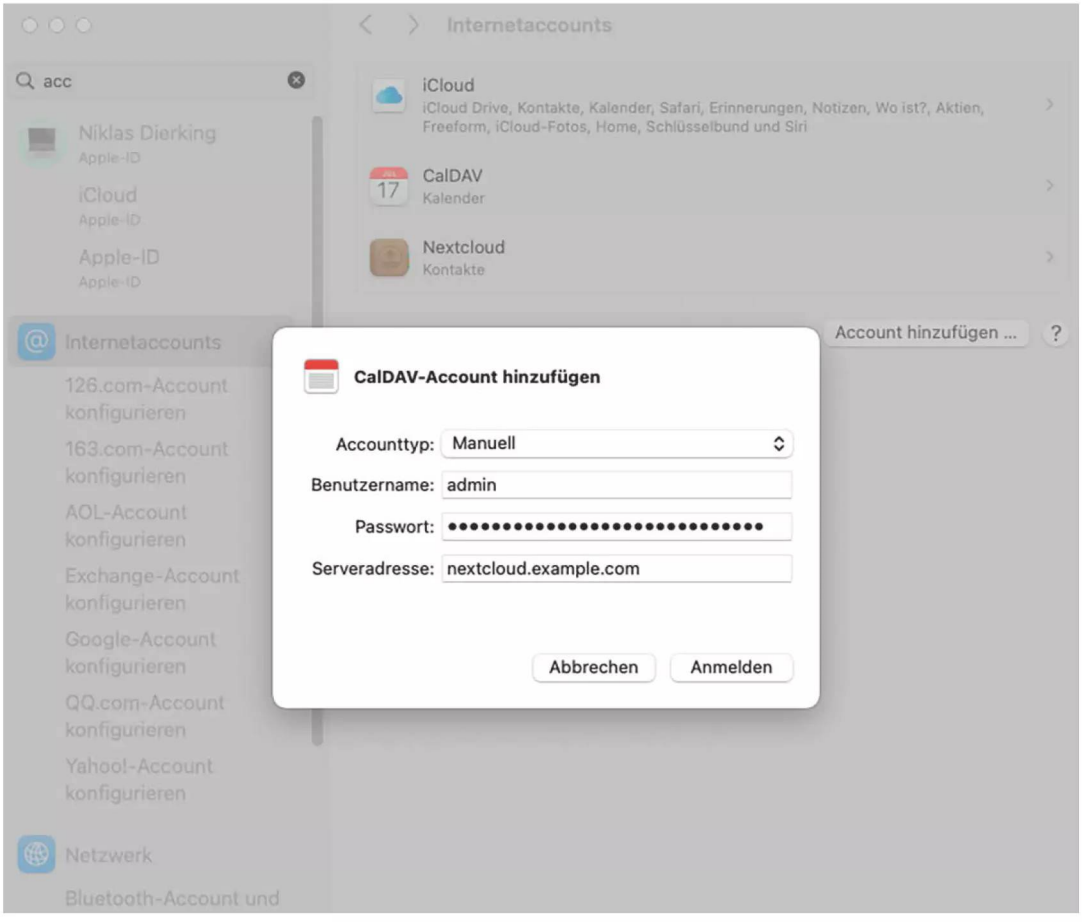
Es gibt auch die Möglichkeit, das Datenverzeichnis Ihres Nextcloud-Servers über das WebDAV-Protokoll zugänglich zu machen. Das bietet sich an, wenn eine App nur mit dieser Art des Cloudspeichers umgehen kann, zur Dateisynchronisation eignen sich die offiziellen Nextcloud-Clients aber besser, allein schon weil sie deutlich schneller sind.

Kalender und Kontakte

Die Desktop-Clients haben zwar vorgefertigte Menüeinträge, unter anderem für Kalender und Kontakte, die sind aber nur ein Link zu der jeweiligen App in der Weboberfläche. Für den Abgleich von Terminen im Kalender zapfen Sie stattdessen über lokale An-



Nur der Windows-Client kann virtuelle Dateien als Platzhalter anzeigen, um Speicherplatz zu sparen. Die Datei wird erst vom Server geladen, wenn sie gebraucht wird.



Die Endpunkte für CalDAV und CardDAV kann man auch in den Systemeinstellungen hinterlegen, um sie leichter in andere Apps zu importieren.

wendungen die CalDAV-Schnittstelle Ihres Servers an. Kontakte verteilt Nextcloud mit CardDAV.

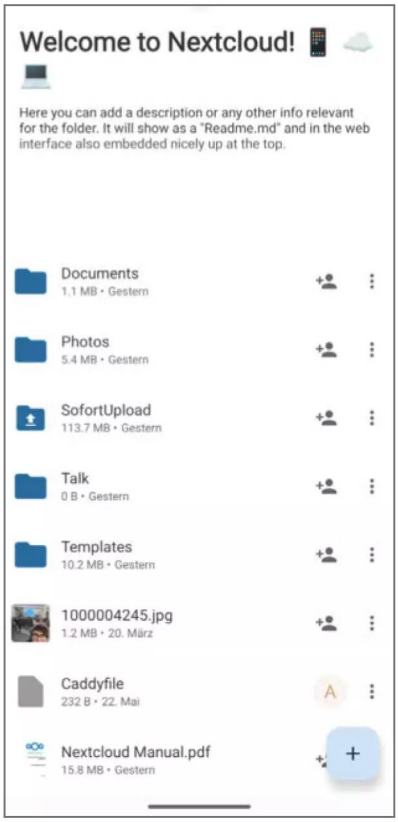
Auf den unterschiedlichen Betriebssystemen gibt es für Kalender jede Menge Anwendungen, die CalDAV beherrschen, aber das Vorgehen ist stets ähnlich: Fügen Sie in den Einstellungen einen neuen Kalender-Account hinzu und halten Sie nach einer Option wie „Anderer CalDAV-Account…“ oder „Mit CalDAV synchronisieren“ Ausschau. Dann müssen Sie Ihren Nextcloud-Benutzernamen, Ihr (App-)Passwort und den Cal- oder CardDAV-Endpunkt Ihres Nextcloud-Servers angeben.

Die URLs finden Sie in der Nextcloud-Weboberfläche etwas versteckt in den Einstellungen der jeweiligen Anwendung: Die Einstellungen der Kalender-App befinden sich in der unteren linken Ecke ihres Fensters. Sie müssen etwas runter scrollen und „Primäre CalDAV-Adresse kopieren“ anklicken. In den Kontakte-Einstellungen finden Sie den Link unter „Adressbücher“, wo Sie auf die Schaltfläche mit den drei Punkten klicken und dann „Link kopieren“ wählen.

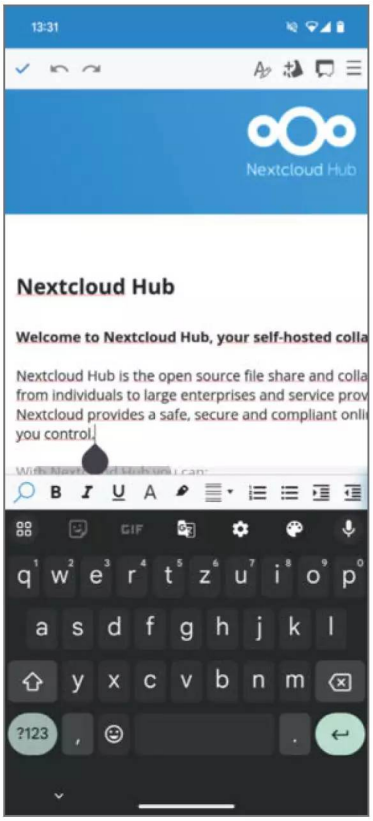
Unter macOS machen Sie die CalDAV und CardDAV-Schnittstellen über die Systemeinstellungen systemweit bekannt. Das erledigen Sie im Menü „Internetaccounts“ wie im Screenshot unten. Eine ähnliche Funktion bieten auch der Gnome- und KDE Plasma Desktop unter Linux (siehe ct.de/wxng).

Auch unterwegs synchron

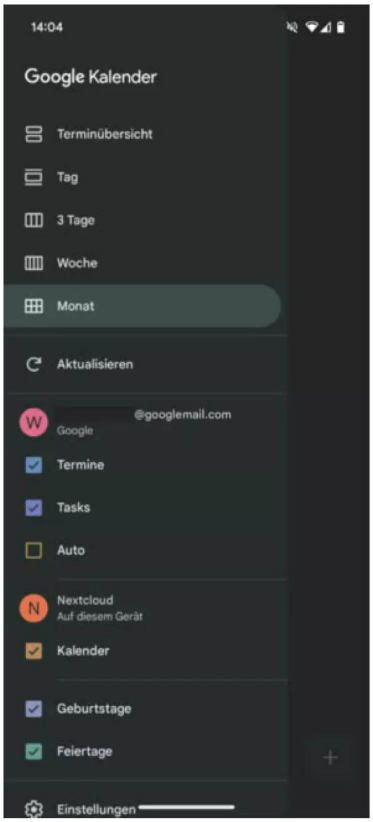
Die Einrichtung der aus dem jeweiligen App-Store für Mobilgeräte heruntergeladenen Nextcloud-App



Die Nextcloud-App, hier die Android-Version, bringt Ihre Nextcloud-Daten aufs Mobilgerät.



Mit den mobilen Nextcloud-Apps bearbeiten Sie auch Dokumente, wenn Collabora Office in der Nextcloud läuft. Spaß macht das mit dem hakeligen Interface allerdings nicht.



Alles an einem Ort: Sobald sie auf dem Gerät bekannt sind, kann man Nextcloud-Kalender auch in andere Apps importieren, beispielsweise Google Kalender.

funktioniert wie die der Desktop-App. Besonders interessant dürfte für viele Nutzer die Option „Automatisches Hochladen“ in den Einstellungen sein. Hier können Sie beispielsweise bestimmte Fotoalben oder direkt den ganzen Kamera-Ordner auswählen, damit jeder neue Schnappschuss automatisch in die Nextcloud wandert. Dafür müssen Sie der App erlauben, im Hintergrund ausgeführt zu werden, was zu einer kürzeren Akkulaufzeit führen kann. Standardmäßig lädt die App neue Dateien nur bei einer bestehenden WLAN-Verbindung hoch.

Den Sync für CalDAV und CardDAV richten Sie in iOS wie in macOS ein. Unter Android gibt es mehr zu tun, weil eine weitere App ins Spiel kommt: DAVx⁵. Wenn Sie kein Android nutzen, überspringen Sie die folgenden Absätze bis zum Fazit oder lesen sie mit Schadenfreude.

Los geht es mit dem Menüpunkt „Kalender und Kontakte synchronisieren“ in der Nextcloud-App, über den Sie zur richtigen App in den Play Store springen. Laden Sie die DAVx⁵App herunter, starten sie und nehmen dann folgende Einstellungen vor: Erlauben Sie der App mindestens, auf den Kalender und Kontakte zuzugreifen. Die anderen Berechtigungen sind optional. Anschließend sollten Sie DAVx⁵ berechtigen, im Hintergrund ausgeführt zu werden,

damit es Kalender und Kontakte regelmäßig synchronisieren kann.

Jetzt legen Sie ein neues Konto an und wählen „Nextcloud“ bei der Provider-spezifischen Anmeldung. Geben Sie die URL Ihrer Instanz ein und melden sich dann im Browser an, um den Zugriff zu gestatten. Wenn Sie nach der Kontaktgruppenmethode gefragt werden, geben Sie an „Gruppen sind Kategorien der Kontakte“. Tippen Sie dann auf dem Startbildschirm von DAVx⁵ auf das zuvor angelegte Konto und wählen die Elemente, die synchronisiert werden sollen.

DAVx⁵ macht die CalDAV und CardDAV-Schnittstellen Ihrer Nextcloud jetzt für andere Apps auf dem Gerät verfügbar, beispielsweise für den Google Kalender. Wenn Sie einen Kalender dort importieren wollen, rufen Sie „Konten verwalten“ in den Einstellungen der Google-Kalender-App auf. Unter „Nicht-Google-Konten“ sollte der Name des Accounts aufgeführt sein, den DAVx⁵ auf dem Gerät verwaltet; Sie müssen ihn nur noch aktivieren. Ab jetzt werden die Termine Ihres Nextcloud-Kalenders synchronisiert und automatisch in die Kalender-App eingetragen.

Downloadlinks für die Desktop- und Mobil-Clients:
ct.de/wxng

Fazit

Für Nextcloud gibt es eine umfangreiche App-Landschaft. Wenn Sie die Clients erstmal eingerichtet haben, bekommen Sie von Ihnen in der Regel nicht mehr viel mit, weil sie stumm und brav im Hintergrund arbeiten. Um die Anbindung an die eigene Cloud auf allen Geräten herzustellen, ist etwas mehr Arbeit nötig als bei den Cloudspeichern der etablierten Anbieter. Das liegt manchmal, aber nicht immer an Nextcloud, sondern auch an den Plattformen, die Alternativen zu ihren eigenen Diensten nicht unbedingt die Tür aufhalten. Der Aufwand lohnt sich, wenn Sie Wert darauf legen, Ihre Daten für sich zu behalten. (ndi) ct

Bild: Moritz Reichartz

DSGVO-konforme gehostete Nextclouds

Nextcloud selbst zu installieren erfordert Administrationsaufwand und Know-how. Diese Arbeit nehmen einem Hoster ab und bieten von ihnen gewartete Nextcloud-Instanzen bereits ab fünf Euro pro Monat an. Wir haben uns einige Angebote für Sie angesehen.

Von **Holger Bleich**

Mit Nextcloud steht eine ausgewachsene Alternative zu kommerziellen Storage- und Groupware-Produkten der großen Anbieter bereit. Diese Erkenntnis hat sich mittlerweile herumgesprochen. Sowohl Privatleute als auch Vereine, die öffentliche Verwaltung und kleinere Unternehmen nutzen die Open-Source-Software, um ihren digitalen Alltag zu organisieren.

Doch viele zögern auch vor einem Umstieg. Denn sich auf Nextcloud einzulassen, kann im Vergleich zu den Angeboten von Google, Microsoft & Co. einigen Mehraufwand bedeuten: Wer eine Instanz selbst

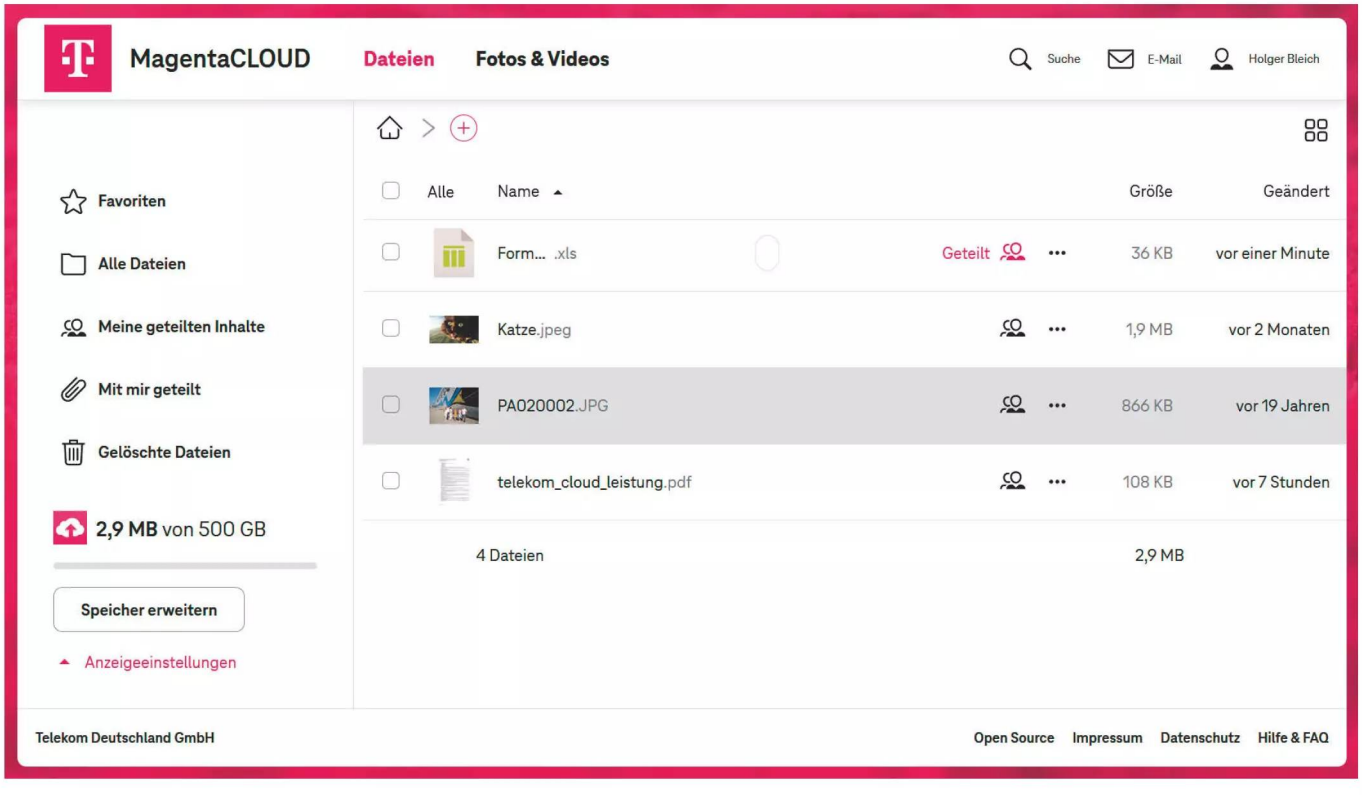
hosten möchte, muss einen gut angebundenen Server mit ausreichend Speicherplatz haben oder anmieten. Nextcloud selbst will korrekt installiert, gepflegt und stets mit nötigen Updates versorgt werden. Unternehmen mit eigenen IT-Abteilungen haben dafür eher Kapazitäten als die Arztpraxis um die Ecke oder die kleine Werbeagentur.

Für diese Kunden bieten einige Hosting-Provider mit ihren sogenannten „Managed Nextclouds“ eine tolle Alternative. Bei diesen Angeboten klicken Sie sich als Kunde im Shop eine Nextcloud-Instanz zusammen, die der Provider für Sie auf seinen Servern installiert. Meist binnen weniger Stunden oder sogar Minuten erhalten Sie Ihre Nextcloud in Form des Admin-Zugangs und können loslegen. Um die Systemwartung kümmert sich der Hoster fortan im Hintergrund.

Nextcloud von der Stange

Die Nextcloud GmbH als Betreiber des Softwareprojekts kooperiert mit vielen Hostern im In- und Ausland, um sie bei ihren Managed-Cloud-Angeboten zu unterstützen. Auf der Website finden sich diese Hoster, unterteilt in Silber- Gold- und Platin-Partner. Bis auf wenige Ausnahmen geht es allerdings um B2B-Angebote für größere Kunden, etwa mittelständische Unternehmen. Wer beispielsweise konkrete Preise erfahren will, muss erst einmal anfragen.

Für diese Marktübersicht haben wir uns nach Produkten „von der Stange“ umgesehen, die konkrete Preisschilder tragen und auch Vereinen und Familien kein großes Loch ins Budget reißen. Wichtig war uns insbesondere, dass diese Nextcloud-



Kaum zu erkennen: Die MagentaCloud von der Telekom ist hinter den Kulissen eine umgelabelte und stark funktionsreduzierte Nextcloud-Instanz.

Pakete in deutschen Rechenzentren betrieben werden und die Anbieter garantieren, DSGVO-konform zu agieren. Schließlich geht es vielen bei Nextcloud ja auch darum, zugunsten von mehr Datenschutz einen Bogen um die datengetriebenen US-Konzerne zu machen.

Wir haben einige Angebote deutscher Hoster ausgewählt, die uns besonders interessant erschienen und die Breite des Angebots im unteren bis mittleren Preissegment widerspiegeln. Namentlich handelt es sich um Managed Nextclouds der Hoster Hetzner Online, Hosting.de, Ionos, Keyweb und der Deutschen Telekom. Letztere bietet neben der von uns gewählten MagentaCloud außerdem die Nextcloud-Lösung MagentaBusiness Cloud an, allerdings ausschließlich an Geschäftskunden.

Die hier aufgeführten Angebote können Sie ohne allzu große Investition selbst auf Herz und Nieren testen, denn sie kennen keine langen Mindestvertragslaufzeiten. Bis auf die MagentaCloud (3 Monate) sind sie sogar sofort beziehungsweise zum Monatsende wieder kündbar. Ein einmaliger Einrichtungspreis, wie er früher oft üblich war, fällt nirgends an.

Admin-Freiheit vs. Ressourcen

Bevor Sie sich fest für ein Angebot entscheiden, sollten Sie ungefähr ausgelotet haben, wie viele Personen gemeinsam die Nextcloud nutzen werden. In der Tabelle am Ende des Artikels sehen Sie, wie viele Nutzer der Provider maximal zulässt. Doch diese Angabe ist mit Vorsicht zu genießen: Ionos etwa gestattet zwar eine unbegrenzte Anzahl, weist aber darauf hin, dass das die zugewiesenen Ressourcen für das Paket „500 GB“ nur für bis zu fünf gleichzeitig aktive Nutzer ausgelegt sind. Außerdem dürfen nur fünf Nutzer Collabora-Office (Nextcloud Office) gleichzeitig nutzen, das Zugriff auf einen externen Dokumentenserver hat.

Hier zeigt sich für die Hoster eine Krux bei der Managed Nextcloud: Sie möchten den Kunden möglichst große Freiheiten gewähren, also idealerweise auch Administratorrechte. Damit wiederum geht die Option einher, unbegrenzt Nutzer und Gruppen anzulegen und Apps zu installieren, die den Funktionsumfang von Nextcloud erweitern – bei begrenzten und wenig skalierenden Ressourcen. In unserer Übersicht sehen Sie, dass Hosting.de und die Telekom wohl auch deshalb das Admin-Recht nicht gewähren. Bei den anderen Hostern besteht die Gefahr, dass Performance-Engpässe entstehen, wenn man die Möglichkeiten überreizt. Sie bieten wenigstens alle die Möglichkeit, in höhere Pakete zu migrieren.

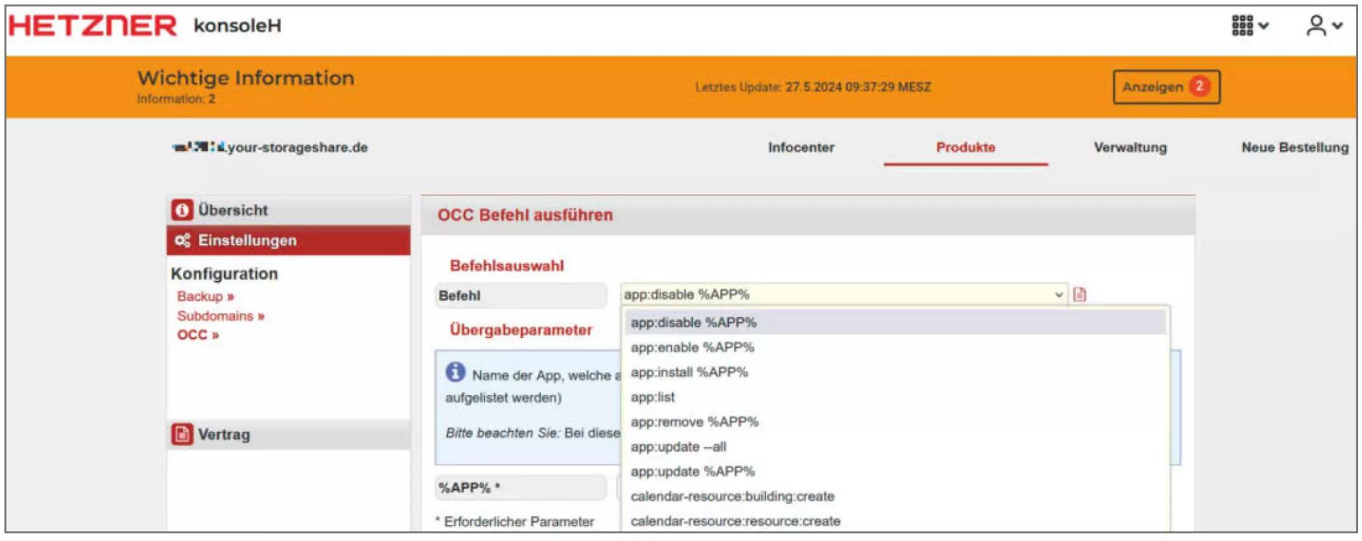
Dies gilt auch für den gebuchten Speicherplatz, den sich alle Nutzer der Nextcloud teilen. Wir haben uns bei der Auswahl der Testkandidaten an der Marke 500 GByte orientiert. Nur Hetzner schert aus, weil bereits das kleinste Angebot „Storage Share NX11“ ein sattes Terabyte Platz bietet. 500 GByte sollten für die Familie oder den Verein, dessen Nutzer Dokumente und Fotos ablegen, locker reichen. Doch wenn die Mitarbeiter der Medienagentur massenhaft RAW-Dateien aus den Digitalkameras archivieren oder gar 4K-Videos tauschen, wird es schnell eng. Deshalb ist auch hier wichtig: Upgrades sind möglich. Im Zweifel checken Sie die mit Aufpreis erhältlichen Maximal-Volumina, bevor Sie sich gänzlich auf einen Hoster einlassen.

Up- und Downloads der Nextcloud-Nutzer erzeugen beim Hoster IP-Traffic – und das mitunter nicht zu knapp. Macht nichts, sollte man meinen, weil IP-Traffic billig geworden ist und daher in der Gesamtkalkulation von Hosting-Angeboten kaum noch ins Gewicht fällt. Dennoch setzen zwei der fünf von uns herausgepickten Hoster Limits: Hosting.de kappt den Datentransfer nach der 2-TByte-Monatsgrenze komplett, diese dürften kleinere Nutzergruppen allerdings kaum jemals erreichen.

Das Transferlimit zur „MagentaCloud L“ haben wir eher zufällig im Kleingedruckten der Leistungsbeschreibung entdeckt. Lediglich 200 GByte Up- und Download-Traffic gewährt der Rosa Riese, danach sperrt er den Transfer bis zum Monatsende. Skurril, denn mit diesem Transfervolumen lässt sich der 500-GByte-Storage nicht einmal zur Hälfte befüllen. Ein Kollege kommentierte treffend: „Die 90er lassen grüßen!“ Diesen Pferdefuß im Angebot sollte die Telekom schnellstmöglich beseitigen.

Die Hoster legen für die Managed Nextclouds ihrer Kunden jeweils eine IPv4-Adresse sowie eine recht kryptische Subdomain unter der für das Angebot vorgesehenen Second-Level-Domain an. Bei Hetzner ist dies your-storageshare.de, bei Hosting.de nextcloud.hosting.zone, bei Ionos nextcloud-ionos.com und bei Keyweb key-cloud.de. Kunden der MagentaCloud erreichen ihre Nextcloud so nicht, sie müssen sich unter magentacloud.de einloggen und werden in ein Unterverzeichnis weitergeleitet.

Alle in der Tabelle aufgeführten Angebote sind HTTPS-transportverschlüsselt. Ihre Daten wandern also abhörsicher durchs Netz. Bei allen Hostern außer bei der Telekom kann man eine Second-Level-Domain inklusive SSL-Zertifikat hinzubuchen,



Im Kundenmenü zu Hetzners StorageShare darf man sogar occ-Befehle an die eigene Nextcloud-Instanz senden. Bei occ handelt es sich um ein Kommandozeilenwerkzeug, das Ihnen Zugriff auf den Maschinenraum von Nextcloud gibt.

unter der die Managed Nextcloud erreichbar sein soll. Beim Ionos-Angebot ist diese sogar bereits im Preis enthalten. Dort erhält der Admin überdies auf Wunsch kostenfrei einen Account im Ionos-Mailsystem. Auch die Telekom bietet dies an, die anderen drei Hoster nicht.

Oberflächen-Wirrwar

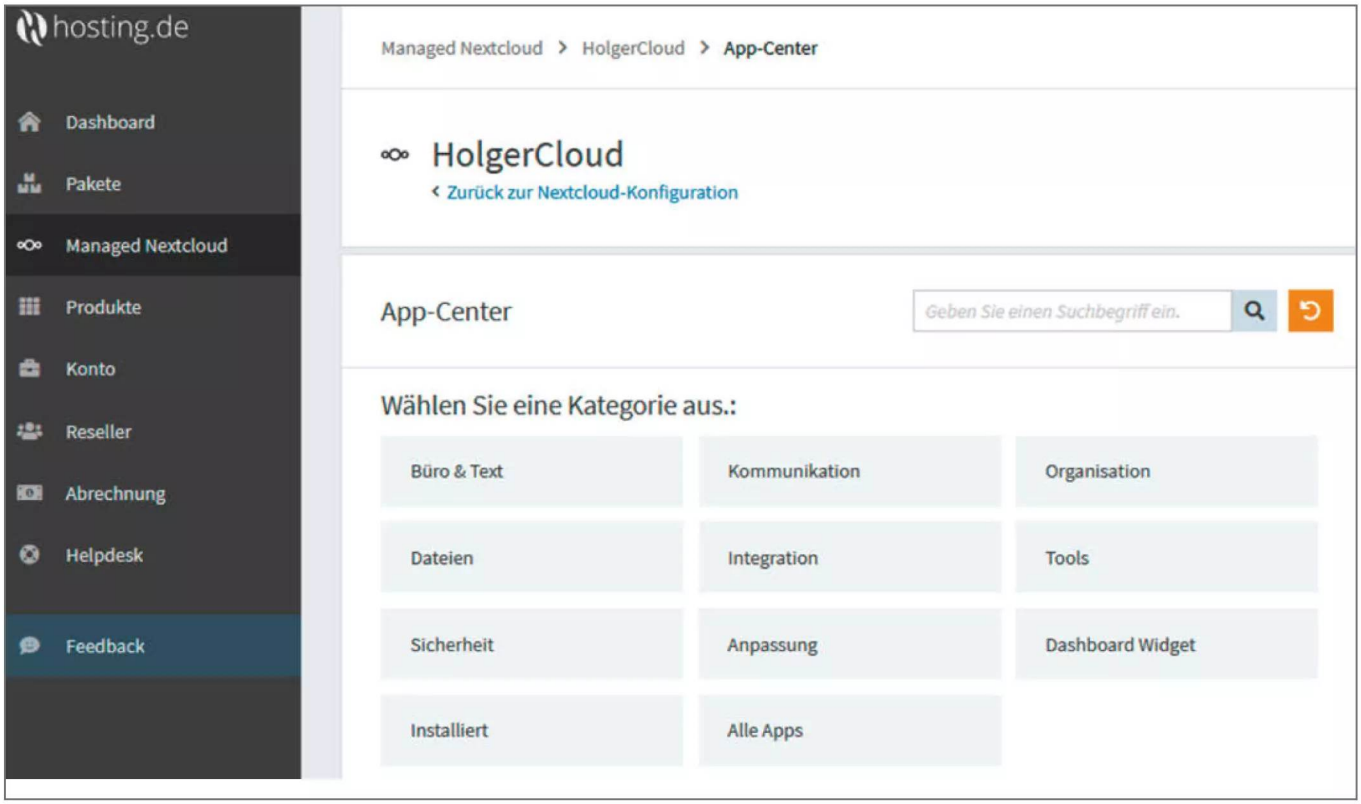
Bei Hostern ist es üblich, dass die Kunden ihr Konto über eine Weboberfläche administrieren. Hier findet man die Vertragsmodalitäten, kann Funktionen hinzubuchen oder beispielsweise Domains bestellen. Für diese Oberfläche erhält man eigene Zugangsdaten. Legt man dort die Managed Nextcloud an, liefert der Hoster hierfür ein separates Start-Passwort – entweder für einen Admin- oder Nutzerzugang (siehe Tabelle „Managed Nextclouds vom Hoster – eine Auswahl“).

Nur bei der Telekom ist es anders: Hier landet man direkt als einziger Nutzer auf der Nextcloud-Oberfläche, die der Provider nach dem eigenen Markendesign stark umgestaltet hat. Administrationsoptionen existieren hier nicht. Die Telekom vermarktet das Angebot als Consumer-Produkt und in erster Linie als teilbaren Dateispeicher, deshalb verfährt sie augenscheinlich nach dem Motto „Keep it simple“.

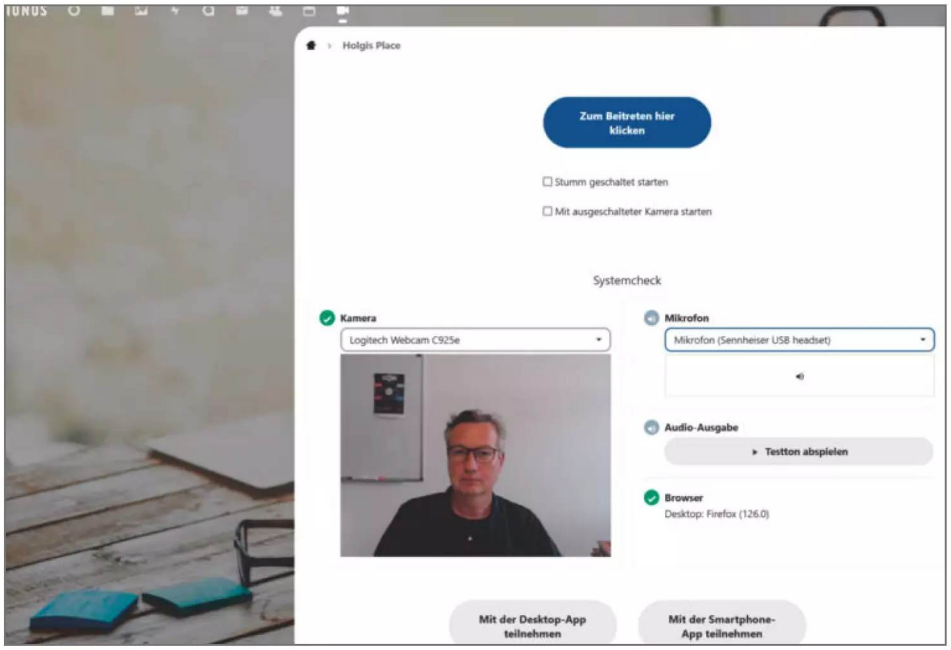
Dies kann man von der „konsoleH“ genannten Nutzer-Kommandozentrale des Hosters Hetzner nicht gerade behaupten. Das mächtige Interface erschließt sich nicht eben von selbst, ermöglicht aber eine Menge mehr als die anderer Hoster. So lassen sich hier weitere Subdomains anlegen, unter denen die Managed Nextcloud erreichbar sein soll. Vor allem aber macht die konsoleH täglich gefertigte Backup-Dumps der Nextcloud-Instanz zugänglich, die eine Woche zurückreichen. Über die Oberfläche kann man selbst ein Restore anstoßen, findet hier also Netz und doppelten Boden vor. Andere Hoster in der Übersicht (Ionos und Telekom) bieten einen solchen Backup-Service gar nicht an oder lassen ihn sich zusätzlich vergüten (Hosting.de und Keyweb).

Einblicke

Als Open-Source-Softwarepaket ermöglicht Nextcloud den Hostern viel Gestaltungsspielraum für ihre Angebote. Tatsächlich unterschieden sich die von uns in Augenschein genommenen Produkte erheblich. Vermarkten Hetzner und die Telekom ihre



Bei Hosting.de installiert man Apps nicht im Nextcloud-Store nach, sondern über die Weboberfläche zur Vertragsverwaltung.



Ionos stellt in seiner Managed Nextcloud das Videokonferenz-Tool Jitsi bereit, das extern gehostet wird und deshalb keinen Performance-Engpass in der Instanz verursachen kann.

Managed Nextcloud in erster Linie als teilbaren Dateispeicher, liegt der Schwerpunkt bei Hosting.de, Ionos und Keyweb auf den Groupware-Funktionen wie Kalender, Chat und Online-Office. Das heißt aber keineswegs, dass diese Funktionen woanders nicht vorhanden sind oder sich nicht nachrüsten lassen. Im Folgenden zeigen wir an den gewählten Beispielen, wie verschieden die Hoster ihre Managed Clouds umgesetzt haben.

Hetzner offeriert mit StorageShare eine schlichte Standard-Nextcloud mit Anpassungen im Design. Der Kunde erhält einen vollen Admin-Zugang und kann beliebig viele Nutzer anlegen. Obwohl das Angebot als Dateispeicher daherkommt und in der Beschreibung kaum als vollwertige Managed Nextcloud zu erkennen ist, handelt es sich genau um dies: Der Nextcloud-Appstore ermöglicht es, Anwendungen nachzuinstallieren.

Ein Sprecher bestätigte Nachfrage uns dies auf und schränkte ein: „Eine Garantie für die Apps aus dem Appstore bieten wir jedoch nicht an. Aus dem Appstore entfernen wir via Proxy lediglich Apps, welche nicht funktionieren, zu einem erhöhtem Supportaufwand (bspw. kaputte Instanzen nach Aktivierung) oder Lastspitzen führen."

Hetzner bietet sogar noch mehr: In der Oberfläche konsoleH darf der Kunde seine Nextcloud über eine Art Kommandozeilen-Tool sogar via occ-Befehlssatz steuern. Diese Funktion gewährt unseres Wissens kein anderer Anbieter von Managed Nextclouds. OCC steht für „OwnCloud Console" und lässt den Admin das System über PHP-Skripte konfigurieren.

Einen ganz anderen Weg geht **Hosting.de**: Dort erhält der Kunde keinen Zugang als Administrator, sondern agiert als Nutzer mit erweiterten Rechten. Der Appstore steht also nicht zur Verfügung. Stattdessen installiert man hier ausgewählte Apps über das „App-Center" in der Weboberfläche zur Vertragsverwaltung nach. Dafür liefert Hosting.de die Managed Nextcloud mit vielen bereits vorinstallierten Apps aus. Das Online-Office Collabora kann man nachinstallieren, es darf aber nur von einem Nutzer verwendet werden.

Einige Features behält Hosting.de den teureren Business-Varianten der Managed Nextcloud vor, etwa die LDAP-Anbindung. Ohnehin gibt es viele Funktionen nur gegen Aufpreis, etwa das in der Oberfläche in roten Lettern dringend angeratene Backup.

Ionos setzt auf die besser unterstützte Enterprise-Variante der Nextcloud-Software. Die 1&1-Hosting-Tochter gewährt bei der Managed Nextcloud Admin-Zugang, also auch Zugriff auf den Appstore. Das Paket ist schon vom Start weg reichhaltig ausgestattet. Zur Kommunikation steht den Nutzern nicht nur das Nextcloud-eigene Talk zur Verfügung. Eingebunden hat Ionos darüber hinaus auch eine extern laufende Instanz der Videokonferenz-Software Jitsi, die in unseren Stichproben prima funktionierte. Weil sie isoliert läuft, taucht sie allerdings nicht in den Aktivitätsberichten von Nextcloud auf.

Der Hoster hat die Nextcloud-Oberfläche stark auf sein eigenes Marken-Branding umgestaltet. Die Installation machte einen runden, nutzerfreundlichen und vor allem flotten Eindruck. Alles wirkt gut durchdacht. Man scheint bei Ionos viel Hirnschmalz investiert zu haben.

Wir haben bei Ionos als dem größten deutschen Hoster nachgefragt, wie erfolgreich denn die Managed Nextcloud ist. Ein Sprecher versicherte „eine große und stetig wachsende Nachfrage". Und: „Im vergangenen Jahr konnten wir einen leicht höheren Neukundenzufluss als bei Microsoft 365 und Google Workspace verzeichnen." Allerdings kommuniziere man „generell keine Zahlen zu einzelnen Produkten".

Der eher kleine Provider **Keyweb** aus Erfurt hat sich unter anderem aufs Nextcloud-Hosting spezialisiert. Seine „KeyCloud" kommt sehr schlank konfiguriert zum Kunden. Sie wirkt wie eine recht unfertige Standardinstallation. In den Sicherheits- und Einrichtungswarnungen wurden wir beispielsweise über einen Fehler zu „PHP OPcache" informiert.

Der Kunde erhält volle Rechte auf der Instanz und darf aus dem Appstore nachinstallieren sowie Nutzer und Gruppen verwalten. Keyweb hat die manuelle Update-Option nicht deaktiviert, sodass man als Admin auch selbst Updates anstoßen kann. Dies beißt sich etwas mit dem Rundum-Sorglos-Konzept der Managed Cloud und dürfte bei so manchem Kunden für Verwirrung sorgen.

Aus der Reihe tanzt in unserer kleinen Auswahl das **Telekom**-Produkt. MagentaCloud richtet sich wie erwähnt an Privatnutzer, in erster Linie als Dateispeicher. Der Kunde agiert als stark beschränkter Nutzer, eine Installation von Apps ist ebenso wenig möglich, wie das Anlegen weiterer Nutzerkonten. Immerhin stellt die Telekom für den einen Nutzer Collabora als Online-Office bereit. Er darf darin mit eingeladenen Gästen gemeinsam an Dokumenten arbeiten – ein wenig Groupware-Feeling bleibt gewahrt.

Nutzungshinweise

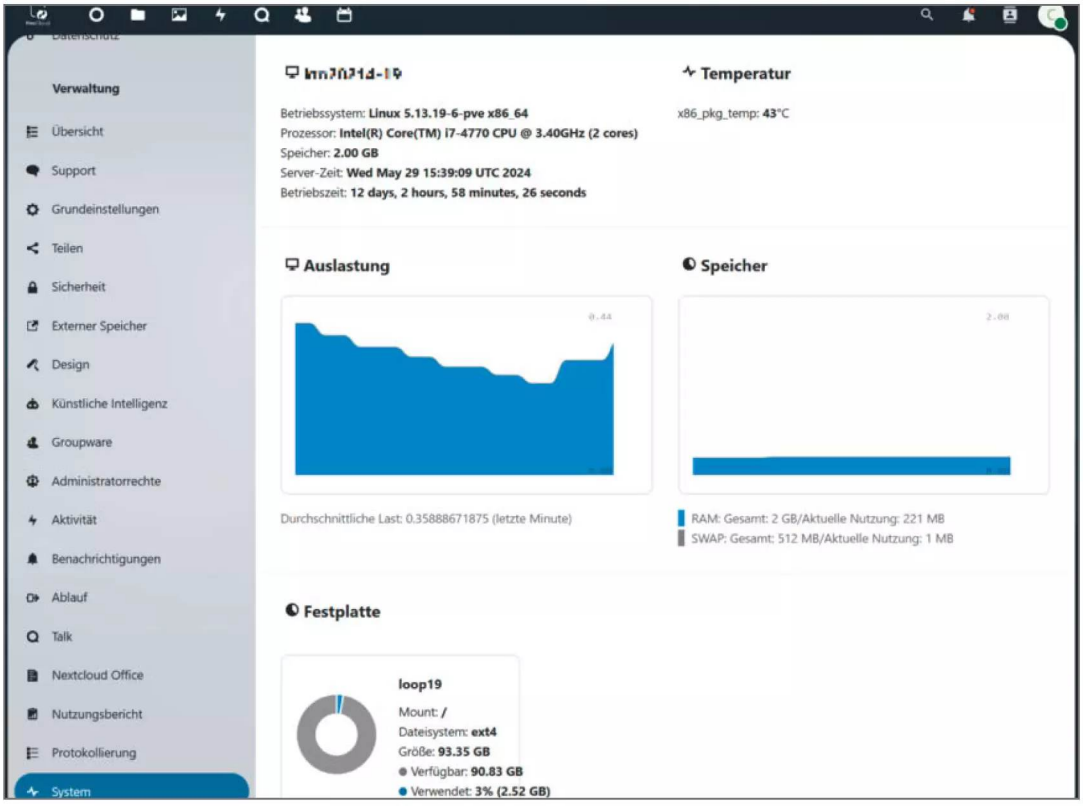
Die starke Vereinfachung und das optische Aufhübschen der Telekom-Instanzen bietet einen Vorteil:

Diese Managed Nextcloud ist die einzige, in der sich auch unerfahrene Nutzer sofort zurechtfinden. Denn selbsterklärend ist eine Standardinstallation keineswegs, obwohl sie von einigen Hostern so angepriesen wird.

Wer mit anderem rechnet, dürfte erst einmal wie der Ochs vorm Berg stehen, wenn er sich zum ersten Mal in seine vom Provider frisch aufgesetzte Instanz einloggt. Einführende Erklärungen oder gar Tutorials haben wir bei keinem Hoster gefunden. Nextcloud-Basiswissen und sogar Admin-Know-how wird offensichtlich vorausgesetzt, ohne dass dies irgendwo explizit erwähnt ist.

Dass alle Hoster Konformität mit dem EU-Datenschutzrecht garantieren, heißt übrigens nicht, dass Sie sensibelste Daten bedenkenlos in der Nextcloud ablegen können. Alle gelangen zwar transportverschlüsselt vom und zum Server, aber der Nextcloud-Speicher selbst ist erst einmal unverschlüsselt. Das bedeutet: Der Hoster, und damit auf richterlichen Beschluss hin etwa auch Strafverfolgungsbehörden, können auf die Daten zugreifen. Als Nextcloud-Administrator die Option „Serverseitige Verschlüsselung“ zu aktivieren, bringt in diesem Fall auch nichts, denn der Schlüssel zum Entschlüsseln der Dateien liegt in Datenverzeichnis der Nextcloud. Dateien, die wirklich niemand außer Ihnen zu sehen bekommen soll, gehören schon vor dem Hochladen in die Cloud mit einer zusätzlichen Software wie Kryptomator Ende-zu-Ende-verschlüsselt.

Bieten Sie im geschäftlichen Bereich, also etwa im Unternehmen, Ihre Managed Nextcloud anderen Personen zur Nutzung an, sollten Sie außerdem einen Auftragsverarbeitungsvertrag mit dem Web-



Tiefe Einblicke: Als Admin hat man in der Managed Nextcloud von Keyweb sogar Zugriff auf den Hardware-Monitor.

Managed Nextclouds vom Hoster – Auswahl

Anbieter	Hetzner	Hosting.de	Ionos	Keyweb	Telekom
Produkt	Storage Share NX11	Managed Nextcloud 500 GB	Managed Nextcloud 500 GB + Collabora Online	KeyCloud 500	MagentaCloud L
URL	https://www.hetzner.com	https://www.hosting.de	https://www.ionos.de	https://www.keyweb.de	https://cloud.telekom-dienste.de
Ausstattung inklusive					
Gemeinsam nutzbarer Dateispeicher	1 TByte	500 GByte	500 GByte	600 GByte	500 GByte
Nutzer maximal	unbegrenzt	10	5	unbegrenzt	1
Server-Standort	Deutschland	Deutschland	Deutschland	Deutschland	Deutschland
Kommandozeile	✓	–	–	–	–
DSGVO-Konfomität garantiert	✓	✓	✓	✓	✓
inkl. Domain	–	–	✓	–	–
inkl. SSL-Zertifikat	✓	✓	✓	✓	–
IP-Traffic pro Monat	unbegrenzt	2 TByte	unbegrenzt	unbegrenzt	200 GByte
Provider-Mailservice	–	–	✓	–	✓
Tägl. Backup	✓	– (4 € / Monat)	–	– (11 € / Monat)	–
Nextcloud-Funktionen					
Admin-Account	✓	–	✓	✓	–
Mail/Kontakte/Kalender	✓/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓	–/–/–
Kanban	– (installierbar)	Deck	Deck	– (installierbar)	–
Umfragen (Forms)	– (installierbar)	✓	✓	– (installierbar)	–
Online-Office (Collabora)	–	✓ (1 Nutzer)	✓ (5 Nutzer)	– (installierbar)	✓ (1 Nutzer)
Chat/Audio/Video (Talk)	– (installierbar)	✓	✓ (außerdem Jitsi)	✓	–
Vertrag					
Preis pro Monat	5,11 €	6,90 €	8,50 €	14 €	4,95 €
Mindestvertragslaufzeit	1 Monat	1 Monat	1 Monat	1 Monat	3 Monate
Kündigungsfrist	monatlich	monatlich	monatlich	monatlich	6 Tage

✓ vorhanden – nicht vorhanden k. A. keine Angabe

hoster abschließen. Denn ab diesem Moment sind sie für dessen Datenverarbeitung im Sinne der DSGVO gegenüber den Dritten verantwortlich und sollten sich vertraglich absichern. Entsprechende PDF-Vordrucke oder Online-Formulare bieten inzwischen alle uns bekannten Webhoster im Kundenmenü an.

Fazit

Einige Hoster bieten erstaunlich viel Managed Nextcloud für wenig Geld. Insbesondere Hetzner spendiert einiges: Für wenig mehr als fünf Euro monatlich erhält man satte 1 TByte Storage, Admin-Zugang und sogar occ-Zugriff, der die Nextcloud-Nerds unter Ihnen interessieren könnte.

Möchte man als Gruppe schnell und sorglos loslegen, liefert Ionos mit den vielen vorinstallierten Apps sowie einem performanten Videokonferenz-Add-on einen guten Nextcloud-Startpunkt. Nutzer, die lediglich einen Dateispeicher inklusive gelegentlicher gemeinsamer Dokumentenbearbeitung suchen, können auf das simpel gestrickte Telekom-Angebot zurückgreifen.

Bis auf Keyweb verlangen alle von uns vorgestellten Hoster weniger als zehn Euro pro Monat bei kurzen Kündigungsfristen. Eigene Experimente mit den Managed Nextclouds schlagen also wenig ins finanzielle Kontor. Bei diesen Preisen dürfte der eine oder andere Admin, der seine Nextcloud auf dem NAS oder Raspi zu Hause beherbergt, ins Grübeln kommen, ob der Aufwand noch lohnt. (hob) c't

Links zu allen Angeboten
ct.de/wc28

Lohnenswerte Self-Hosting-Projekte

Der Heimserver ist startbereit, das Linux läuft – und jetzt? Open-Source-Software zum Selbsthosten gibt es reichlich. Oft ersetzt sie problemlos kommerzielle Dienste. Eine Auswahl.

Von **Jan Mahn**

Bild: Sven Hauth

An Software, die man auf einem Heimserver betreiben kann, mangelt es wahrlich nicht und auch Lizenzkosten muss man in der Regel nicht einplanen – eine große und aktive Open-Source-Gemeinschaft kümmert sich um Dutzende Anwendungen zum Selbsthosten.

Nextcloud fällt in vielen Aufzählungen zuerst, wenn es um lohnenswerte Software geht. Auf einer selbst betriebenen Instanz speichern Sie Dokumente, synchronisieren sie über mehrere Arbeitsgeräte, teilen sie mit anderen, pflegen Kalender und Adressbücher, können aber auch mit anderen videotelefonieren und Dokumente kollaborativ bearbeiten. Mehr über dieses Komplettpaket lesen Sie ab Seite 98.

Wer gerne viele Fotos schießt und genug hat von den Google- oder Apple-Fotobibliotheken, startet **Immich**. Die Galerieansichten können mit denen der kommerziellen Vorbilder mithalten. Auf Seite 126 erfahren Sie, wie man diese Software selbst betreibt. Will man weiter bei Apple bleiben und die Daten zusätzlich auf dem eigenen Server vorhalten, empfiehlt sich die automatische Sicherung mit **Icloudpd**.

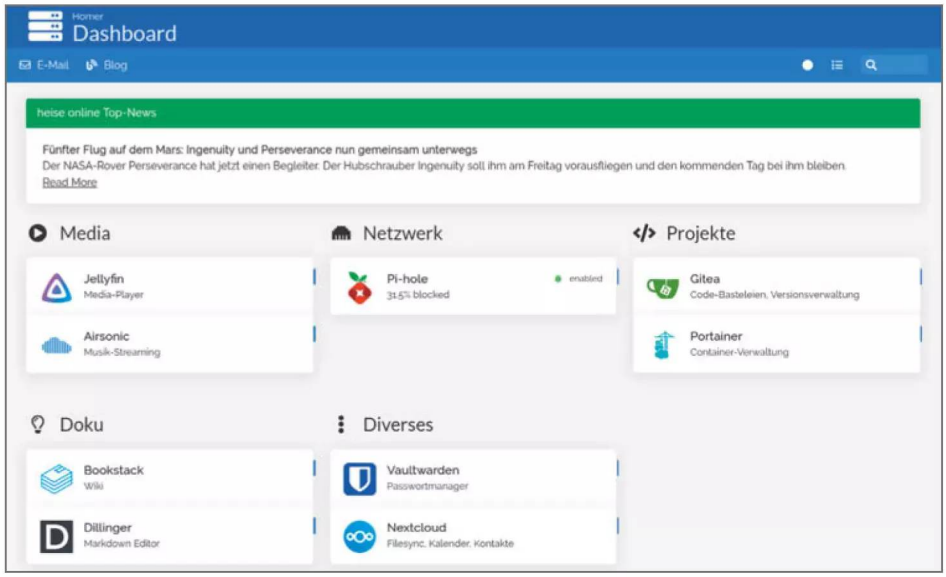
Soll der Server dem eigenen Zuhause dienen, kommen Dienste wie **Pi-hole** oder **Adguard Home** infrage. Die arbeiten lokal als DNS-Server und filtern Werbung und Domains mit schädlichen Inhalten raus. Ebenfalls nützlich für zu Hause ist die breite Palette der Hausautomationsserver wie **Home Assistant, OpenHAB oder Node-Red**. Wer eine PV-Anlage und eine Wallbox besitzt, kann beide mit **EVCC** zur Zusammenarbeit bringen.

Passwortmanager mit Synchronisation sind praktisch, mit anderen teilen will man die Geheimnisse aber nicht unbedingt. Mit einem selbst gehosteten Server wie **Vaultwarden** bleiben sie unter eigener Kontrolle.

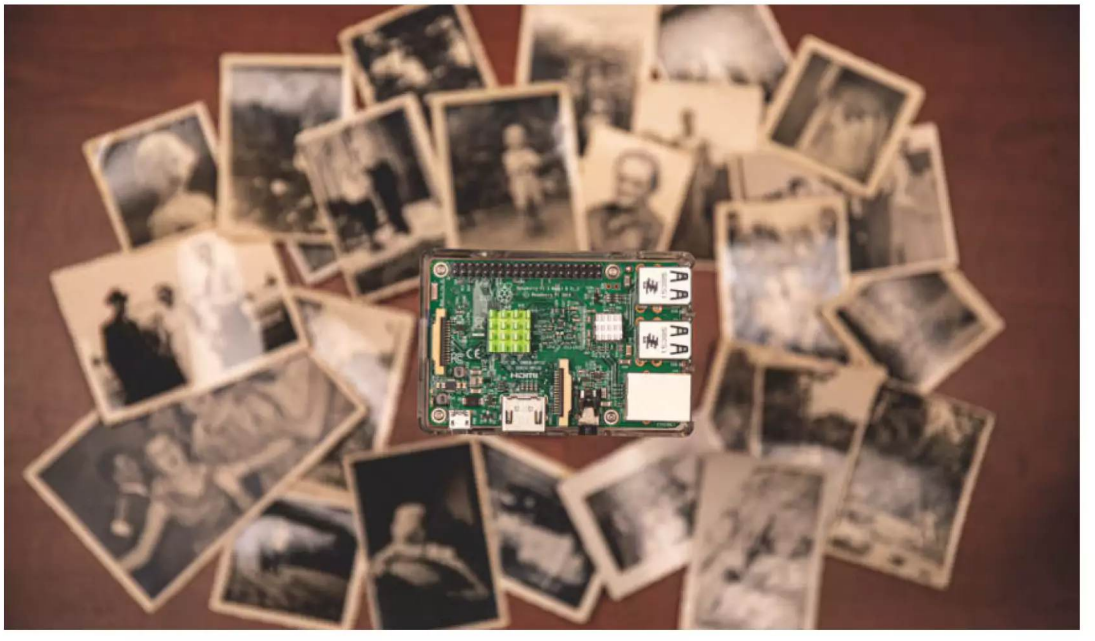
Schlechten Tag gehabt? Wenn sich das häuft, lohnt sich vielleicht ein Stimmungstracker, eine Art Tagebuch mit spielerischem Ansatz. So was gibt es mit Cloudanbindung im App-Store zuhauf, aber die sensiblen Daten müssen das Haus nicht verlassen: **HabitTrove** bewahrt sie auf dem eigenen Server auf.

Wenn Sie viel unterwegs sind und die Routen gern dokumentieren, diese sensiblen Daten aber nicht unbedingt Unternehmen wie Google anvertrauen wollen, ist der Open-Source-Standortprotokollierer **Dawarich** eine Empfehlung. Mehr zum Betrieb der Software auf einem eigenen oder gemieteten Server lesen Sie ab Seite 132. In eine ähnliche Rubrik fällt die Software **Traccar** für das persönliche Flottenmanagement. Damit behalten Sie zum Beispiel die Übersicht, wo sich Ihre mit GNSS-Sender ausgestatteten Fahrzeuge und Werkzeuge befinden. Ein weiterer naheliegender Einsatzbereich für einen Heimserver: Backups verwalten. Auf Seite 138 machen wir einen Vorschlag, wie ein solcher Server aussehen kann. (jam) c't

Links zu allen erwähnten Diensten:
ct.de/wfev



Wenn sich viele Webanwendungen im Netzwerk tummeln, kann man schon mal den Überblick verlieren. Das Dashboard „Homer" sorgt für Übersicht über die selbst betriebenen Dienste.



Eigene Fotocloud mit Immich

Viele Nutzer haben kein Backup ihrer Smartphone-Fotos. Und falls doch, liegen die Bilder bei Apple oder Google in der Cloud. Wer viel knipst, wird für Speicherkontingent zur Kasse gebeten. Es geht aber besser: Mit der kostenlosen Software Immich setzt man eine eigene Foto-Cloud auf, die man selbst kontrolliert und die den etablierten Diensten kaum nachsteht.

Von **Stefan Porteck**

Apple und Google bieten eigene Fotogalerien an, die die Fotos automatisch in der Cloud sichern, aber diese Lösungen mag nicht jeder: Manche Nutzer haben Datenschutzbedenken, ihre privaten Fotos in die Cloud eines US-amerikanischen Anbieters zu schicken, andere machen so viele Bilder, dass sie schnell ans Speicherlimit geraten. Dann bleibt nur eine kostenpflichtige Erweiterung des Speicherkontingents. Ein Ausweg ist eine App zur Dateisynchronisation, die die Fotos regelmäßig auf den heimischen PC oder ein NAS sichert. So bleiben Bilder beim Verlust des Smartphones zwar erhalten, am Handy fehlt aber eine schicke Galerie-App mit starker Suchfunktion. Es scheint, als müsste man in wenigstens einen sauren Apfel beißen: entweder hat man Kontrolle, Sicherheit und

Datenschutz oder bekommt Komfort und praktische Features.

Doch mit einem Raspberry Pi und einer USB-Festplatte klappt die Quadratur des Kreises: Die kostenlose Open-Source-Software Immich (ausgesprochen wie das englische Wort Image) sichert, organisiert und präsentiert die eigenen Schnappschüsse ganz automatisch.

Die Optik von Immich gleicht der von Google Fotos fast wie ein Ei dem anderen. Auch beim Funktionsumfang steht Immich der Fotoverwaltung von Google in kaum etwas nach: Fotos werden automatisch verschlagwortet, sodass man in der Volltextsuche nach Bildern mit gewünschtem Inhalt suchen kann. Darüber hinaus lässt sich auch klassisch nach Aufnahmen mit einem bestimmten Datum oder von einem Ort suchen. Letzteres sogar grafisch über eine Kartenansicht. Zudem erkennt und unterscheidet Immich Personen und blendet wie das Vorbild aus Mountain View über der Zeitleiste Erinnerungen mit Fotos vergangener Jahre ein.

Das Beste daran: Trotz der komplexen Serverarchitektur und dem großen Funktionsumfang ist Immich kinderleicht installiert und eingerichtet und die KI läuft lokal auf dem Raspi – es verlassen also keine persönlichen Daten das Haus.

Der Zugriff klappt so aber nur über das heimische Netzwerk. Sollen die Urlaubsfotos sofort hochgeladen und präsentiert werden, muss man über ein VPN auf den eigenen Router zugreifen. Besonders leicht geht das mit der Fritzbox: Sie unterstützt das schnelle und stromsparende Wireguard-Protokoll, für das es kostenlose Apps für Android und iOS gibt. Alternativ gibt man die Ports im Router frei und greift von außen über einen DynDNS-Dientst auf Immich zu. Das sollte dann aber über eine HTTPS-Verbindung geschehen. Immich unterstützt dafür die Einbindung selbst signierter SSL-Zertifikate.

Nicht am falschen Ende sparen

Da die KI der Bildanalyse Rechenleistung benötigt und man in der Immich-App auf dem Smartphone auch auf ältere und bereits vom Handy gelöschte Bilder zugreifen will, sollte mindestens ein Raspi der vierten Generation zum Einsatz kommen. Für diesen Artikel haben wir auf ein Modell mit 8 GByte Arbeitsspeicher zurückgegriffen.

Wer nicht täglich Dutzende Fotos und Videos aufnimmt, kommt theoretisch mit einer SD-Karte von 128 oder 256 GByte etliche Jahre über die Runden. Es ist aber keine gute Idee, einen Raspi-Cloud-Server mit einer SD-Karte zu betreiben. Zum einen sind die Lese- und Schreibzugriffe der Speicherkarten nicht besonders flott, was sich vor allem beim Scrollen in großen Fotosammlungen durch verzögert angezeigte Vorschaubilder bemerkbar macht.

Eine Alternative ist es, die Fotos auf eine an den Raspi angeschlossene externe USB-Festplatte auszulagern. Das bringt aber eine kleine Hürde: Mechanische Platten mögen es nicht so gerne, wenn ihre Scheiben rund um die Uhr ununterbrochen kreiseln. Um die Lebensdauer zu erhöhen, fahren die meisten USB-Platten nach 15 oder 30 Minuten ins Standby. Greift man dann in der App oder im Browser auf die Bildersammlung zu, geht es erst richtig los, wenn die Platte wieder hochgefahren ist. Für diesen Artikel haben wir deshalb eine handliche USB-SSD mit einem Terabyte Speicher besorgt (Portable SSD T7 von Samsung) und Immich und Raspberry OS wie üblich auf einer SD-Karte installiert. Die Fotos hingegen liegen in Ordnern auf der USB-SSD. Alternativ installiert man Raspberry OS, Docker und Immich direkt auf der SSD und spart sich die SD-Karte.

Im Trockendock

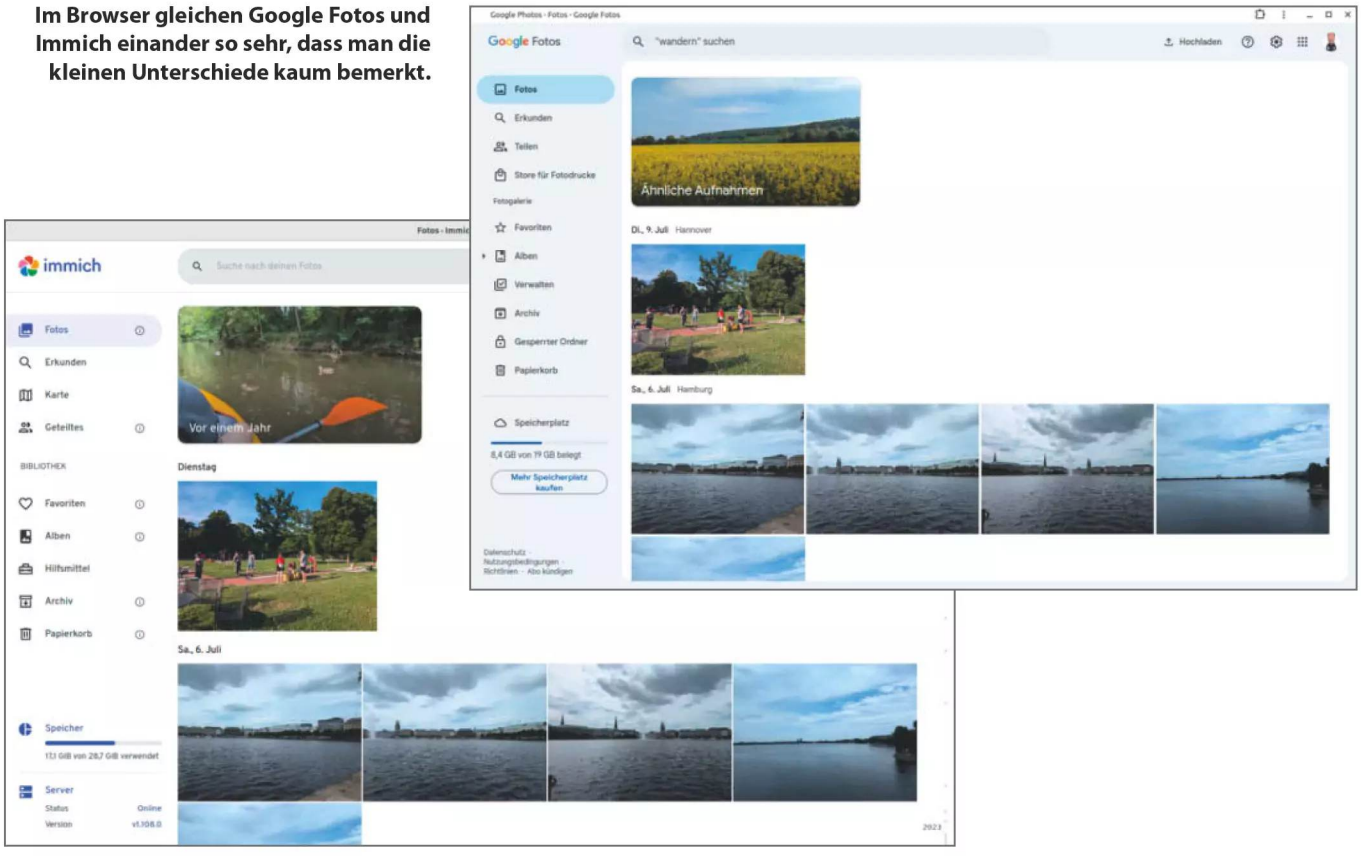
Der einfachste Weg, Immich mit all seinen Komponenten zu installieren, führt über Docker. Zunächst installiert man das aktuelle Raspberry Pi OS mithilfe des Raspberry Imagers auf der SD-Karte. Nach dem Hochfahren des Systems werden dort Docker und dessen grafische Oberfläche Portainer anhand der Befehlssammlung installiert, die wir unter ct.de/wr2p verlinkt haben.

Schließen Sie nach der Installation die Festplatte an und überprüfen Sie auf der Kommandozeile via SSH mit dem Befehl `df -h`, unter welchem Pfad die Platte automatisch gemountet wurde. In unserem Fall wurde sie als /dev/sda1 erkannt und unter „/media/Benutzer/Name der Platte“ eingehängt. Wechseln Sie mit `cd` in das Hauptverzeichnis der Platte und legen Sie mit `mkdir` einen Ordner namens „immich“ und darin einen Ordner „intern“ an.

Danach ruft man im Browser Portainer die IP-Adresse des Raspi unter Port 9443 auf, also beispielsweise über https://192.168.178.105:9443. Beim ersten Öffnen spuckt der Browser eine Sicherheitswarnung wegen des selbst signierten SSL-Zertifikats aus, die man aber ignorieren und zukünftige Warnungen ausschalten kann.

In Portainer wechselt man anschließend unter „Home“ und „Local“ in den Bereich „Stacks“. Dort

Im Browser gleichen Google Fotos und Immich einander so sehr, dass man die kleinen Unterschiede kaum bemerkt.



lassen sich mehrere Docker-Container in einem Rutsch installieren und einrichten. Dafür lädt man zunächst aus dem GitHub-Repository von Immich die Dateien docker-compose.yml und example.env herunter (siehe ct.de/wr2p).

In Portainer klicken Sie nun im Bereich Stacks auf die Schaltfläche „Add Stack“, tragen unter „Name“ einfach „immich“ ein und klicken in der nun geöffneten Ansicht auf „Web Editor“, falls die Option nicht vorausgewählt ist. In das Textfeld darunter wird nun der Inhalt der Docker-Compose-Datei eingefügt. Im Text finden Sie unter den Einträgen `env_file` den Verweis auf die Datei mit den Umgebungsvariablen des Stacks. Der Dateiname muss dort von „.env“ auf „stack.env“ geändert werden.

Danach scrollen Sie etwas herunter, klicken unterhalb von „Environment Variables“ auf „Advanced Mode“ und fügen darunter im Textfeld den Inhalt der heruntergeladenen Datei example.env. Ändern Sie bei der Gelegenheit im Eintrag `DB_PASSWORD` auch gleich das Passwort für die Datenbank in ein beliebiges, sicheres Passwort. Zudem geben Sie in einem Eintrag `UPLOAD_LOCATION` den Pfad zum vorab auf der USB-Platte angelegten Ordner „intern“ an. Mit einem Klick auf „Deploy the stack“ am unteren Ende der Seite richtet Portainer alle Container mit den benötigten Serverkomponenten ein.

Alles automatisch

Nach der Installation ruft man Immich im Browser unter der IP-Adresse des Raspi und angehängter Portnummer 2283 auf – also etwa nach dem Schema http://192.168.178.105:2283. Dort begrüßt die Fotoverwaltung einen mit einem simplen Einrichtungsdialog, bei dem man einen Hauptnutzer anlegt und danach auf die Hauptseite geleitet wird, auf der zunächst noch gähnende Leere herrscht.

Doch bevor man erste Fotos in die Galerie schaufelt, gilt es noch ein paar Vorarbeiten zu erledigen: Dafür wechselt man oben auf Verwaltung und danach in der Menüleiste am linken Rand auf Einstellungen. Da ein Raspi wahrlich kein Hochleistungscomputer ist, bietet es sich an, unter Job-Einstellungen die parallelen Ausführungen einiger Bilderkennungsalgorithmen anzupassen.

Gute Erfahrungen haben wir damit gemacht, die Generierung der Vorschaubilder auf zwei parallele Prozesse zu beschränken und die intelligente Suche, die Gesichtserkennung und die Gesichtszuordnung sowie das Transkodieren von Videos auf einen Prozess. Kippt man in einem Rutsch ein paar hundert Fotos in Immich, ist die KI-Bilderkennung so oder so einige Stunden mit der Analyse beschäftigt. Mit herabgesetzten parallelen Jobs war er währenddessen wenigstens noch einigermaßen flott, wenn wir per App oder im Browser derweil in den schon vorhandenen Fotos stöberten. Die CPU erwärmte sich bei der Klassifizierung großer Mengen neuer Fotos auf etwas mehr als 70 Grad, weshalb gute Kühlkörper und ein Gehäuse, das Wärme effektiv abführt, ein Muss sind. Im späteren Betrieb, wenn nur dann und wann ein neues Foto hochgeladen wird, dümpelt der Raspi bei rund 40 Grad herum.

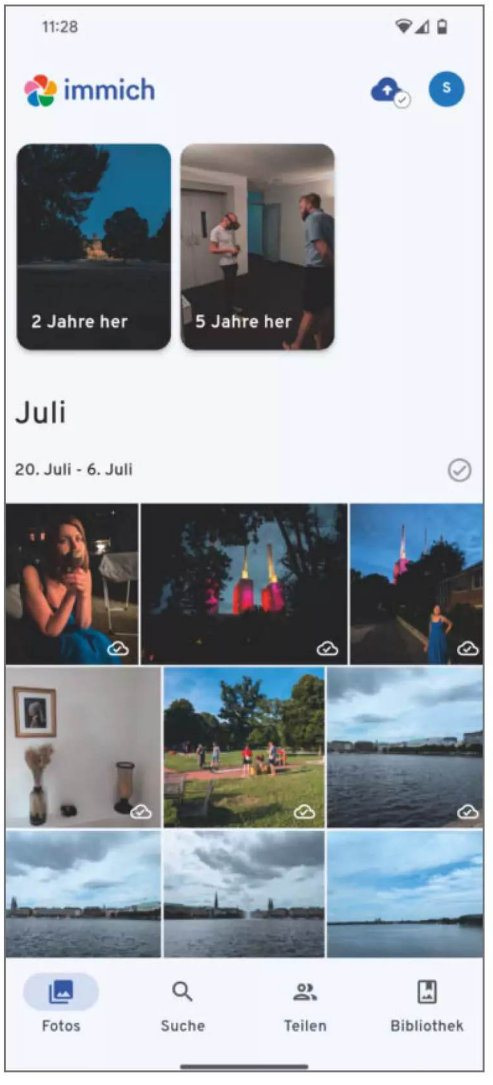
Danach wechseln Sie in den Bereich „Einstellungen für maschinelles Lernen“ und wählen unter „CLIP-Modell“ (Contrastive Language-Image Pre-Training) das Modell „ViT-SO400M-14-SigLIP2-378__webli“, das zum einen eine gute Bilderkennung bietet und zum anderen die Suche auf Deutsch ermöglicht.

Nach der Einrichtung installiert man die Immich-App auf dem Smartphone und meldet sich mit dem vorab festgelegten Benutzernamen und Passwort an. Die App beginnt daraufhin, alle Fotos aus dem Kamera-Ordner automatisch in die eigene Cloud – also auf den Raspi – hochzuladen. In den Einstellungen der App lassen sich auch weitere Ordner für den automatischen Upload auswählen und festlegen, dass etwa nur dann hochgeladen wird, wenn das Smartphone mit einem WLAN verbunden ist oder wenn es am Ladegerät hängt. Anhand des Icons unten rechts in den Thumbnails ist zu erkennen, welche Fotos lokal auf dem Smartphone liegen und welche schon hochgeladen wurden.

Archiv per USB übernehmen

Neben der automatischen Sicherung vom Smartphone erlaubt Immich, im Browser Bilder manuell hochzuladen, entweder per Drag & Drop oder über eine Dateiauswahl. Der Upload im Browser ist jedoch relativ langsam, da alle Fotos und Videos übers (W)LAN auf den Raspi geschaufelt werden. Deutlich schneller geht es, die gesammelte Sammlung aller Fotos der vergangenen Jahre in Immich zu integrieren, wenn man die USB-Platte kurz an den PC hängt und alle Fotos direkt aufs Laufwerk kopiert. Anders als beim Upload der Fotos dauert das Kopieren dann keine Stunden, sondern nur wenige Minuten.

Damit das klappt, fährt man den Raspi herunter, zieht die Platte ab und legt am PC im Immich-Ordner neben dem Verzeichnis „intern“ einen neuen Ordner an, nennt ihn beispielsweise „extern“ und kopiert alle gewünschten Fotos hinein. Danach steckt man die Platte wieder um und fährt den Raspi hoch. Nun muss der neue Ordner dem Docker-Container von Immich zugeordnet werden. Öffnen Sie dafür Portainer analog dazu wie bei der Ersteinrichtung und



Am Smartphone zeigt Immich einen Zeitstrahl aller Fotos und informiert, welche Bilder lokal, in der Cloud und an beiden Orten gespeichert sind.

legen Sie unter „Environment Variables“ einen neuen Eintrag namens `EXT_LOCATION` an und geben als Wert den Pfad zum neu angelegten Ordner „extern“ an. Anschließend scrollen Sie herunter und klicken auf die Schaltfläche „Update the Stack“.

Danach wechselt man im Browser zu Immich und dort über die Verwaltung zu „Externe Bibliotheken“ und erstellt eine neue externe Bibliothek. In deren Optionen, die man über die Schaltfläche mit den drei Punkten öffnet, lässt sich unter „Importpfade bearbeiten“ und „Pfad hinzufügen“ der externe Ordner auswählen, und zwar über seinen Docker-internen Pfad „/usr/src/app/external“. Nach dem Hinzufügen brauchen Sie über das Optionsmenü nur noch den Scan nach neuen Bibliotheksdateien anzustoßen. Je nach Anzahl der Bilder wird Immich danach mehrere Stunden mit dem Katalogisieren beschäftigt sein.

Nach erfolgreichem Scan sind die manuell hochgeladenen Fotos der externen Bibliothek nahtlos in die Galerie eingebunden und lassen sich genauso per Volltextsuche durchsuchen und nach Orten oder Personen filtern wie die zukünftig automatisch vom Smartphone hochgeladenen Bilder.

Fazit und Ausblick

Die Entwickler von Immich beschreiben ihr noch junges Projekt als in besonders aktiver Entwicklung, weshalb man sich stets auf Fehler und größere Funktionsänderungen einstellen sollte. Das Projekt versteht sich eher als ein Tool zur Fotoanzeige statt als eine Backup-Lösung. In unserem Test lief Immich mit einer Sammlung von rund zehntausend Bildern grundsätzlich stabil, doch auch weil Immich die Dateien umbenennt und in eine datenbankoptimierte Ordnerstruktur einsortiert, empfiehlt es sich trotzdem, regelmäßige Backups seiner Schnappschüsse anzulegen. Besonders fix geht das, wenn man im Browser mit einem Häkchen den Monat auswählt und alle Originale in einem Archiv herunterlädt.

Kleine Fehler, die uns auffielen, waren unter anderem, dass die Smartphone-App beim Scrollen durch die Zeitleiste ruckelte und die App in seltenen Fällen den automatischen Foto-Upload nicht im Hintergrund ausführte, sondern erst, nachdem wir die App manuell geöffnet hatten – was auch am Stromsparverhalten des Smartphones liegen kann. Die KI-Suchfunktion überzeugte schon in ihrem frühen Stadium, bislang dauert eine Suche auf dem Raspi aber rund fünf Sekunden und Immich scheint in der Ergebnisliste noch keinen Schwellenwert für die Wahrscheinlichkeiten zu haben: Während die ersten Treffer einer Volltextsuche überraschend gut den gesuchten Bildinhalt liefern, werden die Ergebnisse gegen Ende der Trefferliste ziemlich erratisch. Andere Apps begrenzen die Ergebnisliste. Abgesehen von diesen Kleinigkeiten funktioniert Immich bereits jetzt sehr gut und bietet sinnvolle Funktionen. (spo) **c't**

Downloads, Dokumentationen und Befehlslisten
ct.de/wr2p

IMPRESSUM

Redaktion

Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.heise.de

Leserbriefe und Fragen zum Heft:
sonderhefte@ct.de

Die E-Mail-Adressen der Redakteure haben die Form xx@heise.de oder xxx@heise.de. Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

Chefredakteur: Torsten Beeck (tbe, verantwortlich für den Textteil), Dr. Volker Zota (vza)

Konzeption: Wilhelm Drehling (wid), Peter Siering (ps), Sylvester Tremmel (syt)

Koordination: Jobst Kehrhahn (keh, Leitung), Pia Groß (piae)

Redaktion: Holger Bleich (hob), Niklas Dierking (ndi), Ronald Eikenberg (rei), Keywan Tonekaboni (ktn), Jan Mahn (jam), Stefan Porteck (spo), Peter Siering (ps), Sylvester Tremmel (syt), Christian Wölbert (cwo)

Mitarbeiter dieser Ausgabe: Falk Steiner, Daniel Szöke, Daniel Ziegener

Assistenz: Susanne Cölle (suc), Tim Rittmeier (tir), Martin Triadan (mat)

DTP-Produktion: Vanessa Bahr, Dörte Bluhm, Lara Bögner, Beatrix Dedek, Madlen Grunert, Laura-Sophie Gruhn, Cathrin Kapell, Steffi Martens, Marei Stade, Matthias Timm, Christiane Tümmler, Nicole Wesche

Digitale Produktion: Christine Kreye (Leitung), Thomas Kaltschmidt, Martin Kreft, Pascal Wissner

Illustration, Fotografie: Thorsten Hübner, Albert Hulm, Moritz Reichart

Titel: Steffi Martens, www.freepik.com

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Beate Gerold

Mitglieder der Geschäftsleitung: Jörg Mühle, Falko Ossmann

Anzeigenleitung: Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

Leiter Vertrieb und Marketing: André Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3–11, 86650 Wemding

Vertrieb Einzelverkauf:
DMV DER MEDIENVERTRIEB GmbH & Co. KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1815
E-Mail: info@dermedienvertrieb.de
Internet: dermedienvertrieb.de

Einzelpreis: € 14,90; Schweiz CHF 27.90;
Österreich € 16,40; Luxemburg € 17,10

Erstverkaufstag: 15.09.2025

Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

INSERENTENVERZEICHNIS

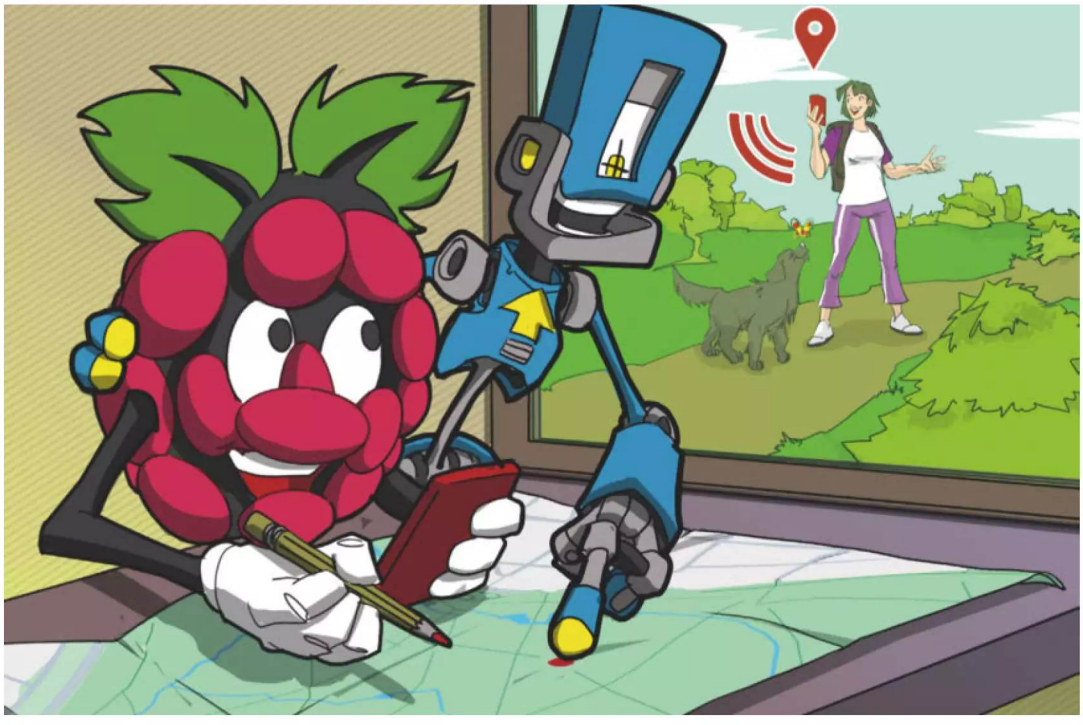


Bild: Thorsten Hübner

Auf Schritt und Tritt: Dawarich

Mit einer Open-Source-Software speichert man einen persönlichen Standortverlauf auf einem eigenen Server. So bleiben die Daten privat und unter Kontrolle.

Von **Stefan Porteck**

Wer den Standortverlauf von Google Maps benutzt, muss sich damit auseinandersetzen, dass der Dienst derzeit aus der Cloud aufs Smartphone wandert. Google begründet die Umstellung mit besserem Datenschutz, da die Standortdaten nicht mehr auf den Servern des Suchmaschinenbetreibers gespeichert werden, sondern auf dem Gerät des Nutzers. Das ist zwar löblich, hat aber auch Nachteile: So kann man nicht mehr im Desktopbrowser auf den Verlauf zugreifen, sondern nur noch auf dem kleinen Handy-Screen.

Googles Umstellung schafft deshalb einen Anlass, die alten Zöpfe ganz abzuschneiden und die Daten selbst zu erheben und auszuwerten. So hat man nicht nur volle Kontrolle, sondern behält auch die komfortable Ansicht im Browser.

Mittlerweile gibt es eine weitere spannende Alternative zum Standortverlauf von Google Maps: Der in Berlin lebende Programmierer Evgenii Burmakin entwickelt seit Juni 2024 die Zeitachse Dawarich. Der etwas sonderbare Name ist offenbar inspiriert von der Fotogalerie Immich (siehe S. 126) und beschreibt einfach die Funktion: Da war ich.

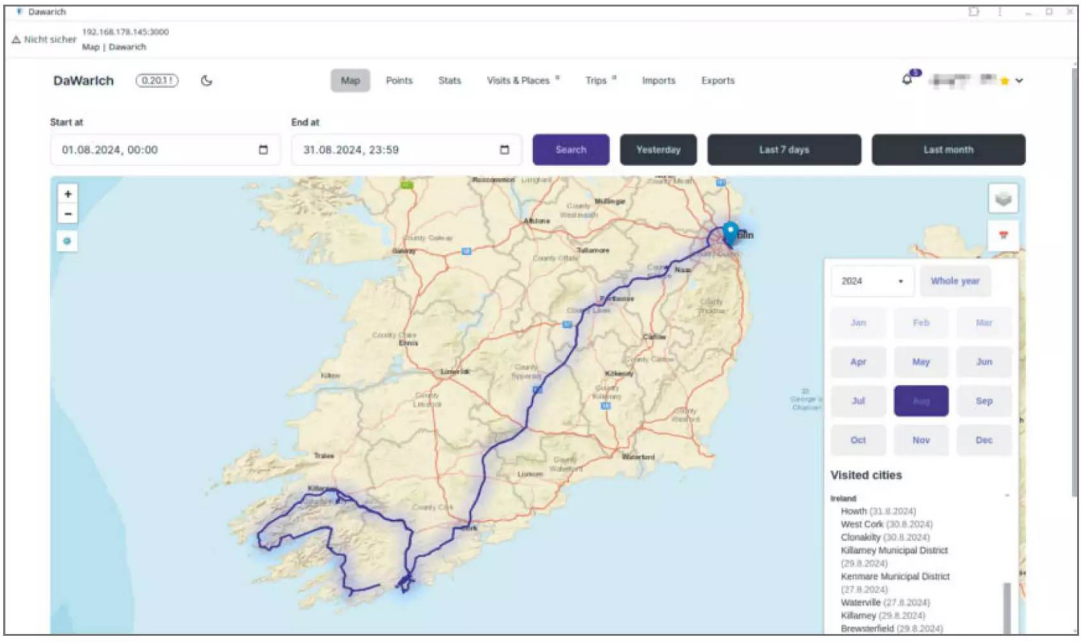
Trotz mehrerer Programmkomponenten ist Dawarich dank Docker in weniger als 15 Minuten aufgesetzt und bietet jetzt schon einen Funktionsumfang, der dem von Googles Standortverlauf recht nahekommt. So verfügt die Anwendung über ein Reverse-Geocoding, das GPS-Koordinaten automatisch in Ortsnamen auflöst. Damit ist es Dawarich möglich, spannende Statistiken anzuzeigen.

Dazu präsentiert Dawarich neben einer Kartenansicht auch ein Balkendiagramm, das die zurückgelegte Strecke nach Monaten sortiert, und nennt unter anderem die besuchten Städte und Länder. Bis vor kurzem nutzte Dawarich für die Auflösung der GPS-Koordinaten in Geodaten den Demo-Server photon.komoot.io. Wegen der vielen Abfragen ist der Zugang mittlerweile begrenzt. Wer Dawarich dauerhaft nutzen und sogar den bestehenden Verlauf von Google dorthin portieren will, der sollte entweder einen eigenen Photon-Server aufsetzen oder Dawarich auf Patreon unterstützen, um Zugang zu einem unlimitierten Reverse-Geocoding-Dienst zu erhalten. Für bis zu 3.000 Geopunkte pro Tag reicht alternativ auch ein kostenloser Account bei geoapify.com.

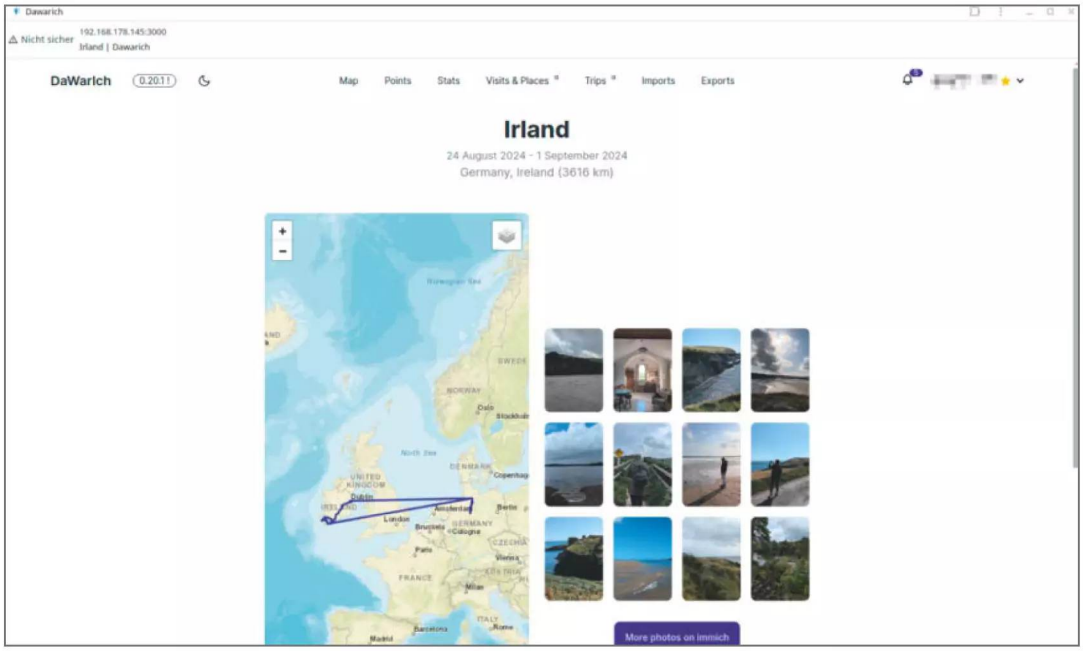
Datenhalde

Für unseren Test haben wir Dawarich auf einem Raspberry Pi 5 installiert. Die Installation ist in wenigen Minuten erledigt. Zunächst schreibt man mit dem Raspberry-Pi-Imager das Betriebssystem auf eine SD-Karte und installiert anschließend die Container-Umgebung Docker. Für eine etwas komfortablere Administration empfiehlt es sich zusätzlich, die grafische Oberfläche Portainer zu installieren. Die nötigen Schritte haben wir in einer Videoanleitung zusammengefasst (siehe ct.de/wywr).

Nach der Installation von Docker lädt man von der Dawarich-Projektseite bei GitHub dessen Installationsdatei docker-compose.yml herunter, sucht darin alle Einträge namens `POSTGRES_PASSWORD` und ändert dahinter das Passwort in ein sicheres eigenes. Zudem muss bei der Installation auf einem Raspi der Eintrag `image: postgis/postgis:17-3.5-alpine` in `image: imresamu/postgis:17-3.5-alpine` geän-



In der Kartenansicht von Dawarich lassen sich Verläufe beliebiger Zeiträume einblenden.



Dank der Integration der Fotogalerie Immich landen auch Fotos des Nutzers auf der Karte und in der Reiseansicht.

dert werden. Wer einen Heimserver mit x86-Prozessor betreibt, kann den Eintrag in der Compose-Datei belassen.

Wer ein Reverse-Geocoding wünscht, dass die Koordinaten in Ortsnamen auflöst und den Dawarich-Entwicker auf Patreon unterstützt, trägt zudem in den Bereichen `dawarich_app:` und `dawarich_sidekiq:` jeweils unter environment: die Einträge `PHOTON_API_HOST: photon.dawarich.app` und `PHOTON_API_KEY: EIGENER-API-KEY` ein. Für Nutzer von Geoapify unterscheiden sich die Einträge leicht, eine Anleitung für dessen Einbindung findet sich auf der Dawarich-Webseite.

Danach kopiert man die Docker-Compose-Datei ins Home-Verzeichnis auf dem Raspberry Pi, öffnet dort eine Kommandozeile und gibt den Befehl `docker compose up -d` ein. Docker lädt dann gemäß der Installationsbeschreibung aus der YML-Datei alle nötigen Komponenten herunter und richtet sie automatisch ein.

Wer sich für die grafische Einrichtung entschieden hat, ruft stattdessen Portainer über https://<IP-des-raspi>:9443 auf und klickt nach dem Anmelden auf der Startseite auf die Kachel namens „local“, dann in der Menüauswahl links auf „Stacks“ und abschließend oben rechts auf den Button „+Add Stack“. Stacks sind unter Portainer das Pendant zu Docker Compose – quasi ein Bündel von Containern, zu einem funktionierenden Gesamtsystem zusammengefasst.

Im nun geöffneten Fenster benennen Sie den Stack in Kleinbuchstaben in „dawarich“ und fügen in das Textfeld unter „Web editor“ den Inhalt der docker-compose.yml ein. Anschließend muss nur noch am unteren Ende der Seite auf „Deploy the Stack“ geklickt werden, worauf Portainer beziehungsweise Docker alles passend einrichtet. Danach können Sie den Stack anklicken und sehen eine Übersicht der vier Container, die Dawarich nutzt. Der Clou: Für jeden Container zeigt Portainer Schaltflächen an, etwa um die Log-Dateien des jeweiligen Containers anzuzeigen oder seine Kommandozeile zu öffnen. Das ist vor allem für Backups oder eine Fehlersuche hilfreich.

Derzeit wird Dawarich sehr aktiv entwickelt und es erscheinen mehrere Updates pro Woche. Die spielt man ein, indem man in der Stack-Ansicht auf „Editor“ klickt und einfach den Inhalt der neuen docker-compose.yml einfügt. Zuvor müssen in der neuen Datei jedoch individuelle Anpassungen wie etwa ein eigenes Datenbankpasswort wieder eingepflegt werden.

Unabhängig vom Installationsweg lässt Dawarich sich nach wenigen Minuten im Webbrowser unter http://<IP-des-Raspi>:3000 öffnen. Der Benutzername ist zunächst „demo@dawarich.app“ und das Passwort lautet „password“. Beides sollte man direkt nach dem Login ändern. Möchte man seine Fotos mit dem Standortverlauf verknüpfen, führt der nächste Schritt in die Einstellungen. Dort gibt man unter „Integrations“ die URL und den API-Key seiner Immich-Instanz an – sofern man eine betreibt. Das erlaubt es Dawarich, die Fotos einer Reise in der Trip-Ansicht einzubinden und auf Wunsch generell Thumbnails aller Fotos in der Kartenansicht anzuzeigen.

Protokollant

Während der Server flott installiert ist und wenig Konfiguration braucht, ist auf dem Smartphone einmalig etwas mehr Handarbeit nötig. Es muss schließlich die Geodaten erheben, speichern und an den Server schicken. Als Datenspender unterstützt Dawarich nativ die Clients Overland und OwnTracks.

Wer sich Feintuning wünscht oder die eigenen Standorte ganz ohne Dawarich-Instanz aufzeichnen möchte, greift zur Open-Source-App GPSLogger (siehe ct.de/wywr). Dank ihrer Flexibilität kann auch sie Datensätze an Dawarich schicken und erlaubt verschiedene Profile mit unterschiedlichen Einstellungen. Beispielsweise eins, wenn man draußen unterwegs ist, und eins für zu Hause oder den Arbeitsplatz. So erreicht GPSLogger einen sehr guten Kompromiss zwischen genauen Standortverläufen und einem akzeptablen Energieverbrauch – dazu später mehr.

Wer den Aufwand gering halten will, der kommt fürs Erste mit einem Einstellungsprofil aus, weshalb wir im Folgenden zunächst die grundsätzliche Einrichtung beschreiben: Installieren Sie zunächst GPSLogger aus dem F-Droid-Store. Über das Hamburger-Menü rufen Sie die „Allgemeinen Einstellungen“ auf und setzen den obersten Schalter, damit die App beim Start des Handys mit dem Logging beginnt. Danach legen Sie in den „Aufzeichnungsinformationen“ fest, dass die App in eine GPX- und eine CSV-Datei speichert, und geben weiter unten den Speicherort an. Der sollte auf der SD-Karte oder im allgemeinen Speicher liegen, damit sich die Rohdaten leicht auf den PC sichern lassen.

Unter „Leistung“ wählt man, dass GPS/GNSS- und Netzwerkstandorte protokolliert werden. Die Aufzeichnung von anderen Apps erhobener Standorte (Passive Standorte aufzeichnen) sollten Sie ausschalten. Bei uns führte das dazu, dass bei der Navigation mit Maps oder Waze jede Sekunde ein Datensatz anfiel, was große Datenmengen erzeugte und pro Stunde etwa zehn Prozentpunkte der Akkukapazität kostete.

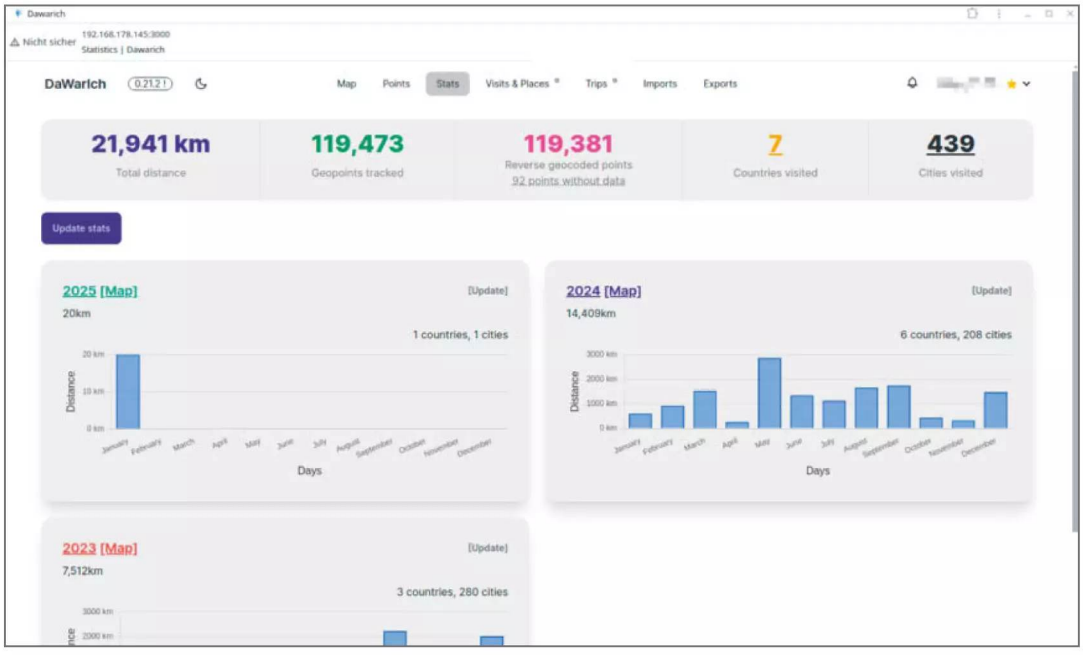
Passable Werte für das Aufzeichnungsintervall, die Entfernung zwischen den Messpunkten und die Genauigkeit, ab der aufgezeichnet werden soll, sind 90 Sekunden sowie jeweils 20 bis 30 Meter. Die Zeitspanne, bis die Genauigkeit erreicht wurde, und die maximale Zeit bis zum GPS-Fix haben wir auf 60 beziehungsweise 90 Sekunden gesetzt.

Im letzten Schritt wählt man den Menüpunkt „Automatisches Senden“ und aktiviert die Funktion mit dem obersten Schalter. Im zweiten Menüpunkt lässt sich das Upload-Intervall festlegen. Werte zwischen zwei und sechs Stunden reichen völlig aus, sofern man keine Echtzeitüberwachung braucht. Mit diesen Einstellungen sammelt GPSLogger die Geo-Koordinaten zunächst in einer CSV-Datei und schreibt sie im gewünschten Intervall gesammelt in eine GPX-Datei, um sie in einem Rutsch zum Dawarich-Server zu schicken.

Das gebündelte Hochladen in festen Intervallen belastet den Akku des Smartphones viel weniger, als jede Geo-Koordinate in Echtzeit abzuschicken. Obwohl GPS den Ruf hat, kräftig am Akku zu saugen, fielen in unseren Tests die Uploads stärker ins Gewicht. Eine Standortbestimmung mit regelmäßigem Hochladen alle 90 Sekunden führte auf unserem Testhandy – einem Pixel 8 – dazu, dass GPSLogger am Ende des Tages mit rund 5 bis 10 Prozent in der Akkustatistik auftauchte. Stellten wir einen gebündelten Upload alle 120 Minuten ein, blieb GPSLogger in der Akkustatistik unter einem Prozent. Das änderte sich selbst dann nicht, als wir das Intervall der Standortbestimmung von 90 auf 60 Sekunden heruntersetzten. Ein seltenerer Upload erlaubt also eine genauere Wegstreckenaufzeichnung ohne gesteigerten Stromverbrauch.

Da es sich aus Datenschutz- und Sicherheitsgründen ohnehin nicht anbietet, den Dawarich-Server über einen Reverse-Proxy via Internet zugänglich zu machen, sollte man noch den Schalter „Nur über WLAN senden“ aktivieren. Falls die App in einem fremden WLAN den Upload versucht und Dawarich deshalb nicht erreicht, sind die Daten nicht verloren, sondern landen beim nächsten Upload im heimischen Netz am Ziel.

Die Adresse der eigenen Dawarich-Instanz trägt man unter „Benutzer URL“ im selben Menü ein: Aktivieren Sie den Schalter und im neuen Menü auch



Die Statistiken von Dawarich geben herunter bis auf Wochenebene interessante Einblicke ins persönliche Bewegungsprofil.

den für „Automatisches Senden erlauben". Unter URL fügen Sie nun die Adresse Ihrer Dawarich-Instanz ein, die Sie aus dessen Account-Einstellungen kopieren. Diese hat das Format: http://<IP-des-Raspi>:3000/api/v1/owntracks/points?api_key=EIGENER_API_KEY

Zwei Zeilen tiefer trägt man unter „HTTP-Text" folgende Parameter ein:

```
{
"_type": "location",
"t": "u",
"acc": "%ACC",
"alt": "%ALT",
"batt": "%BATT",
"bs": "%ISCHARGING",
"lat": "%LAT",
"lon": "%LON",
"tst": "%TIMESTAMP",
"vel": "%SPD"
}
```

Die HTTP-Kopfzeile bekommt den Wert `Content-Type: application/json` und als HTTP-Methode legen Sie `POST` fest. So gerüstet sendet GPSLogger die Daten fortan mit derselben Formatierung wie der OwnTracks-Client, sodass Dawarich sie problemlos verarbeiten kann. Fortan läuft GPSLogger im Hintergrund und nach einiger Zeit sehen Sie bereits die ersten Bewegungsverläufe im Dawarich-Frontend.

Feintuning

Zeichnet GPSLogger immer mit den obigen Einstellungen auf, geht man einen Kompromiss zwischen Genauigkeit und Stromverbrauch ein. Wer unterwegs viele Geopunkte für einen möglichst exakten Verlauf wünscht und zu Hause oder auf der Arbeit möglichst wenig Akkukapazität opfern will, der legt in GPSLogger für diese beiden Szenarien unterschiedliche Profile an.

Dafür öffnet man das Hamburger-Menü, tippt auf den Kreis neben dem Profilnamen und fügt ein neues Profil mit dem Namen „Unterwegs" hinzu. Es erbt die Einstellungen des Standardprofils, sodass man nur die Parameter für die Häufigkeit und Genauigkeit anzupassen braucht. Sinnvoll ist ein Aufzeichnungs-

intervall von 60 Sekunden. Alle übrigen Einstellungen können dem obigen Beispiel entsprechen. Auf die gleiche Art legt man nun ein Profil namens „Drinnen“ an und setzt dort das Aufzeichnungsintervall auf 1800 Sekunden – also 30 Minuten.

Durch den Wechsel zwischen einem intensiven und einem sparsamen Profil, lässt sich der Akkuverbrauch merklich senken. Der Nachteil: Man muss die Profile in der App von Hand umschalten und auch beim Losgehen und Heimkommen daran denken. Wer sich daran stört, der bastelt sich optional eine Automatisierung: Das geht besonders gut mit der Automatisierungs-App Tasker, die für 3,59 Euro im Play Store erhältlich ist.

Tasker löst nach dem Wenn-Dann-Prinzip eine gewünschte Aktion aus, sobald ein festgelegtes Ereignis eintritt. Über sogenannte Intents ist Tasker in der Lage, unterstützte Apps zu steuern. Für die Unterscheidung, ob man drinnen hockt oder unterwegs ist, bietet sich der WLAN-Zustand des Handys an. Für das automatische Wechseln der Profile von GPSLogger tippt man im Hauptfenster von Tasker auf das Pluszeichen am unteren Bildrand und legt so einen neuen Task an. Im folgenden Dialog wird der Auslöser abgefragt. Unter „Status“ und „Netzwerk“ wählt man nun „Wifi Verbunden“. In der nun geöffneten Maske wird nur das Häkchen bei „Umkehren“ gesetzt. Die Bedingung löst also aus, wenn das Handy nicht mit einem WLAN verbunden ist.

Direkt im Anschluss fragt Tasker nach der auszulösenden Aktion, also dem Task. Hier legt man einen neuen Task an und nennt ihn „Unterwegs“. In der nun geöffneten Ansicht tippt man auf das Pluszeichen und wählt „System“ und dort „Sende Intent“. Darauf öffnet sich eine Maske, in der man unter „Aktion“ den Wert `com.mendhak.gpslogger.TASKER_COMMAND` einträgt, unter „Paket“ den Wert `com.mendhak.gpslogger`, unter „Klasse“ den Wert `com.mendhak.gpslogger.TaskerReceiver`, unter „Ziel“ den Wert `Broadcast Receiver` und abschließend unter „Extra“ die Aufforderung, in das Profil „Unterwegs“ zu wechseln, in unserem Beispiel also den Wert `switchprofile:Unterwegs`.

Damit hat man Trigger und Task angelegt, sodass künftig in GPSLogger das Unterwegs-Profil aufgerufen wird, sobald das Handy nicht mehr mit einem WLAN verbunden ist. Allerdings fehlt noch die Umkehr ins stromsparende Profil. Tasker nutzt dafür „Exit-Tasks“. Sie werden ausgeführt, sobald die ursprüngliche Bedingung wegfällt. Um den passenden Exit-Task anzulegen, halten Sie den Finger auf den Task gedrückt und wählen im nun erscheinenden Kontextmenü die Option „Ausgang Task Zufügen“. Nun lässt sich ein neuer Task anlegen, der exakt dem obigen entspricht, mit dem Unterschied, dass unter „Extra“ nun `switchprofile:Drinnen` angegeben wird.

Sobald Sie den Task gespeichert haben, wird Tasker in Abhängigkeit einer WLAN-Verbindung zwischen den Logging-Profilen umschalten und GPSLogger somit entweder jede Minute oder jede halbe Stunde einen Geopunkt aufzeichnen.

Meins bleibt meins

Damit der Umstieg auf Dawarich keinen Neuanfang darstellt, bietet die Software mehrere Wege, Standortdaten zu importieren. Dateien in den standardisierten Formaten GPX und GeoJSON lassen sich im Web-Frontend auswählen und über einen Dateiauswahldialog zu Dawarich hinzufügen.

Nutzer, die sich von Google Maps abkehren, lässt Dawarich ebenfalls nicht im Stich: Sobald man die eigenen Daten mittels Google Takeout heruntergeladen hat, lassen sich die JSON-Dateien der sogenannten „Google Semantic History“ ebenfalls über das Frontend importieren. Das ist allerdings mit etwas mehr Aufwand verbunden, da Google diesen Verlauf nach Jahren und Monaten aufteilt und jede Datei einzeln importiert werden muss.

Einzig die Datei Records.json eines Google Takeout enthält alle Daten. Sie ist aufgrund der Metadaten aber so groß, dass man sie auf Datenbankebene importieren muss, was auf der Dawarich-Webseite ausführlich beschrieben wird. Doch selbst dann zieht sich der Import eines mehrjährigen Standortverlaufs je nach Hardware über mehrere Stunden hin, und das Reverse-Geocoding kann sogar mehrere Tage in Anspruch nehmen.

Im GitHub-Forum von Dawarich finden sich mehrere Diskussionen zum Umgang mit mehreren GByte großen Archiven. Dort finden sich unter anderem Python-Skripte und andere Tipps, wie man große Archive in kleinere Häppchen aufteilt, sodass der Import in Dawarich gelingt.

Fazit

Googles Verschieben des Standortverlaufs aus der Cloud aufs Gerät bringt ein deutliches Plus an Datenschutz. Der Wechsel beraubt den Dienst aber auch einiger praktischer Features und macht das Sichern und Wiederherstellen der Daten komplizierter. Mit der Open-Source-Anwendung Dawarich betreibt man selbst einen Standortverlauf-Server. (spo) c't

Weitere Infos

ct.de/wywr

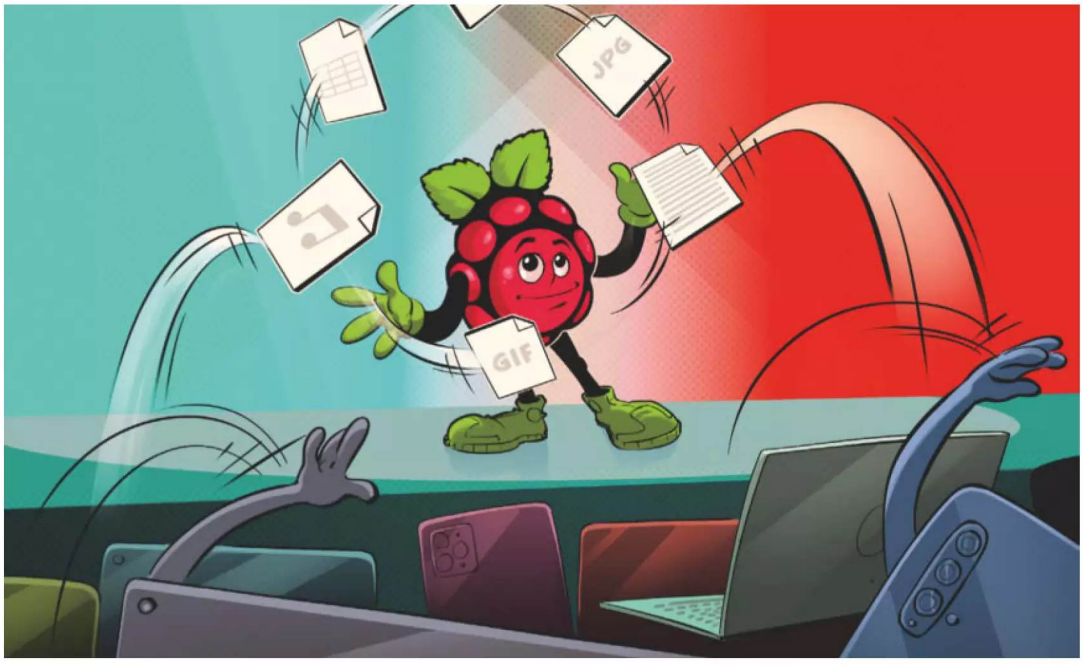


Bild: Albert Hulm

BASPi: Backup und Sync ohne Cloud

Unser BASPi synchronisiert Ihre Dateien auf all Ihren Geräten und kümmert sich auch noch um sichere Backups. Das klappt ohne Cloud und nach der Einrichtung völlig automatisch. Sie können dafür jeden alten Raspi oder Rechner nutzen – oder unseren Raspi-5-Bauvorschlag: Das Kästchen hat bis zu 8 TByte flotten SSD-Speicher.

Von **Ronald Eikenberg**

Wenn Sie mit Ihrem Smartphone ein Foto schießen, landet es wahrscheinlich ohne Ihr Zutun in der Cloud. Auch Dokumente, Videos und vieles mehr speichert man häufig in der Datenwolke, ohne groß darüber nachzudenken. So kann man nicht nur mit allen Geräten auf die Dateien zugreifen, sondern hat auch automatisch ein Backup.

Das geht so lange gut, bis der Account gesperrt oder gehackt wird. Denn dann sind alle Dateien futsch oder gar in fremden Händen – und der Schaden ist groß. Hinzu kommt, dass Webdienste hochgeladene Dateien fürs KI-Training einspannen könnten oder sich eventuell anderweitig Rechte daran einräumen. Kurzum: Alles in irgendwelche Clouds

zu schieben, ist zwar unglaublich praktisch, kann aber böse enden.

Doch Sie können diese Situation leicht ändern, ohne in die digitale Steinzeit zurückzufallen und Dateien von Hand kopieren zu müssen: Unser BASPi-Projekt (**B**ackup **A**nd **S**ync **Pi**) bietet vergleichbaren Komfort, aber maximalen Datenschutz. Dafür müssen Sie auch nicht tief in die Tasche greifen, denn die nötige Hardware besitzen Sie wahrscheinlich schon. Sie können langfristig sogar noch etwas Geld sparen, wenn Sie teure XXL-Speicherabos für Clouddienste kündigen.

BASPi läuft grundsätzlich auf jedem Rechner, die verwendete Software gibt's für Linux, Windows und macOS. Sie könnten zum Beispiel einen ausrangierten PC oder einen alten Raspi aus der Rente holen und ihn als zentralen Backup- und Sync-Server verwenden. Im besten Fall ist das System leise und sparsam, da es im Dauerbetrieb läuft. Gut geeignet sind ausrangierte Thin Clients, die Sie beim Refurbished-Händler schon für unter 100 Euro bekommen. Diese Geräte sind kompakt und häufig erweiterbar, so können Sie bei manchen Modellen eine SSD oder größere Festplatte einbauen, die für dieses Projekt nützlich ist.

Wir haben uns für einen Raspberry Pi 5 entschieden, der inzwischen wieder zu moderaten Preisen verfügbar ist. Der Mini-Rechner bietet in der fünften Generation einen PCI-Express-Anschluss, an den man leicht flotte M.2-SSDs anschließen kann. Die fassen bis zu 8 TByte, sind in dieser Größe aber noch unverhältnismäßig teuer. Wir haben daher eine 2-TByte-SSD für 110 Euro bestellt. Weiterer Speicher ließe sich einfach per USB hinzufügen. Unser Projekt kommt mit wenig RAM aus. Wenn Sie exklusiv für diesen Zweck einen Raspi 5 samt SSD anschaffen möchten, reicht die Version mit 2 GByte RAM für rund 55 Euro völlig aus.

Klein, aber oho: In diesem kompakten Gehäuse steckt ein Raspi 5 mit einer flotten M.2-SSD, die bis zu 8 TByte fassen kann.

Wir fanden mit dem Argon NEO 5 M.2 NVME PCIE ein kompaktes und preiswertes Gehäuse, das für unser Projekt ideal ist: Es bringt eine aktive Kühlung mit und vor allem eine PCIe-Erweiterung für SSDs. Eine M.2-SSD (maximal 2280er Bauformat) findet unten im Gehäuse unter einer verschraubten Abdeckung Platz. Raspi und SSD stecken so in einem kleinen, gut durchlüfteten Schächtelchen, das neben dem Router kaum auffällt.

Das Argon-Gehäuse kostet je nach Anbieter ungefähr 45 Euro. Die Details, wie man Raspi und SSD in dieses spezifische Gehäuse installiert, ersparen wir Ihnen an dieser Stelle – wir sind schlicht nach der mitgelieferten Anleitung vorgegangen. Hilfreich beim Zusammenstecken und -schrauben waren auch Video-Anleitungen auf YouTube, die wir unter ct.de/w61j verlinkt haben.

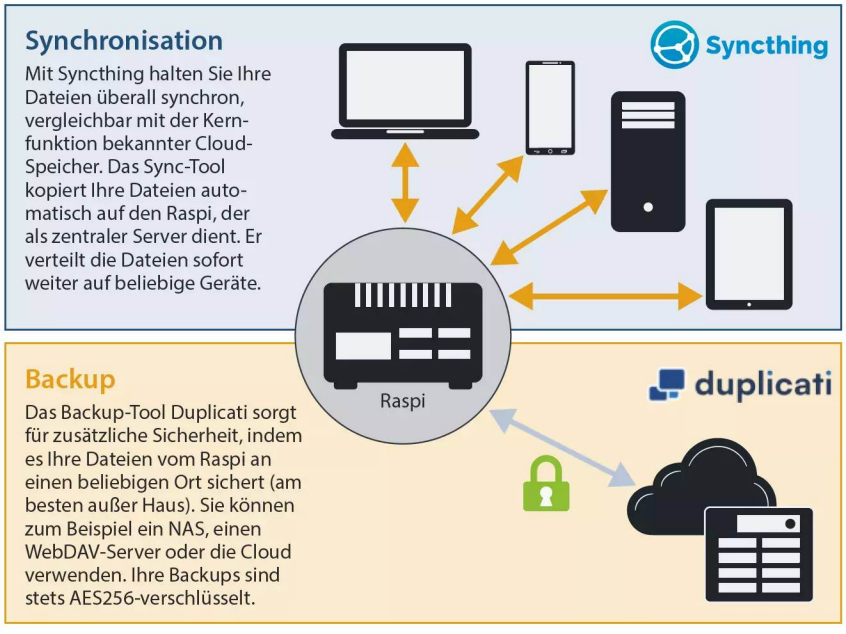
Andere Hersteller bieten ebenfalls geeignete Raspi-Gehäuse mit SSD-Anschluss feil, alternativ greifen Sie zu einem separaten PCIe-Erweiterungsboard. Einige davon haben wir in c't 19/2024 getestet [1]. Falls Sie den Raspi nicht nackt betreiben möchten, müssten Sie sich dann allerdings selbst nach einem passenden Gehäuse umschauen, in dem auch die PCIe-Erweiterung Platz findet. Oder Sie drucken sich eines mit einem 3D-Drucker.

Die Performance Ihrer Hardware ist bei diesem Projekt nicht entscheidend, da Sie normalerweise nicht in Echtzeit auf die gesicherten Dateien zugreifen. Die Daten werden automatisch im Hintergrund synchronisiert und das dauert so lange, wie es eben dauert. Wir haben das Projekt auch mit einem acht Jahre alten Raspi 3B aufgebaut, an den wir eine noch ältere USB2.0-Platte angeschlossen hatten. Das sieht nicht ganz so elegant aus, funktioniert aber auch. Wenn Sie eine größere microSD-Karte verwenden, reicht Ihnen deren Speicher eventuell schon aus, um die wichtigsten Dateien zu sichern; dann können Sie in dieser Konfiguration ebenfalls auf externe Datenspeicher verzichten.

Wenn Sie einen alten PC, Mac, Ihr Linux-NAS oder etwas ganz anderes als Backup- und Sync-Server

BASPi-Projekt: Raspi als Backup- und Sync-Server

Unser BASPi ist das Rundum-Sorglos-Paket für Ihre Daten: Er synchronisiert Ihre Dateien mit allen Geräten und kümmert sich um katastrophensichere Backups – automatisch, privat und sicher.



verwenden möchten, können Sie die Raspi-spezifischen Handgriffe in diesem Artikel einfach überspringen. Die eingesetzten Tools werden über eine Weboberfläche gesteuert, die man auf allen Plattformen gleich bedient.

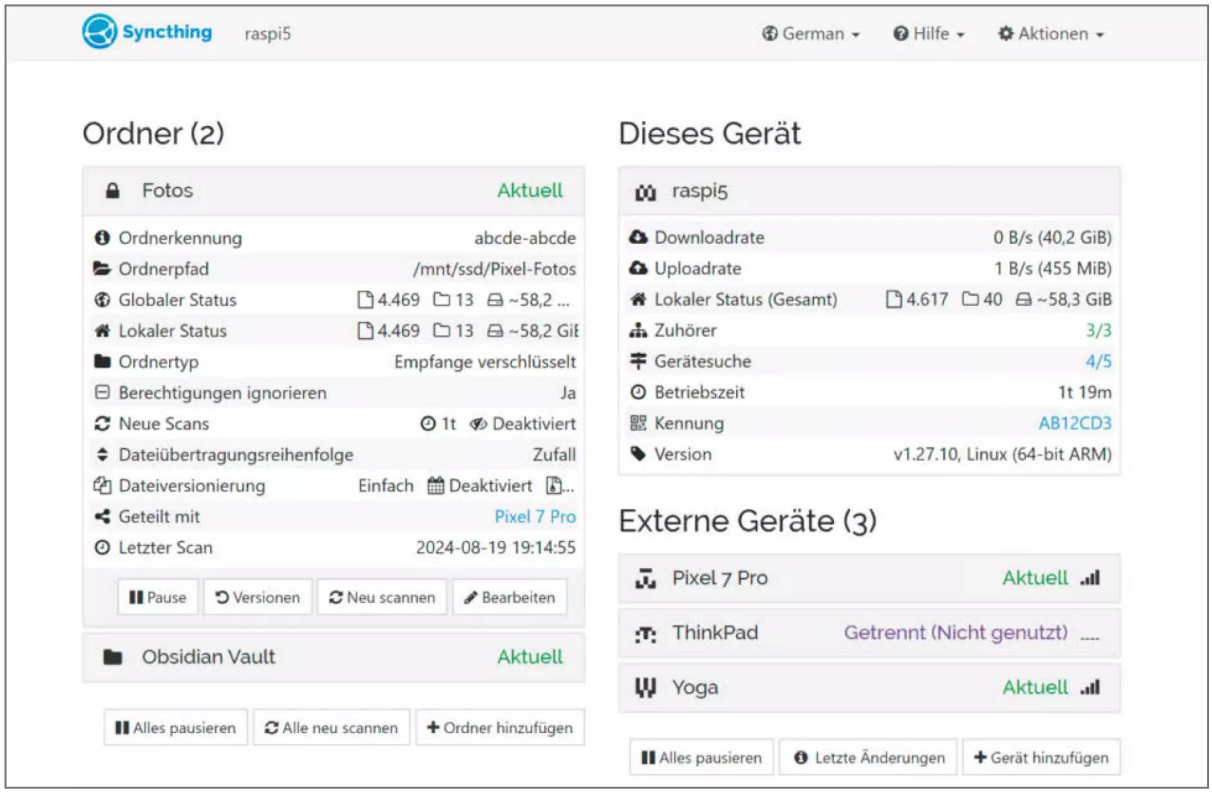
Sync ohne Cloud

Wenn man an Cloud-Alternativen denkt, kommt ganz schnell der Nextcloud-Server ins Spiel, der allerhand Dienste wie Speicher, Kalender und Web-Office bereitstellt. Doch Nextcloud ist eine komplexe Serveranwendung, die auch administriert und regelmäßig aktualisiert werden muss. Man schießt mit Kanonen auf Spatzen, wenn es nur um Dateien geht.

Das BASPi-Projekt funktioniert sehr viel einfacher: Auf dem BASPi-Rechner läuft unter anderem das Open-Source-Tool Syncthing, das Dateien zwischen Geräten synchronisiert. Es arbeitet nach dem Peer-to-Peer-Verfahren und der BASPi-Rechner dient als zentraler Sync-Peer, der immer erreichbar ist und alle Dateien vorhält.

Er verteilt die Dateien an beliebige andere Geräte weiter, ohne dass diese gleichzeitig aktiv sein müssen. Welche Dateien Sie synchronisieren, spielt dabei keine Rolle. Neben Fotos, Musik und Dokumenten könnten Sie zum Beispiel auch Ihren KeePass-Passworttresor oder Ihre Obsidian-Notizen auf allen Geräten synchron halten.

Syncthing ist super flexibel und läuft fast überall. Passende Sync-Apps gibt es für alle Desktopbetriebssysteme, Smartphones, Tablets, diverse NAS und vieles mehr – selbst FireTV-Stick oder Webserver lassen sich einbeziehen. Kurz gesagt: Wenn Sie auf einem Gerät Software ausführen können, ist die Wahrscheinlichkeit groß, dass es dafür auch Syncthing gibt.



Sie steuern Syncthing über eine moderne Weboberfläche.

Das Sync-Tool funktioniert nicht nur im lokalen Netz, sondern auch übers Internet – Sie können also unterwegs mit Ihrem Raspi daheim synchronisieren oder auch Dateien mit Freunden austauschen. Die Übertragung ist dabei stets verschlüsselt. Optional speichert Syncthing die Daten auf der Empfängerseite sogar verschlüsselt, sodass nur Sie diese wieder entschlüsseln können.

Auf diese Weise können Sie auch ein sicheres Sync-Ziel außer Haus betreiben, das Ihnen aus der Patsche hilft, wenn Ihre Hardware daheim nach einem Blitzschlag, Hochwasser oder ähnlichen Ereignissen das Zeitliche gesegnet hat. Wenn Sie auch einen Freund oder jemanden aus der Familie mit einem BASPi beglücken und jeder die verschlüsselten Backups des jeweils anderen speichert, helfen Sie sich gegenseitig.

Syncthing hat noch einen weiteren praktischen Trick auf Lager: Es bietet eine Dateiversionierung, die Sie gezielt für einzelne Ordner einschalten. Wenn Sie darin enthaltene Word-Dokumente am Rechner bearbeiten, bewahrt Ihr BASPi automatisch ältere Fassungen auf, die sich bei Bedarf wiederherstellen lassen, sollten Sie mit Ihren aktuellen Änderungen doch nicht zufrieden sein. Wie Sie all das einrichten, erfahren Sie gleich.

Am Ende dieses Artikels zeigen wir außerdem, wie Sie ergänzend zu Syncthing das Backup-Tool Duplicati auf dem Raspi installieren. Es ist darauf spezialisiert, Daten auf konventionelle Art zu sichern, also ohne P2P-Synchronisation. Sie wählen einfach die Ordner aus, die Sie sichern möchten und geben an, wo Duplicati die Backups speichern soll. Den Rest erledigt das Tool künftig automatisch.

Eine der Stärken von Duplicati ist, dass es etliche Speicherziele unterstützt: von der USB-Platte über Netzwerkfreigaben und NAS bis hin zur FTP- und WebDAV-Servern sowie diversen Cloud-Speicher-

diensten ist alles dabei. Duplicati kopiert Ihre Dateien nicht einfach ans gewünschte Ziel – es arbeitet inkrementell und verschlüsselt sie vorher mit AES256.

Deshalb können Sie die Sicherungen Ihrer wichtigen Dateien selbst in Cloud-Speichern oder in Ihrem Webspace ablegen. Ohne das zur Entschlüsselung nötige Passwort sind die Backup-Dateien nur kryptischer Datenmüll und für Dritte wertlos. Das Passwort sollte bei der Außer-Haus-Speicherung allerdings möglichst lang sein.

In Kombination sind Duplicati und Syncthing ein starkes Team: Syncthing schafft Ihre Dateien von allen Geräten automatisch auf Ihren zentralen Raspi und hält sie überall aktuell. Und Duplicati auf dem Raspi sichert Ihre Dateien von dort an beliebigen weiteren Orten, etwa verschlüsselt auf ein Speicherziel außer Haus. Getreu dem Motto: Better safe than sorry. Dabei können Sie genau einstellen, welche Daten Sie via Duplicati noch mal extra sichern möchten.

Auf los geht's los

Wie Sie Ihren Raspi an den Start bringen, haben wir ausführlich im Schnellstart-Artikel erklärt [3]. Wir empfehlen den Einsatz von Raspberry Pi OS Lite, um das System schlank zu halten. Es wird per SSH übers Netzwerk konfiguriert und ist optimal für den 24-Stunden-Betrieb.

Für die beste Performance verbinden Sie den Raspi per Netzwerkkabel mit Ihrem Router, eine WLAN-Verbindung ist aber auch schnell genug. Wie Sie nach der Raspi-Einrichtung Ihre SSD oder Ihren USB-Speicher einbinden, damit er unter einem festen Pfad wie `/mnt/daten` bereitsteht, erfahren Sie ebenfalls in dem Schnellstart-Artikel.

Syncthing auf dem Raspi installieren

Um Syncthing auf einem Rechner zu verwenden, ist es damit getan, eine ausführbare Datei zu starten. Auf einem Smartphone oder Tablet installieren Sie einfach eine App. Die Einrichtung als Dienst auf dem Raspi ist etwas aufwendiger, kostet Sie aber höchstens einen verregneten Nachmittag.

Sie sollten Syncthing über die Paketverwaltung apt installieren, um es später leicht damit aktualisieren zu können. Da das Tool nicht von den vorgegebenen Paketquellen angeboten wird, fügen Sie zunächst das Syncthing-Repository hinzu. Verbinden Sie sich über SSH mit dem Raspi und führen Sie die folgenden Befehle aus:

```
sudo curl -s -o /usr/share/keyrings/⤶
    ↳syncthing-archive-keyring.gpg ⤶
    ↳https://syncthing.net/release-key.gpg

echo "deb [signed-by=/usr/share/keyrings/⤶
    ↳syncthing-archive-keyring.gpg] ⤶
    ↳https://apt.syncthing.net/ syncthing ⤶
    ↳stable" | sudo ⤶
    ↳tee /etc/apt/sources.list.d/syncthing.list
```

Danach aktualisieren Sie die Paketquellen mit `sudo apt update` und installieren Syncthing schließlich mit `sudo apt install syncthing -y`

Ist das geschafft, aktivieren und starten Sie den Syncthing-Dienst wie folgt:

```
sudo systemctl enable syncthing@pi.service
sudo systemctl start syncthing@pi.service
```

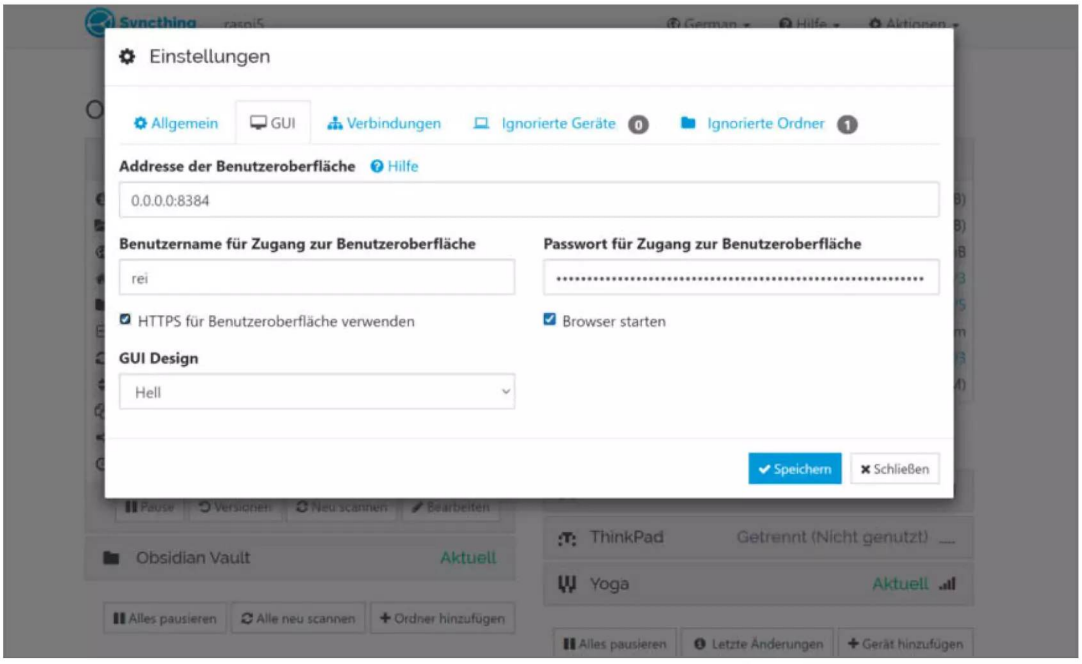
`pi` ersetzen Sie durch Ihren Benutzernamen, den Sie bei der Einrichtung über den Raspberry Pi Imager vorgegeben haben. Sie können ihn auch mit `whoami` ausgeben lassen.

Syncthing wird über ein Webinterface gesteuert, das standardmäßig nur lokal auf dem Raspi über sein loopback-Interface (http://127.0.0.1:8384) erreichbar ist. Damit Sie die Weboberfläche komfortabel von anderen Rechnern im lokalen Netz aus steuern können, ist eine Konfigurationsänderung nötig. Öffnen Sie die Syncthing-Konfiguration zunächst mit dem nano-Texteditor: `nano ~/.local/state/syncthing/config.xml`

Ändern Sie im `gui`-Abschnitt die IP-Adresse in der Zeile mit der loopback-Adresse von `127.0.0.1` zu `0.0.0.0`, damit die Weboberfläche auf allen Netzwerkinterfaces erreichbar ist. Den Port belassen Sie bei `8384`: `<address>0.0.0.0:8384</address>`

Abschließend speichern Sie die Datei mit Strg+O, Eingabetaste und beenden nano mit Strg+X. Danach starten Sie den Syncthing-Dienst neu, um die geänderte Konfiguration zu verwenden (ersetzen Sie `pi` wieder durch Ihren Benutzernamen): `sudo systemctl restart syncthing@pi.service`

Jetzt können Sie von Ihrem Rechner auf das Webinterface zugreifen. Im einfachsten Fall klappt es direkt mit http://raspi:8384, wobei „raspi" für den eingestellten Hostnamen steht, den Sie im Zweifel auch auf dem Raspi mit `hostname` ausgeben lassen können. Mitunter müssen Sie auch ein `.local` an den Host-



Auf Nummer sicher: Setzen Sie ein Passwort, um die Syncthing-Weboberfläche vor Zugriffen durch andere Nutzer im lokalen Netz zu schützen.

namen hängen, um den Raspi zu erreichen. Wenn auch das nicht gelingt, steuern Sie den Raspi einfach über seine IP-Adresse an, `hostname -I` zeigt sie an.

Konfiguration per Weboberfläche

Den größten Teil der Reise haben Sie damit geschafft. Syncthing fragt Sie beim ersten Besuch der Weboberfläche, ob Sie anonyme Nutzungsberichte teilen möchten, was Sie ablehnen können. Danach fordert Sie die Oberfläche auf, ein Konfigurationspasswort zu setzen. Das sollten Sie tun, insbesondere, wenn Sie in Ihrem lokalen Netz nicht allein sind. Hierzu wechseln Sie über „Aktionen“ (oben rechts) in die Einstellungen, klicken dort auf „GUI“ und geben einen Benutzernamen und ein Passwort vor. Anschließend rufen Sie das Webinterface erneut auf und loggen sich ein.

Wenn Sie auf Nummer sicher gehen und verhindern möchten, dass Ihre Zugriffe auf die Oberfläche im Klartext übertragen werden, können Sie auch HTTPS für das Webinterface einschalten. Standardmäßig nutzt Syncthing dann ein selbst generiertes Zertifikat, das Sie in den Zertifikatsspeicher Ihres Betriebssystems oder Browsers importieren müssen. Sonst erscheint bei jedem Zugriff auf die Weboberfläche ein Zertifikatsfehler.

Apps für alle Plattformen

Syncthing auf dem Raspi ist jetzt bereit, es fehlen noch Geräte, die damit Dateien synchronisieren. Das kann zum Beispiel Ihr Rechner sein, Ihr Smartphone oder Ihr Tablet. Für Desktop-Betriebssysteme empfehlen wir das Open-Source-Programm „Syncthing Tray“ (siehe ct.de/w61j). Das portable Tool läuft unter Windows, Linux und macOS. Es bringt Syncthing schon mit und bietet zudem ein übersichtliches GUI, über das Sie den aktuellen Status im Blick behalten.

Unter Android nehmen Sie am besten die App Syncthing-Fork (siehe ct.de/w61j), die zusätzliche Funktionen und Verbesserungen gegenüber der offiziellen App bietet. Für iOS und iPadOS gibt es die Drittanbieter-App Möbius Sync (siehe ct.de/w61j), die einzige kommerzielle App unter den hier aufgeführten. Sie kostet einmalig 6 Euro, bis zu 20 MByte kann

man jedoch auch kostenlos synchronisieren. Das reicht zumindest für die wichtigsten Dokumente.

Syncthing Tray für Windows & Co.

Um zum Beispiel Dateien von einem Windows-PC mit Ihrem Raspi abzugleichen, laden Sie das erwähnte „Syncthing Tray“ herunter und entpacken es an einem Ort, an dem Sie es dauerhaft behalten möchten. Da das Programm portabel ist, gibt es keine Installation. Das Tool klinkt sich in den Autostart ein und sollte daher nach der Einrichtung nicht mehr bewegt werden.

Starten Sie die ausführbare Datei syncthingtray-1.6.0-x86_64-w64-mingw32.exe (die Versionsnummer kann abweichen), woraufhin sich der Einrichtungsassistent meldet. Klicken Sie im ersten Schritt auf „Starte geführte Einrichtung“. Das Tool wird feststellen, dass Syncthing noch nicht auf Ihrem Rechner läuft, was Sie bestätigen.

Danach wählen Sie „Starte die in Syncthing Tray eingebaute Version von Syncthing“ und im nächsten Schritt „Starte Syncthing Tray beim Login“, damit es sich in den Autostart einklinkt. Bestätigen Sie Ihre Auswahl und damit sind Sie auch schon fast fertig. Das Tool versucht nun, unter Windows eine Firewall-Regel anzulegen, die Sie ebenfalls bestätigen, damit es ungehindert im lokalen Netz synchronisieren kann.

Syncthing Tray erscheint jetzt im Windows-Tray mit einem grün gefärbten Syncthing-Logo. Ein einfacher Klick darauf öffnet eine kompakte Übersicht über den Sync-Status. Da ist noch nichts los – aber das ändern Sie schnell: Klicken Sie in dem Mini-Fenster oben rechts auf das Syncthing-Logo (oder alternativ mit rechts auf das Tray-Symbol und „Syncthing öffnen“), um die Ihnen schon bekannte Weboberfläche von Syncthing im Browser zu öffnen, aber dieses Mal lokal auf dem Rechner.

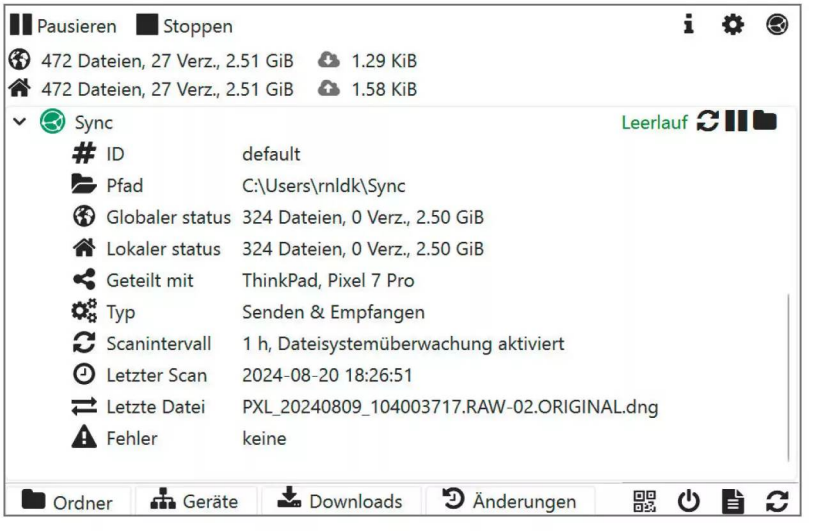
Das Setzen von Benutzername und Passwort für den Zugriff ist empfohlen, aber bei dem lokal ausgeführten Syncthing nicht ganz so wichtig, weil dessen Weboberfläche standardmäßig nicht übers Netzwerk erreichbar ist. Sie verhindern mit dem Passwort vor allem, dass andere Nutzer Ihres Rechners die Konfiguration ändern.

Geräte verkuppeln

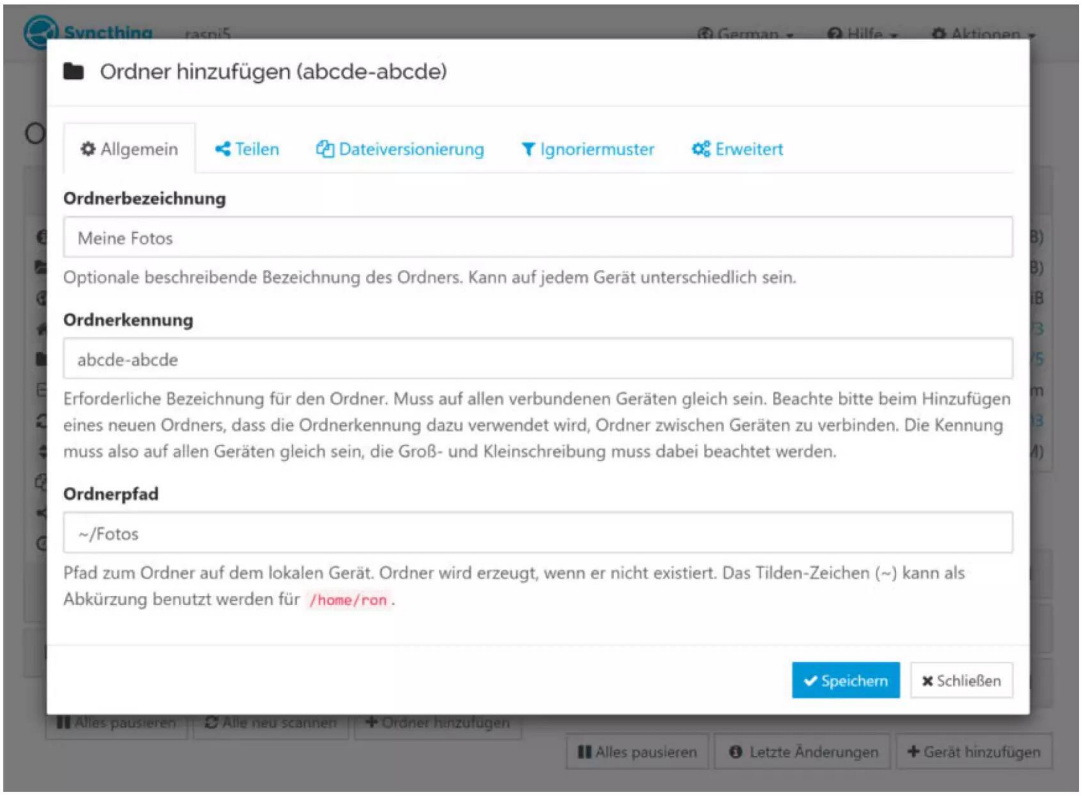
Zeit für die erste Synchronisation. Hierzu müssen beteiligte Geräte – in unserem Fall also Raspi und Windows-PC – die „Gerätekennung“ des jeweils anderen wissen. Hierbei handelt es sich um eine lange Zeichenfolge, die Syncthing zum sicheren Aufbau der verschlüsselten Verbindungen verwendet. Die Kennung eines Geräts können Sie unter „Aktionen/Eigene Kennung“ anzeigen lassen.

Um zwei Geräte, die Daten austauschen sollen, miteinander zu verkuppeln, klicken Sie bei einem der beiden unten rechts auf „+ Gerät hinzufügen“. Im besten Fall bietet Ihnen Syncthing die Kennung des potenziellen Partners schon zur Auswahl an, ansonsten müssen Sie diese von Hand eintippen. Die App Syncthing-Fork für Android scannt die Kennung auch per QR-Code ein. Darunter geben Sie bei „Gerätename“ noch eine sinnvolle Bezeichnung für das Gerät ein, das Sie hinzufügen, etwa „Windows-Notebook“ oder „Raspi“.

Kurz darauf sollte auf der Weboberfläche des Gegenübers ein deutlich sichtbarer Hinweis darauf erscheinen, dass sich jemand verbinden möchte. Hier klicken Sie einfach auf „+ Gerät hinzufügen“ und dann auf „Speichern“. Erscheint kein Hinweis, gehen Sie die eben beschrieben Schritte zum Hinzufügen noch mal auf diesem Gerät durch. Sind die beiden ordnungsgemäß verknüpft, taucht der jeweilige Partner anschließend auf der Übersichtsseite der Web-GUI unter „Externe Geräte“ auf, hier können Sie auch jederzeit den Verbindungsstatus überprüfen.



Mit „Syncthing Tray“ synchronisieren Sie Ihre Dateien im Handumdrehen mit Desktop-Betriebssystemen wie Windows und macOS. Es bringt Syncthing direkt mit und läuft ohne Installation.



Um einen Ordner zu synchronisieren, fügen Sie ihn ganz einfach über die Weboberfläche hinzu. Sie können dabei auch ein Passwort setzen, um die Dateien auf der Gegenseite verschlüsselt zu speichern.

Ordner freigeben & verschlüsseln

Jetzt fehlt nur noch ein Ordner mit Dateien. Klicken Sie am Rechner auf „+ Ordner hinzufügen“ und wählen Sie oben eine passende Bezeichnung für Ihr Vorhaben – etwa Dokumente, Fotos, Projekte oder Musiksammlung. Ganz unten geben Sie den Pfad des Ordners ein, den Sie synchronisieren möchten. Sie können hier `~\` als Abkürzung zu Ihrem Benutzerordner verwenden (unter Windows `C:\Users\Benutzername`), aber auch beliebige andere Pfade angeben. Wenn Sie es bei der Vorgabe belassen, legt Syncthing einen leeren Ordner mit der oben gewählten Bezeichnung im Benutzerordner an, sofern es ihn noch nicht gibt.

Wechseln Sie auf „Teilen“ und wählen Sie den Raspi aus. Rechts daneben können Sie ein Passwort eingeben. Damit lassen sich Ihre Dateien lokal vor der Synchronisation verschlüsseln. Auf der Gegenseite werden dann nur die verschlüsselten Dateien gespeichert. Ein solcher Schutz ist nicht nur für sensible Daten interessant: Sollten sich Dritte Zugriff auf Ihren Raspi verschaffen – etwa, indem sie ihn einfach mitnehmen –, könnten diese Ihre Daten ohne das Passwort nicht entschlüsseln.

Auch wenn Sie Ihre Daten mit einem Gerät außer Haus synchronisieren, zum Beispiel mit einem Raspi bei einem Freund, ist es ratsam, ein Passwort für die Verschlüsselung einzugeben. Verwenden Sie am besten einen Passwortmanager wie Bitwarden, um ein möglichst langes Zufallspasswort zu generieren und zu speichern.

Die Verschlüsselung funktioniert auch, wenn mehrere Rechner oder Smartphones in die Synchronisierung involviert sind: Hinterlegen Sie auf den vertrauenswürdigen Geräten, die die Dateien entschlüsseln sollen, einfach das Passwort für den Ordner. Danach bekommen Sie nichts mehr davon mit, Syncthing kümmert sich automatisch ums Ver- und Entschlüsseln Ihrer Dateien. Eine Transportverschlüsselung (TLS) ist übrigens auch ohne Passwort immer aktiv.

Interessant ist auch der Bereich „Dateiversionierung“: Hier können Sie einstellen, dass Syncthing alte Fassungen von Dateien aufbewahrt, wenn sie durch andere Geräte geändert werden. Lokale Änderungen werden dadurch nicht erfasst; daher ist es sinnvoller, die Versionierung später auf dem Raspi einzuschalten und nicht auf dem Rechner. Klicken Sie auf „Speichern“, um den Ordner hinzuzufügen.

Der Raspi informiert Sie jetzt auf der Weboberfläche, dass ein Ordner mit ihm geteilt werden soll und Sie klicken auf „Hinzufügen“. Ändern Sie den unten vorgegebenen Ordnerpfad nach Bedarf: Standardmäßig würde Syncthing wieder im Benutzerordner speichern (`~/`), der sich beim Raspi im Zweifel auf der Speicherkarte befindet. Wenn Sie eine USB-Platte oder SSD verwenden, ersetzen Sie den Pfad entsprechend, etwa mit `/mnt/ssd/MeinSyncOrdner`.

Dateiversionierung

Danach können Sie die Dateiversionierung auf dem Raspi einschalten, die auf dieser Seite mehr Sinn ergibt: Wenn Sie auf dem PC zum Beispiel ein Dokument in einem synchronisierten Ordner ändern, würde Ihr Raspi die vorherige Fassung zusätzlich aufheben. Die können Sie bei Bedarf wiederherstellen, wenn Sie mit einer aktuellen Änderung nicht zufrieden sind. Es gibt verschiedene Versionierungsmodi (siehe ct.de/w61j) zur Auswahl. Im einfachen Modus stellen Sie schlicht ein, wie viele alte Kopien Sie aufheben wollen und nach wie vielen Tagen diese gelöscht werden sollen (0 steht für niemals).

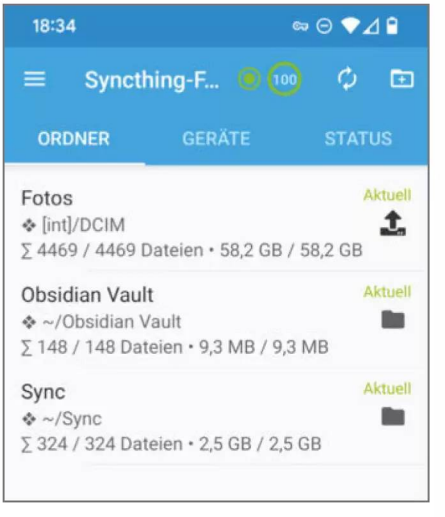
Nach einem Klick auf „Speichern“ wird der Ordner hinzugefügt und die Synchronisation beginnt. Auf diese Weise können Sie Ordner für beliebig viele Ihrer Geräte freigeben. Achten Sie hierbei darauf, von wo Sie teilen: Wenn Sie auf dem Rechner einen Ordner direkt mit einem anderen Rechner oder Smartphone teilen, wird Syncthing die Daten direkt zwischen diesen Geräten syncen. Das klappt aber immer nur dann, wenn beide Geräte gleichzeitig laufen.

In der Regel ist es daher sinnvoller, den Ordner vom Raspi aus mit weiteren Geräten zu teilen. Weil der Raspi immer läuft, tauscht er Ihre Dateien dann automatisch mit den anderen Geräten aus, wenn diese aktiv sind, ähnlich einem zentralen Cloudserver. So haben Sie quasi Ihre private Speichercloud – ohne Cloud.

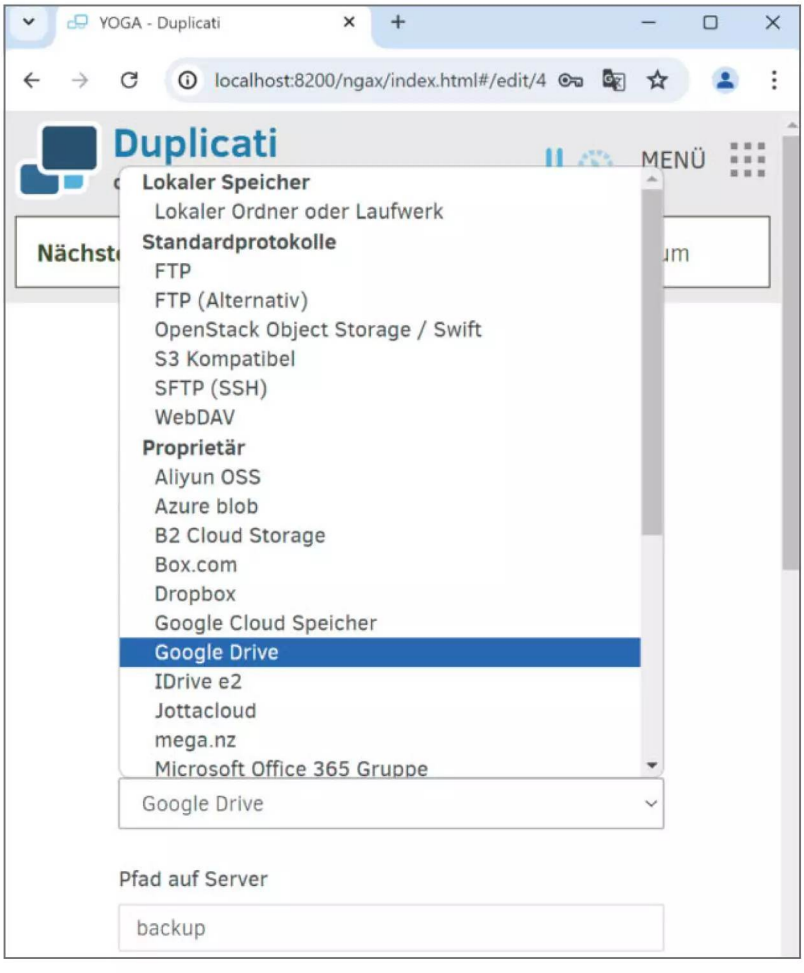
Das Hinzufügen von Ordnern erfordert nur wenige Klicks und geht schnell in Fleisch und Blut über. Wenn Sie es sich noch leichter machen möchten, können Sie auf dem Raspi rechts oben unter „Aktionen/Einstellungen/Ordnervorgaben bearbeiten“ den beim Hinzufügen vorgegebenen Ordnerpfad (~ für den Benutzerordner) korrigieren, damit er gleich passend vorgeschlagen wird. Sie können zudem einstellen, dass der Raspi die Ordnerfreigaben bestimmter Geräte automatisch akzeptiert: Klicken Sie auf der Raspi-Weboberfläche auf ein Gerät und dann auf „Bearbeiten/Teilen/Automatisch annehmen“.

Mobil und unterwegs

Eine Besonderheit von Syncthing ist, dass die Synchronisation auch mit Geräten klappt, die sich gerade nicht im lokalen Netz befinden. Wenn Sie zum Beispiel unterwegs ein Foto mit dem Smartphone knipsen, kann Syncthing es automatisch auf dem Raspi daheim sichern. Das ist ähnlich komfortabel wie der Sync mit Google Fotos oder der iCloud, aber privat und sicher. Genauso haben Sie die aktuellen Fassungen Ihrer Dokumente immer dabei, um sie auf dem Notebook oder Smartphone zu bearbeiten.



Mit Syncthing-Fork gibt es auch eine passende App für Android. Damit können Sie Ihr Smartphone sogar unterwegs mit dem Raspi daheim synchronisieren, da Syncthing auch übers Internet funktioniert. Frisch geknipste Fotos werden so automatisch gesichert, lange bevor Sie aus dem Urlaub zurück sind.



Das Backup-Tool Duplicati ist sehr vielseitig. Sie können es einsetzen, um die synchronisierten Dateien auf dem Raspi verschlüsselt an einen Ort Ihrer Wahl zu sichern. Im besten Fall befindet sich der außer Haus, damit Ihre Backups auch vor Naturereignissen wie Blitzschlag oder Hochwasser geschützt sind.

Für den Austausch mit externen Geräten probiert Syncthing verschiedene Verbindungswege (siehe ct.de/w61j). Der direkteste und schnellste Weg setzt im Router eine Port-Weiterleitung in Richtung Raspi voraus (Port 22000 über TCP und UDP). Wichtig ist, dass Sie das Webinterface auf Port 8384 niemals über das Internet erreichbar machen, denn dafür ist es nicht ausgelegt.

Wenn Sie das nicht möchten, findet Syncthing automatisch einen anderen Weg, etwa über das sogenannte UDP Hole Punching, das auch Smart-Home-Geräte verwenden, um für bestimmte Verbindungspartner im Internet erreichbar zu sein. Klappt auch das nicht, greift das Sync-Tool zum letzten Strohhalm und leitet die verschlüsselten Daten über einen Relay-Server im Internet. Auf welche Art ein Gerät gerade verbunden ist, erfahren Sie, indem Sie es im Webinterface unter „Externe Geräte“ anklicken („Verbindungstyp“).

Damit kennen Sie die wichtigsten Handgriffe, um mit Syncthing beliebige Daten zwischen beliebigen Geräten auszutauschen. Die grundlegenden Schritte sind auf allen Plattformen gleich. Mitunter bieten die Apps noch ein paar Extras. So können Sie etwa bei Syncthing-Fork für Android genau einstellen, unter welchen Bedingungen die Synchronisation aktiv sein soll, um den Akku und das Inklusivvolumen Ihres Mobilfunkvertrags zu schonen.

Wenn Ihnen ein gelegentliches Update reicht, stellen Sie unten in der App unter „Laufkonditionen“ ein, dass nur synchronisiert wird, wenn WLAN und Ladekabel verbunden sind. Unter „Syncthing-Optionen/WebUI-Fernzugriff“ können Sie die Weboberfläche der Android-App im lokalen Netz erreichbar machen, um die Konfiguration bequem vom Rechner aus zu erledigen. Denken Sie in diesem Fall wieder daran, ein Zugriffspasswort zu setzen.

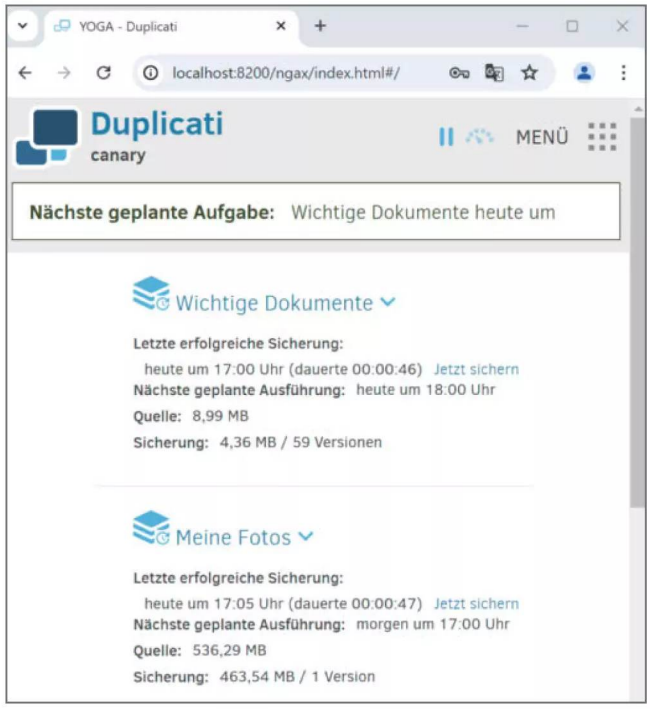
Kein Backup, kein Mitleid

Mit Syncthing können Sie Ihre Dateien auf all Ihren Geräten synchron halten und im besten Fall dient Ihr Raspi als zentraler Sync-Peer, der immer alle aktuellen Dateien aller Gerät vorhält. Nachdem Ihr digitales Hab und Gut jetzt zentral an einem Ort versammelt ist, ist die Gelegenheit günstig, diese Daten noch mal gezielt zu sichern, um sie im Katastrophenfall wiederherstellen zu können. So ein katastrophensicheres Backup sollte sich außer Haus befinden, für den Fall, dass Ihre Technik zu Hause durch Hochwasser, Blitzeinschlag oder Feuer außer Gefecht gesetzt wird. Solche Ereignisse sind glücklicherweise selten, aber eben auch verheerend.

Wie oben beschrieben, können Sie auch dafür Syncthing verwenden: Installieren Sie es außer Haus, etwa bei Freunden, Familie oder auf einem Cloudserver, und setzen Sie für alle so synchronisierten Ordner ein Passwort, damit sie auf der anderen Seite verschlüsselt sind und niemand Ihre Daten lesen kann.

Sie könnten zum Beispiel einen zweiten Raspi wie oben beschrieben einrichten und innerhalb der Familie verschenken – vielleicht finden Sie ja noch einen in der Schublade und dazu eine alte USB-Festplatte. So schlagen Sie zwei Fliegen mit einer Klappe: Auch der Beschenkte kann seine Dateien fortan ohne Cloud synchronisieren und Sie bewahren sich gegenseitig Ihre Backups extern auf.

Wenn sich so eine Gelegenheit nicht bietet, stellen Sie Syncthing einfach das konventionelle Backup-Tool Duplicati zur Seite, das ebenfalls auf dem Raspi läuft und per Weboberfläche gesteuert wird. Es sichert Ihre Ordner an nahezu beliebige Orte, etwa auf USB-Platten, NAS, WebDAV- und FTP-Server. Zudem unterstützt es eine Reihe von Cloud-Speicherdiensten wie Google Drive und OneDrive. Da das Backup-Tool sämtliche Daten vor dem Speichern mit AES256 verschlüsselt, können Sie Ihre Backups auch in der Cloud ruhigen Gewissens ablegen – der Cloudbetreiber kann damit nichts anfangen.



Duplicati läuft fast überall, auch auf Ihrem Raspi. Es wird wie Syncthing komfortabel über eine Weboberfläche konfiguriert.

Duplicati-Installation

Die Installation von Duplicati auf dem Raspi ist einfach. Laden Sie zunächst das aktuelle Installationspaket herunter. Den aktuellen Dateinamen finden Sie unter https://updates.duplicati.com/stable/. Halten Sie Ausschau nach der aktuellsten Version mit linux-arm64-gui.deb im Dateinamen, beispielsweise duplicati-2.1.0.5_stable_2025-03-04-linux-arm64-gui.deb. Den Download erledigen Sie direkt auf dem Raspi mit: `wget https://updates.duplicati.com/stable/duplicati-2.1.0.5_stable_2025-03-04-linux-arm64-gui.deb`

Danach installieren Sie das Paket mit dem folgenden Befehl (passen Sie den Dateinamen an die aktuelle Version an, die Sie heruntergeladen haben): `sudo apt install ./duplicati-2.1.0.5_stable_2025-03-04-linux-arm64-gui.deb -y`

Daraufhin werden auch diverse Abhängigkeiten heruntergeladen und installiert, darunter die Mono-Runtime. Duplicati ist ein .NET-Programm und benö-

tigt diese Laufzeitumgebung. Damit Sie das Webinterface von Duplicati aus dem lokalen Netz erreichen können, ist wieder eine Änderung an der Konfigurationsdatei nötig. Öffnen Sie die Datei mit: `sudo nano /etc/default/duplicati` und ändern Sie die letzte Zeile wie folgt: `DAEMON_OPTS="--webservice-interface=any --webservice-allowed-hostnames=*"`

Danach speichern Sie wieder mit Strg+O, Eingabetaste und beenden nano mit Strg+X. Damit Duplicati künftig beim Booten startet, aktivieren Sie dessen Dienst mit `sudo systemctl enable duplicati` und starten ihn einmalig manuell mit `sudo systemctl start duplicati`.

Sie können jetzt über http://[Raspi-Hostname oder IP]:8200 auf das Duplicati-Webinterface zugreifen. Es wird Sie auffordern, ein Passwort zu setzen, um den Zugriff darauf zu schützen. Willigen Sie ein und wählen Sie ein Kennwort.

Mein erstes Backup

Das Webinterface von Duplicati ist übersichtlich gestaltet und bedient sich intuitiv: Klicken Sie auf „+ Sicherung hinzufügen“, „Weiter >“ und legen Sie einen Namen für das Backup fest, sowie ein Passwort für die AES-Verschlüsselung. Danach wählen Sie zunächst das Sicherungsziel, also den Ort, an dem Sie Ihre Backups speichern möchten.

Das kann zum Beispiel ein WebDAV-Server oder ein Clouddienst wie Google Drive sein. Wenn Sie sich entschieden haben, geben Sie die Zugangsdaten für das Sicherungsziel ein. Bei Cloudspeichern erteilen Sie den Zugriff über das OAuth2.0-Verfahren, indem Sie auf „AuthID“ klicken und den Anweisungen folgen. Unter „Pfad auf dem Server“ legen Sie den Zielordner fest; existiert er noch nicht, legt Duplicati ihn für Sie an. Klicken Sie danach auf „Verbindung prüfen“, um zu checken, ob das Tool auf das gewünschte Ziel schreiben kann.

Hat das geklappt, klicken Sie auf „Weiter >“ und wählen den oder die Ordner aus, die Sie sichern möchten, zum Beispiel den Sync-Ordner auf der SSD oder USB-Platte Ihres Raspi. Im Zusammenspiel mit Syncthing gilt es jetzt für den Fall vorzusorgen, dass der Backupauftrag läuft, während Syncthing noch mit der Übertragung beschäftigt ist.

Syncthing fügt „.tmp“ an den Namen einer Datei an, die gerade übertragen wird. Damit solche Bruchstücke nicht in der Duplicati-Sicherung landen, geben Sie in Ihrem Backup-Auftrag unter „Filter“ einen Filter „Dateiendung ausschließen“ für `tmp` ein. Problem gelöst.

In den nächsten Schritten legen Sie noch fest, wie oft das Backup ausgeführt werden soll und wie lange Duplicati alte Sicherungen aufbewahren soll – standardmäßig löscht es nichts. Nach einem abschließenden Klick auf „Speichern“ gelangen Sie wieder auf die Übersichtsseite, die jetzt Ihren neuen Backupauftrag anzeigt. Wählen Sie „Jetzt sichern“, um einen ersten Testlauf zu starten.

Wenn das geklappt hat, wechseln Sie auf „Wiederherstellen“ und probieren Sie, die Dateien aus dem Backup wiederherzustellen. Denn nur ein Backup, das nachweislich funktioniert, ist ein wahres Backup. Möchten Sie sich näher mit Duplicati beschäftigen, finden Sie in c’t 19/2024 [2] einen ausführlichen Artikel darüber. Er beschreibt den Einsatz von Duplicati auf einem Windows-Rechner, aber genau wie Syncthing läuft das Backup-Tool auf allen möglichen Plattformen und bedient sich überall gleich.

Abschließend möchten wir Ihnen noch empfehlen, den Raspi und seine Programme von Zeit zu Zeit auf den aktuellen Stand zu bringen, da Updates häufig Bugs oder sogar Sicherheitslücken beseitigen. Das meiste – alles außer Duplicati – aktualisiert der folgende Einzeiler: `sudo apt update && sudo apt full-upgrade -y`

Anschließend ist ein Neustart sinnvoll (`sudo reboot`). Sie können die Installation der Updates auch mit unattended-upgrades (siehe ct.de/w61j) automatisieren, dürfen aber den Raspi nicht vom Strom trennen, solange die Aktualisierung läuft. Da sich Duplicati nicht in einem Repository befindet, müssen Sie neue Versionen wie oben beschrieben über die alte installieren.

Rundum sorglos

Unser Projektvorschlag, bestehend aus Syncthing und Duplicati, ist ein Rundum-sorglos-Paket für Ihre Dateien. Einmal eingerichtet, sind Sie nicht mehr auf die Dienste von Google Drive, OneDrive, iCloud & Co. angewiesen – Sie synchronisieren Ihre Dateien fortan einfach selbst. Das spart Ihnen nicht nur laufende Kosten, es ist auch viel privater, da Sie die volle Kontrolle über Ihre Daten haben.

Auch das Thema Backups wird kein schlechtes Gewissen mehr hervorrufen, denn die erledigen sich künftig ganz von allein. Wenn Sie unser Projekt mit einem Raspi 5 und einer SSD nachbauen, steckt das alles in einem kleinen Schächtelchen, das neben dem Router kaum auffällt. Aber auch ein älterer Raspi oder ausgedienter PC kann Ihnen noch wertvolle Dienste als Backup- und Sync-Server leisten. (rei) **ct**

Literatur

[1] Lutz Labs, Christof Windeck, Raspadapter, SSD- und PCIe-Adapter für den Raspberry Pi 5: Test und Technik, c’t 19/2024, S. 82

[2] Ronald Eikenberg, Backups: Keine Ausreden mehr, Windows-Sicherheitspaket: Backups ganz einfach, c’t 19/2024, S. 18

[3] Ronald Eikenberg, Showtime für den Raspi, So richten Sie den Raspberry Pi schnell und komfortabel ein, c’t 21/2024, S. 146

Syncthing, Duplicati & weitere Infos:

ct.de/w61j

Adé Copilot: lokale KI-Coding-Assistenten

GitHub Copilot sammelt Daten und kostet Geld. Wir stellen zwei kostenlose Programme vor, mit denen Sie eine lokale KI in Ihre Entwicklungsumgebung holen.

Von **Daniel Szöke und Daniel Ziegener**

Viele Programmierer arbeiten bereits mit KI-Tools beim Coding: Sie helfen beim Vervollständigen von Codezeilen direkt in der Entwicklungsumgebung oder beantworten als Chatbot Fragen zur Programmiersprache. Das beliebteste ist wohl GitHub Copilot vom US-Konzern Microsoft, das für mehrere integrierte Entwicklungsumgebungen (IDE) verfügbar ist.

GitHub bewirbt Copilot als persönlichen Pair-Programmer, der beim Coden unterstützt. Die kostenlose Version ist aber auf 2000 Code-Vervollständigungen und 50 Chatanfragen im Monat limitiert. Danach werden mindestens 10 US-Dollar im Monat oder 100 US-Dollar im Jahr fällig. Dieser Artikel stellt zwei Alternativen vor, die nicht nur kostenlos, sondern auch datenschutzfreundlich sind: Continue und Tabby.

Continue ist eine Erweiterung für Jetbrains und VS Code, die Open-Source-LLMs (Large Language Models) lokal direkt in die IDE einbettet. **Tabby** ist eine selbst gehostete KI-Coding-Umgebung, die Autocomplete und Chat in die eigene Entwicklungsumgebung bringt. Beide Programme führen Sprachmodelle offline auf dem eigenen Rechner aus und machen Programmierer so unabhängig von kommerziellen Clouddiensten. Wir beschreiben die Installation, Einrichtung und den Funktionsumfang und testen, was aufs Programmieren spezialisierte LLMs wie Qwen2.5-Coder auf normalen Laptops leisten.

Die richtigen Sprachmodelle auswählen

Continue und Tabby binden drei separate Sprachmodelle ein. Das **Chat-Modell** erklärt den Code und ist hauptsächlich auf Daten trainiert, die in natürlicher Sprache geschrieben sind. Es funktioniert wie die bekannten Chatbots ChatGPT, Claude oder Le Chat.

Das **Autocomplete-Modell** liefert automatisch Vorschläge für die nächsten Codezeilen. Spezialisierte Modelle wie Starcoder2 wurden mit Datensätzen in hunderten Programmiersprachen trainiert. Auf einen Prompt wie „schreibe eine Funktion, die die Quadratwurzel des Integers berechnet“ würde laut den Entwicklern Starcoder2 schlechtere Antworten liefern, als ein mit natürlicher Sprache trainiertes Modell. Das liegt daran, dass sie Starcoder2 dazu trainierten, aus natürlicher Sprache Code zu generieren, statt mit natürlicher Sprache wie Englisch zu antworten.

Als Letztes benötigen beide Anwendungen ein **Embedding-Modell** wie Nomic Embed Text. Das konvertiert einen eingegebenen Text oder Code in einen Vektor, um die Bedeutung der eingegebenen Inhalte mathematisch darzustellen. Durch den Vektor versteht das Modell, was Sie von ihm möchten. Alle Links zu den genannten Modellen und weitere Informationen finden Sie unter ct.de/w6ea.

Sprachmodelle haben Parameter. Das sind die Variablen, die das Modell dem Trainings-Datensatz entzieht. Sie geben an, wie stark eine Eingabe die Ausgabe beeinflusst (Gewichte) und wie stark das jeweilige Neuron im Modell feuert (Bias). Je mehr Parameter, desto präziser ist die Textausgabe oder die Autovervollständigung. Die Präzision kommt jedoch auf Kosten der Rechenleistung.

Die Entwickler von Tabby empfehlen, Modelle unter einer Milliarde Parameter einzusetzen, wenn Sie diese auf einer CPU ausführen. Es eignen sich etwa Qwen2.5-Coder-0.5B (Autocomplete-Modell) mit Qwen2.5-Coder-0.5B-Instruct (Chat-Modell). Für Apple Silicon oder Nvidia-Grafikkarten ab der RTX 10 Series eignen sich Modelle mit ein bis drei Milliarden Parametern. Auf unserem Apple Silicon M1 Pro lief Qwen2.5-Coder-1.5B einwandfrei. Für größere Sprachmodelle wie CodeLlama-13B empfehlen die Tabby-Entwickler mindestens eine Nvidia-Grafikkarte der RTX-30-Serie oder besser.

Auch die Entwickler von Continue raten zu speziell trainierten Modellen. Für die beste Autocomplete-Qualität empfehlen sie Codestral. Das Modell ist über die API von Mistral verfügbar. Die lokale Version ist mit 22 Milliarden Parametern vergleichsweise groß und für den lokalen Betrieb entsprechend ungeeignet: Der Softwareentwicklungs-Plattform GitLab zufolge benötigt Codestral 22B mindestens zwei Nvidia A100 für den Betrieb (siehe ct.de/w6ea).

Continue

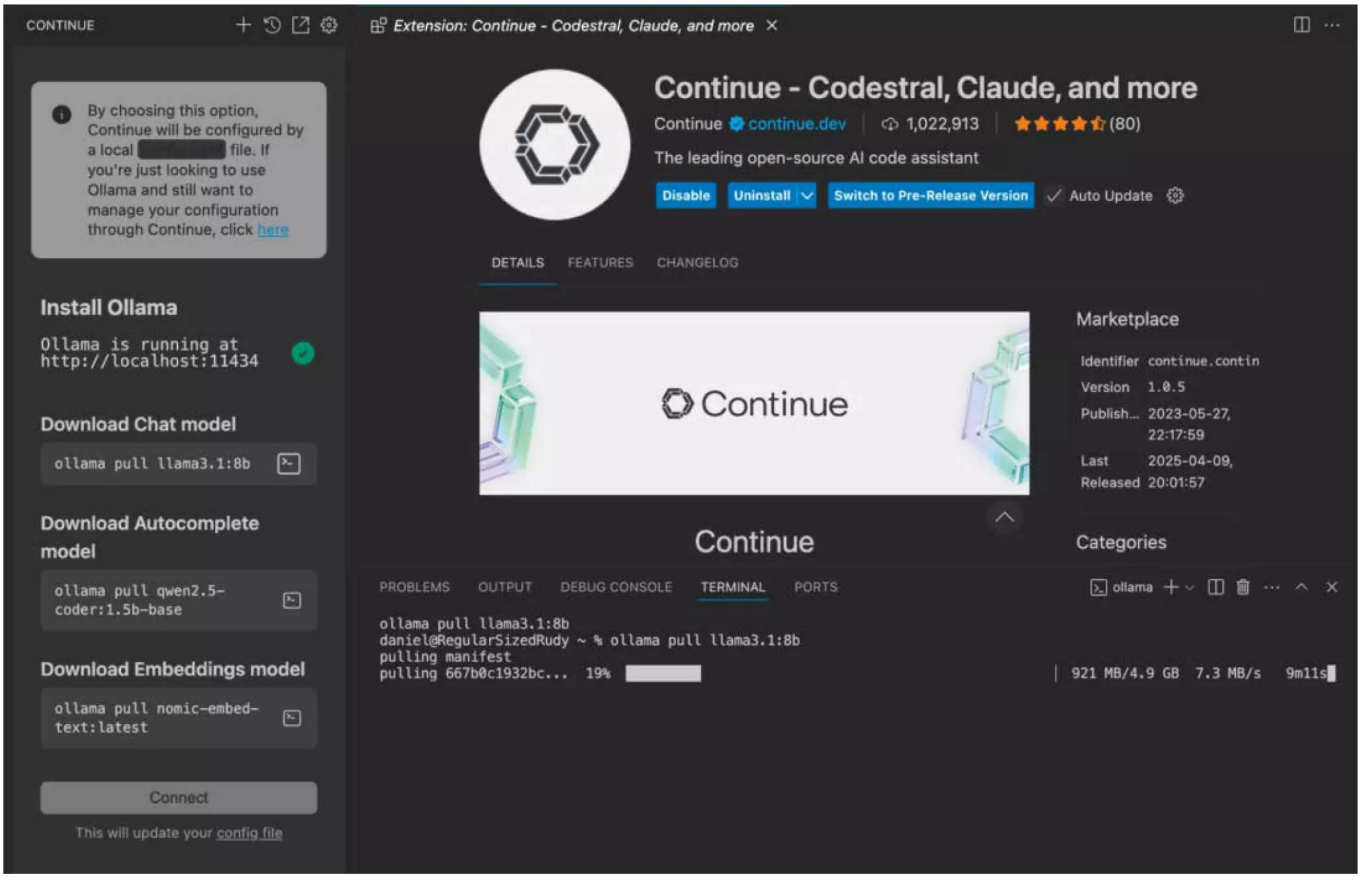
Continue ist eine Erweiterung für Entwicklungsumgebungen, um eigene KI-Code-Assistenten zu integrieren. Der Download für Jetbrains und Visual Studio Code (VS Code) ist kostenlos. In unserem Test verwenden wir VS Code als eine der beliebtesten Programmierumgebungen, die Installation über das Plug-in für IntelliJ funktioniert aber ähnlich.

Wer Assistenten in Continue mit mehreren Mitgliedern eines Teams teilen will, benötigt ein kostenpflichtiges Abo. Für die lokale Installation eines Sprachmodells ist das ebenso wenig notwendig wie ein Benutzerkonto bei Continue. Installation und Bedienung erfordern nur wenig Aufwand.

Continue installieren

Die VS-Code-Extension findet man auf Microsofts Marketplace. Ein Klick auf „Installieren“ öffnet Visual Studio, ein weiterer startet die Installation. Alternativ klickt man in VS Code links unten auf das Zahnrad, wählt im Pop-up-Menü „Extensions“ und gibt „Continue“ in die Suchzeile ein.

Continue selbst bringt noch keine KI-Funktionen mit. Um lokale Sprachmodelle für Autocomplete und Chat zu verwenden, braucht man mit Ollama ein weiteres Tool. Ollama ist eine kostenlose Open-Source-Anwendung, die KI-Modelle auf dem eigenen Rechner lädt und ausführt. Ollama wird nach Download und Installation über die Kommandozeile ge-



Die Continue-Erweiterung zeigt in VS Code bereits alle Ollama-Befehle zum Download der empfohlenen Modelle an.

startet. In diesem Beispiel verwenden wir macOS, die Befehle sind in Linux und Windows identisch (siehe ct.de/w6ea).

Die Entwickler von Continue empfehlen als Sprachmodelle Llama3.1 8B als Chat- und Qwen2.5-Coder-1.5B als Autocomplete-Modell. Beide Modelle sind feingetunte Varianten der zugrundeliegenden großen Sprachmodelle und benötigen weniger Speicherplatz und (V)RAM. 8B oder 1.5B gibt jeweils die Anzahl der Parameter in Milliarden an.

Wählt man in der VS-Code-Erweiterung von Continue die Option, ohne Anmeldung lokale Modelle zu nutzen, werden die Kommandozeilenbefehle zum Download der empfohlenen Modelle direkt angezeigt. Sie lassen sich per Klick in VS Code direkt ausführen. Continue füllt dann auch seine Konfigurationsdatei automatisch aus.

Manuelle Konfiguration in VS Code

Möchten Sie andere Modelle nutzen, startet der Befehl `ollama pull` den Download des gewünschten LLM. Das Verzeichnis von Ollama listet mehrere frei verfügbare Sprachmodelle mit verschiedenen Parameter-Größen (siehe ct.de/w6ea).

Die Konfiguration des gewünschten Sprachmodells erfolgt über eine YAML-Datei. Im Benutzerver-

zeichnis unter „~/.continue/config.yaml“ öffnen wir diese in VS Code. Die separaten Sprachmodelle für Autocomplete, Chat und Embed werden mit folgenden Zeilen konfiguriert:

```
models:
  - name: Llama 3.1 8B
    provider: ollama
    model: llama3.1:8b
    roles:
      - chat
      - edit
      - apply
  - name: Qwen2.5-Coder 1.5B
    provider: ollama
    model: qwen2.5-coder:1.5b-base
    roles:
      - autocomplete
  - name: Nomic Embed
    provider: ollama
    model: nomic-embed-text:latest
    roles:
      - embed
```

Nach dem Speichern der Datei und einem Neustart von VS Code sind die lokalen KI-Modelle einsatzbereit.

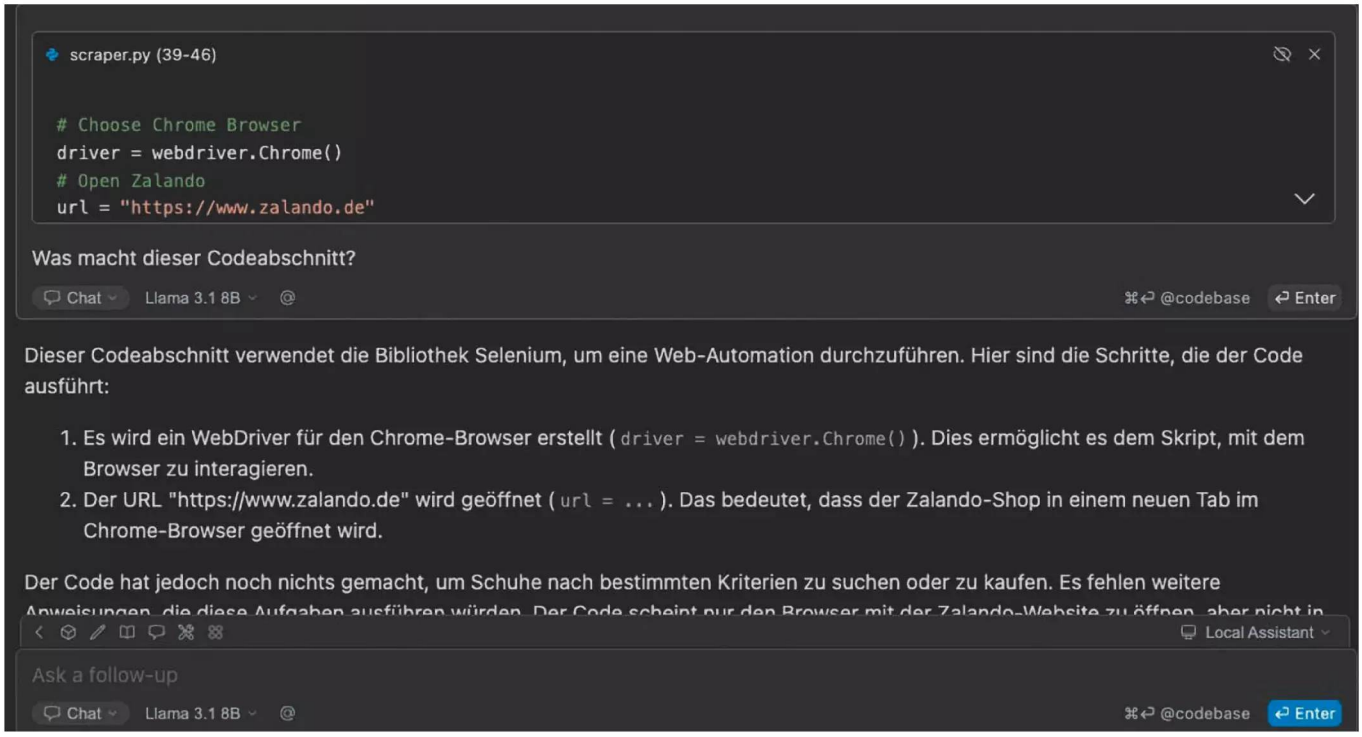
Autocomplete und Chat

In unserem Test verwenden wir Llama 3.1 als Chat-Modell. Chats funktionieren damit auf Deutsch und Englisch und liefern meist plausible Erklärungen des Codes.

Die Tastenkombination Strg + L (bzw. Cmd + L auf macOS) kopiert markierte Codezeilen direkt in das Chatfenster. Mit einer Frage oder Aufgabe ergänzt, erklärt das Chat-Modell so etwa die Funktion einer Zeile oder schlägt Veränderungen vor.

Vollkommen fehlerfrei sind die Antworten aber nicht. Fragen zu einzelnen Codezeilen oder -abschnit-

heise online



Per Chatfenster erklärt uns Llama 3.1 direkt in VS Code, wie Teile dieses Scraping-Scripts funktionieren.

ten werden in der Regel korrekt beantwortet. Die Funktion eines ganzen Python-Scripts zum Scrapen von Webshops konnte das verwendete Sprachmodell (in diesem Fall von Llama 3.1) allerdings nicht erklären.

Bewegt man den Mauscursor in die rechte obere Ecke eines Codeblocks im Chatfenster, erscheint ein Menü. Ein Klick auf die mittlere Schaltfläche fügt generierten Code direkt an der Position des Cursors in die aktuell geöffnete Datei ein.

Automatische Vorschläge für einen neuen Code werden direkt im Code angezeigt, wenn der Cursor im Fenster aktiv ist. Continue ruft von den Sprachmodellen mehrere Vorschläge ab, die über Pfeile in einem kleinen Pop-up über der Codezeile durchgeschaltet werden. Ein Druck auf die Tab-Taste fügt den Code ein.

Tabby

Tabby ist eine Open-Source-Anwendung, mit der Nutzer einen KI-Coding-Assistenten auf eigener Hardware selbst hosten können. Für die lokale Installation ist Tabby kostenlos. Eine kommerzielle Version für größere Teams ist gegen ein Abonnement erhältlich.

Tabby für die CPU installieren

Wer nur eine CPU hat, installiert Tabby am einfachsten per Installer. Windows-Nutzer installieren die Datei „tabby_x86_64-windows-msvc.zip“, die auf GitHub gespeichert ist (siehe ct.de/w6ea). Sie extrahieren die .zip-Datei und finden die Anwendung im Ordner „tabby_x86_64-windows-msvc“.

Wer Linux oder Windows-Subsystem für Linux 2 (WSL2) betreibt, navigiert zum Terminalemulator. Tippen Sie dort folgenden Befehl ein, um die Datei herunterzuladen:

```
wget https://github.com/TabbyML/tabby/releases/download/v0.27.1/tabby_x86_64-manylinux_2_28.tar.gz
```

Passen Sie den Pfad gegebenenfalls an die aktuelle Version an. Entpacken Sei anschließend das heruntergeladene Archiv:

```
tar -xvzf tabby_x86_64-manylinux_2_28.tar.gz
```

Wechseln Sie in das entpackte Verzeichnis und machen Sie die Dateien ausführbar:

```
cd tabby_x86_64-manylinux_2_28/
chmod +x tabby llama-server
```

Hinweis: Wenn Tabby unter Windows langsam läuft, versuchen Sie die Anwendung in WSL2 zu installieren. Wir konnten dadurch einige Fehlermeldungen vermeiden. Unser Modell lief bei der Autovervollständigung in WSL2 deutlich schneller.

macOS-Nutzer haben es einfacher: Tabby unterstützt den Paketmanager Homebrew. Auf macOS installiert der folgende Befehl im Terminal zunächst Homebrew:

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Wenn Homebrew eingerichtet ist, können Sie damit Tabby installieren:

```
brew install tabbyml/tabby/tabby
```

Homebrew installiert Tabby global. Also können Sie Tabby in jeglichem Dateipfad ausführen.

Tabby für die GPU installieren

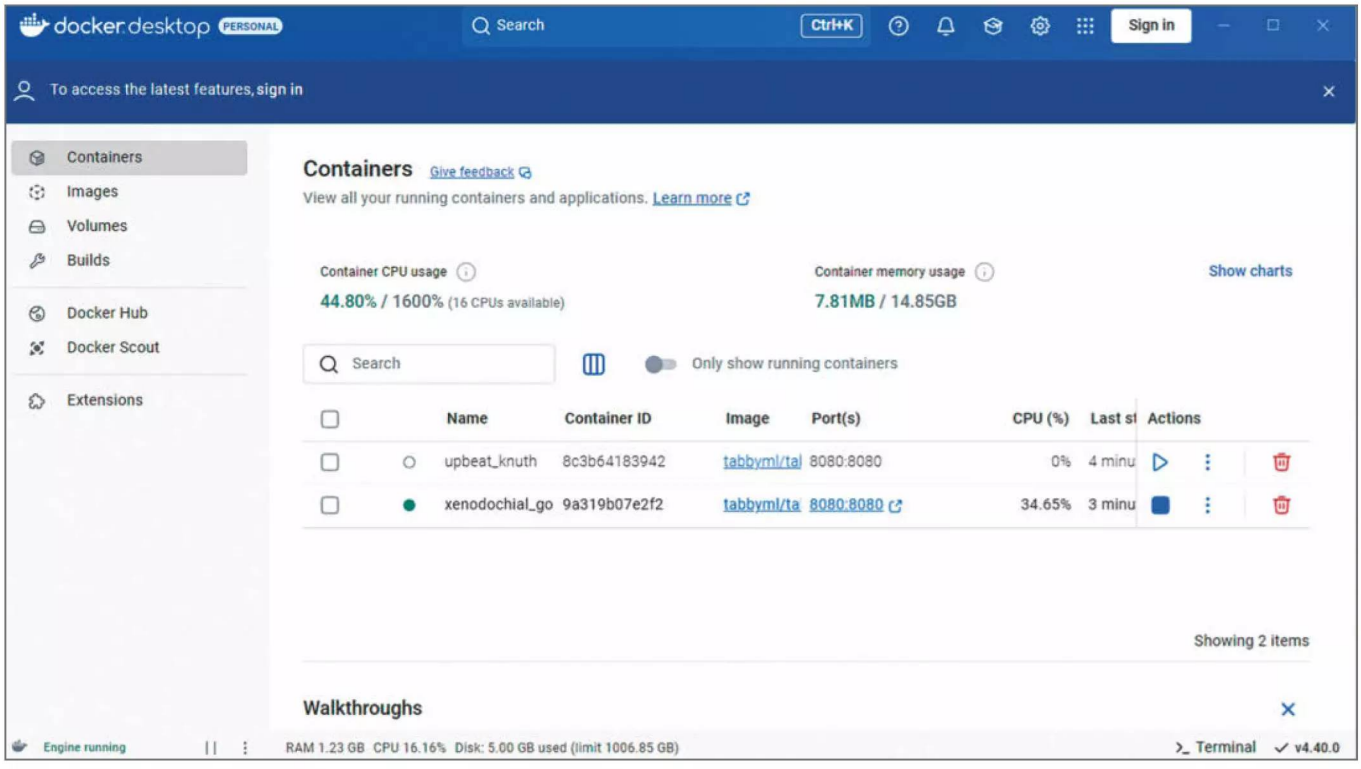
Wenn Sie Tabby mit einer Grafikkarte betreiben möchten, ist zusätzliche Software erforderlich. Windows-Nutzer sollten zuerst Visual Studio herunterladen. Eine weitere Voraussetzung ist WSL2, das Windows-Nutzer in der PowerShell mit `--wsl --install` aufsetzen.

Sie benötigen CUDA (Compute Unified Device Architecture), um die Berechnungen auf die Grafikkarte auszulagern. Windows- und Linux-Nutzer installieren dafür das CUDA Toolkit per Installer. Prüfen Sie, ob die Installation erfolgreich war, indem Sie einen Befehl im Terminalemulator ausführen:

```
nvcc --version # zeigt die CUDA-Version
nvidia-smi # zeigt die Grafikkarte
```

macOS-Nutzer müssen dagegen CUDA gar nicht installieren, denn Tabby verwendet die bereits vorinstallierten Frameworks Accelerate und CoreML. Die Dokumentation von Tabby liefert weitere Details zur Installation (siehe ct.de/w6ea).

Der Rechner kann nun die Nvidia-Grafikkarte ansprechen. Die Entwickler empfehlen, für die GPU-Version von Tabby außerdem Docker zu verwenden. Das ist eine Software, die virtuelle Container erstellt: Umgebungen, in denen Anwendungen und deren



Docker setzt die Tabby-Instanz isoliert auf.

abhängige Softwarepakete vom restlichen Betriebssystem abgekoppelt sind. Es setzt auf den Linux-Kernel, weswegen Windows-Nutzer WSL2 installieren müssen. Nach der Installation von Docker prüfen Sie mit `docker --version` im Terminal, ob die Anwendung läuft.

Eine Instanz starten

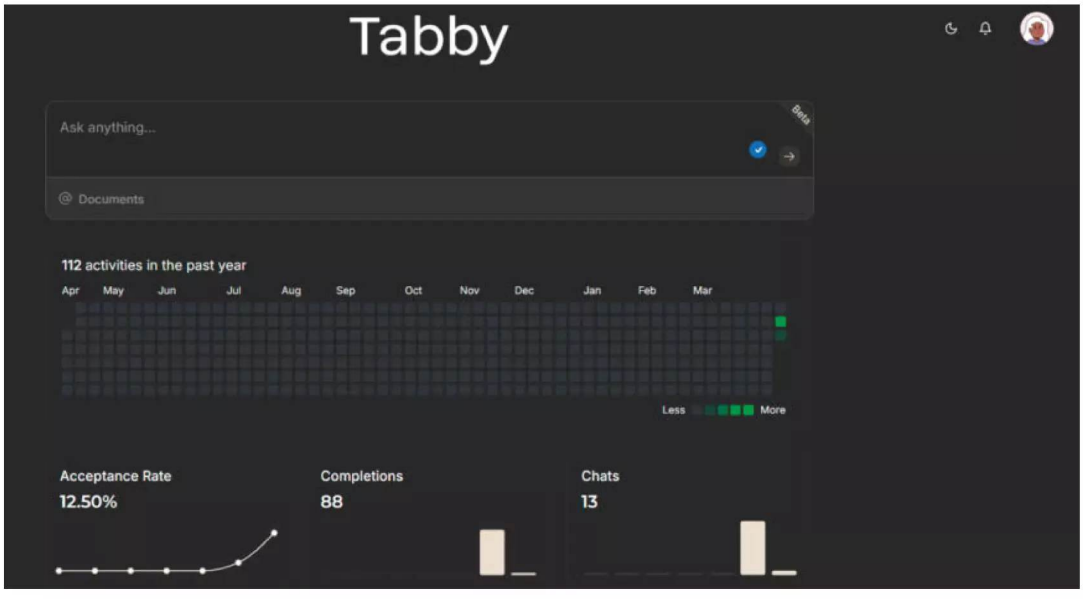
Tabby lädt die Modelle automatisch von der LLM-Plattform Hugging Face herunter. Um eine Instanz zu starten, navigieren Sie zum Dateipfad, in dem Tabby gespeichert ist. Bei uns ist das in Windows der Dateipfad „C:\Users\szo\Desktop\tabby\tabby_x86_64-windows-msvc“ und in WSL2 unter „~/tabby_x86_64-manylinux_2_28“ (zur CPU-Version). Docker lässt sich von jeglichem Dateipfad ausführen. Folgendes Kommando setzt unter Windows, WSL2 und Linux die Instanz auf:

```
./tabby serve --model Qwen2.5-Coder-0.5B ↵
  ↳--chat-model Qwen2.5-Coder-0.5B-Instruct
```

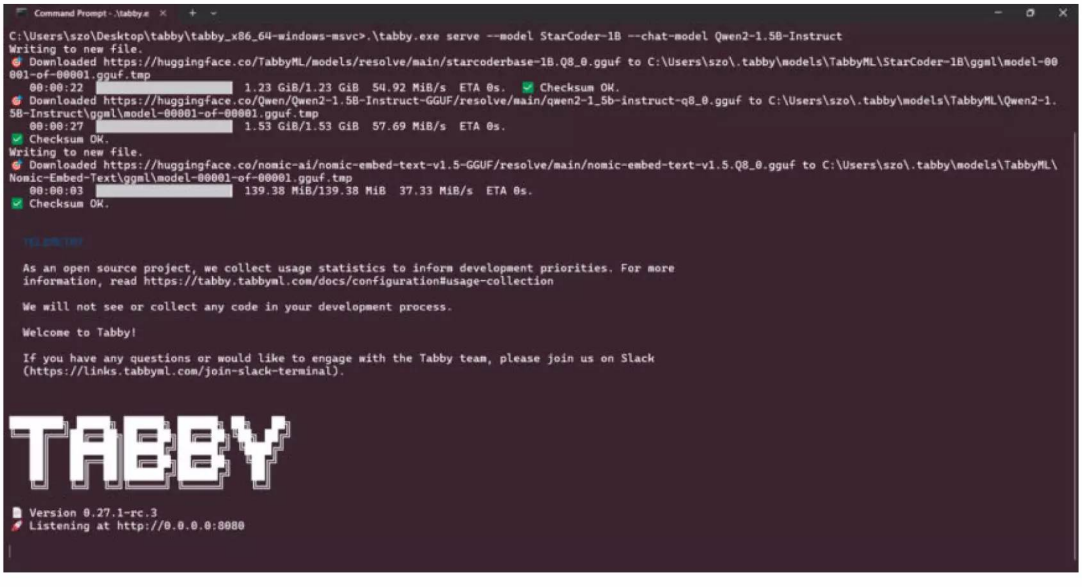
Unter macOS mit Apple Silicon lautet der Befehl:

```
tabby serve --device metal --model StarCoder-3B ↵
  ↳--chat-model Qwen2-1.5B-Instruct
```

Wenn Sie Tabby unter Docker mit einer Grafikkarte verwenden wollen, geben Sie folgenden Befehl ein. Passen Sie den Accountnamen beziehungsweise den Pfad an.



Das GUI von Tabby zeigt die vorherigen Autocompletes und Fragen an.



Für uns ließ sich Tabby am einfachsten in WSL2 installieren.

```
docker run -it --gpus all -p 8080:8080 -v ↵
  ↳C:\Users\szo/.tabby:/data ↵
  ↳registry.tabbyml.com/tabbyml/tabby serve ↵
  ↳--model TabbyML/Qwen2.5-Coder-14B ↵
  ↳--chat-model Qwen2.5-Coder-14B-Instruct --cuda
```

`serve` startet die Instanz. Nach der Anweisung `--model` folgt die ID des jeweiligen Modells, die Sie in der Dokumentation finden (siehe ct.de/w6ea). Die Anweisung `--chat-model` gibt das Chat-Modell an. Das Embedding-Modell fügt Tabby selbst hinzu, stan-

dardgemäß ist es Nomic-Embed-Text. Falls die CPU-Version ständig abbricht: Fügen Sie `--device cpu` hinzu.

Docker hingegen startet nach `docker run`. Die Flagge `-it` erlaubt, mit dem Container im Terminal zu interagieren. Das `--gpus all` und das zugehörige `--device cuda` setzen den Zugriff auf die Grafikkarte und `-p 8080:8080` wählt den standardgemäßen Port. Nach der Flagge `-v`, schreiben Sie unter welchem Dateipfad die Modelle gespeichert sein sollen. Etwa können Sie vor `/.tabby:/data` einen absoluten Dateipfad setzen, wie `C:\Users\szo/.tabby:/data`. Sie können hier aber auch einen relativen Dateipfad nutzen, wie `$HOME/.tabby` (Linux) oder `%USERPROFILE%/.tabby:/data` (Windows). Die darauf folgenden Befehle wählen die Modelle aus.

Ist die Instanz gestartet, erreichen Sie die Weboberfläche von Tabby unter http://localhost:8080. Mit einer E-Mail-Adresse registrieren Sie einen Admin-Account. Den benötigen Sie, um sich einzuloggen. Anschließend öffnet sich die Bedienoberfläche mit allen weiteren Einstellungen.

Tabby mit dem Editor verknüpfen

Tabby wird per Plug-in mit der gewünschten Entwicklungsumgebung verknüpft. Wir benutzen VS Code. Standardmäßig synchronisiert das nicht mit einer Cloud, außer Sie sind unter „Einstellungen für Sicherung und Synchronisierung“ mit einem Microsoft- oder GitHub-Konto angemeldet. Möchten Sie ganz auf Microsoft-Produkte verzichten, funktioniert Tabby auch mit den Entwicklungsumgebungen IntelliJ, Pycharm (benötigen die Installation der JavaScript-Runtime Node.js) und Neovim (siehe ct.de/w6ea).

Die Tabby-Extension lässt sich einfach in den Erweiterungen von VS Code installieren. Diese benötigt zur Verbindung mit Tabby einen Token. Sie starten dafür eine Tabby-Instanz und navigieren im Browser zu http://localhost:8080. Nach einem Klick auf das Profil-Icon (oben rechts) erscheint das gesuchte Token, beispielsweise `auth_cdfd38f12`.

In VS Code öffnet die Tastenkombination Strg + Shift + P die Einstellungen, in denen Sie „Tabby: Connect to Server“ suchen und localhost:8080 klicken. In der Leiste ploppt der Text „Status: Unauthorized“ auf. Sie klicken diesen an und fügen das Token ein.

In den Werkseinstellungen sendet Tabby anonymisierte Daten an die Entwickler. Die zeigen ihnen laut der Datenschutzerklärung, wie oft das Plug-in verwendet wird. Die Datenübertragung lässt sich abstellen. Ein Klick in VS Code auf „Tabby: Open Agent Settings“ öffnet die Konfigurationsdatei, die im Benutzerverzeichnis unter „.tabby-client/agent/config.toml“ liegt. Der Code-Abschnitt `[anonymousTracking]` trägt den Kommentar `#disable = false`. Also entfernt man das # und ändert die Variable zu `disable = true`.

VS Code aktiviert zuerst seine eigenen Plug-in-Einstellungen und erst danach das „config.toml“. Indem Sie die Einstellung „Tabby: Connect to Server ... / Use Configuration“ in Tabby Agent Settings auswählen, überschreiben Sie das. So startet die Instanz immer mit den Einstellungen, die Sie in der Konfigurationsdatei eingestellt hatten.

```
#config.toml
[server]
endpoint = "http://localhost:8080"
token = "auth_07f2c96032d84d6b82e6bcfcfbb311fb"

# Datenübertragung stoppen
[anonymousUsageTracking]
disable = true
```

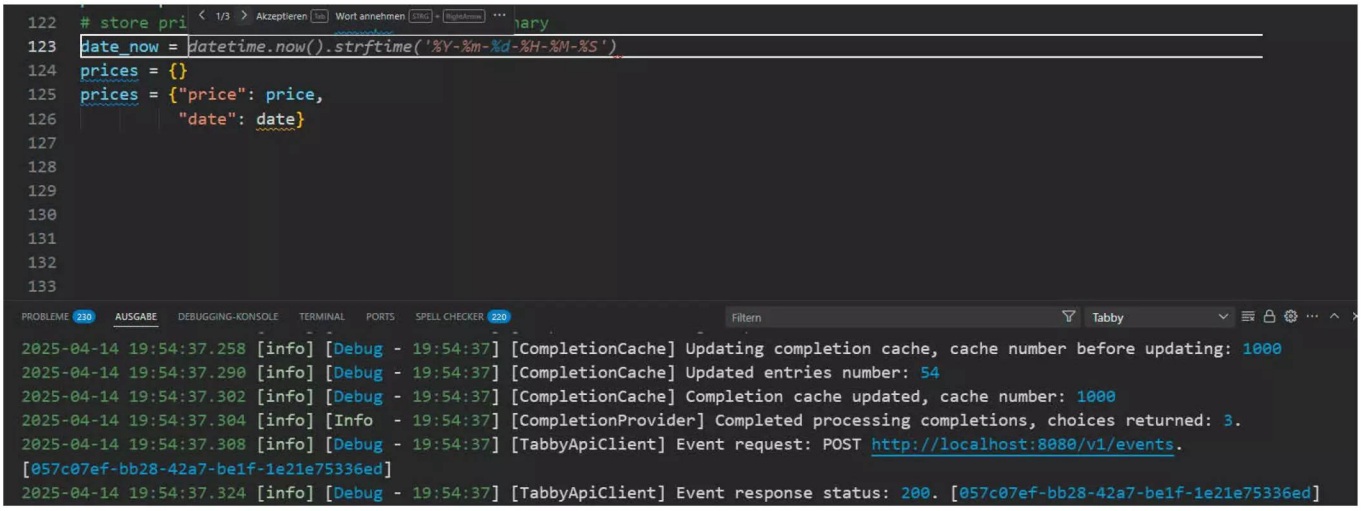
In der „config.toml“ können Sie auch `endpoint` und `token` auskommentieren und mit ihrer Serveradresse und dem Token versehen. Nach einem Neustart oder Abbruch des Plug-ins verbindet sich VS Code dann automatisch mit der Instanz.

Autocomplete und Chat

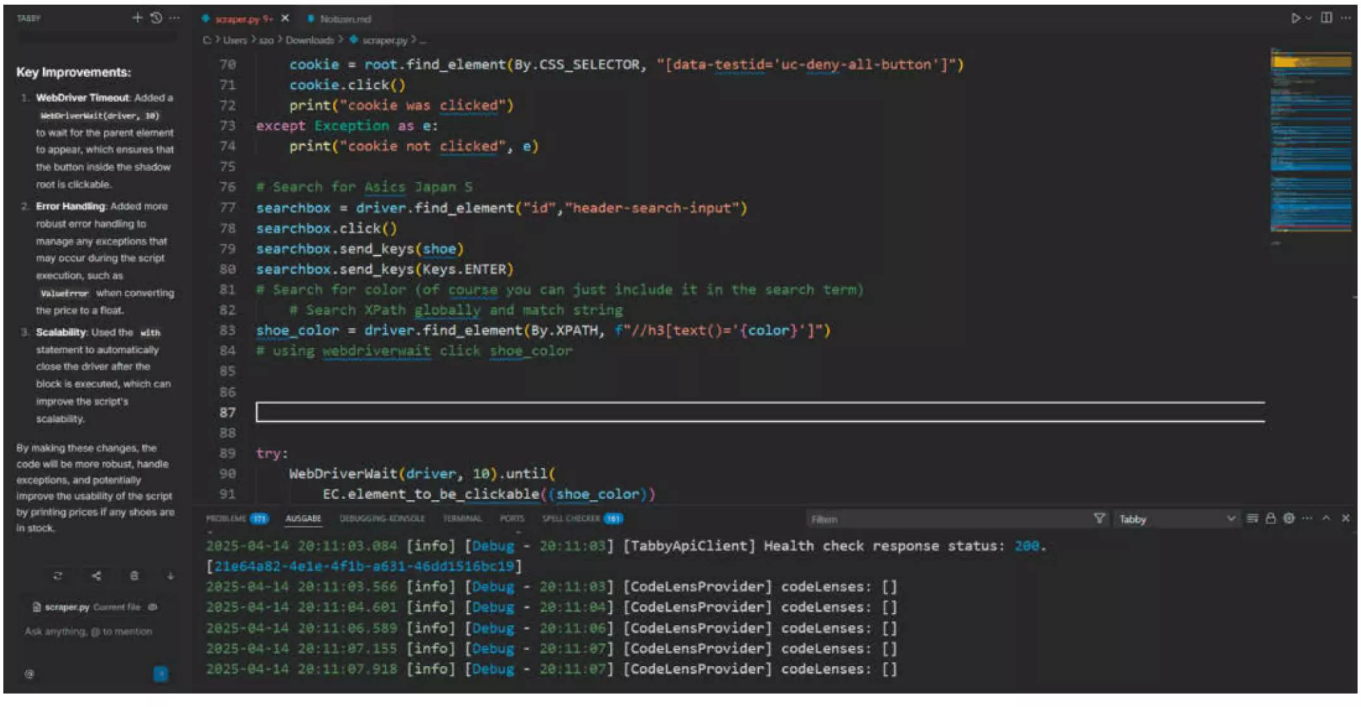
Wir haben Tabby auf einem handelsüblichen Lenovo-Laptop mit einer Intel i5-1135G7 CPU mit einer Leistung von 2.4 GHz getestet. Wer für Tabby nur eine CPU nutzen möchte, sollte meist den manuellen Autocomplete wählen, weil sonst die CPU überlasten kann. Manueller Autocomplete bedeutet: Nur nach einem Tastendruck holt sich Tabby den Autocomplete vom Sprachmodell. Das funktioniert mit „Tabby: Code Completion Trigger Mode (Automatic / Manual)“.

Drückt man die `Tab`-Taste, zeigt Tabby den Autocomplete: Ein ausgegrauter Text in der IDE. Insgesamt liefert Tabby ein bis drei Vorschläge. In einem kleinen Pop-up über dem ausgegrauten Text wählt man eines von diesen aus. Der erste Vorschlag lässt sich aber auch ohne weiteres mit einem weiteren Druck auf `Tab` annehmen. Mit Strg + rechte Pfeiltaste übernimmt man den Autocomplete nur Wort für Wort.

Tabby spricht per API auch mit dem Chatbot-Modell. Nach der Option „Tabby: Explain this“ fasst dieses den Code zusammen. An der linken Seite der



Tabby blendet den Autocomplete in grau ein.



Im Chatfenster gibt Tabby Tipps und erklärt den Code.

IDE poppt, wie bei Continue, ein Fenster auf. In diesem kann man dann mit dem Chat-Modell über den Code quatschen. Die Option „Tabby: Code Review“ liefert sogar Vorschläge zum Code, etwa wo sich mehr Error-Handling einbauen lässt oder ein Syntax-Fehler stecken könnte.

Vergleich von Continue und Tabby

Continue lagert den Betrieb der lokalen Modelle an die Open-Source-Anwendung Ollama aus. Mit wenigen Klicks integriert man so KI-Funktionen in VS Code. Die Installation von Tabby gestaltet sich hingegen komplizierter. Dafür bringt Tabby eine eigene, browserbasierte Bedienoberfläche mit, die beispielsweise nachverfolgt, wie viele Zeilen tatsächlich von KI beeinflusst wurden.

Bei den Funktionen in VS Code unterscheiden sich Continue und Tabby kaum. Beide Anwendungen integrieren Code-Autovervollständigung und einen Chatbot mit lokal laufenden Sprachmodellen. Wer dafür seinen leistungsstarken Heimserver oder die GPU des Gaming-PCs nutzen möchte, kann das mit beiden tun.

Die Bedienung ist innerhalb der IDE nahezu identisch, mit einem Chatfenster in der linken Seitenleiste und Code-Vorschlägen im Editor selbst, die Nutzer per Tab annehmen.

Für wen sich Continue und Tabby eignen

Die Autovervollständigung per Sprachmodell nimmt Programmierern in erster Linie lästige Routineaufgaben ab. Ob exakte Formatierung eines Strings oder sich wiederholender Boilerplate-Code: Ein paar mal die Tab-Taste drücken ist schneller, als alles selbst zu tippen.

Praktisch: Sowohl Continue als auch Tabby erkennen Kommentare als Prompt. Wer sich eine ganze Funktion generieren lassen will, kann diese in einem Kommentar direkt im Code beschreiben. Das jeweils verwendete Sprachmodell macht dann

einen oder mehrere Vorschläge zur Umsetzung. Trotzdem muss man immer darauf achten, was der KI-generierte Code wirklich macht. Gelegentlich kommt es in unserem Test selbst bei simplen Aufgaben zu fehlerhaftem Code.

Programmier-Anfänger profitieren von dem Chatfenster in der IDE. Dort stellen sie Verständnisfragen oder lassen sich Verbesserungsvorschläge geben. So spart man sich den Wechsel in Browsertabs und behält seinen Code stets im Blick.

Leistung: einfacher Büro-Laptop vs. MacBook

Unterschiede in Performance und Qualität der Ausgaben hängen primär von den gewählten Sprachmodellen und den Systemressourcen ab. Größere Modelle mit mehr Parametern tendieren zu besseren Ergebnissen, aber benötigen auch leistungsstärkere und teurere Hardware. Wir testeten die Sprachmodelle einmal mit einem herkömmlichen Lenovo-Laptop mit einem i5 mit 2,4 GHz sowie auf MacBooks mit M1- und M1-Pro-Prozessor.

Auf der Intel-i5-CPU ließ sich fast nur das kleine Sprachmodell Qwen2.5-Coder-0.5 betreiben. Zwar funktionierte auch StarCoder-1B, aber es benötigte für einen manuellen Autocomplete bis zu zehn Sekunden. Manchmal brach es ganz ab. Auch empfehlen wir bei der CPU-Version auf den manuellen Autocomplete zu setzen. Der automatische Autocomplete führte in unserem Test oft dazu, dass die vielen Anfragen die CPU auf 100 Prozent Auslastung springen ließen und der Cursor in der IDE stockte.

Das dreimal so große Qwen2.5-Coder-1.5B liefert im direkten Vergleich zwar genauere und umfangreichere Code-Vorschläge, lief aber nur auf dem Apple Silicon (M1 Pro) wirklich performant. Der packte ebenso das Chat-Modell Llama 3.1. Das acht Milliarden Parameter große Modell antwortet auf einem M1-Pro-Prozessor auf einfache Nachfragen binnen weniger Sekunden. Beim herkömmlichen M1 (ohne die Pro-Version) dagegen kam das 8B-Modell ins Stocken. Die Entwickler von Tabby empfehlen, die 7B- bis 13B-Sprachmodelle eher auf eine Nvidia-Grafikkarte ab der 30er-Serie zu betreiben (siehe ct.de/w6ea).

Code Qualität der Sprachmodelle im Vergleich

Selbst das kleine Sprachmodell Qwen2.5-Coder-0.5B löste simple Aufgaben famos. Nur hin und wieder schlichen sich Fehler ein. So ließen wir ein Python-Dictionary mit Schlüsseln und Werten befüllen, die bereits im Skript standen. Nach nur einer Sekunde generierte das kleine Sprachmodell drei Schlüssel mit passenden Werten. Leider war einer der Schlüssel eine Variable, die nicht in das Dictionary gehörte. Also prüften wir eine weitere Aufgabe: Im Dictionary das aktuelle Datum speichern. Dieses Mal generierte das Modell keinen Fehler und nahm uns die lästige Formatierung eines Strings ab.

Nun zu größeren Aufgaben: Boilerplate-Code. Das sind Codezeilen, die man immer und immer wieder schreiben muss. Wir nahmen dieses Beispiel: Das Skript soll die Daten im Python-Dictionary an eine E-Mail senden. Also schrieben wir einen Kommentar – auf den das 0.5B-Sprachmodell überraschenderweise präzise antwortete. Es wählte mit `smtplib` die richtige Python-Bibliothek. Danach ratterte es die Standardeinstellungen runter: Variablen für Absender, Empfänger und Port einrichten, verschlüsseln und die Nachricht verfassen.

Der Nachteil des kleinen Sprachmodells ist aber, dass es den Boilerplate-Code schlecht zu reproduzieren scheint. Als wir ein weiteres Mal den Autocomplete auf denselben Kommentar ausführten, gab das Modell unvollständigen Code aus. Ein zweites Mal verstand es nicht mehr, dass wir `smtplib` nutzen möchten. Je genauer wir den Kommentar formulieren, desto reproduzierbarer wird der Autocomplete. Mit der dafür verschwendeten Zeit hätten wir den Code eigentlich selbst tippen können.

```
# take data in python dictionary and
# send it to an email
with smtplib.SMTP("smtp.gmail.com", 587) as smtp:
    smtp.ehlo()
    smtp.starttls()
    smtp.login("goblin@gmail.com", "password")
    smtp.sendmail("goblin@gmail.com",
    "goblin@gmail.com",
    f"New price for {prices['price']}\n
↳{prices['date']}")
```

Das wurde bei einem größeren Modell wie StarCoder-3b deutlich besser. Es spuckte mehr Codezeilen als das kleinere Sprachmodell aus. Und wogegen Qwen2.5-0.5B oft verschiedene Antworten auf die gleiche Frage lieferte, schien StarCoder-3B für den Boilerplate-Code meist dasselbe Format beizubehalten: `smtplib` einstellen, Variablen für den `sender` und den `receiver` setzen und die Nachricht schreiben. Auch Fragen zu einzelnen Codezeilen oder -abschnit-

ten beantwortete das größere Sprachmodell in der Regel korrekt.

Fehlerfrei waren beide Sprachmodelle nicht. Das kleine Sprachmodell zeigte eine klare Grenze auf: Bei Aufgaben, die viel Kontext benötigen. Etwa tippten wir den Autocomplete für eine Funktion, die mit dem Python-Framework Selenium ein bestimmtes CSS-Element auswählen sollte. Das kam zwar schon mal in unserem Skript vor. Trotzdem wählte das Sprachmodell keinmal das richtige Element. Auch das Chat-Modell Llama 3.1 8B erklärte, im Vergleich zu einem ChatGPT, einzelne Funktionsweisen eines einfachen Python-Scripts zum Scrapen undetailliert.

Fazit

Continue und Tabby bringen Open-Source-Sprachmodelle in verschiedene Entwicklungsumgebungen. Dafür reichen jeweils ihre kostenlosen Angebote aus. Über welches der Tools Entwickler eine LLM installieren, ist letztlich Geschmackssache.

Einfacher als mit Continue und Ollama lassen sich lokale KI-Modelle wohl kaum in VS Code einbinden. Die Installation erfordert wenige Klicks und hat kaum Hürden. Tabby hingegen unterstützt mehr Entwicklungsumgebungen. Neben Jetbrains und VS Code kann man es auch in Android Studio, Eclipse und Neovim einbinden.

Lokal ausgeführte Sprachmodelle sind nützlich, auch sie im Vergleich zu Cloudversionen im Rechenzentrum mit eingeschränkter Leistung laufen. Im Gegensatz zu kommerziellen Angeboten von GitHub oder OpenAI spart man Abogebühren. Außerdem arbeitet man auf jeden Fall datenschutzkonform, da Daten nur offline auf dem eigenen System verarbeitet werden.

Lokale LLMs mit Continue und Tabby sind nützliche Ergänzungen zum Arbeitsablauf, solange man sich nicht darauf verlässt, dass Llama oder Qwen einem die ganze Arbeit abnehmen. Denn: Der Programmierer bleibt noch immer der Mensch vor dem Computer. (tlz) c't

Weitere Infos:
ct.de/w6ea

Vorschau c't Desinfec't

Ab dem 26. September im Handel und auf ct.de

Das Rettungssystem bei Virenbefall

Desinfec't 2025/26 untersucht Windows auf Virenbefall. Dafür bringt es unter anderem Virenscanner von Eset und Ikarus mit. Damit die Scanner auch aktuelle Bedrohungen finden, sind ein Jahr lang kostenlose Signaturupdates inklusive. Schlägt ein Scanner Alarm, kann man Funde einschätzen, um mögliche Fehlalarme zu erkennen. Ist es wirklich ein Virus, macht Desinfec't ihn unschädlich.

Damit das in einer so sicheren Umgebung wie möglich geschieht, bringt Desinfec't sein eigenes Live-System auf Linuxbasis mit und startet direkt von einem USB-Stick statt Windows. Weil ein Virus in diesem Zustand wie Windows ebenfalls inaktiv ist, kann er nicht noch mehr Unheil anrichten. So untersucht man das System aus einer sicheren Entfernung. Außerdem kann man persönliche Daten in Sicherheit bringen und direkt auf einen Desinfec't-Stick kopieren.

Das c't-Sicherheitstool richtet sich an Computereinsteiger, es bringt aber auch mehrere Analysetools für Malwareprofis mit. Überdies kann man sich via TeamViewer Hilfe vom Familien-Admin auf einen möglicherweise verseuchten Computer holen, wenn man nicht mehr weiterweiß.

Weitere c't-Sonderhefte: heise.de/s/00MxL

Themenschwerpunkte

c't Desinfec't: Das Rettungssystem bei Virenbefall

- Die Funktionen und Möglichkeiten von Desinfec't vorgestellt
- Schritt-für-Schritt-Anleitung: So installiert und startet man Desinfec't
- So nutzt man das c't-Sicherheitstool am effizientesten
- Viren jagen und löschen
- Daten in Sicherheit bringen
- Versehentlich gelöschte Dateien wiederherstellen
- Fernhilfe
- Malwareanalyse mit Expertentools
- Aktuelle PC-Bedrohungen eingeordnet