Raus aus den US-Clouds!

Gründe, heute nach Alternativen zu suchen

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 Cloud Act verpflichtet, den US-Behörden den Zugriff auf gespeicherte Daten unabhängig von deren Aufenthaltsort zu gewähren, was der Artikel auf Seite 30 näher aufdröselt. Dieser Durchgriff ist der Hauptgrund, die Trump-Zone zu verlassen.

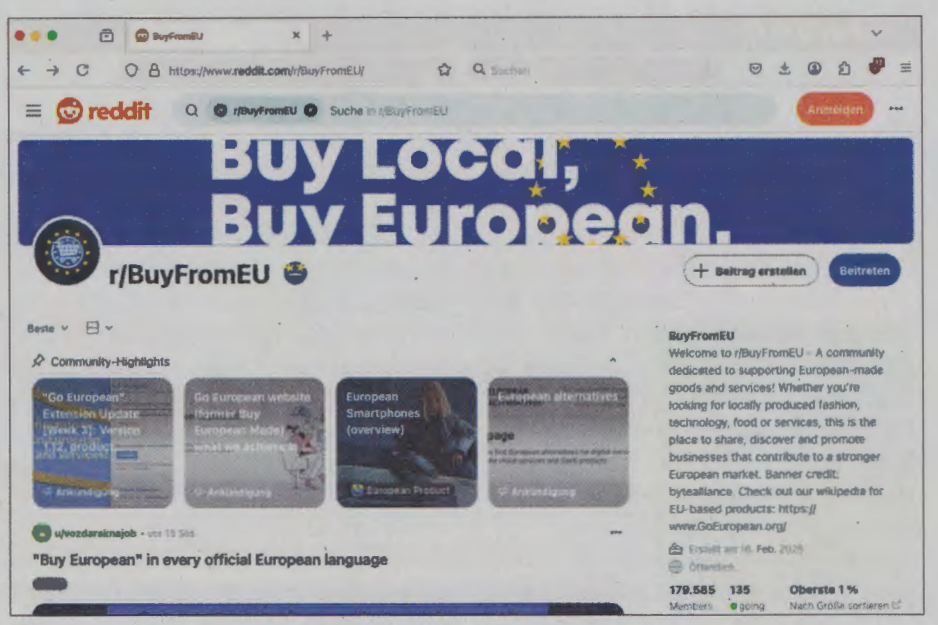
Leider ist es heutzutage wenig offensichtlich, ob digitale Angebote ohne US-Cloudtechnik auskommen. Der Betreiber einer Chatplattform könnte zwar in Europa seinen Sitz haben, aber die nötige Rechenleistung in einer US-Cloud einkaufen. Das hieße dann, dass auch die US-Behörden Zugriff auf die dort verarbeiteten 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 Diens-



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.

Bild: KI, Collage c't

te 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, zeigt sich gerade in Großbritannien: Dort verlangt die Regierung von Apple, die Ende-zu-Ende-Verschlüsselung für deren Bürger zu deaktivieren. Cloud bleibt immer Vertrauenssache.

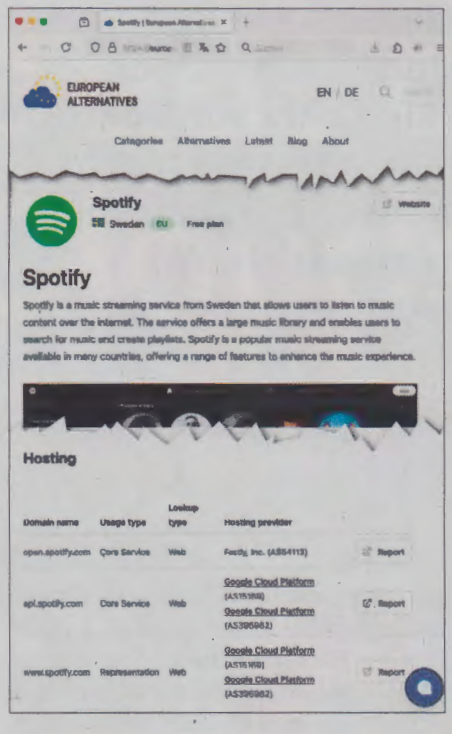
Chip-Hersteller und Cloudbetreiber versuchen mit hochkomplexen Techniken wie Trust Domain Extensions in Prozessoren auch Firmen die Cloud schmackhaft zu machen. Sie versprechen, die Daten der Kunden (auch untereinander) zu schützen. Der Aufwand, den sie für diese Confidential Computing genannte Technik 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



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.

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 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/ymu3) 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@ct.de)* c't

Websites und Diskussionen zu europäischen Alternativen: ct.de/ymu3

Bild: KI, College c't

Die Trump-Zone verlassen

Datensparsame 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.

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?

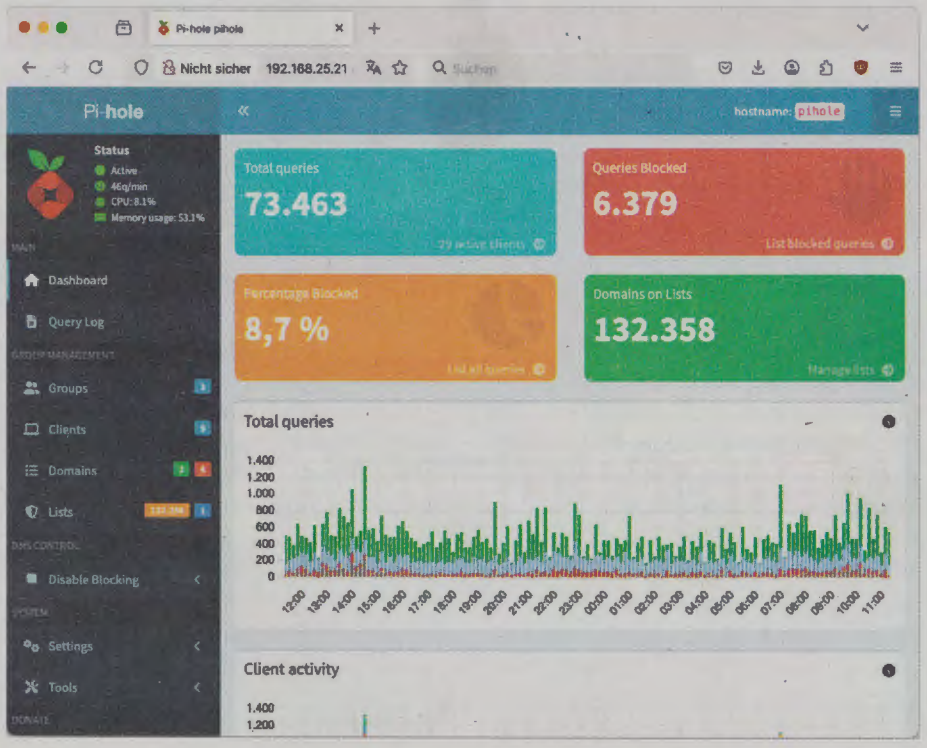
Es wäre witzlos, wenn Sie Ihre DNS-Spuren verwischen und Tracker ausfiltern, aber stets weiter Google oder Bing konsultieren, wenn Sie etwas suchen – im schlechtesten Fall auch noch, während Sie dort mit Ihrem Benutzerkonto angemeldet sind. Die Suchmaschinenbetreiber schürfen mit den Anfragen das Datengold, 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

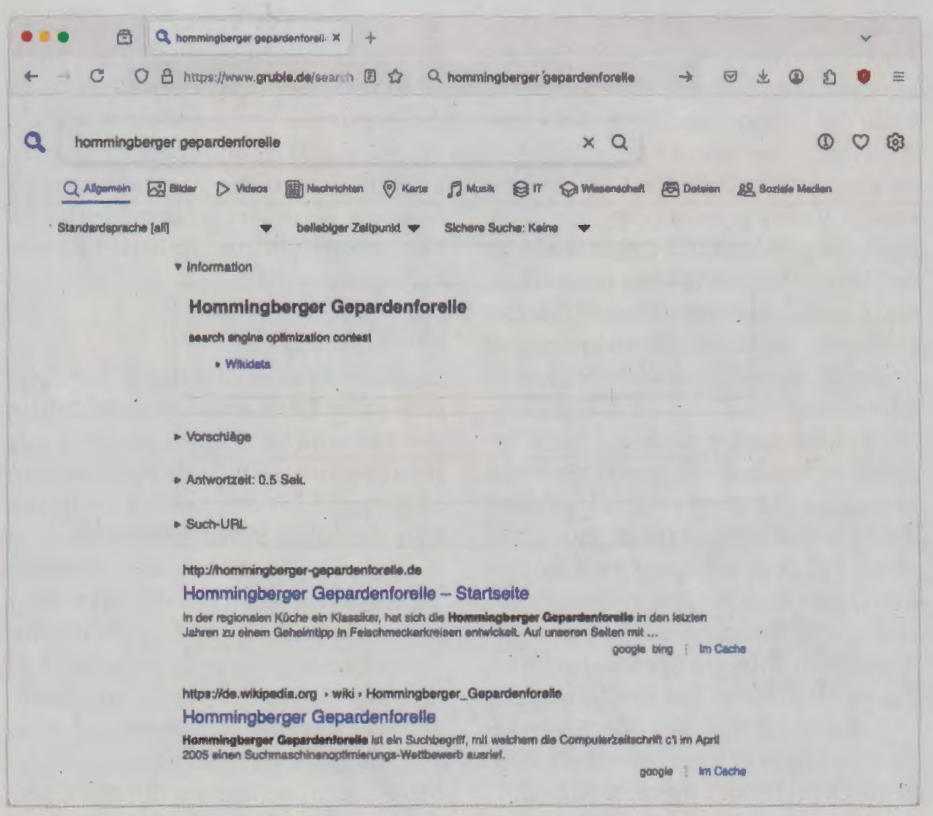
Ein ähnliches Geschäftsmodell verfolgt inzwischen die deutsche Suchmaschinenalternative metaGer. Kostenlose Nutzung für alle konnte der Verein nicht mehr finanzieren, über den Erwerb von Token steht die Suchmaschine aber Interessierten weiter offen. Neben Werbefreiheit, Trackingverzicht und Privatsphärenschutz 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



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.

Bild: KI, Collage c't



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.

geringem Aufwand eine eigene Instanz aufsetzen. SearXNG wirkt als Filter zwischen den Suchenden und den befragten Suchmaschinen. Falls Sie sich wundern, warum das viel empfohlene 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 vormachen, sich nämlich als Stellvertreter vor andere Dienste zu setzen und damit den Datenaderlass 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

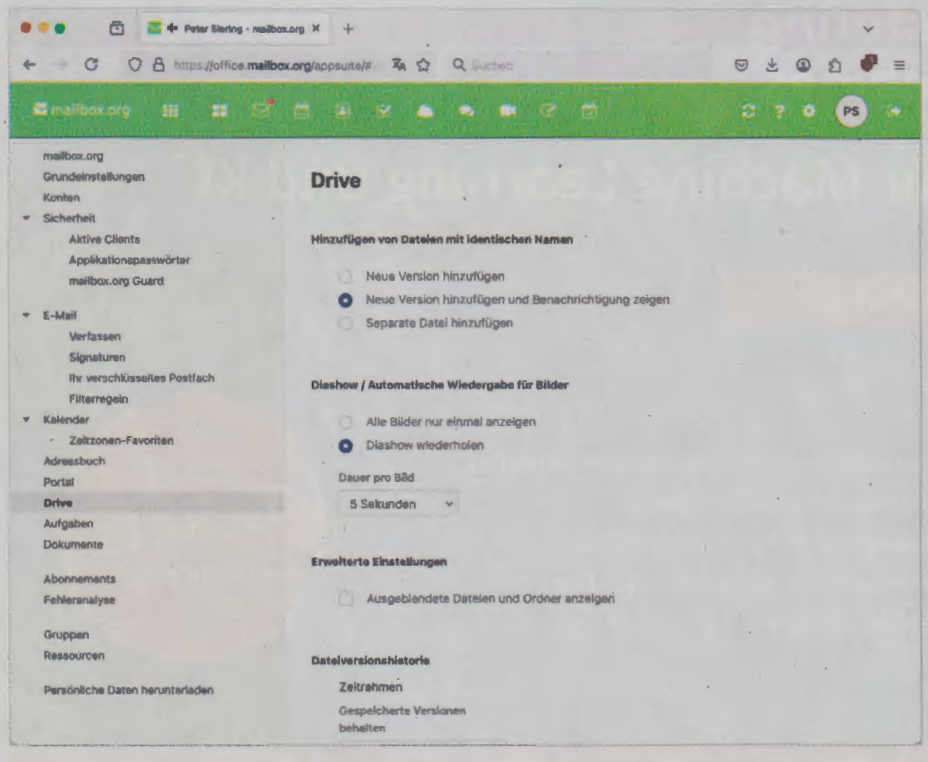
Ein **E-Mail**-Postfach enthält oft sensible Daten. Darin findet sich Persönliches, aber vor allem Hinweise auf Beziehungen zu anderen Personen, Geschäften, Vereinen et cetera. Fast jeder dürfte dort auch kompromittierende Dinge aufheben, etwa Kommunikation über Dritte, die niemals in deren Hand geraten 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



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.

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 Card-DAV). 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 spezialisiert, Nextcloud schlüsselfertig anzubieten [3]. 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.

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 Spionierrerei 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 [4].

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

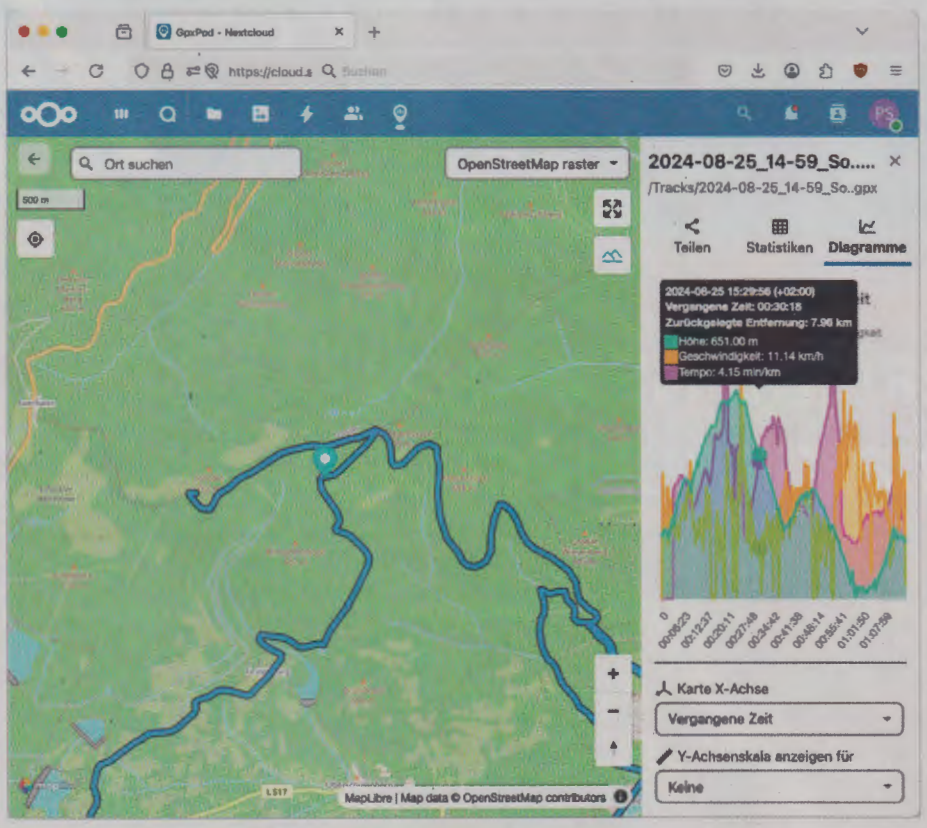
Manche Unabhängigkeit ist trügerisch. Der beliebte Community Store für Home Assistant (HACS), eine Oberfläche, um komfortabel Erweiterungen zu installieren und zu aktualisieren, verwendet unter der Haube GitHub – einen Dienst, den Microsoft für Entwickler betreibt. Die Home-Assistant-Schöpfer nutzen 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.

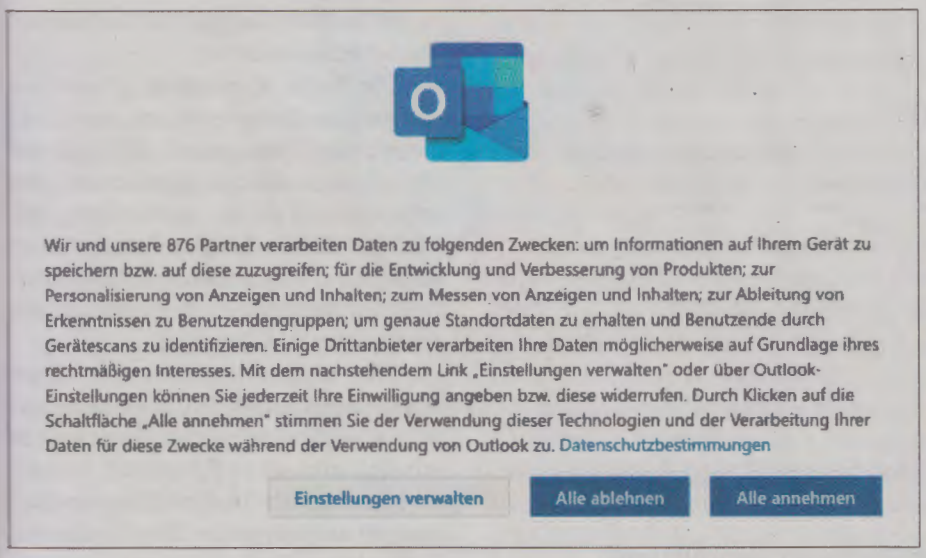
Sie werden während der Nutzung der Geräte später auch wieder darauf hingewiesen, dass ein solches Konto notwendig sein kann. Nehmen Sie dieses Angebot nur an, wenn es sich für Ihre Nutzungsszenarien nicht vermeiden lässt. Ein Beispiel: Apple-Geräte erlauben ohne Anmeldung im AppStore nicht die Installation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



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.



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

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, 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.

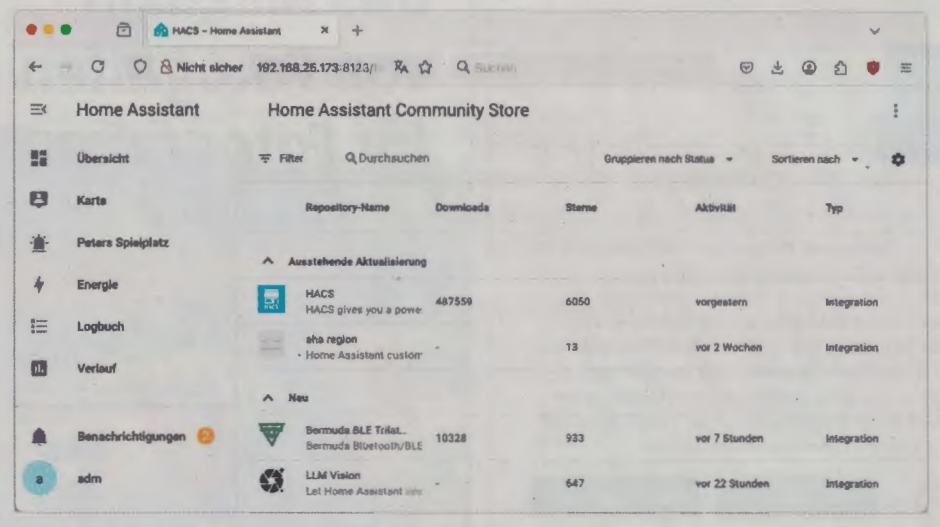
Die Idee, unabhängige Instanzen eines Diensts miteinander in den Austausch zu bringen, ist nicht auf Mastodon beschränkt: Pixelfed verwendet ebenfalls das ActivityPub-Protokoll, um eine Instagram-Alternative auf die Beine zu stellen, die vor allem für Fotofans interessant ist. Mit Radicle gibt es sogar 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 (siehe Seite 118). 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 [5]. 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 Hilfestel-

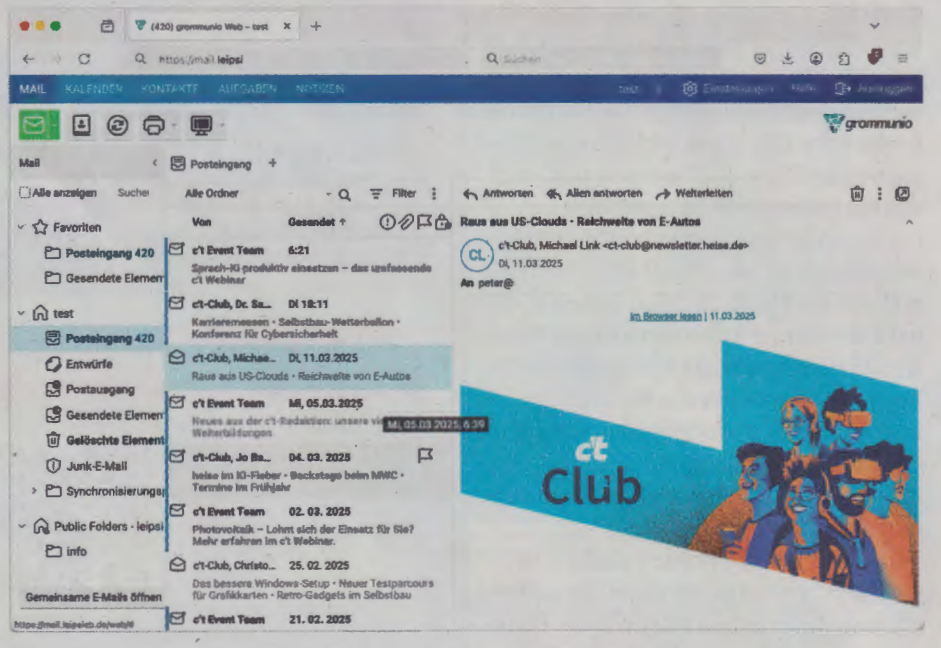


Oft heißt es, genau hinsehen: Der Komfort im Community Store für Home Assistant (HACS) stellt sich erst ein, wenn man eine Anmeldung bei GitHub toleriert – schwupps, unterläuft man die eigenen Vorsätze, das smarte Heim nicht an US-Clouds zu koppeln.

lungen, 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



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.

immer noch viel Google drinsteckt und oft die Sicherheit leidet [6].

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 [7].

Konsequent sein

Für den Weg raus aus der US-Clouddabhängigkeit 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.

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 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@ct.de)* 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] Holger Bleich, Betreute Nextcloud, Marktübersicht: DSGVO-konforme Managed Nextclouds vom Webhoster, c't 14/2024, S. 20

[4] Stefan Porteck, Privater Protokollant, Eigenen Standortverlauf aufzeichnen und anzeigen – ohne Google, c't 15/2024, S. 142

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

[6] 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/

[7] Christian Wölbert, Die Trittbrettfahrer, Wie Behörden und ihre Auftragnehmer Open-Source-Software ausbeuten. c't 6/2025, S. 34

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

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	
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	

Bild: KI, Collage c't

Transatlantischer Drahtseilakt

Wie die EU Recht anpasst, um US-Clouds trotz aller Bedenken nutzbar zu halten

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.

Am 14. März 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 am 24. März) 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 schon sehr bald 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 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. Bis zum Redaktionsschluss dieser Ausgabe war auf Nachfrage keine Reaktion und kein Plan B in Erfahrung zu bringen. 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.

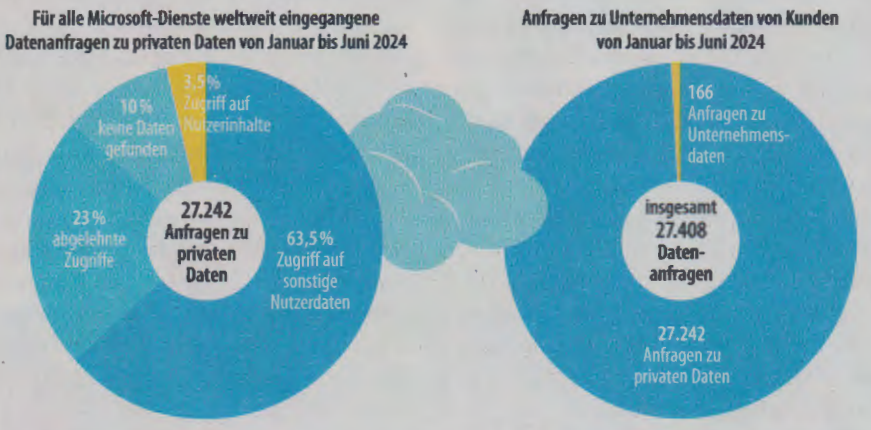
Bild: EU-Kommission

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).

Bild: KI, Collage c't

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

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 insbesondere 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". Anfang Februar hat die polnische Ratspräsidentschaft nun vorgeschlagen, dieses Vorhaben erst einmal ad acta zu legen und stattdessen möglichst bald die freiwillige Kontrolle zu entfristen oder zumindest zu verlängern. Polen war seit jeher ein Gegner der Chatkontrolle. Ob der

polnische Justizminister Adam Bodnar die streitenden Mitgliedsstaaten überzeugen kann, ist bislang offen.

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 vom 27. Februar.

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@ct.de)* 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