c't

SICHER INS NETZ

So sperren Sie Überwacher und Angreifer aus

Schluss mit dem Passwort-Chaos

Accounts mit Zwei-Faktor-Authentifizierung absichern
Passwort und zweiten Faktor richtig einsetzen

Sperren und Zensur umgehen

Test: Elf VPN-Dienste mit WireGuard im Vergleich
Tipps: Mehr Privatsphäre in Windows einstellen

Android sicherer machen

Tracker finden und Datenlöcher stopfen
Apps für mehr Privacy · Custom-ROMs im Test



Bild: Andreas Martini

Anonym surfen

Tor-Browser: Tipps, wie Sie tatsächlich unerkannt bleiben
Mehr Privatsphäre mit schützendem DNS-Proxy herstellen

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

4 197665 614904 02

heise Security TOUR

WISSEN SCHÜTZT

Angriffe auf die IT erfolgreich abwehren

23.06. KÖLN | 28.06. STUTTGART | 05.07. ONLINE



Angesichts eines realen Kriegs gewinnt IT-Sicherheit eine neue Bedeutung. Es geht nicht mehr „nur" darum, gut organisierte Kriminelle abzuwehren; auch Cyber-Angriffe durch staatliche Akteure werden zur realen Gefahr.

Die eintägige Konferenz **heise Security Tour** hilft Ihnen dabei, den Überblick zu bewahren, Maßnahmen zu priorisieren und diese in der Praxis richtig umzusetzen.

DIE THEMEN

- **Lagebild IT-Security**: Auswirkungen des Kriegs, Ransomware, Cybercrime & Co.
- **Datenschutz**: US-Datentransfer, Cookies, Google Analytics
- Erfahrungen eines CISOs mit **Anti-Phishing**
- Sichern der **Supply Chain**
- **Sicheres Backup**: Immutable Storage, Air Gaps und andere Konzepte
- Die **Wahrheit des Patchens**

Ticketpreis Köln oder Stuttgart: 599,-

Ticketpreis Online-Konferenz: 499,-

Jetzt Tickets sichern: heise-security-tour.de

Editorial

Liebe Leserin, lieber Leser,

nicht erst der Krieg in der Ukraine zeigt, wie anfällig das Internet gegen Zensur und Sperren ist: Staaten oder Unternehmen können Inhalte für Nutzer blockieren – sei es aus politischen oder aus rechtlichen Gründen. Sichern Sie Ihre Privatsphäre und entgehen Sie Geolokalisierung sowie Sperren, indem Sie Anonymisierungsdienste richtig einsetzen.

In diesem Heft erfahren Sie, welche Stärken und Schwächen VPN-Angebote haben und welche Dienste wirklich empfehlenswert sind. Wir helfen Ihnen bei der Auswahl der besten Methode für jeden Zweck. Manchmal sollte es gar das technisch überzeugendste, aber etwas weniger komfortable Anonymisierungsnetzwerk Tor sein. Mit unserer Anleitung gelingt der Start in die anonyme Tor-Welt mit jedem Betriebssystem.

Als anfällig für den Abfluss persönlicher Daten erweist sich immer wieder Android, das meistgenutzte mobile Betriebssystem. Nicht nur, dass es selbst Informationen zu Google in die USA pumpt, es gewährt auch Apps umfangreiche Datensammelei. Erfahren Sie, wo Daten abfließen und wie Sie dies verhindern können. Wir stellen App-Alternativen vor und zeigen, wie sich das komplette Smartphone-Betriebssystem gegen eine Privacy-schonendere Variante austauschen lässt.

Alle Bemühungen um mehr Datenschutz und -sicherheit helfen allerdings nichts ohne die richtige Strategie, Online-Konten gegen fremden Zugriff zu schützen. In unserem Leitfaden erfahren Sie, wie Sie Ihre Passwörter einfach gut verwalten und welche zusätzlichen Schutzmaßnahmen der Anbieter tatsächlich sinnvoll sind.

Wir wünschen Ihnen ungestörte und allzeit sichere Reisen durchs Netz.



Holger Bleich

Inhalt

ANONYM IM NETZ

VPN-Anbieter versprechen, geografische Sperren aufzuheben, zensierte Dienste zugänglich zu machen und Anonymität herzustellen. Wir erklären Technik und Fallstricke – und haben elf Anbieter getestet. Den besten Schutz der Privatsphäre bietet das Anonymisierungsnetz Tor. Mit dem Tor Browser und unserer Anleitung gelingt der Einstieg mit jedem Betriebssystem. Vor Lauschern und Angriffen im Surf-Alltag schützt ein eigener DNSCrypt-Proxy.

6 Wie Surfer Sperren und Zensur umgehen
10 VPN: Schutz oder trügerische Sicherheit?
16 Elf VPN-Anbieter im Vergleich
24 Unterschiede gängiger VPN-Varianten
30 Mehr Privatsphäre in Windows einstellen
36 Tor einfach und sicher nutzen
40 Privatsphärenschutz mit DNSCrypt-Proxy

OPTIMAL EINLOGGEN

Sie sind es leid, mit dutzenden Passwörtern zu jonglieren und trotzdem ständig um Ihre Accounts bangen zu müssen? Unser Leitfaden zeigt Ihnen Verfahren und auch Geräte, mit denen Sie ganz einfach Ihre Konten optimal absichern können. Mit der richtigen Strategie hält sich auch der Frust bei Passwort-Verlust in Grenzen.

48 Schluss mit dem Passwort-Chaos
50 Online-Accounts mit 2FA besser absichern
56 Passwort und zweiten Faktor einsetzen
64 Vorbeugen statt Frust bei 2FA-Verlust
68 FAQ: Kennwörter, FIDO2 und TOTP

ANDROID ABER SICHER

Schon einfache Maßnahmen können die Privatsphäre auf Android-Smartphones stark erhöhen. Gewöhnen Sie Apps die Plapperei ab und schließen Sie Sicherheitslücken ganz einfach mit Bordmitteln. Oder gehen Sie ans Eingemachte und tauschen das vorinstallierte Android gegen ein Custom-ROM aus. Wir helfen dabei.

72 Datenlöcher bei Android stopfen
78 Android und Apps datensparsam nutzen
86 Custom-ROMs für Android im Vergleich
94 Android-Apps selbst auf Tracker prüfen

IHR EIGENER MESSENGERDIENST

Es gibt durchaus datenschutzfreundliche Alternativen zu WhatsApp, sogar eine, die man selbst betreiben kann: Ein Matrix-Server ist mit unserer Anleitung schnell aufgesetzt und macht sowohl Privatleute als auch Unternehmen zum Privacy-freundlichen Messenger-Dienst, der sogar Schnittstellen zu herkömmlichen Anbietern ermöglicht.

100 Mit Matrix selbst Chatserver betreiben

108 Andere Messenger an Matrix anbinden

ZUM HEFT

3 Editorial

107 Impressum



Wie Surfer Sperren und Zensur umgehen

Findige Bürger nutzen VPNs, Tor und Anti-Zensur-Dienste, um Internetsperren zu umgehen. Der folgende Überblick zeigt die Stärken und Schwächen der aktuell beliebtesten Tools.

Von **Ronald Eikenberg**



Bild: www.freepik.de

Tools für Privatsphäre und gegen Zensur	6
VPN: Schutz oder trügerische Sicherheit?	10
Elf VPN-Anbieter im Vergleich	16
Unterschiede gängiger VPN-Varianten	24
Mehr Privatsphäre in Windows einstellen	30
Tor einfach und sicher nutzen	36
Privatsphärenschutz mit DNSCrypt-Proxy	40

Das freie und unzensierte Internet, wie wir es kennen, scheint ein Auslaufmodell zu sein: Zunehmend werden Inhalte gesperrt, sei es aus politischer Motivation oder aus Jugendschutzgründen. Was in China durch die Great Firewall Alltag ist, erreicht auch andere Länder, nicht zuletzt Russland. Einen Eindruck davon liefern beispielsweise Daten des Open Observatory of Network Interference (OONI). Sie zeigen, wie der Kreml parallel zum Angriff auf die Ukraine den Zugriff auf die internationale Berichterstattung von BBC, Deutsche Welle und Voice of America einschränkte (siehe ct.de/wh1u).

Dienste wie VPNs oder Tor leisten in solchen Situationen wertvolle Hilfe, wenn man ansonsten vom freien Internet abgeschnitten wäre. Auch in weniger dramatischen Fällen ist es nützlich, dass sie wirkungsvoll die IP-Adresse des Surfers verschleiern und damit für Anonymität und ein Plus an Sicherheit sorgen. So kann man mit ihnen auch Geoblockaden überlisten und so Streaming-Dienste und TV-Stationen nutzen, die ansonsten (meist aus urheberrechtlichen Gründen) nicht empfangbar wären.

Allheilmittel VPN?

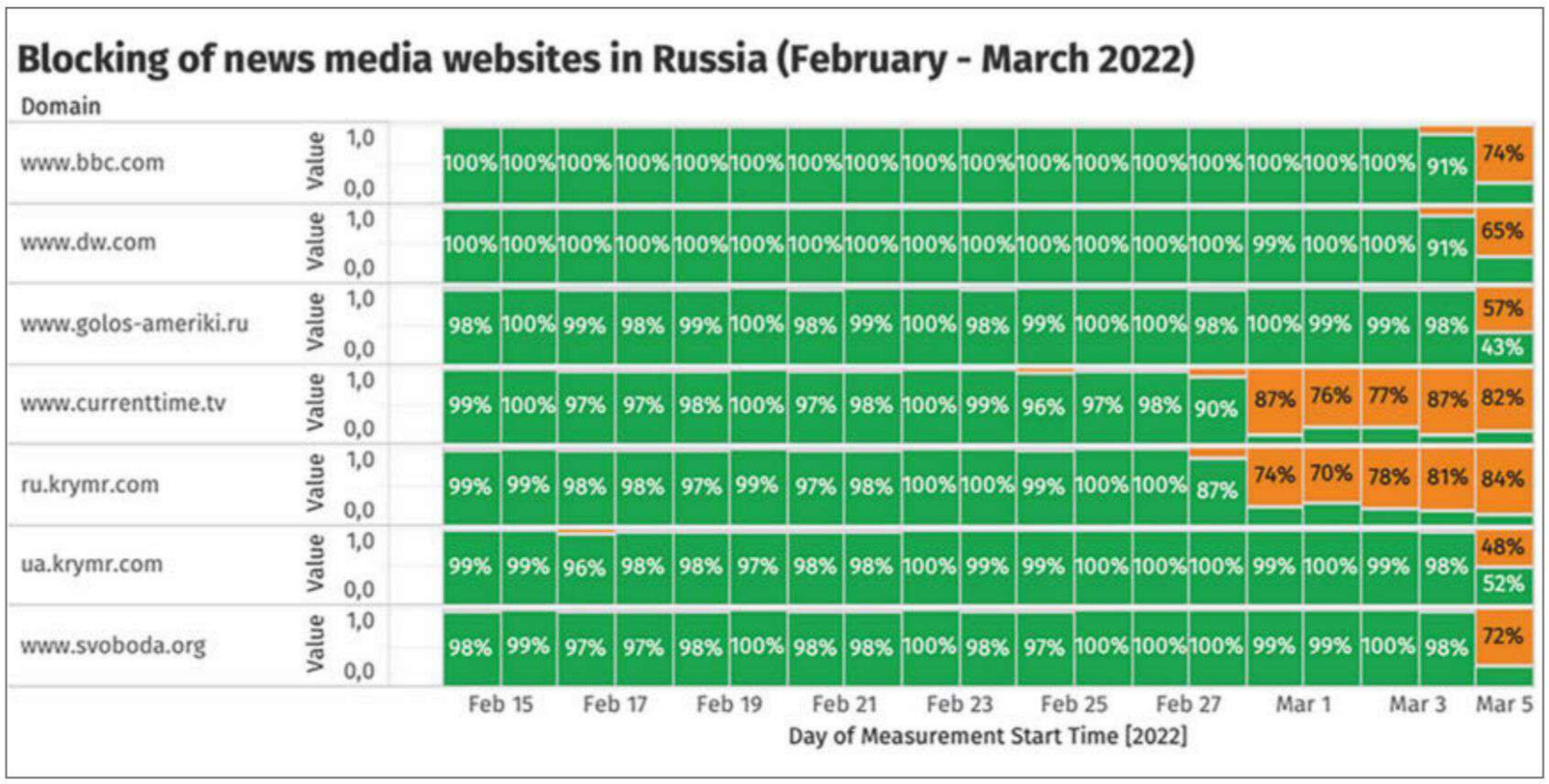
Angesichts der Kriegssituation und der Sperren von Medien verwundert es nicht, dass kurz nach Ausbruch des Krieges VPN-Apps die Top 10 der App-Stores bei Abrufen aus Russland dominierten. Überraschend ist es dennoch, denn in Russland ist der Gebrauch von Methoden, die Sperrungen für unerwünschte Inhalte umgehen, seit 2017 verboten (siehe ct.de/wh1u). Aber anscheinend hat Russland – anders als China – die App-Store-Betreiber bisher nicht zwingen können, VPN-Apps aus dem länderspezifischen Angebot zu tilgen. Außerdem deutet der intensive Gebrauch von VPN-Apps darauf hin, dass der russische Gesetzgeber die Nutzung zumindest nicht merklich ahndet, wenn überhaupt.

Bekannt ist immerhin, dass der Kreml Zugriffe auf einige VPN-Dienste gesperrt hat. Es gibt aber immer noch Ausweichmöglichkeiten zu anderen VPN-Diensten von Unternehmen und Initiativen gegen Zensur. Außerdem kann man Tunnel in Eigenregie aufsetzen, beispielsweise über SSH zu Root-Servern im Ausland.

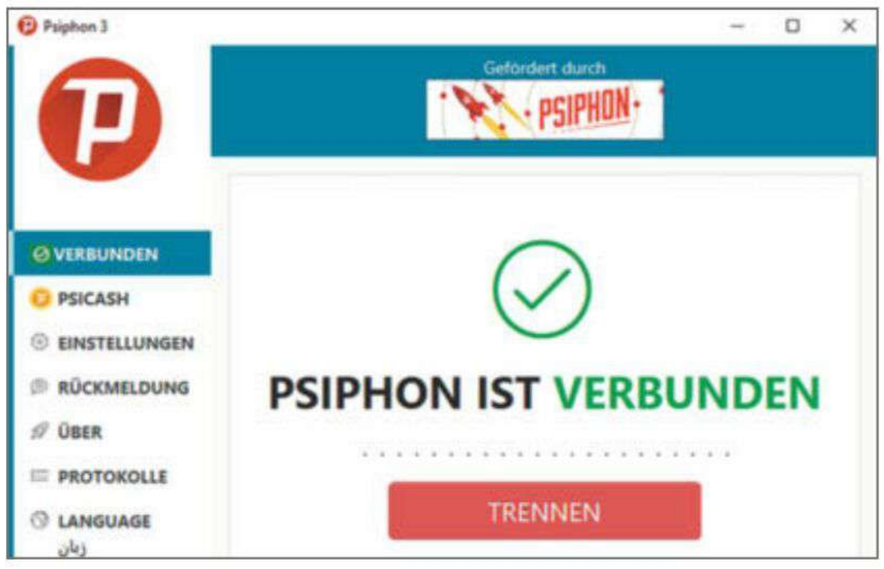
Bei VPN baut man über den lokalen Internetzugang einen verschlüsselten Tunnel zum VPN-Server eines Anbieters auf. Der Server kann in einem beliebigen Land stehen und von dort aus geht der Verkehr weiter ins Internet – fast so, als sei man vor Ort. Wovor ein Zugang zum VPN schützt und wovor nicht, erklärt der Artikel ab Seite 10 im Detail.

Zentrale Erkenntnis: Man muss dem Anbieter vertrauen. Kommerzielle VPN-Angebote sind deshalb

Bild: OONI



Das Open Observatory of Network Interference (OONI) beobachtet seit Ende Februar Anomalien beim Zugriff auf internationale Websites aus Russland.



Die Psiphon-App baut auch unter schwierigen Bedingungen einen Tunnel ins freie Internet auf.

oft nur eingeschränkt empfehlenswert. Auch wenn viele behaupten, die Internet-Bewegungen ihrer Kunden nicht zu protokollieren, überprüfen kann man das nicht. Grundsätzlich ist es eine gute Idee, sich an jene zu halten, die sich beharrlich einen guten Ruf aufgebaut haben und nicht mit aggressiven Rabattaktionen auffallen. Eine Übersicht finden Sie auf den Seiten 22 und 23. Einen soliden Eindruck haben dort zum Beispiel AzireVPN, IVPN und Mullvad hinterlassen. Warum man besonders als Admin bei der Wahl des VPN-Providers auch technisch genauer hinschauen sollte, erfahren Sie im Artikel ab Seite 24.

Abstand nehmen sollte man in aller Regel von Gratisangeboten, denn bei denen gilt der Grundsatz „wenn du nicht der Kunde bist, dann bist du die Ware“. Der Betrieb eines VPN-Servers kostet Geld und das holt sich der Betreiber so oder so. Im besten Fall ist der Gratiszugang ein Lockversuch, um Kunden für kostenpflichtige Abos zu gewinnen, im schlechtesten Fall interessiert sich der Anbieter für die übertragenen Daten.

Man kommt also vom Regen in die Traufe. Es gibt bei den Gratisdiensten aber auch Ausnahmen: Bei spendenfinanzierten VPN-Diensten wie RiseUp VPN geht es den Betreibern darum, Kommunikationswege zu schaffen, die nicht von Unternehmen oder Regierungen kontrolliert werden.

Anti-Zensur-Tool Psiphon

VPN-Traffic ist meist anhand der IP-Adressen der VPN-Server und der Kommunikations-Ports erkennbar. Eine Firewall kann solche Verbindungen leicht identifizieren und blockieren. Mittels Traffic Fingerprinting ist der VPN-Verkehr sogar dann identifizierbar, wenn er unübliche Ports nutzt. Dann helfen spezialisierte Dienste und Tools wie Psiphon weiter.

Durch die weltpolitischen Ereignisse verzeichnete Psiphon jüngst einen deutlichen Anstieg an Nutzern aus Russland, Belarus und der Ukraine. Die quelloffene Anti-Zensur-Software, die aus einem Projekt des Citizen Lab der University of Toronto hervorgegangen ist, probiert mehrere Verbindungswege und Server durch, bis eine Verbindung steht. Zu den Verbindungswegen zählen das VPN-Verfahren L2TP mit IPsec, HTTP-Proxy und Obfuscated SSH (OSSH), welches den Verkehr vor gängigen Fingerprinting-Methoden verbirgt. Die vollständige Serverliste ist dem Client zu keinem Zeitpunkt bekannt, um Zensur zu erschweren.

In der kostenlosen Version liefert der Dienst maximal 2 Mbit/s, was zum Surfen knapp ausreicht. Zudem gibt es moderate Werbung. Mehr Speed und Werbefreiheit kosten ein paar Euro im Monat. Der Client ist auf https://psiphon.ca für Windows, macOS, Android und iOS erhältlich.

Internationale Sender wie BBC und Deutsche Welle (DW), die von den Netzsperren unmittelbar betroffen sind, empfehlen Psiphon, um ungehindert auf deren Nachrichtenangebote zugreifen zu können. In die von der Deutschen Welle angebotenen App „Breaking World News“ ist Psiphon sogar integriert. Schaltet man in den Einstellungen „Proxy aktivieren“ ein, kommuniziert die App über das Anti-Zensur-Netz und ist so auch in Ländern nutzbar, die den üblichen Zugriff auf DW blockiert haben.

Tor zur Welt

Geht es um maximalen Schutz der Privatsphäre, dann ist das Anonymisierungs-Netzwerk Tor das Mittel der Wahl (siehe S. 36). Dabei wird der Traffic zwischen Client und Internet verschlüsselt durch drei zufällig ausgewählte Relays geschleust, die jeweils nur die nächste Zielstation kennen, nicht aber die vollständige Route.

Tor hat allerdings auch Nachteile: Durch die Verschlüsselung und die zusätzlichen Relays nimmt die Signallaufzeit zu, was zu einem deutlich verlangsamten Aufbau von Webseiten führen kann. Und das letzte Glied in der Kette, der Exit Node, ist kritisch: Auch er weiß zwar nicht, für welche Nutzer er arbeitet, kann den Traffic Richtung Internet jedoch mitlesen und manipulieren, was für manche autokratisch regierten Länder bereits belegt wurde. Daher sollte man mit Tor nur transportverschlüsselte Protokolle wie HTTPS nutzen.

Snowflake gegen Tor-Sperren

Auch Tor lässt sich blockieren, etwa durch Firewallsperren für bestimmte Ports. Dann kann man sich behelfen, indem man austauschbare Übertragungsarten (Pluggable Transports) verwendet, die den Tor-Traffic zum Beispiel als Surfverkehr tarnen (siehe ct.de/wh1u). Solche Übertragungsarten kann man in den Einstellungen des Tor-Browsers unter „Bridges“ aktivieren.

Snowflake lebt von freiwilligen Helfern, denn je mehr es davon gibt, desto schwieriger lassen sich die Verbindungen blockieren. Mithelfen kann jeder: Installiert man etwa die Browser-Erweiterung für Chrome oder Firefox (siehe ct.de/wh1u), wird der eigene PC zum Snowflake-Proxy, der anderen Nutzern ins Tor-Netz hilft.

Den Tor Browser gibt es für Windows, macOS, Linux, Android und iOS (siehe https://torproject.org). Wer seinen digitalen Fußabdruck auch auf dem lokalen Rechner so gering wie möglich halten möchte, kann zu dem Live-Linux Tails greifen, das standardmäßig über Tor mit dem Internet spricht.

Alternative DNS-Server

Nicht immer ist es nötig, den kompletten Internetverkehr umzuleiten, um Zensurmaßnahmen zu umgehen. In manchen Fällen werden Web-Zugriffe nur anhand von Filtern in DNS-Servern zensiert. Fragt der PC oder das Smartphone nach einer gesperrten Domain, antwortet der Server, dass er die Domain nicht kennt oder liefert eine falsche IP-Adresse.

In diesem Fall genügt es, einen anderen Server zu konfigurieren, zum Beispiel den zensurfreien DNS-Server von Digitalcourage (siehe ct.de/wh1u). Wer das Mitlesen des DNS-Verkehrs verhindern will, richtet eine verschlüsselte DNS-Kommunikation ein (DNS-over-HTTPS, DoH oder DNS-over-TLS, DoT) [1]. Neuerdings lässt sich die DNS-Kommunikation auch anonymisieren, wie der Artikel ab Seite 40 erklärt.

Fazit

Der freie Zugriff auf Informationen ist keine Selbstverständlichkeit, wie die aktuellen Entwicklungen zeigen. Doch findige Programmierer haben diverse Methoden implementiert, um die Restriktionen zu umgehen. Dabei sind einfache VPN-Dienste nicht immer die beste Wahl, da sie sich leicht blockieren lassen. Anti-Zensur-Tools wie Psiphon oder Tor helfen jedoch auch unter schwierigen Bedingungen. (rei) c't

Literatur

[1] Dušan Živadinović, FAQ: Verschlüsselte DNS-Anfragen, c’t 22/2021, S. 178

Statistiken & Tools

ct.de/wh1u

Do-it-yourself-Security

für Maschinen & Anlagen



Per Firewall Netzwerkbereiche schnell & einfach sichern, ohne Eingriff in IP-Set-Up oder sonstige Einstellungen:

- Reduziert Fehler- & Ausfallrisiko auf ein Minimum
- Ermöglicht Integration & Management ohne Kenntnisse der Netzwerkumgebung

Mach jetzt Nägel mit Köpfen:

wut.de/diy

W&T

www.WuT.de



Bild: Andreas Martini

VPN: Schutz oder trügerische Sicherheit?

VPN-Anbieter versprechen, die übertragenen Daten stets zu verschlüsseln, geografische Sperren aufzuheben und Anonymität herzustellen. Doch auch wenn die Technik selbst über jeden Zweifel erhaben ist, hat sie ihre Tücken. Man sollte sich schon deshalb nicht blind einem Anbieter anvertrauen.

Von **Peter Siering**

Sie haben sicher auch schon davon gehört, dass es ganz einfach sei, gesperrte Serien oder Sportereignisse in einem Streamingportal über ein VPN anzusehen. Sie sind bestimmt schon davor gewarnt worden, offene WLANs ohne VPN zu verwenden, weil Ihre Daten dann leicht abhörbar durch den Äther fliegen. Sie haben vielleicht auch mal darüber nachgedacht, anonym ins Internet zu gehen, um sich die dunkle Seite der Macht anzusehen, und haben dazu VPN-Anbieter empfohlen bekommen. Doch ist das immer eine gute Wahl und welcher Anbieter ist seriös?

Anvertrauen

Virtual Private Network (VPN) als Technik baut verschlüsselte Tunnel zwischen Netzwerken auf. Ursprünglich diente daws vor allem dazu, Netze über unsichere Verbindungen zu koppeln und mobile Nutzer (Road Warriors) sicher ins Firmennetzwerk zu holen. Beim Firmeneinsatz ist das Verhältnis eindeutig: Der Firmenadmin, der dazu die Zugangsdaten oder Schlüssel ausgibt, wird zumeist vertraglich vom Arbeitgeber zu Vertraulichkeit verpflichtet. VPN-Anbieter hingegen erlegen sich solche Pflichten

selbst auf. Kunden sollten deswegen wissen, dass die Anbieter stets alle Schlüssel kennen, um Klartext mitzulesen.

Dass das keine theoretische Möglichkeit ist, sondern in der Praxis ausgeschöpft wird, um aus den Nutzungsdaten Profit zu schlagen, ist kein Geheimnis: Bei VPN-Anbietern, die ihre Dienste kostenlos anbieten, besteht darin oft das Geschäftsmodell. Sie machen daraus nicht mal einen Hehl, sondern gestehen das in Geschäftsbedingungen und Datenschutzerklärung ein. Aber nicht jeder: Facebook kaufte 2013 den Dienst Onavo mit seinem VPN-Angebot und nutzte ihn heimlich zum Sammeln von Nutzerdaten. 2019 verschwand das Angebot.

Doch nicht nur mit den Daten wird getrickst. Es tauchen immer mal wieder auch Anbieter auf, die VPN kreativ interpretieren. 2015 machte die Runde, dass der Anbieter Hola die Internet-Anschlüsse der Kunden seines Gratisangebots benutzt, um dort den Datenverkehr anderer Kunden auszuleiten. Das klingt auf den ersten Blick elegant, aber hat rechtliche Implikationen. Wenn nämlich ein anderer VPN-Nutzer Urheberrechtsverletzungen begeht, könnten sich die auf den Plan gerufenen Anwälte an den nichts ahnenden Anschlusseigner halten. In der FAQ weist Hola auf die Technik hin, ohne aber vor möglichen Gefahren zu warnen. Zahlende Kunden sollen nicht betroffen sein.

Misstrauen

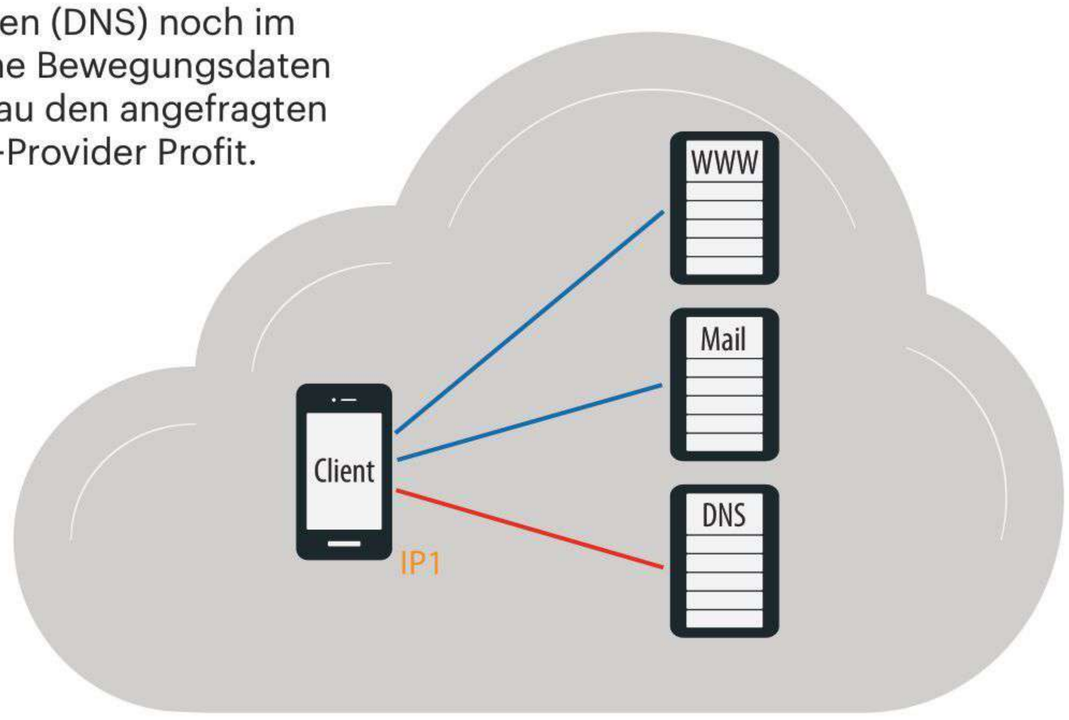
Wer vorschnell zu einem VPN-Angebot greift, läuft also Gefahr, über den Tisch gezogen zu werden. Besonders gilt das, wenn man sich an einer der vielen im Internet zugänglichen Bestenlisten orientiert. Viele dieser Sites leben vom Affiliate-Geschäft, also von Provisionen, die der Betreiber erhält, wenn ein Besucher direkt per Link in den Shop des VPN-Providers hüpft. Der eine oder andere VPN-Provider wirbt unterdessen damit, dass er sich an diesem Zirkus nicht beteiligt. All das sind Indizien, die bei der Wahl eines geeigneten VPN-Providers helfen können. Wir haben uns elf VPN-Provider genauer angesehen und stellen deren Angebote ab Seite 16 im Detail vor.

Alle, die gern tüfteln, können auch einen eigenen VPN-Dienst aufsetzen: Dazu braucht man entweder einen Router, der das schon von sich aus beherrscht, oder einen dauerhaft laufenden Computer wie einen Raspi. Ihr VPN-Tunnel überbrückt dann fremde Netze, etwa unverschlüsselte WLANs im Hotel, bis zu Ihrem Heimnetzwerk. Erst dort wird der verschlüsselte

Ohne VPN mit TLS

Wenn heute ein PC oder ein Smartphone Internet-Dienste anspricht, geschieht das in der Regel verschlüsselt. Die globale IP-Adresse des Clients ist den angesprochenen Servern bekannt. Web- und E-Mail-Server lassen sich heute nicht mehr auf Klartextverbindungen ein. Häufig aber laufen Namensanfragen (DNS) noch im Klartext durchs Netz. So entstehen schon recht umfangreiche Bewegungsdaten eines Surfers. Obendrein verpetzt der TLS-Verbindungsaufbau den angefragten Hostnamen (SNI). Aus solchen Daten schlagen dubiose VPN-Provider Profit.

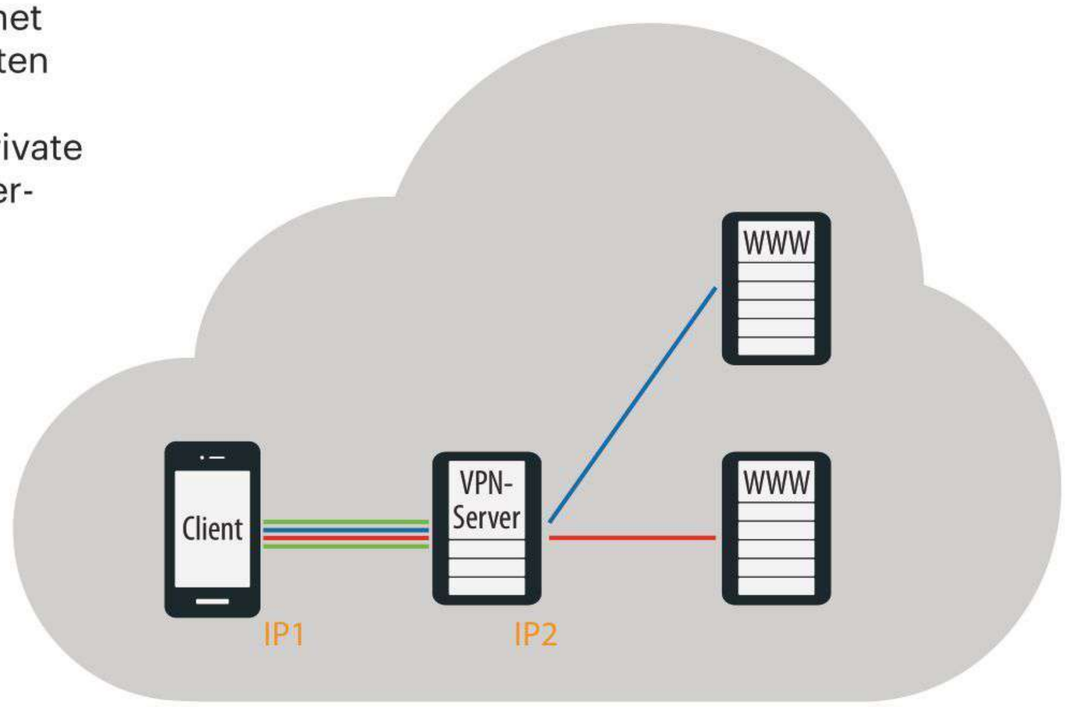
IPX unterschiedliche, globale IP
— verschlüsselte Verbindung (TLS)
— unverschlüsselte Verbindung



Mit VPN

Ein VPN-Tunnel verschlüsselt alle darin transportierten Daten. Aber der Tunnel führt letztlich nur von einer Stelle im Internet zu einer anderen. Hinter dem VPN-Server reisen Klartextdaten lesbar weiter. Die angesprochenen Server erfahren nur die IP-Adresse des VPN-Servers. Viele Schaubilder zu Virtual Private Networks tun so, als würde ein Client erst durch die VPN-Verbindung Zugriff aufs Internet erhalten, aber das ist falsch: Der Client benutzt seinen Internet-Zugang ja schließlich, um auf den VPN-Server zuzugreifen.

IPX unterschiedliche, globale IP
verschlüsselte Verbindung (TLS)
verschlüsselte Verbindung (VPN-Tunnel)
unverschlüsselte Verbindung



Verkehr entpackt und gelangt über den dortigen Anschluss ins Internet. Dadurch entstehen keine Kosten und Sie müssen sich nicht Dritten anvertrauen. Hilfestellung in Form von c't-Artikeln finden Sie unter ct.de/wn14.

Für all diejenigen, die schon dem eigenen Internet-Provider misstrauen, ist das keine Lösung. Wenn Sie Ihre Aktivitäten hinter den IP-Adressen eines VPN-Providers verstecken wollen, dann müssen Sie sich eben solchen Angeboten anvertrauen. Oft aber ist der Gewinn, den sich Kunden dadurch versprechen, ein Irrtum: Die IP-Adresse, mit der Sie sich im Internet bewegen, lässt vor allem dann Rückschlüsse auf Sie zu, wenn es hart auf hart kommt und sich jemand mit juristisch berechtigtem Interesse bemüht, Ihre Identität ermitteln zu lassen. Internet-Provider geben Ihre Daten dann heraus. VPN-Provider behaupten, das nicht zu tun.

Für die Betreiber von Websites und anderen Diensten ist eine IP-Adresse nicht so sehr viel wert. Zum einen verbergen sich hinter einer Adresse oft viele Nutzer, zum anderen wechselt sie häufig. Bei IPv6 sorgen die Privacy Extensions dafür, dass Windows alle 12 Stunden die Adresse ändert. So haben die Anbieter längst bessere und perfidere Methoden entwickelt, Benutzer wiederzuerkennen. Erst wenn man sich auf das mühsame Unterfangen eingelassen hat, all diese Plagegeister aus dem Fell zu schütteln (siehe ct.de/wn14), gewinnt man noch mehr Anonymität durch das Verschleiern der IP-Adresse per VPN.

Einen Vorteil verspricht eine andere IP-Adresse allerdings: Dienste erkennen nicht mehr zwangsläufig, in welcher geografischen Region der Internetanschluss liegt. Anhand der Adresse lässt sich das nämlich ziemlich exakt bis hinunter zur Stadt ermitteln. Größere VPN-Provider betreiben weltweit mehrere tausend Server, sodass ihre Kunden sich gezielt auf andere Kontinente begeben können – jedenfalls denken die Dienste das anhand der IP-Adresse, die sie zu sehen bekommen.

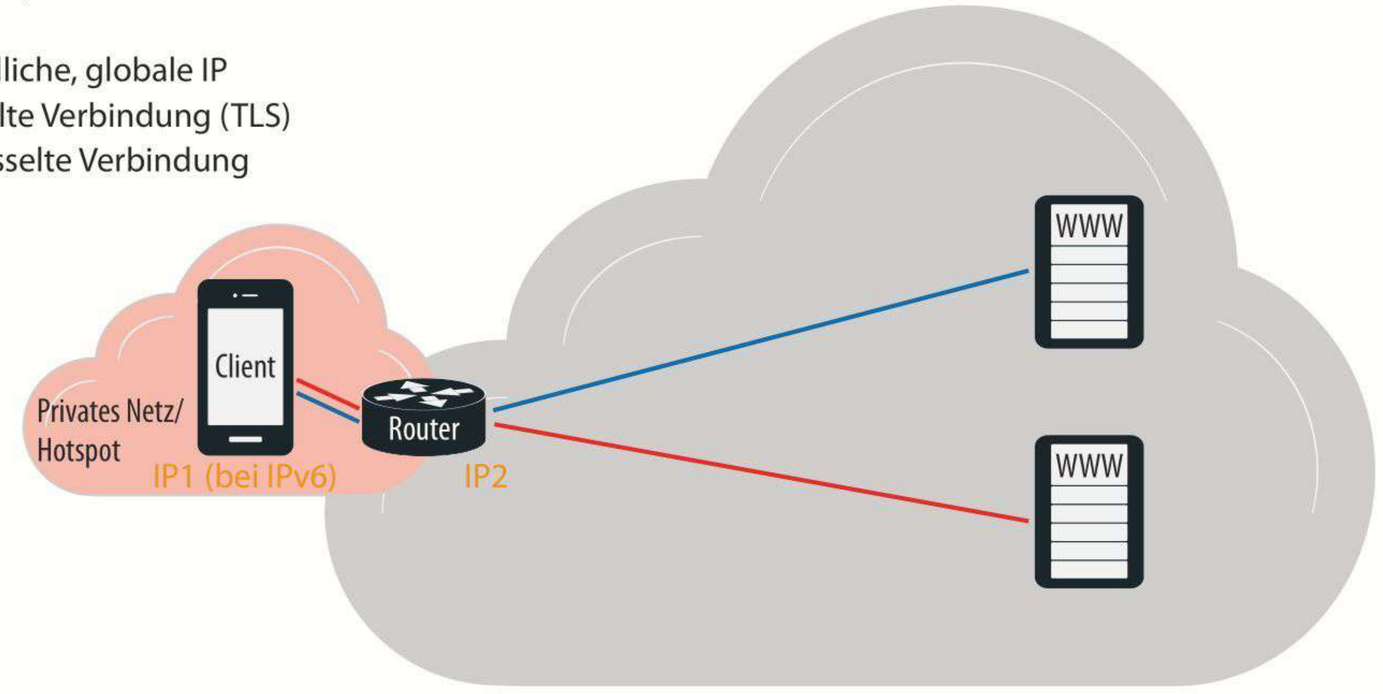
Urvertrauen

Anbieter von urheberrechtlich geschütztem Material, das noch dazu unterschiedliche Veröffentlichungstermine auf verschiedenen Kontinenten oder in verschiedenen Ländern hat – Streamingdienste oder lokale Mediatheken –, haben sich allerdings längst auf die VPN-Trickserei eingestellt. Sie blockieren Zugriffe, die von ihnen bekannt gewordenen VPN-Servern stammen. Allzu schwer ist das nicht, weil die von den Providern in Rechenzentren angemieteten Server typischerweise andere IP-Adressbereiche verwenden als die Kunden, die von ihren DSL-, Kabel- und Glasfaseranschlüssen aus die Angebote nutzen.

Eigene IP ohne VPN verstecken

Offene WLAN-Hotspots, viele Mobilfunkprovider oder andere große Netzwerke, die Clients eine private IP-Adresse verpassen, erreichen einen ähnlichen Effekt wie ein VPN-Server: Ein aufs Internet zugreifender Client versteckt sich in der Masse der anderen Clients hinter der öffentlichen IP-Adresse dieses Netzes. Wie detailliert der Betreiber protokolliert und ob er einen konkreten Nutzer zu fassen bekommt, dazu gibt es meist keine Auskunft. VPN-Provider versprechen, das nicht zu tun. Im Fall globaler IPv6-Adressen, wie sie Mobilfunkprovider heute vergeben, funktioniert das Verstecken nicht.

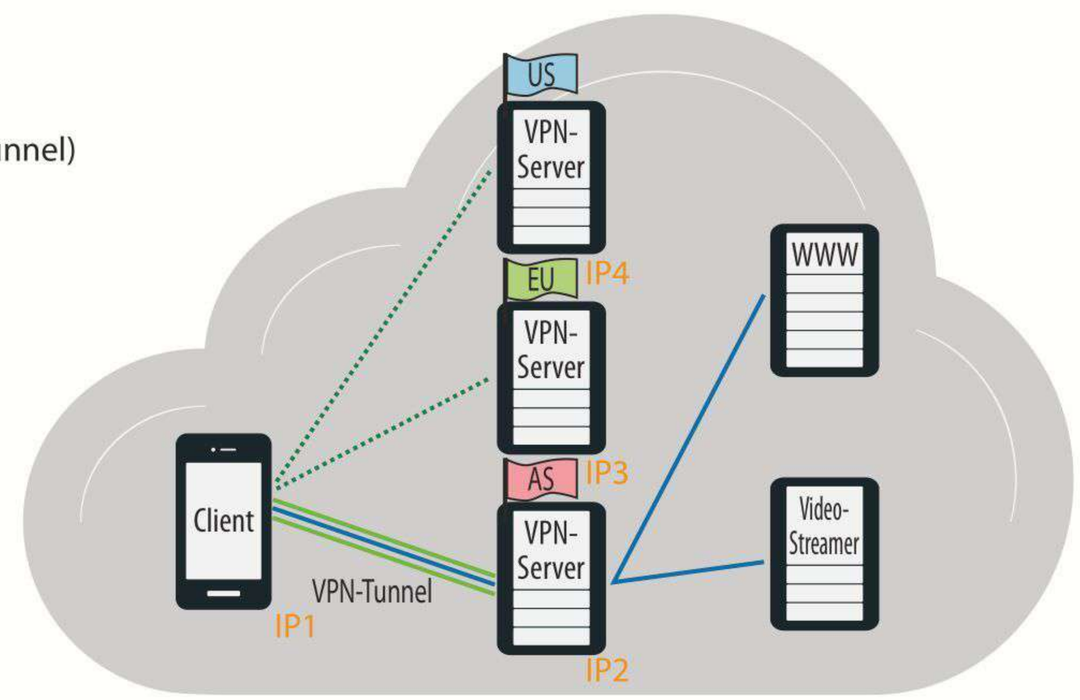
IPX unterschiedliche, globale IP
verschlüsselte Verbindung (TLS)
unverschlüsselte Verbindung



Virtuelle Ortswechsel per VPN

VPN-Provider betreiben Server in vieler Herren Länder. So erhält der Kunde eine IP-Adresse, die Internet-Dienste dem Land zurechnen. Videostreaming-plattformen werten die aus. Allerdings pflegen die auch Blacklisten mit den IP-Adressen der VPN-Server, sodass ein Zugriff auf die Plattform über das VPN früher oder später misslingt.

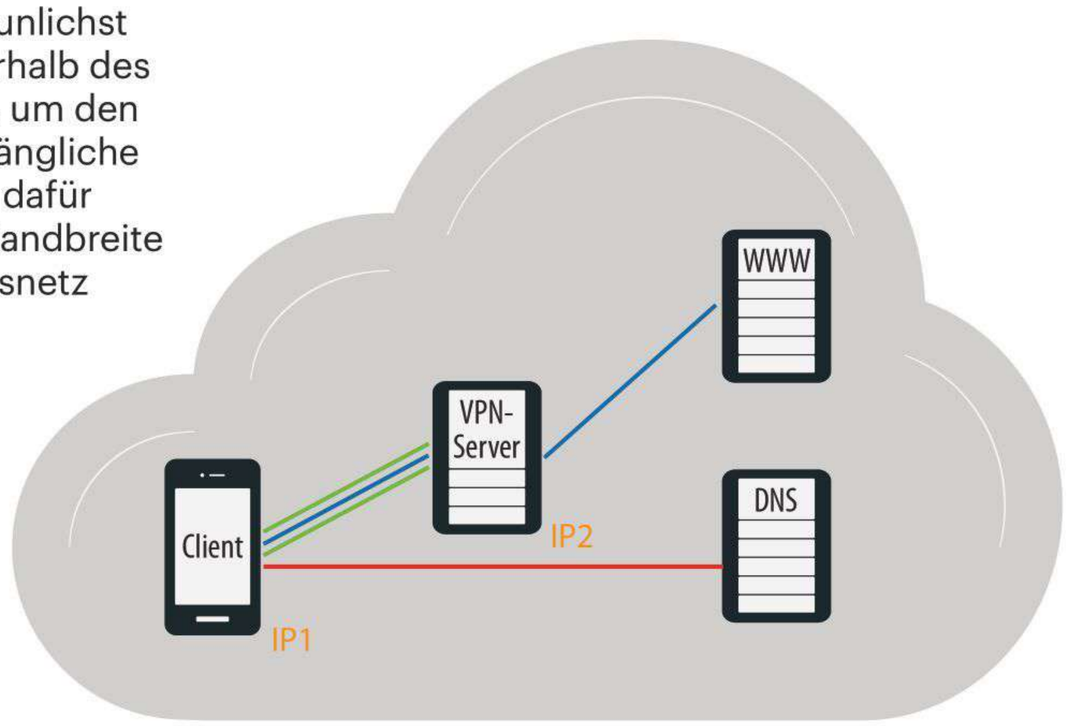
IPX unterschiedliche, globale IP
verschlüsselte Verbindung (TLS)
verschlüsselte Verbindung (VPN-Tunnel)
alternative Verbindung (VPN)



Split-Tunneling im VPN

Wer sich hinter einem VPN-Server verstecken möchte, sollte tunlichst vermeiden, dass – vom VPN-Verkehr abgesehen – Daten außerhalb des Tunnels den Client verlassen. Schon ein Paket könnte reichen, um den Schutz auffliegen zu lassen. DNS-Anfragen oder nicht vollumfängliche IPv4- und IPv6-Unterstützung durch das VPN können Ursache dafür sein. Firmen schätzen hingegen das Verhalten, wenn Sie die Bandbreite Ihres VPN-Servers schonen wollen: Nur der fürs Unternehmensnetz gedachte Verkehr fließt dann durch den Tunnel.

IPX unterschiedliche, globale IP
— verschlüsselte Verbindung (TLS)
— verschlüsselte Verbindung (VPN-Tunnel)
— unverschlüsselte Verbindung



Von der Tatsache, heute mit einem VPN-Provider hierzulande noch nicht erhältliche US-Serien ansehen zu können, sollte man nicht auf Morgen schließen. Wer das allzu voreilig tut und stark rabattierte Zwei-Jahres-Verträge abschließt, tappt in die Muckibudenfalle des Internet. Obendrein: Viele VPN-Provider brüsten sich zwar mit einer riesigen Zahl von Servern weltweit. Gezielt ansteuern kann man die aber oft nicht – die Provider versuchen, Kunden gleichmäßig auf die Server zu verteilen, sodass man mit Pech und ohne Handarbeit vielleicht nur an die Server gerät, die auf Blacklisten stehen.

Apropos Handarbeit: Achten Sie darauf, die Dienste eines VPN-Providers ohne dessen Spezialsoftware nutzen zu können. Zum einen können Sie so selbst beeinflussen, mit welchem seiner VPN-Server Sie sich verbinden. Zum anderen stellen Sie so sicher, dass der Betreiber keine Extras einbaut, etwa Ihren Internetanschluss andere Kunden mitbenutzen lässt (wie das eingangs erwähnte Hola). Im Zweifel ist die offizielle Software der Open-Source-Projekte wie WireGuard oder OpenVPN oder die bereits in Client-Betriebssystemen integrierte VPN-Zugangssoftware die beste Wahl.

Wenn Sie dieser Empfehlung folgen, vergeben Sie ein viel gepriesenes Feature, den sogenannten Kill-Switch. Darunter verstehen die VPN-Provider eine Funktion, die sicherstellen soll, dass sämtliche Daten von Ihrem Client nur durch den VPN-Tunnel fließen. Bei einer VPN-Störung sollen so – für den Nutzer womöglich unbemerkt – keine Daten über den regulären Internetzugang des Clients laufen. Vom Prinzip her ist das eine gute Idee. Wer das aber wirklich in Perfektion braucht, sollte das anders sicherstellen: Filterregeln auf Ihrem DSL-Router, die nur Verbindungen zum VPN-Server zulassen, sind aus unserer Sicht weitaus vertrauenswürdiger.

Ähnliches gilt auch für die weiteren Extras, mit denen einige VPN-Provider ihren Nutzwert aufhübschen wollen: Sie betreiben eigene, filternde DNS-Server, um ihren Kunden Werbung vom Hals zu halten. Aus unserer Sicht sind solche Angebote eine gute Idee. Aber sie zahlen sich vor allem dann voll aus, wenn sie unabhängig betrieben werden – also ohne etwaige andere Interessen. Wenn Sie wirklich darauf angewiesen sind, sich maximal zu schützen, bieten sich vertiefende Artikel aus c’t an, die Sie als Digitalabonnent über den Link erreichen (siehe ct.de/wn14). Betreiben Sie gegebenenfalls einen eigenen filternden DNS-Server wie Pi-Hole oder Adguard und lassen Sie den verschlüsseltes DNS verwenden (siehe ct.de/wn14).

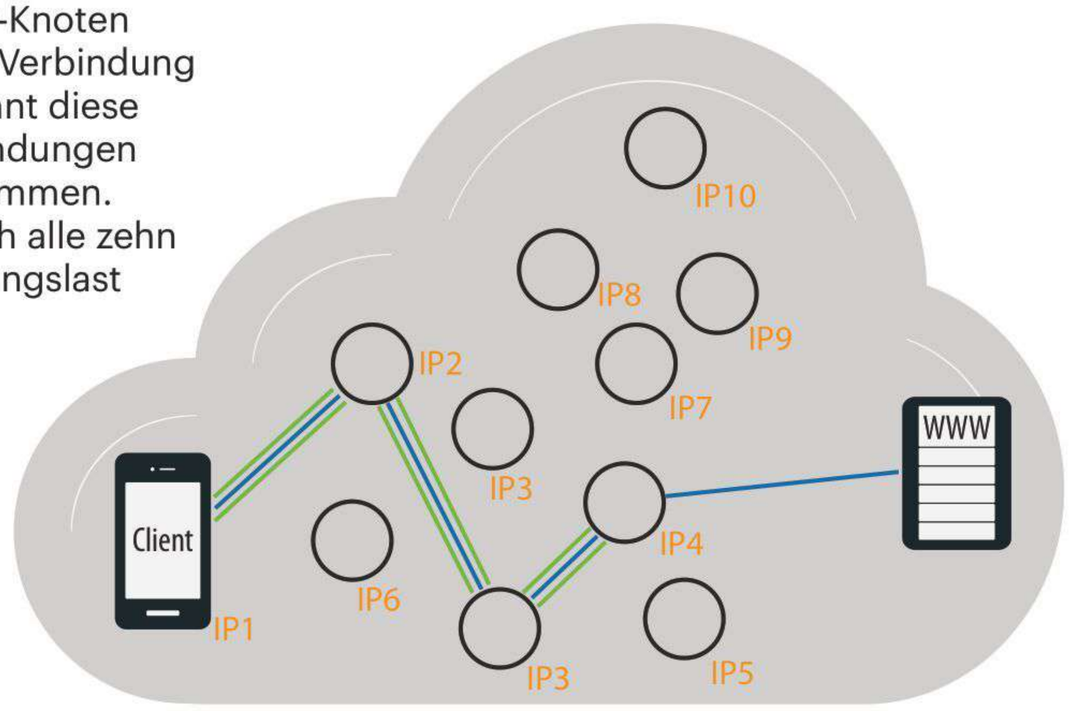
Vertrauen

Auch wenn gegenüber den VPN-Providern eine Grundskepsis angebracht ist, liefern sie doch einen sinnvollen und durchaus empfehlenswerten Dienst:

Tor als VPN-Alternative

Im Tor-Netzwerk wählt ein Client aus der Gesamtzahl der Tor-Knoten einen Eintritts-, Vermittlungs- und Austrittsknoten. Auf jeder Verbindung kommt ein anderer Schlüssel zum Einsatz. Nur der Client kennt diese und gibt jeweils einen an den beteiligten Node weiter. Verbindungen scheinen stets von der IP-Adresse des Austrittsknoten zu stammen. Der Knoten und damit die IP-Adresse ändert sich automatisch alle zehn Minuten. Die vielen beteiligten Knoten und die Entschlüsselungslast verlangsamen den Datenfluss.

IPX unterschiedliche, globale IP
verschlüsselte Verbindung (TLS)
verschlüsselte Verbindung (via Tor)
Tor-Nodes



Vertiefende Artikel

ct.de/wn14

Sobald Sie sich mit Ihren Geräten in einem öffentlichen, offenen, nicht verschlüsselten WLAN bewegen, sollten Sie das nur mit einer VPN-Verbindung tun. Die stellt sicher, dass alle Daten verschlüsselt sind, die Ihr Client verschickt und empfängt. Selbst wenn Sie sich versehentlich in den Maschen eines Netzes verfangen, das Bösewichte mit dem Ziel betreiben, Daten abzufischen, wären Sie dann sicher.

Sollte Ihr Ziel sein, unerkannt im Internet aktiv zu werden, sind VPNs ein zweifelhaftes Mittel: Wie Ihr Internet-Provider kennt der VPN-Betreiber meist Ihre Identität. Wie haltbar seine Versprechen sind, nichts zu protokollieren und die Identität seiner Kunden nicht preiszugeben, ist meist unbelegt. Hinweise, dass einzelne VPN-Server übernommen worden sind, gibt es. Ob das genügt, um Ihre Identität aufzudecken, steht auf einem anderen Blatt. Mit Tor (siehe S. 36) oder auch offenen WLANs, die von nicht kommerziellen Initiativen wie Freifunk betrieben werden, gibt es gute Alternativen. Keine der Methoden garantiert jedoch unter allen Umständen Anonymität beim Surfen und anderen Aktivitäten. (ps) c't

Es gibt 10 Arten von Menschen.
iX-Leser und die anderen.



Jetzt Mini-Abo testen:
3 Hefte + Tastatur nur **19,35 €**

www.iX.de/testen

www.iX.de/testen
49 (0)541 800 09 120
leserservice@heise.de

iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK



Bild: Andreas Martini

Elf VPN-Anbieter im Vergleich

Intransparente Rabatte, vollmundige Versprechen, fragwürdige Werbeprogramme: Die VPN-Branche gibt kein gutes Bild ab, dabei geht es doch um Vertrauen. Wer genau hinschaut, findet aber auch datenschutzfreundliche VPN-Anbieter mit klaren Tarifen und nützlichen Funktionen.

Von **Keywan Tonekaboni**

Wenn das Internet die Datenautobahn ist, dann sind die VPN-Anbieter die Gebrauchtwagenhändler des Internets. Es gibt unzählige Anbieter mit teils sehr großspurigen Versprechen zu Anonymität, Privatsphäre und Sicherheit. Dabei sind einige der vollmundigen Behauptungen schlicht falsch und andere lassen sich nicht verifizieren.

Dieser Artikel soll etwas Klarheit in die trübe VPN-Angebotssuppe bringen. Der Fokus liegt auf Anbietern für Privatpersonen, die sich in öffentlichen WLANs schützen wollen oder sich im Netz mit einer

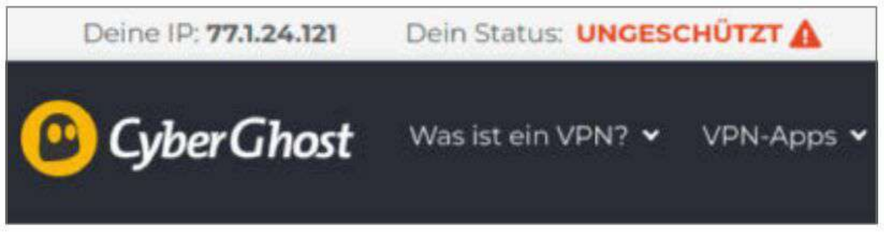
im Ausland verorteten IP-Adresse bewegen möchten. Wir erklären, worauf es bei der Auswahl eines VPN-Anbieters ankommt und von welchen gewagten Werbeaussagen Sie sich nicht blenden lassen sollten.

Wer ein VPN verwenden möchte, muss dem Anbieter vertrauen. Was auf dem Server passiert, bleibt für Außenstehende verborgen. Daher sollte zumindest der Verbindungsaufbau so transparent wie möglich sein. Unsere Übersicht haben wir deshalb auf solche Dienstleister eingeschränkt, die Verbindungen mittels WireGuard über die im Betriebssystem integrierte VPN-Funktion oder die Zugangssoftware des WireGuard-Projekts anbieten. Dazu müssen die Anbieter die VPN-Konfiguration oder Zugangsdaten bereitstellen. WireGuard ist sicher, schnell und besonders für den mobilen Einsatz geeignet [1]. Anbieter, die den Quelltext ihrer eigenen Zugangssoftware veröffentlicht haben, haben wir ebenfalls mit aufgenommen.

Wir haben elf Anbieter ausgemacht, die diesen Kriterien entsprechen: AzireVPN, Hide.me, IVPN, Mullvad, OVPN, Private Internet Acccess (PIA), ProtonVPN, StrongVPN, VPN.AC, WeVPN und Windscribe. Anbieter wie CyberGhost oder NordVPN fielen durchs Raster, da sie WireGuard nur mit eigenen Apps zulassen; Mozilla VPN verkauft Mullvads Dienste zu höheren Kosten. Was uns bei diesen Anbietern aufgefallen ist, haben wir dennoch im Text festgehalten.

Marktschreier

Viele VPN-Anbieter arbeiten zum Ankurbeln der Nachfrage mit Affiliate-Marketing. Blogs und Websites mit fadenscheinigen Produkttests erhalten für Empfehlungen eine Vergütung. Das ist an sich nicht verwerflich, wenn dies dem ratsuchenden Publikum transparent gemacht wird. Das ist leider nicht immer der Fall, beziehungsweise sind die Hinweise darauf sehr versteckt. Zudem besteht die Gefahr, dass die Aussicht auf eine Provision das Testergebnis beeinflusst. Das geht sogar so weit, dass in einem Test von WireGuard-Anbietern ein VPN-Provider gewinnt, der der über WireGuard überhaupt keinen Zugang bereitstellt. Firmen wie IVPN oder Mullvad lehnen dieses Geschäftsgebaren als unseriös ab und haben ihre Affiliate-Programme, wenn überhaupt vorhanden, eingestellt (siehe ct.de/w7mk).



Mit Warnungen versuchen VPN-Anbieter, zum Abschluss eines Abonnements zu drängen.

Neben mutmaßlich gekauften Reviews und massiver Werbung in sozialen Netzwerken nutzen VPN-Anbieter noch eine weitere Masche: das Spiel mit der Angst. Wer die Webseiten von VPN-Anbietern besucht, sieht häufig eine auffällige Warnung: Die eigene Internetverbindung oder IP-Adresse sei ungeschützt. Um die Behauptung zu bekräftigen, enthält die Warnung der IP-Adresse zugeordnete Daten wie den Internet-Provider oder den vermuteten geografischen Standort. Daneben heißt es in markigen Aussagen, nur der angebotene VPN-Dienst biete Schutz, damit niemand in den Datenverkehr reinschauen kann. Dass sowohl der VPN-Anbieter selbst als auch Lauscher auf dem Weg zwischen VPN-Gateway und Zielhost weiter Einblick in den Datenstrom haben können, verschweigen die Marketing-Sprüche hingegen oft. Deutschsprachige Kundinnen und Kunden werden außerdem mit angeblich erhöhtem Datenschutz geködert.

Dagegen fragt IVPN prominent auf der eigenen Startseite „Brauchen Sie wirklich ein VPN?“ und rät explizit vom unnötigen Einsatz eines VPN-Dienstes ab. Anonymität, Schutz vor Internetkriminalität und Datensammlern wie Facebook oder Google gewährleiste ein VPN nicht. Nur wer seinem Internet-Provider nicht vertraue oder Schutz vor einem Angreifer in einem ungeschützten Netzwerk suche, oder Zensur und Geoblocking umgehen wolle, solle einen VPN-Dienst buchen.

Manchen Menschen geht es aber gar nicht um Privatsphäre, sondern um den Zugang zu medialen Inhalten, wie ausländischen Streamingangeboten, etwa Netflix USA oder dem BBC iPlayer. Auch diese Klientel umwerben die VPN-Anbieter. Sie listen auf, welche der eigenen Server sich dafür besonders eignen. StrongVPN geht sogar so weit, detailliert zu erklären, wie man eine gefälschte Rechnungsadresse erzeugt, um sich bei einem US-Streaming-Dienst anzumelden.

Keiner der Anbieter blockiert P2P-Filesharing und Torrent-Software, obwohl deren Nutzung rechtlich meist unzulässig ist. Vielmehr ist es wohl ein Verkaufsargument. IVPN bittet lediglich höflich

darum, für Filesharing nicht die US-Server zu verwenden; aufgrund zahlreicher Urheberrechtsbeschwerden (DMCA Takedown Notices) seien die von einer Abschaltung bedroht. Windscribe missbilligt floskelhaft den Einsatz seines Dienstes für illegale Aktivitäten, während es an anderer Stelle penibel erklärt, wie man Torrents sicher und ohne Sorge vor juristischer Verfolgung nutzt. Ähnliche Anleitungen stellen auch Hide.me und OVPN bereit. VPN.AC gibt Tipps, welche Server für Filesharing die beste Anbindung haben und CyberGhost hat in seiner Zugangssoftware eine eigene Kategorie dafür.

Tunnel ins Steuerparadies

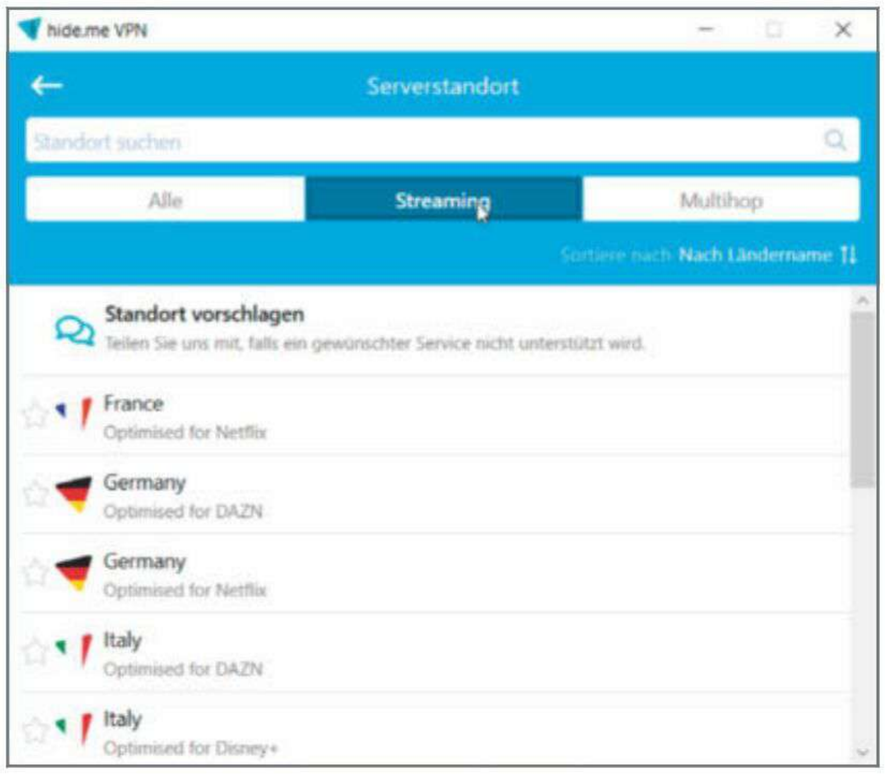
Die Firmensitze der VPN-Anbieter lesen sich wie eine Liste bekannter Steueroasen: Britische Jungferninseln, Gibraltar, Malaysia oder Panama. Dadurch hoffen die Anbieter, sich dem Zugriff der Sicherheitsbehörden und der Justiz aus den USA, der Europäischen Union und anderen Ländern zu entziehen. Wer vor hiesigen Behörden zu solchen Firmen flüchtet, darf anderseits aber auch nicht auf europäisches Verbraucherschutzrecht hoffen. Oft fehlt es schon an einem Impressum, Kontaktdaten oder klaren Angaben, welche Firma hinter dem Angebot steckt.

Es gibt aber auch etliche Anbieter aus der EU: AzireVPN und Mullvad aus Schweden, VPN.AC aus Rumänien. Beide Länder haben den Ruf einer datenschutzfreundlichen Gesetzgebung.

Vertrauensbildende Maßnahmen

Um für Vertrauen zu werben, versprechen alle Anbieter, für die VPN-Nutzung keine Protokolle (Logs) zu speichern. Die einen speichern zumindest temporär die dem Client vom VPN-Server zugewiesene IP-Adresse, andere haben eine strikte „Zero Logs“-Policy. All diese Angaben sind jedoch kaum unabhängig überprüfbar. Windscribe musste 2021 eingestehen, dass in der Ukraine zwei ihrer Server beschlagnahmt wurden. Brisant an der Geschichte: Die Server waren nicht verschlüsselt und auf ihnen lief OpenVPN mit einer unsicheren Konfiguration.

Als Steigerung werben einige Betreiber mit datenträgerlosen Servern, deren Systeme ausschließlich im Arbeitsspeicher laufen. AzireVPN und WeVPN betreiben laut eigenen Angaben ihre Server im „Blind Operator Mode“. Ein Kernel-Modul verwehrt selbst Root den Zugriff auf den Netzwerkverkehr und versteckt die von WireGuard genutzten IP-Adressen. WireGuard-Erfinder Jason A. Donenfeld hat das Modul auf Initiative von AzireVPN entwickelt. Ironischerweise bezeichnet er selbst das Modul als Quacksalberei, rät von der Nutzung ab und macht sich darüber lustig („Für ahnungslose Betreiber, die noch ahnungsloser werden wollen“, siehe ct.de/w7mk).



Hide.me listet für Streaming-dienste geeignete VPN-Server in einer eigenen Kategorie auf.

Ein Siegel für vertrauenswürdige VPN-Anbieter gibt es nicht. Einige Anbieter haben immerhin unter dem Label „VPN Trust Initiative“ (VTI) gemeinsame Prinzipien vereinbart. Die freiwillige Selbstverpflichtung klingt plausibel, lässt aber auch Schlupflöcher offen und es fehlen Mechanismen zur Durchsetzung. Zur VTI gehören unter anderem Hide.me, NordVPN, StrongVPN und WeVPN. Mullvad und IVPN waren an einer ähnlichen, mittlerweile scheinbar eingeschlafenen Initiative beteiligt („Trustworthy VPNs“).

Indizien für die Glaubwürdigkeit der Zero-Logs-Bekundungen liefern Gerichtsverfahren, wenn VPN-Anbieter trotz entsprechender Beschlüsse keine Daten aushändigen und vor Gericht versichern, über keine Nutzungsdaten zu verfügen. OVPN hat gegen einen Urheberrechtsverband ein Verfahren gewonnen und wirbt damit.

Aussagekräftiger sind Audits, in denen unabhängige Firmen die Infrastruktur und Software auf Sicherheitslücken untersuchen und die Aussagen der Anbieter bestätigen. So soll PricewaterhouseCoopers (PwC) laut NordVPN ein Audit durchgeführt haben. Merkwürdigerweise haben weder NordVPN noch PwC den vollständigen Bericht veröffentlicht, was übrigens gegen die VTI-Prinzipien verstößt. Andere Berichte stellt NordVPN vollständig im Kundenbereich bereit. Die Berliner Sicherheitsfirma Cure53 hat

bei mehreren VPN-Anbietern, darunter IVPN, Mullvad und Surfshark, Audits durchgeführt und veröffentlicht. Darin sind auch die gefunden Schwachstellen dokumentiert. Wenn ein VPN-Anbieter mit einem Audit wirbt, achten Sie darauf, ob der Bericht veröffentlicht und was genau geprüft wurde: die Sicherheit der Server, nur eine Browser-Extension oder die No-Log-Policy? Zudem sind Audits immer nur eine Momentaufnahme.

Zur Beruhigung der Kundschaft pflegen AzireVPN, IVPN und WeVPN einen sogenannten Warrant Canary. Wie der Kanarienvogel im Bergbau soll dieser vor Gefahren warnen: Gesetze wie der berüchtigte Patriot Act erzwingen unter Strafandrohung eine stille Zusammenarbeit mit Sicherheitsbehörden. Um dem vorzubeugen, veröffentlicht der Betreiber turnusmäßig eine PGP-signierte Erklärung, dass weder gerichtliche Verordnungen oder Beschlagnahmungen vorliegen noch Durchsuchungen stattgefunden haben. Bleibt deren Aktualisierung aus, ist die Kundschaft gewarnt, ohne dass für den Anbieter eine Strafe droht. So zumindest die Theorie. Die Wirksamkeit eines Warrant Canary ist umstritten, da dessen Erneuerung erzwungen werden könnte.

Damit erst gar keine Daten in falsche Hände geraten, sollten möglichst wenige erhoben werden. Gut die Hälfte der Anbieter verlangt für die Registrierung eine gültige E-Mail-Adresse, bei den anderen ist selbst die optional. Mullvad und IVPN beschränken sich auf eine anonyme Zugangsnummer. Für die Registrierung bei WeVPN muss man ein Google-Captcha lösen, was dem Versprechen von mehr Privatsphäre zuwiderläuft.

Preiskarussell

Wer einen VPN-Tarif buchen will, hat die Wahl zwischen Monatstarifen und Verträgen von mehreren Monaten bis hin zu einem oder zwei Jahren Laufzeit, bei manchen Anbietern sogar bis hin zu drei Jahren. Um Anbieter, die gegen Einmalzahlung einen lebenslangen VPN-Zugang versprechen, sollten Sie einen großen Bogen machen, da dies kein seriöses Geschäftsmodell ist.

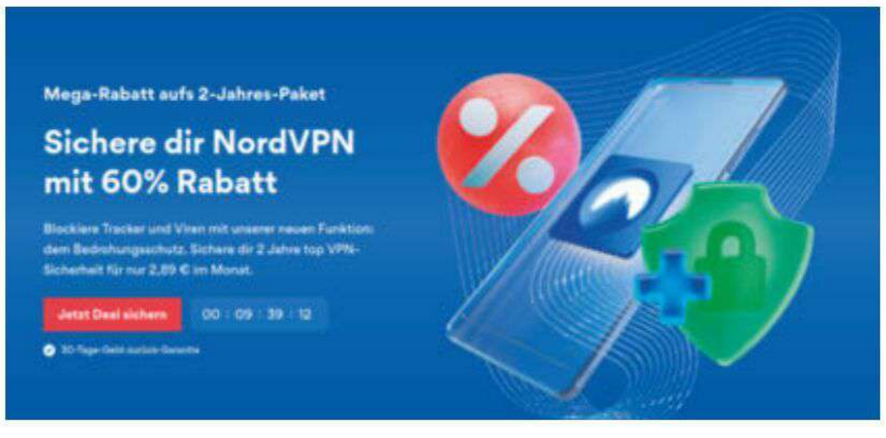
Das gilt aber auch für die Mehrjahresverträge. Viele VPN-Anbieter locken mit hohen Rabatten. So kostet ein Monatstarif meist um die 10 Euro, der Jahrestarif nur 60 Euro, also umgerechnet 5 Euro im Monat. Aber ob der Dienst auch in Zukunft die gewünschte Bandbreite oder den Zugang zur Lieblingsmediathek bietet, kann niemand garantieren. In unsere Vergleichstabelle haben wir Preise für einen Monat, drei Monate und ein Jahr aufgenommen. Positiv sticht Mullvad hervor, der unabhängig von der Laufzeit nur 5 Euro pro Monat berechnet. Zudem sollte man sich bei den langfristigen Verträgen nicht vom angezeigten niedrigen Monatspreis täuschen lassen. Anders als beim Mobilfunkvertrag wird der Preis für die gesamte Laufzeit sofort fällig und im Voraus eingezogen.

Bei fast allen Anbietern ist die automatische Vertragsverlängerung voreingestellt. Azire-VPN und Mullvad bieten auch Einmalzahlungen an. Alle VPN-Dienste akzeptieren die Bezahlung per Kreditkarte, fast alle auch per PayPal und Kryptowährung. Über ein Bankkonto (Giropay, SEPA-Lastschrift) nehmen nur vier Anbieter das Geld entgegen. Wer ganz viel Wert auf Datenschutz legt, schickt per Post Bargeld an Azire-VPN, IVPN, Mullvad oder OVPN. Wählerisch gibt sich Mozilla, das ausschließlich per Kreditkarte abrechnet.

Manchmal weicht der beworbene vom abgebuchten Preis ab, da einige Anbieter die Mehrwertsteuer erst während des Bestellvorgangs aufschlagen. Bei Anbietern, die die Preise in US-Dollar berechnen, können zusätzliche Bankgebühren für Zahlungen in Fremdwährung anfallen. Auskunft dazu gibt Ihnen Ihre Bank oder die Ausgabestelle Ihrer Kreditkarte.

Die Rabatte sind teilweise undurchsichtig. So gibt OVPN als Referenz für den Rabatt Mondpreise an, die deutlich höher sind als der Monatstarif über die gleiche Laufzeit. Die Ersparnis für den Zweijahresvertrag schrumpft so von angeblichen 264 Euro auf real 120 Euro, was immer noch beachtlich hoch ist. Auch VPN.AC und VyprVPN werben bei ihren Mehrjahresverträgen mit einem prozentual geringfügig zu hohen Rabatt. WeVPN rechnet in den Rabatt auch die zusätzlichen Gratismonate ein und drückt so den Durchschnittspreis. Bei PIA sind in der Bestellübersicht für den Zweijahrestarif knapp 278 Euro aufgelistet. Der versprochene Preis von gut 52 Euro ergibt sich durch einen fiktiven Rabatt. Nur ein kleiner

Mit angeblich zeitlich begrenzten Rabatten erhöhen manche VPN-Provider den Verkaufsdruck. Das identische Angebot sahen wir aber an mehreren Tagen.



Hinweis gibt an, dass nach den ersten zwei Jahren die 52 Euro jährlich fällig werden.

Um eine Kaufentscheidung zu forcieren, zeigen beispielsweise CyberGhost oder NordVPN einen Countdown für den versprochenen Rabatt an, der sekundenweise herunterzählt. Dieses „Pressure Selling“ ist nach EU-Recht eigentlich unzulässig, muss laut Verbraucherzentrale Bayern aber im Einzelfall juristisch geklärt werden. Unser Tipp: Lassen Sie sich von Sonderangeboten nicht unter Druck setzen, denn die Rabatt-Aktionen werden ständig neu aufgelegt.

Erfreulicherweise unterscheiden sich die verschiedenen Tarife abseits der Laufzeit kaum. Den Jahresverträgen vorbehalten oder zusätzlich kostenpflichtig sind höchstens nicht zwingend notwendige Zusatzfunktionen wie VPN-Verbindungen über mehrere Server (Multihop), Port-Forwarding oder eine öffentliche IP-Adresse.

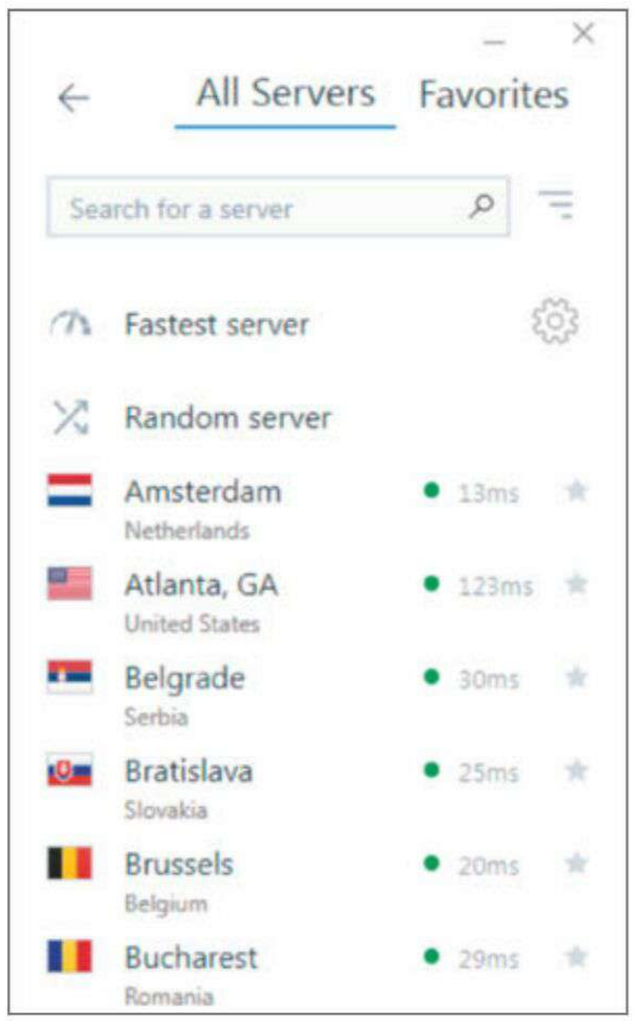
Alle Anbieter versprechen unbegrenztes Datenvolumen oder schränken es nicht von vornherein ein. Meist sind gleichzeitige Verbindungen von fünf bis zehn Geräten im Tarif enthalten. IVPN bietet auch einen vergünstigten Tarif für maximal zwei Geräte an. Im Unterschied dazu erlaubt Windscribe, beliebig viele Geräte gleichzeitig per VPN zu verbinden, solange der VPN-Zugang nur im engsten Familienkreis geteilt wird.

Die Verbindungsgeschwindigkeit schwankte bei unseren Stichproben zwischen den Anbietern, jedoch war sie in der Regel deutlich höher als 100 MBit/s, oft auch ein Mehrfaches davon. Eine richtige Schnarchnase fiel uns nicht auf. Die gebotene Geschwindigkeit kann jederzeit schwanken, abhängig vom zugeteilten Server, dessen Auslastung und weiteren Faktoren.

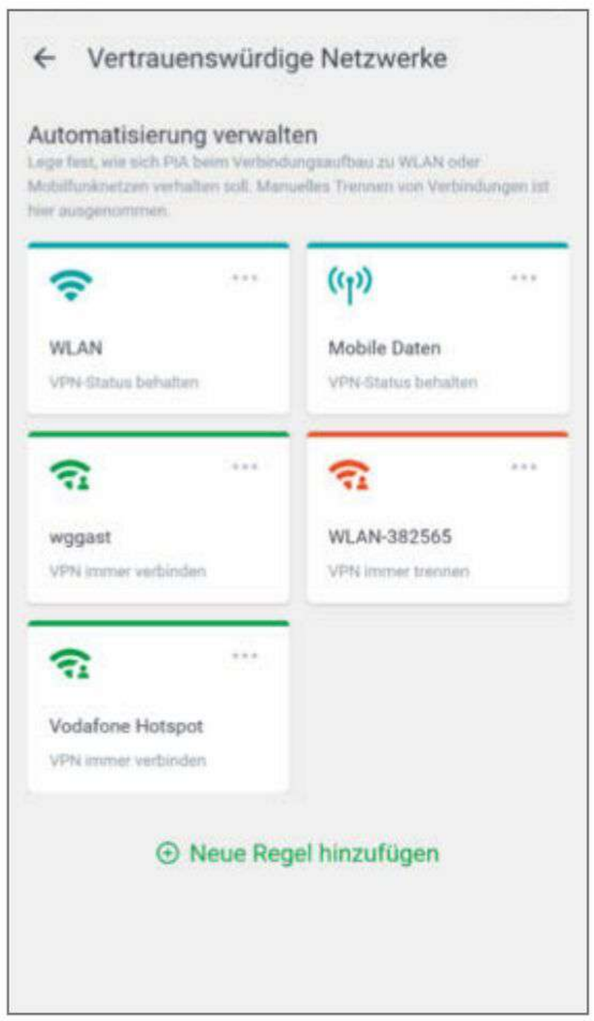
Die Anzahl der Serverstandorte schwankt zwischen 19 bei AzireVPN und 110 bei Windscribe. Gateways zu beliebten VPN-Ausflugszielen wie Großbritannien oder die USA stellen alle bereit, ebenso Server in Deutschland, den Niederlanden oder Schweden. Wenn Sie ein bestimmtes Land benötigen, prüfen Sie vor der Buchung die verfügbaren Standorte. Die sind meist auf der Webseite aufgeführt.

App ins VPN

Das WireGuard-Protokoll ist bei VPN-Anbietern nicht unumstritten. Der minimalistische Code überzeugt zwar durch Einfachheit und Geschwindigkeit. Kritiker bemängeln jedoch, WireGuard sei nicht optimal auf Privatsphäre ausgerichtet. Üblicherweise wird die dem VPN-Tunnel zugewiesene IP-Adresse fest in die WireGuard-Konfiguration geschrieben. Da man so bei jeder Verbindung die gleiche IP-Adresse verwendet, lässt sich das Surfverhalten einem Account zuord-



Die VPN-Apps der Anbieter sortieren die Server nach Reaktionszeit, Region oder gewünschter Anwendung.



Erlaubt man der VPN-App den Zugriff auf den Standort, schaltet sie abhängig vom verbundenen WLAN das VPN an oder ab.

nen. Das gilt vor allem für die nur intern im VPN-Netz verwendete private IP-Adresse, während Webserver meist nur die nach außen sichtbare IP-Adresse des Gateways sehen.

WireGuard gibt diese feste Zuordnung nicht vor; sie resultiert aus der besonders einfach gestalteten Konfiguration mit `wg-quick`. Unter anderem Hide.me, Mozilla und NordVPN haben eigene Lösungen entwickelt, um die WireGuard-Verbindung mit dynamisch vergebenen IP-Adressen aufzubauen. Wie oft eine neue IP-Adresse zugeteilt wird, variiert zwischen den Diensten.

Dafür ist aber die Nutzung der anbieterspezifischen Zugangssoftware notwendig. In der Regel gibt man nur die Anmeldedaten an und die App generiert dann die benötigten WireGuard-Schlüssel und kümmert sich um den Schlüsselaustausch mit dem VPN-Server. Letztlich muss man auf die eine oder andere Weise dem VPN-Anbieter vertrauen. Mehrere Anbieter haben ihren Client unter einer Open-Source-Lizenz veröffentlicht.

Auch sonst erleichtert eine Zugangssoftware das Surfen durch den VPN-Tunnel. In der App wählt man bequem aus einer Liste die gewünschte Region aus oder lässt sich mit dem schnellsten Server verbinden. Die Programme listen die Standorte sortiert nach Ländern oder Latenzen auf, vereinzelt werden Server für Streaminganbieter oder Filesharing hervorgehoben. Hinzu kommen diverse Zusatzfunktionen wie der automatische Verbindungsaufbau bei unsicheren Hotspots oder Ausnahmeregeln für einzelne Programme oder Hosts. Der Kill-Switch soll unbeabsichtigten Netzwerkverkehr außerhalb des VPN-Tunnels verhindern, aber darauf sollten Sie sich im Ernstfall nicht verlassen.

Alle VPN-Dienste verhinderten DNS-Leaks, da sie eigene DNS-Server anbieten und die Domainanfragen dort und nicht beim eigenen Internet-Provider landen. Der IPv6-Verkehr wird entweder ebenfalls durchs VPN getunnelt oder abgeklemmt. Lediglich WeVPN patzte dabei. Windscribe bietet unter Windows eine Option IPv6 abzuschalten, aber die verlangt einen Neustart. AzireVPN teilt eine globale IPv6-Adresse zu, aber Server im Netz sehen nur die des VPN-Gateways.

Wir haben uns den Netzwerkverkehr der Apps, die eine Verbindung per WireGuard aufbauen, unter Windows und Android angeschaut. Bei den meisten Anbietern mussten wir WireGuard explizit in den Einstellungen als Verbindungsprotokoll auswählen. Auch unter Windows ähneln die Programme vom Aussehen eher Handy-Apps. Die Anwendungen von StrongVPN und WeVPN verlangten bei jedem Start Admin-Rechte.

Positiv: Alle Programme und Apps verschlüsselten wie versprochen. Auch bei der Anmeldung beim VPN-Dienst selbst plauderten sie nichts aus. So konnten wir auch nicht kontrollieren, welche Daten durch den Tunnel gehen. Die Apps von StrongVPN, WeVPN und Windscribe enthalten laut der Tracker-Datenbank von „Exodus Privacy“ Bestandteile von Googles Analytics-Modulen Crashlytics und/oder Firebase Analytics. Ob die Bibliotheken fürs Tracking verwendet werden, bleibt unklar. IVPN schickt anonyme Fehlerberichte zu den Entwicklern, aber das lässt sich abschalten. Mozilla VPN fragt vorher, ob es Daten sammeln darf.

Handarbeit

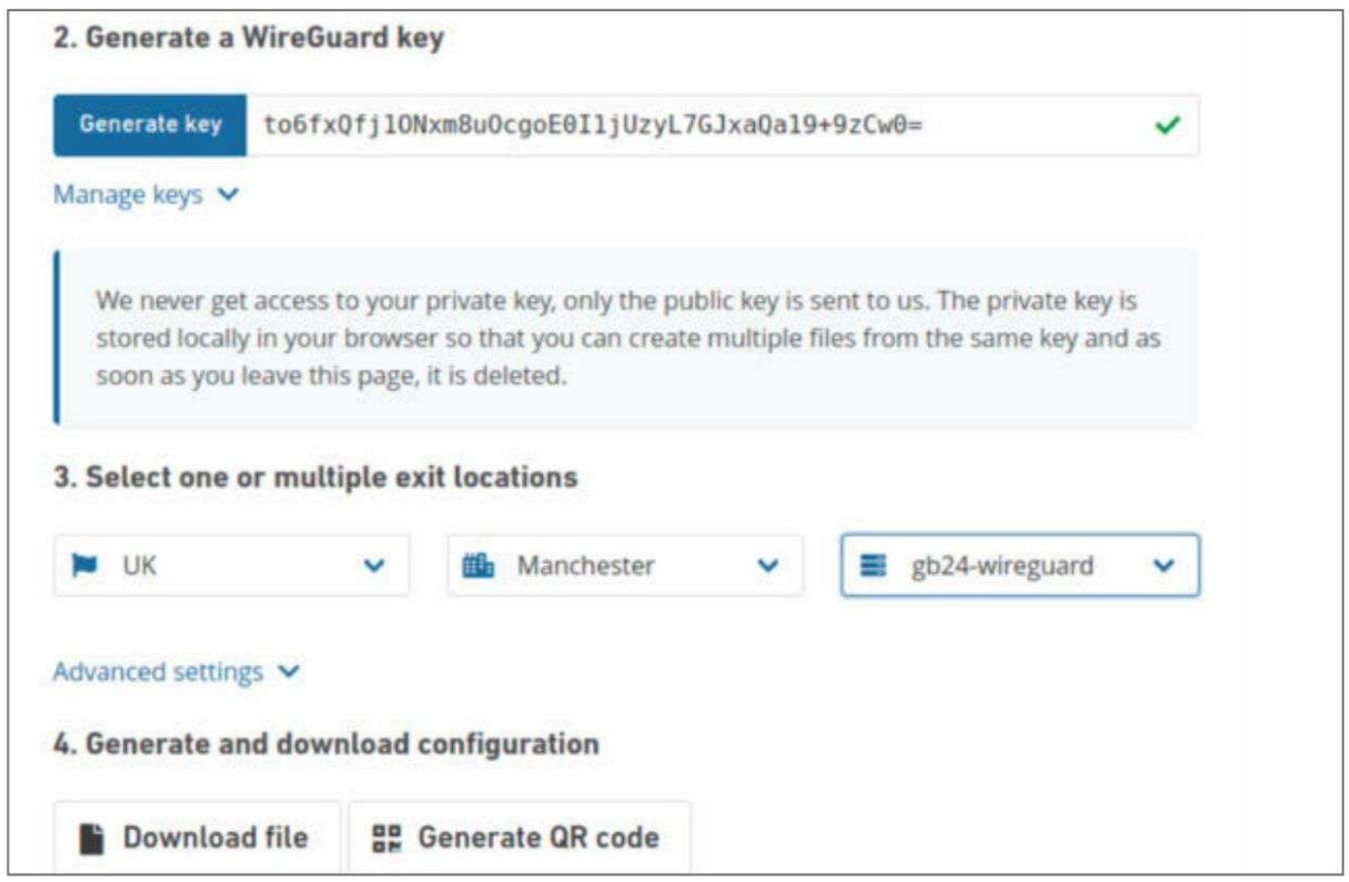
Wenn Sie sich nicht mit den speziellen Apps herumschlagen wollen, erhalten Sie bei etlichen VPN-Anbietern die für WireGuard oder Ihr Betriebssystem passenden Zugangsdaten. Meist gibt es einen Web-Generator, der im Browser die WireGuard-Keys erzeugt oder wo Sie einen vorhandenen Public Key eintragen können. Nach der Auswahl der gewünschten Server und weiterer Optionen erzeugt der Webdienst eine Konfigurationsdatei und bietet diese

Literatur

[1] Holger Zuleger, **Maskierungsspiel**, Unterschiede und Gemeinsamkeiten gängiger VPN-Varianten, c’t 18/2021, S. 26

Erklärungen zum Affiliate-Marketing und Blind Operator Mode

ct.de/w7mk



Mit dem Web-Generator erzeugt man die passende WireGuard-Konfiguration. Fürs Mobiltelefon muss man nur noch den QR-Code scannen.

zum Download an, teilweise auch als QR-Code direkt zum Einscannen mit dem Handy oder als Zip-Archiv mit den Konfigurationsdateien für mehrere oder gar alle Server. Die Web-Generatoren von Mullvad und StrongVPN bieten für Linux an, über iptables-Regeln einen Kill-Switch einzubauen. Bis auf Windscribe hatten alle auf IPv4 beschränkten Anbieter die Konfigurationsdatei so erstellt, dass es keinen IPv6-Leak gab.

Merkwürdig ist der Ansatz von PIA: Für den Download der Konfigurationsdateien stellt der Anbieter nur einen komplexen Satz von Skripten bereit, die man als Root ausführen muss. Ebenso enttäuscht das Angebot von IVPN, denn dort muss man sich um alles selber kümmern: mit den WireGuard-Befehlen im Terminal ein Schlüsselpaar erzeugen, dann auf der IVPN-Webseite den Public Key hochladen und dort die Server-Daten heraussuchen und alles zusammen von Hand in eine Konfigurationsdatei eintragen.

Ganz gleich ob Download oder QR-Code: Der Preis für die Autonomie ist das mit Ihrem Account

VPN-Dienste mit WireGuard

Name	AzireVPN	Hide.me	IVPN	Mullvad
Anbieter, Firmensitz	Netbouncer AB, Schweden	eVenture Ltd., Malaysia	Privatus Limited Inc., Gibraltar	Mullvad VPN AB, Schweden
URL	azirevpn.com	hide.me	www.ivpn.net	mullvad.net
Anbieter-Apps mit WireGuard				
Windows / macOS / Linux	✓ / – / –	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
Android / iOS	✓ / –	✓ / ✓	✓ / ✓	✓ / ✓
App Lizenz	proprietär / GPLv2	proprietär / GPLv2	GPLv3	GPLv3
Unterstützung für alternative Clients				
Konfigurationsdatei erhältlich via	QR-Code, Web-Generator, Skript	–	manuell[2]	QR-Code, Web-Generator
Verbindung				
VPN-Server (IPv4 / IPv6)	✓ / –	✓ / ✓	✓ / –	✓ / ✓
Tunnel (IPv4 / IPv6)	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Schutz vor IPv6-Leak / DNS-Leak	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
IP-Adresse öffentlich oder privat (IPv4 / IPv6)	privat / privat	privat / privat	privat / privat	privat / privat
Kill-Switch	–	✓	✓[4]	✓
maximal verbundene Geräte	5	10	2 (Standard) / 7 (Pro)	5
freie Portwahl	✓	–	Auswahl	✓
Protokolle zusätzlich zu WireGuard				
OpenVPN	✓	✓	✓	✓
IPSec (L2TP / IKEv2)	–	– / ✓	– / ✓	–
Infrastruktur				
Standorte	19	53	45	52
Länder (Anzahl / Auswahl)[5]	14 / CA, FR, DK, RO, TH	46 / AU, BR, ES, HK, IT	32 / CH, IL, JP, SG, UA	33 / BR, CZ, HK, MD, NZ
Abonnement				
benötigte Daten	keine	E-Mail-Adresse	keine	keine
Abonnement / automatische Verlängerung	– / –	✓ / ✓	✓ / ✓	✓ / ✓
Bezahlung per Bankkonto / Kreditkarte / PayPal / Bargeld / Kryptowährung	– / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / – / ✓	– / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓
Preise (mit WireGuard)				
1 Monat / 3 Monate / 12 Monate	5 € / 12 € / 45 €	7,99 € / – / 79,99 €	6 US-$ / – / 60 US-$ (Standard) 10 US-$ / – / 100 US-$ (Pro)	5 € / – / –

[1] nur unter Linux [2] Konfiguration und Keys muss man selber erstellen [3] öffentliche IP-Adresse gegen Aufpreis [4] nur mit Anbieter-App [5] alle Anbieter haben Standorte u. a. in DE, NL, SE, UK, US [6] nur iOS-App

verknüpfte Paar aus Schlüssel und IP-Adresse. Wollen Sie dieses austauschen, müssen Sie von vorne anfangen und neue Schlüssel und Konfigurationsdateien erzeugen. Ob man in einer festen (privaten) IP-Adresse oder in proprietären Apps das größere Übel sieht, ist Ansichtssache.

Fazit

Transparente und günstige Preise bieten AzireVPN, IVPN, Mullvad und ProtonVPN. Über die meisten Serverstandorte in zahlreichen Ländern verfügen PIA, ProtonVPN und Windscribe, bieten aber kein IPv6. Wer WireGuard mit den Apps der Anbieter nutzen will, sollte genau hinschauen, auf welcher Plattform das moderne Protokoll angeboten wird.

Weder der Firmensitz an exotischen Standorten noch die vollmundigen Versprechen der Dienstleister garantieren wirklich Sicherheit. Dank der Vielfalt an VPN-Diensten können Sie den unseriösen Anbietern aber mühelos aus dem Weg gehen, ebenso wie unnötig langen Vertragslaufzeiten. (ktn) c't

	OVPN	PIA	Proton VPN	StrongVPN	VPN.AC	WeVPN	Windscribe
	OVPN Integritet AB, Schweden	Private Internet Access, Inc., USA	Proton Technologies AG, Schweiz	J2 Global, Inc., USA	Netsec (NSIS), Rumänien	WEVPN Ltd., British Virgin Islands	Windscribe Limited, Kanada
	ovpn.com/de	privateinternetaccess.com	https://protonvpn.com/	strongvpn.com	vpn.ac	wevpn.com	windscribe.com
	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / –	– / – / –	✓ / ✓ / – /	✓ / ✓ / ✓
	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	– / –	✓ / ✓	✓ / ✓
	proprietär	GPLv3	GPLv3	proprietär	proprietär	proprietär	proprietär / GPLv2
	QR-Code, Web-Generator	Skript	Web-Generator	QR-Code, Web-Generator	Web-Generator	Web-Generator	Download
	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –
	✓ / ✓	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –
	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓[4] / ✓
	privat[3] / privat	privat / –	– / –	privat / –	privat / –	privat / –	privat[3] / –
	✓[4]	✓	✓ (Apps, Android Einstellungen)	–[1]	–	✓	✓[4]
	4 (mit Jahresvertrag 5)	10	2 (Basic) / 10 (Plus)	12	6	10	unbegrenzt (Haushalt)
	–	–	–	Bereich	–	–	Auswahl
	✓	✓	✓	✓	✓	✓	✓
	–	– / ✓[6]	– / ✓	✓ / ✓	✓ / ✓	– / ✓	– / ✓
	27	106	ca. 80	67	42	66	110
	17 / AU, DK, FR, JP, RO	78 / AU, CN, EG, IN, NZ	63 / (CL, EE, JP, MX, VN)	41 / AE, CO, EE, IE, ZA	23 / FR, JP, NO, PL, TW	47 / AT, BE, MX, PT, RU	63 / AZ, AQ, GR, PA, VN
	keine	E-Mail-Adresse	E-Mail-Adresse	E-Mail-Adresse	E-Mail-Adresse, Land	E-Mail-Adresse	keine
	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
	– / ✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / – / ✓	– / ✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / ✓	– / ✓ / ✓ / – / ✓	✓ / ✓ / ✓ / – / ✓
	11 € / – / 59,88 €	10,69 € / - / 51,74 €	5 € / - / 48 € (Basic) 10 € / - / 96 € (Plus)	10,99 US-$ /– / 79,99 US-$[7]	9 US-$ / 24 US-$ / 58 US-$	9,95 US-$ / - / 49,95 US-$	9 US-$ / – / 49 US-$

[7] 43,99 US-$ im ersten Jahr ✓ vorhanden – nicht vorhanden



Bild: Andreas Martini

Unterschiede gängiger VPN-Varianten

VPN ist nicht gleich VPN: Das eine mag nicht über IPv6 laufen, das andere ruckelt in Mobilnetzen. Der Blick auf die Details klärt, welche Technik für welche Situation am besten taugt. So findet man beim VPN-Provider das optimale Protokoll.

Von **Holger Zuleger**

Ein Virtual Private Network, kurz VPN, kennen alle, die sich aus dem Homeoffice mit einem meist mobilen Gerät in das Firmennetz einwählen. Dort bekommt man nach erfolgreicher Authentifizierung – der Anmeldung mit individuellen Zugangsdaten – Zugriff auf die gewohnte Arbeitsumgebung mit Drucker und Serverdiensten fast wie vor Ort. Da die VPN-Verbindung typischerweise über die Netze mehrerer Provider läuft, ist eine sichere Verschlüsselung unabdingbar, um Vertraulichkeitsvorgaben etwa aus der DSGVO einzuhalten.

Wer aus dem Homeoffice an den Arbeitsplatz zurückkehrt, vermisst nun vielleicht die heimische Netzumgebung. Dann liegt der Gedanke nahe, vom Arbeitsplatz aus mit den gleichen Techniken aufs Heimnetz zuzugreifen wie vorher umgekehrt. Im

Folgenden schildern wir, welche wichtigen Unterschiede es zwischen den VPN-Varianten gibt und welche Rolle die Netztopologie spielt.

Das Wissen um die Zusammenhänge erleichtert die Wahl des passenden VPNs. Denn neben der möglicherweise fehlenden Erlaubnis – viele Unternehmen sehen eine Verbindung aus dem Firmennetz heraus als kritische Sicherheitsverletzung – stehen dem Unterfangen häufig auch technische Gründe entgegen.

Schon Windows 95 und NT hatten einen Client für Microsofts **PPTP** (Point-to-Point Tunneling Protocol). Leider gelten die dort eingesetzten Verschlüsselungs- und Authentifizierungsverfahren seit mehr als einem Jahrzehnt als gebrochen und damit unsicher. Unmissverständlich ausgedrückt: Lassen Sie die Finger von PPTP, auch wenn es in Ihrem Router besonders bequem einzurichten oder gar das einzige angebotene VPN-Verfahren ist!

Als Alternative zu PPTP finden sich etwa in iOS und macOS allein drei Einwahlmethoden für **IPsec** (Internet Protocol Security), das seit Langem als sichere VPN-Methode gilt. Gründe für die IPsec-Vielfalt liegen in der historischen Entwicklung und darin, dass sich neue Standards – besonders in dem sich selbst gern als innovativ feiernden Netzwerkbusiness – nur sehr langsam durchsetzen.

IPsec wurde vor vielen Jahren als ergänzender IP-Header zur Verschlüsselung für IPv6 entwickelt. Damals gab es aber kaum IPv6-fähige Endgeräte und die Internetanbindungen waren ausschließlich für IPv4 ausgelegt. Folglich wurde IPsec für IPv4 zurückportiert – ohne dabei die Unterschiede beider Transportprotokolle gründlich zu beachten.

IPv6 hat einen Mechanismus zur IP-Adressautokonfiguration ab Werk, IPv4 nicht. Deshalb musste anfangs – und auch heute manchmal noch – für die VPN-Einwahl die IPv4-Adresse des Geräts statisch konfiguriert werden. Das war bei den aufkommenden mobilen Endgeräten untragbar. So haben die IPsec-Entwickler nachgebessert und die damalige Authentifizierungsmethode IKEv1 (Internet Key Exchange) um Mechanismen zur IP-Autokonfiguration erweitert.

Mobil nachgeholt

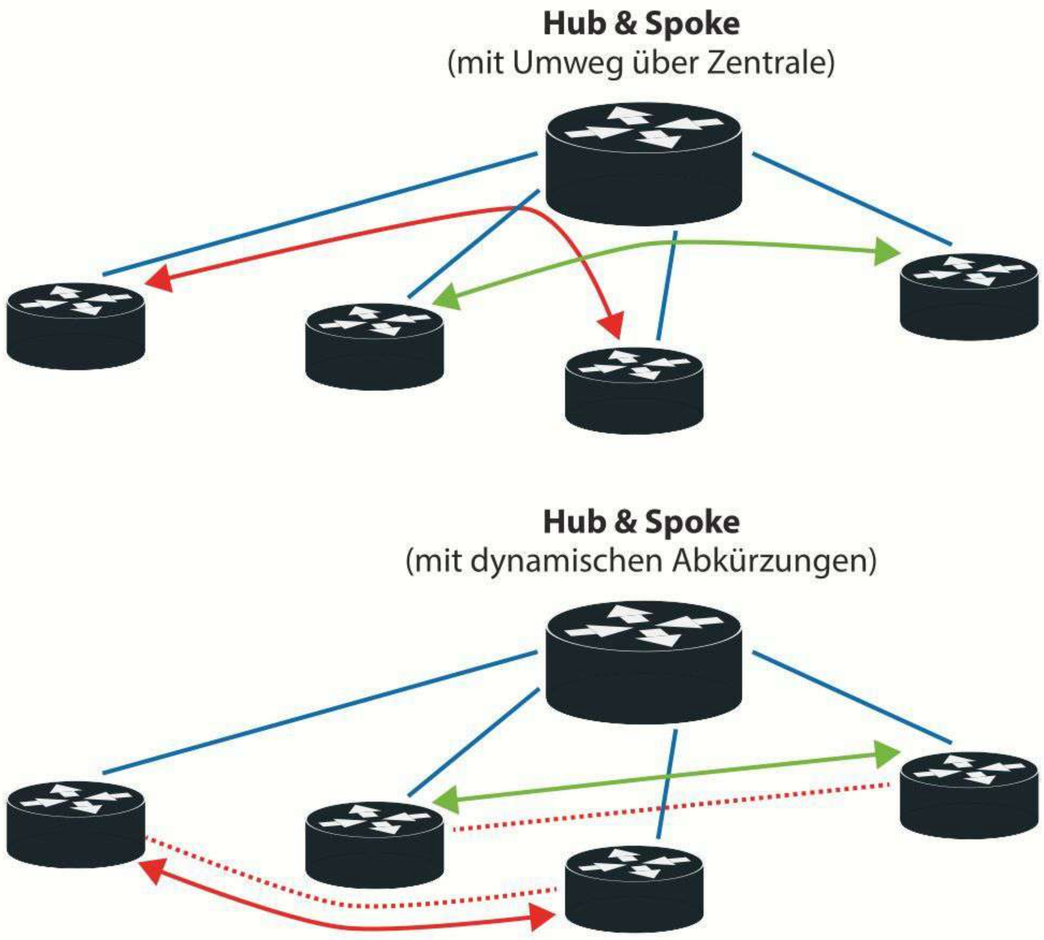
Ein weiteres Problem ergab sich aus der Authentifizierung der Geräte. Als IPsec entwickelt wurde, lag der Fokus auf der Standortvernetzung. Mobile Geräte gab es schlichtweg nicht. IPsec wurde bis dahin nur auf Gateways (Routern) eingesetzt, um Datenverkehr zwischen Standorten zu tunneln und dabei zu verschlüsseln.

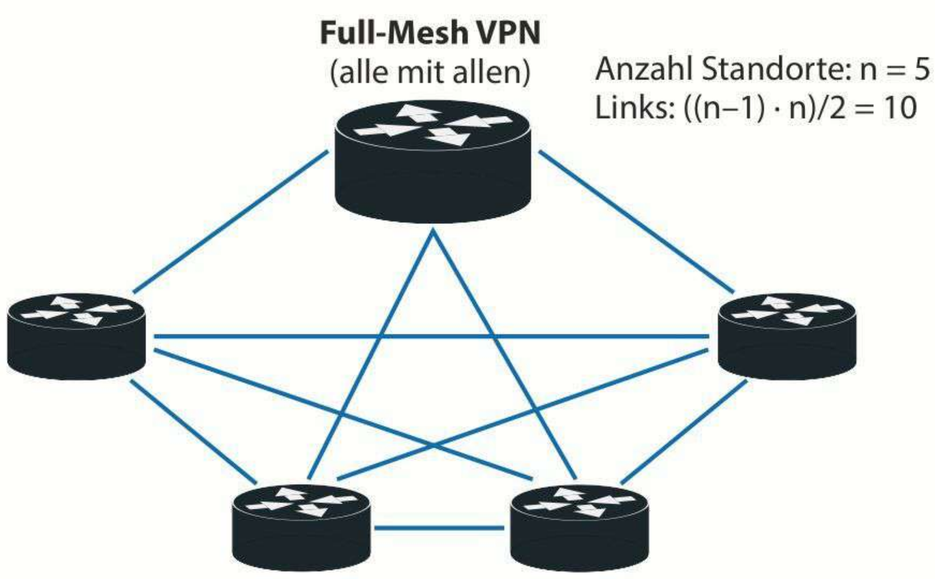
Die Gateways authentifizierten sich gegenseitig über Zertifikate. Für die aufkommenden, immer vielfältigeren mobilen Endgeräte war das aber zu unflexibel, da jedes Gerät ein eigenes Zertifikat benötigt.

Microsoft entwickelte mit dem oben erwähnten PPTP zwar sehr früh ein Protokoll, das zur Authentifizierung und Einwahl auf bekannte Verfahren aus

VPN-Vermaschung

Der Road-Warrior-Ansatz (VPN-Verbindung zur Zentrale à la Hub & Spoke, oben) funktioniert in Firmennetzen mit vielen Standorten wegen der doppelten Übertragungen schlecht. Voll vermaschte VPNs (unten) sind wegen der vielen Verbindungen aufwendig zu administrieren. Hub & Spoke mit dynamischem Linkaufbau hilft den Aufwand im Griff zu halten.





Modemzeiten zurückgreift. Es wurde jedoch bald durch ein Verfahren mit besseren Verschlüsselungskomponenten abgelöst: PPP (Point-to-Point Protocol) über L2TP (Layer 2 Tunneling Protocol) mit IPsec im Transport-Mode (siehe Kasten rechts).

Das Zusammenspiel verschiedener Protokolle bei L2TP/IPsec ist zwar komplex, hat gegenüber reinem IPsec aber mehrere Vorteile: Zum Transport dient L2TPv2, das auf UDP aufsetzt (User Datagram Protocol). Damit ist der Verbindungsaufbau NAT-freundlich (Network Address Translation, IPv4-Adressumschreibtechnik) und setzt zumindest auf einer Seite keine öffentliche IPv4-Adresse mehr voraus. Denn NAT-Router nutzen die von den Datenströmen verwendeten Ports zur eindeutigen Zuordnung der Kommunikationspartner. Bei reinen IPsec-Verbindungen stecken diese Informationen jedoch im verschlüsselten Tunnel und sind für den Router nicht erkennbar.

PPP über den Layer-2-Tunnel bringt einen Vorteil bei der Nutzerauthentifizierung: Sie lief historisch meist mit Name und Passwort, heutzutage mittels EAP (Extensible Authentication Protocol) über diverse andere Verfahren. So lässt sich bei L2TP/IPsec auch eine Gateway-seitige Zertifikatsauthentifizierung für die äußere Verschlüsselung mit vereinfachter PPP-Nutzerauthentifizierung innerhalb des Tunnels kombinieren.

Mit Einschränkungen

So praktisch und vielseitig die Lösung ist, kann sie heutzutage aber nicht mehr generell empfohlen werden: L2TPv2 ist nur für IPv4 als Transportprotokoll definiert und merkwürdigerweise auch nie für IPv6 umgesetzt worden. L2TP/IPSec kann deshalb zwar IPv6 als inneres Protokoll transportieren, der Tunnel selbst muss jedoch über IPv4 aufgebaut werden.

Ähnlich eigenwillig verhält sich IPsec mit IKEv1, wie es beispielsweise die verbreiteten Fritzboxen anbieten. Für jedes transportierte Protokoll (IPv4 oder IPv6) muss ein separater Tunnel mit dem gleichen

VPN-Topologien

Das klassische Road-Warrior-Szenario – ein Gerät verbindet sich per VPN mit der Firmenzentrale – arbeitet in derselben Topologie, die man bei VPN-Dienstleistern findet: Hub & Spoke, also Nabe (Zentrale) und Speichen (Geräte beziehungsweise Fernarbeitende) eines gedachten Rades.

Wenn Firmen ihre Standorte so vernetzen, dann läuft der Verkehr zwischen zwei Niederlassungen immer über die Zentrale. Der Nachteil ist offensichtlich eine Doppelbelastung der VPN-Verbindungen und damit der Internetanbindung. Durch einen VPN-Tunnel läuft nun auch nicht mehr nur der Verkehr des Road-Warriors, sondern der vieler Geräte auf beiden Seiten.

Um die Verkehrsverdopplung zu vermeiden, setzen manche Unternehmen auf ein voll vermaschtes VPN (Full Mesh), in dem jede Niederlassung direkt mit allen anderen Stationen kommunizieren kann. Was die Anbindung der Zentrale entlastet, verkompliziert aber den VPN-Aufbau, steigt doch die Zahl der Tunnel überproportional mit der Zahl der Niederlassungen: Drei Standorte lassen sich mit ebenso vielen VPN-Verbindungen vernetzen. Vier benötigen jedoch schon sechs Tunnel, fünf Standorte gar zehn und bei zehn Standorten müssen ganze 45 Tunnel eingerichtet und überwacht werden.

Als Alternative bieten sich VPNs an, die anfangs als Hub & Spoke konfiguriert werden. Damit steigt die Tunnelzahl nur linear. Wollen zwei Außenstellen kommunizieren, dann errichtet das System dynamisch einen neuen Tunnel zwischen ihnen. Cisco hat das unter dem Namen DMVPN (Dynamic Multipoint VPN) entwickelt. Es basiert auf IPsec in Kombination mit dem Next Hop Routing Protocol (NHRP) und GRE-Tunneln (Generic Routing Encapsulation). Eine vergleichbare, aber technisch völlig anders realisierte Open-Source-Lösung für Full-Mesh-VPN ist Tinc.

L2TP/IPsec

Klassisches IPsec, gleich ob IKEv1 oder IKEv2, verwendet auch bei der Remote-Einwahl IPsec im Tunnel-Modus. Dabei wird ein zweiter äußerer IP-Header vor das eigentliche IP-Datenpaket geschnallt und dieser mit dem Verschlüsselungsheader von IPsec versehen (ESP, Encapsulating Security Payload).

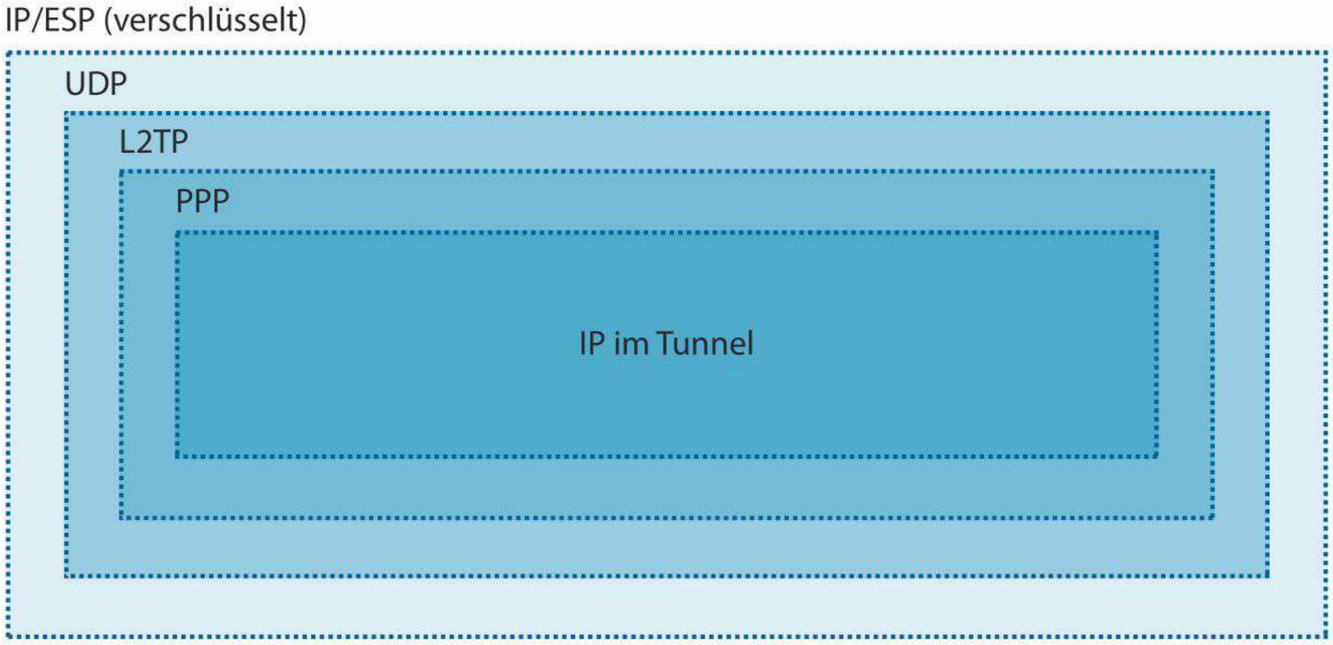
Der VPN-Client muss mit zwei IP-Adressen umgehen, einer aus dem Fremdnetz auf dem physischen Interface und einer zweiten virtuellen aus dem Heimatnetz, die ihm bei der Einwahl zugewiesen wurde. Die getunnelten Datenpakete gehen an das Remote-VPN-Gateway, das diese entschlüsselt, den äußeren Transport-Header entfernt und sie dann wie normale Pakete im internen Netz weiterleitet.

Bei dem oft mit IPsec kombinierten L2TP sieht der Aufbau komplett anders aus: Der VPN-Client baut zum VPN-Gateway eine L2TP-Verbindung auf und nutzt UDP auf Port 1701 als Transportprotokoll. So entsteht ein Layer-2-Tunnel, innerhalb dessen die Geräte wie früher zu Modemzeiten eine PPP-Verbindung aufbauen.

PPP erledigt das Authentifizieren der Benutzer, meist gegen einen Radius-Server. Der Client bekommt im Tunnel eine IPv4-Adresse und einen oder zwei DNS-Server aus dem Heimnetz zugewiesen. Außen drumherum verschlüsselt IPsec im Transport-Mode schließlich den L2TP-UDP-Verkehr. Das Verkapseln kostet 40 Byte, die Verschlüsselung außen noch mal circa 50 Byte.

L2TP/IPsec-Verschachtelung

VPNs verpacken die zu schützenden Daten matroschkamäßig in mindestens zwei zusätzliche äußere Protokollschichten. L2TP/IPsec treibt das mit vier Hüllen auf die Spitze.



Transportprotokoll aufgebaut werden. Für Dual-Stack im Firmennetz wären demnach zwei Tunnel nötig.

Wegen der Adressknappheit bei IPv4 werden Internetanschlüsse zwar vermehrt parallel mit IPv6 ausgestattet. Privatkunden bekommen aber oft gar keine öffentliche IPv4-Adresse mehr. Nutzer von Internet per TV-Kabel und manchen Glasfaser-Anbietern können ein traurig Lied davon singen. Wegen des Provider-NAT muss man für den Betrieb extern erreichbarer Server im eigenen Netz nicht nur Klimmzüge machen [1,2], sondern es steht auch häufig klassischen IPsec-Verbindungen im Weg. Selbst

wenn das Gegenüber, der Peer, eine öffentliche IPv4-Adresse hat, funktioniert IPsec mit IKEv1 und L2TP an solchen Anschlüssen nicht jederzeit stabil.

Aufgeräumt

IPsec Version 2 (IKEv2) soll all diese Probleme lösen. Es bringt unterschiedliche Authentifizierungsverfahren über EAP, NAT-Traversal, Dead Peer Detection zur Ausfallerkennung, IP-Autokonfiguration sowie nicht zuletzt IPv4-über-IPv6-Transport und umgekehrt.

Damit, sollte man meinen, kommt man auch als Internet-Nomade immer ins Heim- oder Firmennetz. Für Privatkundenanschlüsse stimmt das. In Firmennetzen steht jedoch meist eine Firewall am Internetzugangspunkt. Diese kontrolliert nicht nur den eingehenden, sondern häufig auch den ausgehenden Verkehr. IPsec-Verbindungen aus dem Firmennetz in Richtung Internet gelten gerne mal als suspekt und werden unterbunden.

Ähnliche Einschränkungen finden sich auch bei manchem WLAN-Hotspot oder bei Gastzugängen. Letztere lassen sich beispielsweise bei den verbreiteten Fritzboxen auf Surfen und Mailen begrenzen.

Die neuen Wilden

Durch die oben angesprochenen Probleme befeuert, kamen schon früh Alternativen zu IPsec auf. Diese arbeiten nicht auf Ebene 3 (IP) des OSI-Stacks, sondern auf der Transportebene 4 (TCP, Transmission Control Protocol, oder UDP).

OpenVPN zählt zu den ersten solcher VPNs und ist eine inzwischen weitverbreitete Open-Source-Implementierung. Die Peers authentifizieren sich über eine TLS-Verbindung (Transport Layer Security), ähnlich wie man es von HTTPS kennt, und tauschen darüber auch ihre Schlüssel aus. Die zu transportierenden Daten erhalten einen proprietären Verschlüsselungsheader und werden in UDP-Pakete verpackt. Das vermeidet die von reinen IPsec-Verbindungen bekannten NAT-Probleme. Wenn der VPN-Tunnel über UDP scheitert, kann OpenVPN per Konfigurationseingriff dafür auf HTTPS wechseln.

Das OpenVPN-Konzept war so erfolgreich, dass schnell Nachahmer auf den Plan traten, wenn auch für andere Anwendungsbereiche: **Tinc** soll besonders gut für VPNs mit sehr vielen Standorten skalieren. Es kommt bei Overlay-Community-Netzwerken wie etwa dem Freifunk-InterCity-VPN zum Einsatz.

OpenConnect soll in möglichst allen Netzwerksituationen einen verschlüsselten Tunnel errichten können: Es baut anfangs eine HTTPS-Verbindung zum VPN-Gateway auf, notfalls über einen Proxy. Darüber authentifizieren sich die Gegenstellen und tauschen ihre Schlüssel. Die Datenverbindung versucht OpenConnect dann über einen DTLS-gesicherten UDP-Link zum Gateway herzustellen (Datagram Transport Layer Security: TLS-Äquivalent für UDP). Blockiert eine Firewall den UDP-Tunnel, nutzt OpenConnect die bestehende HTTPS-Verbindung. Sie ist zwar nicht so performant, funktioniert aber in so gut wie allen Umgebungen.

VPN-Wunderkind

Das jüngste Kind im Reigen der VPN-Techniken heißt **Wire Guard**. Es wurde konsequent auf Einfachheit und damit auf Geschwindigkeit getrimmt. Ein einziger, nicht änderbarer Schlüsselalgorithmus einhergehend mit nur einem Authentifizierungsverfahren (Public/Private Key) spart nicht nur Programmcode, sondern baut auch die Verbindung wesentlich schneller auf, weil keine Verschlüsselungsparameter ausgehandelt werden müssen.

Zudem findet der IP-Transport inklusive Ein- und Auspacken der Verschlüsselungsheader bei Linux-Implementierungen komplett im Kernel statt. Daraus ergibt sich ein immenser Geschwindigkeitsvorteil gegenüber den anderen Nicht-IPsec-Verfahren. Ferner klappt das Authentifizieren der Gegenstellen unabhängig von deren IP-Adresse. So werden wechselnde IP-Adressen nicht zum Security-Problem und WireGuard funktioniert problemlos an Internetanschlüssen mit dynamischer Adresszuteilung, sogar mobil mit LTE-Routern.

WireGuard bringt auf manchen Plattformen zwar deutlich mehr Geschwindigkeit als IPsec [3,4], doch spielen für die Einzelplatzeinwahl auch andere Eigenschaften eine Rolle, beispielsweise Optionen für die Nutzerauthentifizierung.

Bekannte Fernarbeiter

Kleine Firmen-VPN-Verbünde lassen sich oft noch in „Handarbeit“ administrieren. Wenn sich aber eine größere Zahl Beschäftigte einwählen soll, müssen die VPN-Verfahren ein gut skalierendes Authentifizierungsverfahren mitbringen, das einen zentralen Server befragt.

In Windows-Netzen ist das der Domänencontroller, der das Active Directory führt. Radius-Server haben auch Vorzüge: Beispielsweise erlauben sie mehrere Einwahl-Gateways, um den Verkehr zu ver-

teilen oder Redundanz vorzuhalten, ohne die Nutzerdatenbank zu duplizieren. Zentrale Benutzersperren, zeitliche Einwahlbeschränkungen, nutzerspezifische Access-Listen und weitere Individualisierungsoptionen erhält man obendrauf.

OpenVPN und OpenConnect unterstützen viele Authentifizierungsmethoden (siehe Tabelle unten). Gerade bei Linux/Unix-Systemen lassen sich zusätzliche Verfahren wie etwa eine Zwei-Faktor-Authentifizierung ohne großen Aufwand über das PAM-API integrieren (Pluggable Authentication Modules).

Im Heimnetz genügen hingegen im Router hinterlegte Zugangsdaten (Nutzername, Passwort, optional zusätzlicher Pre-Shared Key) oder ein Public / Private-Key-Verfahren wie bei WireGuard.

Transporter

Jenseits von IPsec – doch selbst dort, wenn NAT-Traversal gebraucht wird – dient stets UDP als Spediteur, mal mit proprietärer Verschlüsselung, mal mit DTLS, oft verknüpft mit einer TLS-Authentifizierungssitzung.

Manche Protokolle schalten bei Problemen mit dem UDP-Transport auf TCP (OpenVPN) oder HTTPS über TCP um (OpenConnect). Dadurch sinkt zwar die Performance, aber die Verfügbarkeit verbessert sich.

IPv6 sollte heute ebenso als Trägerprotokoll wie auch als im Tunnel transportiertes Protokoll möglich sein. Erstens stellen viele Internetanschlüsse keine öffentliche IPv4-Adresse mehr bereit, was – siehe NAT-Problematik oben – stabile VPN-Verbindungen verhindert. Zweitens wird IPv6 längst in vielen Netzen genutzt: Im Sommer 2021 fiel der tageszeitlich schwankende IPv6-Anteil auf heise.de nicht mehr unter 30 Prozent. Google meldete für Deutschland 52 Prozent IPv6-Verfügbarkeit (siehe google.com/ipv6, Österreich: 17 Prozent, Schweiz: 34 Prozent).

Einer der Vorteile von IPv6: Es kann kein Problem mit überlappenden Adressbereichen im VPN entstehen. Bei IPv4 drohen hingegen Kollisionen, wenn im Ziel- und im gerade besuchten Netz der gleiche private Adressblock genutzt wird. Beispielsweise stellen wohl nur wenige Fritzbox-Nutzer die Werksvorgabe 192.168.178.0/24 auf einen anderen Bereich um.

So gesehen sind sowohl IPsec mit IKEv1 als auch die beliebte L2TP/IPsec-Kombination nicht mehr zeitgemäß. Bei den Alternativen ist inzwischen selbst der Oldie OpenVPN voll IPv6-tauglich. Die jüngeren Konkurrenten waren dies ab Start.

Fazit

Profis, die VPNs zur Standortvernetzung einsetzen, schätzen tinc und WireGuard. Für die Auswahl eines VPN-Providers für Endkunden ergibt sich eine andere Rangfolge: WireGuard glänzt bei der Geschwindigkeit und auf mobilen Clients. IPsec spielt dann seine Vorteile aus, wenn es ohne speziellen Client gehen soll. OpenConnect trumpft dann auf, wenn es widrige Netze zu überwinden gilt. Das verbreitete OpenVPN bleibt als die Universallösung, falls die anderen versagen. (ea) c't

Literatur

[1] Reiko Kaps, **Mauerspechte**, Internet-Dienste trotz DS-Lite nutzen, c't 6/2013, S. 178

[2] Ernst Ahlers, **Server-Umleitung**, Heimserver hinter DS-Lite oder CG-NAT erreichbar machen, c't 2/2018, S. 138

[3] Andrijan Möcker, **Fritz'scher Ausblick**, WireGuard-VPN: Was moderne Fritzboxen leisten (könnten), c't 14/2020, S. 130

[4] **Ernst Ahlers, Beta-Firmware für Fritzbox 7590:** Krasse VPN-Beschleunigung mit WireGuard, ct.de/-6332407

VPN-Typen und ihre Eigenschaften

VPN	IPsec	L2TP/IPsec	OpenConnect	OpenVPN	Tinc	WireGuard
Einwahl / Vernetzung	✓ / ✓	✓ / –	✓ / –	✓ / ✓	– / ✓	✓ / ✓
Hub & Spoke / Full Mesh	✓ / ✓[1]	✓ / –	✓ / –	✓ / ✓[1]	✓ / ✓	✓ / ✓[1]
Verschlüsselung	IPsec	IPsec	HTTPS, DTLS	proprietär	proprietär	proprietär
Clients	alle OS	alle OS	Linux, iOS, Android[2]	alle OS	Linux, Windows	Linux[3]
IPv6-Transport	✓[4]	–	✓	✓	✓	✓
Ethernet-Bridging	–	–	–	✓	✓	–
Authentifizierung						
Zertifikate oder asym. Keys	✓	✓	✓	✓	✓	✓
Pre-Shared Key	✓	✓	✓	✓	✓	✓
Radius	nur mit IKEv2	✓	✓	✓	–	–
Windows AD (Kerberos)	nur mit IKEv2	✓	✓	–	–	–
Zwei-Faktor-Authentifizierung	✓	✓[5]	✓	✓[6]	–	–

[1] kleine Anzahl Standorte, da nur manuell konfigurierbar [2] kommerzielle Versionen für macOS und Windows erhältlich [3] originär für Linux-Kernel entwickelt, im Userspace auch für macOS, Windows, iOS und Android [4] bei IKEv1 kein Mixmode [5] implementierungsabhängig [6] über PAM-Oath-Modul ✓ vorhanden – nicht vorhanden



Bild: Andreas Martini

Mehr Privatsphäre in Windows einstellen

Ein neues Windows? Das bedeutet zwangsläufig, sich erneut mit den Datenschutzoptionen auseinanderzusetzen. Mit unseren Tipps für die richtigen Handgriffe schränken Sie den Datenabfluss zu Microsoft sogar stärker ein, als es die Systemeinstellungen vorsehen.

Von **Jan Schüßler**

Es ist der Dauerbrenner in Sachen Windows: der Datenschutz, mit dem Microsoft schon beim Vorgängersystem Windows 10 kein allzu glückliches Händchen hatte. Als problematisch gilt dabei nicht unbedingt die Tatsache, dass Windows in der Lage ist, recht umfassende Telemetrie-, Analyse-, und sonstige Statistikdaten zu erfassen, sondern dass etliche Optionen standardmäßig aktiv sind – und nicht alle werden während der Ersteinrichtung eines Benutzerkontos abgefragt.

Nach einem Upgrade von Windows 10 auf 11 sollte der Installer die Datenschutzeinstellungen

unverändert übernehmen. Die Betonung liegt hier auf „sollte“, denn hin und wieder funktioniert das nicht verlässlich. Auch nach einem Upgrade schadet es also nicht, einmal alle Einstellungen abzugrasen. So machen Sie sich ganz nebenbei gleich mit der neuen Sortierung der Optionen vertraut. Diese Anleitung zeigt die Einstellungen anhand von Windows 11 – in Windows 10 sind die Optionen ebenfalls enthalten, bloß etwas anders sortiert.

Datenschutz-Einstellungen

Das Gros der Schalter, um den Datenabfluss in Windows zu regeln, sitzt in der Einstellungen-App und dort naheliegenderweise in der Rubrik „Datenschutz & Sicherheit“. Die wichtigsten Optionen liegen dort im Abschnitt mit der Überschrift „Windows-Berechtigungen“. Unter „Allgemein“ können Sie die Werbe-ID abschalten, Websites den Zugriff auf Ihre installierten Sprachen verweigern und die Verwendung von App-Start-Statistiken zum Zwecke personalisierter Suchergebnisse sowie Vorschläge in der Einstellungen-App selbst unterbinden. Alle vier Optionen dienen dazu, Ihnen personalisierte Werbung, Suchergebnisse und sonstige Vorschläge zu präsentieren – wir empfehlen, sie abzuschalten.

Unter „Spracherkennung“ stellen Sie ein, ob Windows cloudgestützte Spracherkennung verwenden darf. Auf die Funktion lokaler (Offline-)Spracherkennung hat diese Option keinen Einfluss. Die „Freihand- und Eingabeanpassung“ dient dazu, ein persönliches Wörterbuch anzulegen, inklusive Handschrift-Erkennungsdaten. Ob Sie das abschalten, ist ein Stück weit Geschmackssache: Wer viel auf einem 2-in-1-Gerät mit Touch- und Stifteingabe unterwegs ist oder gern mit der Sprachassistenz Cortana quatscht, profitiert von besserer Erkennungsqualität, wenn Windows sich oft Gesprochenes oder Eingegebenes merkt.

In „Diagnose und Feedback“ finden Sie einen Schalter, mit dem Sie einstellen, ob Windows nicht nur „erforderliche“, sondern auch optionale Diagnosedaten verschickt. Ist das aktiv, wird Windows mehr Telemetriedaten zur Nutzung des PCs und bei Problemen ausführlichere Fehlerberichte verschicken, die dann auch Dokumentinhalte und Ähnliches enthalten können. Ebenso können Sie dort festlegen, ob solche optionalen Daten auch für Spracherkennungs- und Eingabefunktionen übertragen werden dürfen. Solche Daten können Microsoft dabei helfen, die Gerätenutzung und eventuelle Probleme genauer zu analysieren, um die Softwarequalität zu verbessern. Wenn Ihnen die Idee nicht schmeckt, private Daten zur allgemeinen Qualitätsverbesserung beizusteuern, schalten Sie beides ab.

Der Schalter für „Individuelle Benutzererfahrung“ erlaubt oder untersagt Microsoft außerdem, die Telemetriedaten zu Werbezwecken zu verarbeiten – auch das können Sie getrost deaktivieren. Um seltener bei der Arbeit gestört zu werden, empfiehlt es sich außerdem, die „Feedbackhäufigkeit“ von „Automatisch“ auf „Nie“ zu setzen. Zwar fragt Windows nach unserer Erfahrung ohnehin nur selten bis gar nicht nach Ihrer Meinung – es abzuschalten, kann dennoch nicht schaden.

Unter „Aktivitätsverlauf“ lässt sich einstellen, ob sich Windows kürzlich benutzte Apps, besuchte Webseiten und Ähnliches lokal merkt. Das ist in der Standardeinstellung aktiv, nicht aber die zusätzliche Komfortoption, diese Daten auch an Microsoft zu schicken, um den Verlauf auf anderen Geräten nutzen zu können, die mit dem gleichen Microsoft-Konto laufen. Auch die erste Option abzuschalten, verbessert daher nicht den Datenschutz gegenüber Microsoft, sondern führt zu etwas weniger Benutzungsspuren auf dem jeweiligen Gerät. Eine Überlegung wert ist das vor allem, wenn weitere Personen Ihren PC mit Ihrem Benutzerkonto verwenden – wobei wir generell empfehlen, für jeden Benutzer ein eigenes Konto einzurichten.

In „Suchberechtigungen“ sind die Schalter zum „Cloudinhalte durchsuchen“ nur relevant, wenn Sie Windows oder einzelne Apps mit einem Microsoft- oder einem Azure-AD-Konto verwenden. Außerdem können Sie einstellen, ob der Verlauf der Windows-eigenen Suchfunktion lokal gespeichert werden darf und ob die Ergebnisse von Websuchen im Startmenü auf Jugendfreiheit geprüft werden sollen (aber: Die Websuche möchten Sie möglicherweise ohnehin abschalten – dazu unten mehr).

Die Optionen im Menü „Windows durchsuchen“ sind für den Datenschutz nur in Grenzen relevant: Sie können darin festlegen, welche Ordner der bordeigene Indexdienst für schnellere lokale Suchergebnisse scannen darf.

Im Abschnitt „App-Berechtigungen“ der Datenschutzeinstellungen finden Sie insgesamt 25 Menüs, in denen Sie festlegen können, ob und wenn ja welche Anwendungen auf Ressourcen zugreifen dürfen. So können Sie etwa unter „Position“ einstellen, ob Anwendungen auf den Ortungsdienst zugreifen dürfen, um Ihren geografischen Standort zu erfassen, oder dass außer Teams und Zoom keine Programme auf Webcam und Mikrofon zu-

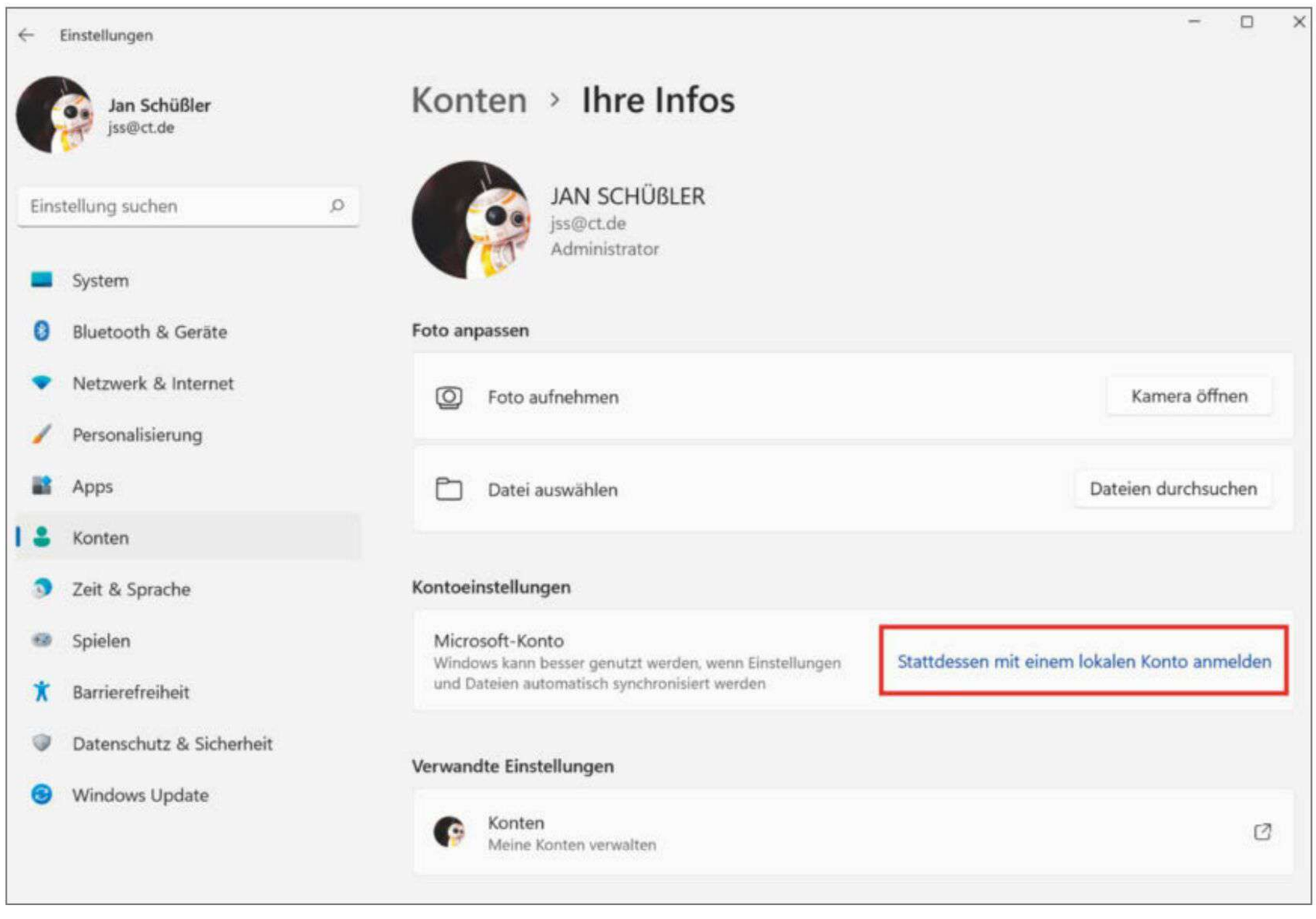
greifen dürfen. Eine kritische Ausnahme bildet das Menü „App-Diagnose“. Darin legen Sie fest, ob Apps ihre Telemetriedaten untereinander austauschen dürfen.

Was Sie ansonsten alles abschalten, ist Geschmackssache. Einerseits kann es kontraproduktiv sein, zu viel abzudrehen: So ist etwa Teams ohne Mikrofon und Kamera nicht sinnvoll zu benutzen, und Karten-Apps werden komfortabler, wenn sie Ihren Standort kennen. Andererseits spricht nicht viel dagegen, erst einmal pauschal alles abzudrehen, was Ihnen unnötig vorkommt. Braucht eine App Zugriff auf eine blockierte Ressource, wird sie Sie darauf hinweisen – dann können Sie die gewünschten Zugriffe gezielt erlauben.

Andere Einstellungen

Überraschung: Nicht nur in der Datenschutz-Rubrik der Einstellungen-App finden sich Optionen, die mehr oder weniger mit Datenschutz zu tun haben oder Tipps und Vorschläge betreffen, wie Sie Ihre Windows-Installation verbessern könnten. So können Sie unter „System/Benachrichtigungen“ am Ende des Menüs festlegen, ob Windows Ihnen Einrichtungstipps und sonstige Vorschläge zur Nutzung unterbreitet. Schalten Sie das ab, es nervt im Alltag nur. Serienmäßig inaktiv hingegen ist immerhin eine Option für Tipps zur Kopplung eines Android-Handys mit der Windows-App „Ihr Smartphone“. Sie befindet sich unter „Bluetooth & Geräte/Ihr Smartphone“.

Unter „System/Zwischenablage“ bietet Windows eine Komfortfunktion, die den Verlauf der Zwischenablage speichern kann. Auch sie ist serienmäßig abgeschaltet. Da der Verlauf lokal gespeichert wird, birgt es kein Datenschutzrisiko, sie zu aktivieren. Bedenken Sie aber, dass andere Personen, die Sie über Ihr Benutzerkonto an den PC lassen, den Verlauf einsehen könnten. Datenschutzrelevant gegenüber Microsoft wird der Zwischenablageverlauf allerdings, wenn Sie sich mit einem Microsoft-Konto am PC anmelden und dann zusätzlich die Option „Auf allen Geräten synchronisieren“ scharfschalten, um



Windows lässt sich problemlos von einem Microsoft- auf ein lokales Konto umstellen – auch in der Home-Edition.

den Inhalt der Zwischenablage auf andere Geräte zu synchronisieren – denn das geschieht über die Microsoft-Cloud.

Noch eine Einstellung, die relevant sein kann, wenn weitere Menschen außer Ihnen den PC mit Ihrem Benutzerkonto verwenden, finden Sie in „Personalisierung/Start“. Wenn Sie „Zuletzt geöffnete Elemente in Start, Sprunglisten und im Datei-Explorer anzeigen“ ausschalten, sehen Sie nicht mehr, welche Dateien Sie zuletzt benutzt haben. Im Startmenü fällt das sofort auf: Der untere Bereich („Empfohlen“) wird geleert.

Bleibt noch ein weiteres Menü, in dem es um personalisierte Tipps geht, die Windows Ihnen unterbreiten kann: Sind unter „Personalisierung/Geräteverwendung“ Schalter aktiviert, kann Windows Ihnen Werbung und Tipps für den jeweiligen Verwendungszweck anzeigen. Serienmäßig sind die Schalter alle aus – es sei denn, Sie haben während der Ersteinrichtung des Systems welche betätigt. Wer mag, kann nun auch noch unter „Zeit & Sprache/Eingabe“ die Eingabevorhersage abschalten – die allerdings ohne personalisierte Tastaturfunktionen ohnehin nicht mehr allzu viel bringt.

Lokales Konto

Eine weitere Möglichkeit, den Datenschutz-Level ein wenig anzuheben, ist es, sich an Windows nicht mit einem Microsoft-Konto, sondern mit einem rein lokalen Profil anzumelden. Bis einschließlich Windows 7 war das außerhalb von Firmenumgebungen die einzige Anmeldemöglichkeit. Seit Windows 8 versucht Microsoft allerdings mal mehr, mal weniger nachdrücklich, Anwender zur Nutzung eines Microsoft-Kontos zu animieren oder gar zu nötigen. Besonders davon betroffen sind in Windows 11 Nutzer der Home-Edition, für die es während der Neuinstallation eines Tricks bedarf, am Microsoft-Konto vorbeizukommen [1].

Um die Anmeldung auf ein lokales Konto umzustellen, klicken Sie in den Einstellungen unter „Konten/Ihre Infos“ auf „Stattdessen mit einem lokalen Konto anmelden“. Vor dem Umstellen verlangt Win-

Business-E-Mail für geschäftskritische Anwendungen und digitale Arbeitsplätze?

100 % DSGVO-konform?

Intelligent und ausfallsicher?

DIE SECURE EMAIL PLATFORM!

retarus.de/secure-email-platform

VIELE WICHTIGE FRAGEN. EINE GUTE ANTWORT.

retarus

dows von Ihnen die Eingabe von PIN oder Microsoft-Konto-Passwort und fordert Sie dann auf, dem lokalen Konto ein neues Passwort zu geben. Das Feld „Kennworthinweis“ darf nicht leer bleiben – wenn Sie das unsinnig finden, tragen Sie einfach irgendwas ein.

Wenn Sie auf einer Windows-Home-Edition die Anmeldung auf ein lokales Konto umstellen wollen und die „Geräteverschlüsselung“ aktiv ist (eine funktionsreduzierte Variante der Laufwerksverschlüsselung BitLocker), werden Sie aufgefordert, zuvor den BitLocker-Wiederherstellungsschlüssel zu sichern. Üblicherweise wird der bei der Ersteinrichtung des Gerätes automatisch im Microsoft-Konto hinterlegt. Dieser Aufforderung sollten Sie unbedingt nachkommen! Denn wenn Ihr System einmal ein Startproblem hat und Sie es zum Beispiel mit dem c’t-Notfall-Windows reparieren möchten, ist der Wiederherstellungsschlüssel der einzige Weg, das verschlüsselte Laufwerk zu öffnen. Um ihn zu sichern, klicken Sie in den Einstellungen unter „Datenschutz & Sicherheit/Geräteverschlüsselung“ auf „BitLocker-Laufwerkverschlüsselung“ und dann auf „Wiederherstellungsschlüssel sichern“.

Ob das lokale Benutzerkonto immer die bessere Wahl ist, ist auch eine Geschmacksfrage. Das Microsoft-Konto hat durchaus Vorteile: Synchronisierung von Einstellungen, Nutzung des Store, Ortungsfunktion für vermisste Geräte und Ähnliches. Zudem sorgt ein lokales Konto als solches nicht automatisch dafür, dass weniger Daten an Microsoft fließen – es wird aber schwieriger, sie Ihnen zuzuordnen. Ein sinnvoller Weg kann es sein, zur Anmeldung an Windows ein lokales Konto zu verwenden, und sich für Funktionen, die ein Microsoft-Konto erfordern, damit nur an der jeweiligen App anzumelden. Dafür klicken sie im Anmeldedialog nach Eingabe von Benutzername und Passwort im Schritt „Dieses Konto überall auf Ihrem Gerät verwenden“ nicht auf „Weiter“, sondern auf „Nur Microsoft-Apps“. Auf diese Weise lassen sich sogar verschiedene Apps oder Systemfunktionen mit verschiedenen Microsoft-Konten verwenden.

Ganz abdrehen

Sie können die Übertragung von Daten an Microsoft noch weiter einschränken. Einen gängigen Tipp von Windows 10 empfehlen wir auch bei Windows 11 anzuwenden: Um den Versand von Telemetriedaten wirklich auf null herunterzudrehen, braucht man eine Windows-Enterprise-Edition, die per firmeninternem WSUS mit Updates versorgt wird – eigentlich, denn man kann auch einfach den Windows-Dienst „DiagTrack“ abschalten. Dazu öffnen Sie die Diensteverwaltung, etwa per Windows-Taste, `services.msc`, Eingabetaste, suchen den Eintrag „Benutzererfahrungen und Telemetrie im verbundenen Modus“ und doppelklicken darauf. Setzen Sie den Starttyp auf „Deaktiviert“, klicken Sie auf „Beenden“ und dann auf OK.

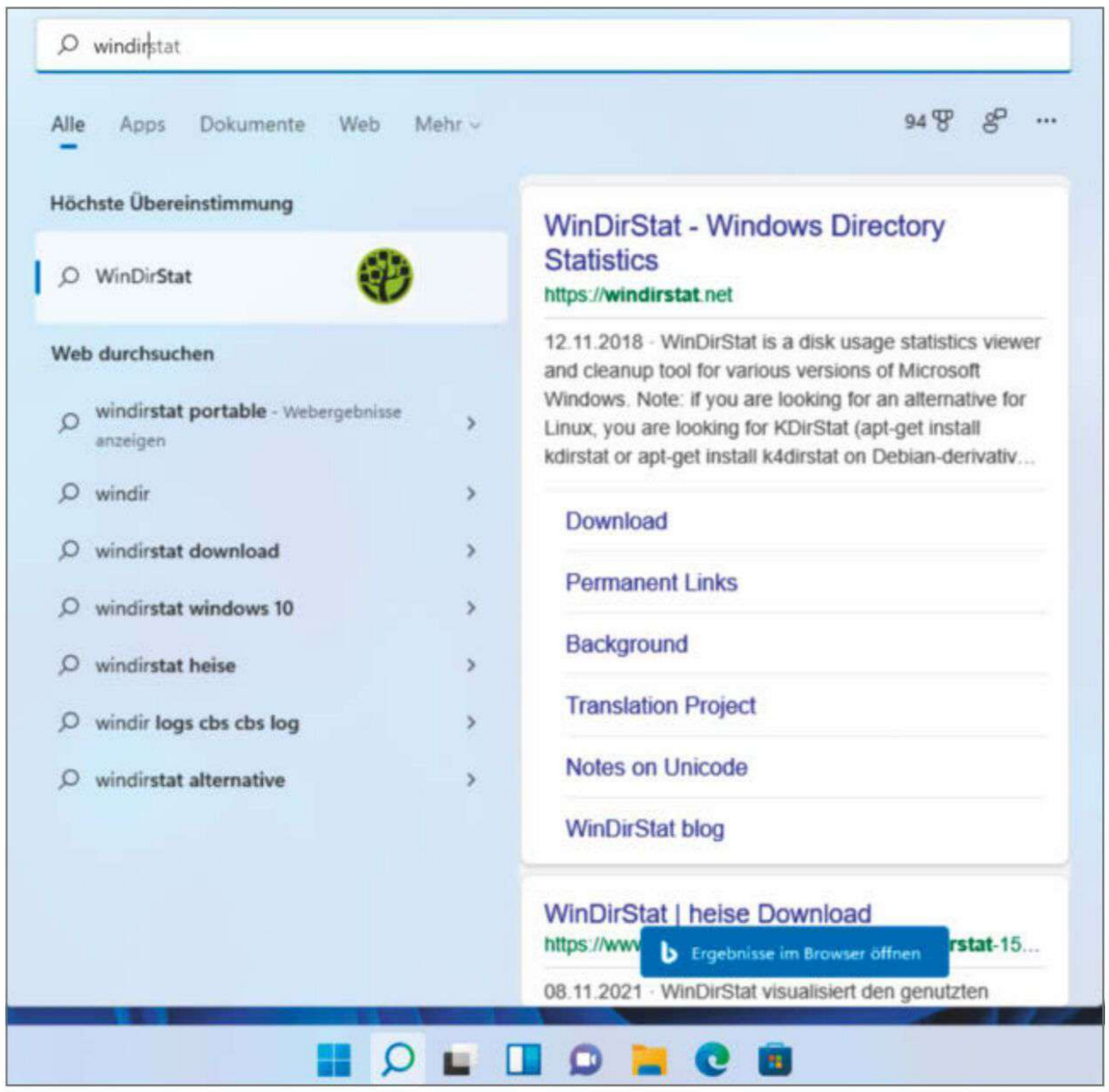
Nachteile durch die Abschaltung des Dienstes sind uns in mehrjähriger Erfahrung mit Windows 10 und inzwischen auch ein paar Monaten Windows 11 nicht aufgefallen; Updates kommen wie geplant und auch ansonsten verhält sich das System unauffällig. Auch konnten wir bislang nicht beobachten, dass Windows den Dienst früher oder später ohne Zutun wieder aktivieren würde. Dennoch empfehlen wir, hin und wieder nachzuschauen, ob der Dienst in der Übersicht noch als „Deaktiviert“ gelistet ist – in jedem Fall nach den großen Funktions-Upgrades, am besten aber auch nach den regulären monatlichen Updates.

Suche nur lokal

Eine beliebte Funktion in Windows, die sich zum Öffnen von Programmen, Einstellungen und Dokumenten eignet, ist die Startmenü-Suche. Auch wir empfehlen sie immer wieder, zum Beispiel im vorigen Tipp: Windows-Taste drücken und drauflos tippen. Aber: In der Standardeinstellung landen alle



Um den Versand von Telemetriedaten so weit wie möglich zu reduzieren, empfiehlt es sich, auch den Dienst „DiagTrack“ abzuschalten.



Die Web-Suchergebnisse im Startmenü nerven? Keine Sorge, das lässt sich abschalten.

Sucheingaben automatisch auch bei Microsofts Suchdienst Bing. Dass sich das selbst dann komisch anfühlt, wenn man nichts hochgradig Geheimes auf dem PC anstellt, ist verständlich.

Abschalten lässt sich das nur mit einem Registry-Eingriff. Öffnen Sie den Registry-Editor (Windows-Taste, `regedit`, Eingabetaste) und klicken Sie sich zum Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows durch. Ist in der Baumansicht in der linken Fensterhälfte der Schlüssel „Windows“ markiert, klicken Sie in der rechten Fensterhälfte mit der rechten Maustaste in den leeren Bereich und legen einen neuen Schlüssel an, dem Sie den Namen „Explorer“ geben. Markieren Sie den neuen Schlüssel wiederum in der Baumansicht und legen Sie darin ein neues DWORD an, das den Namen `DisableSearchBoxSuggestions` bekommt. Doppelklicken Sie auf den neuen Eintrag und ändern Sie seinen Wert auf 1. Nach einem Neustart des Rechners sollte die Windows-Suche keine Webergebnisse mehr anzeigen.

Der Registry-Eintrag schaltet die Startmenü-Websuche systemweit ab. Wenn Ihnen das zu weit geht, können Sie die Änderung stattdessen nur für das gerade angemeldete Benutzerkonto vornehmen – ersetzen Sie dafür das HKEY_LOCAL_MACHINE im Schlüsselpfad einfach durch HKEY_CURRENT_USER. Unter ct.de/wnk8 finden Sie REG-Dateien zum Download, mit denen Sie die Änderung einfach per Doppelklick auf Ihr System anwenden können. Die Dateien funktionieren sowohl mit Windows 10 als auch mit Windows 11.

Viren-Samples

Noch eine Datenschutzeinstellung gefällig? Der bordeigene Virenwächter Defender ist serienmäßig so eingestellt, dass er verdächtige, aber bislang unbekannte Dateien automatisch zur Analyse an die Microsoft-Cloud schickt. Laut Microsoft warnt der Defender, falls die Datei persönliche Daten enthalten könnte – erlebt haben wir so einen Fall noch nicht. Im laufenden Betrieb mit gängigen Anwendungen dürfte man mit dieser Funktion kaum in Kontakt kommen, doch ein wenig anders sieht es für Softwareentwickler aus. Schaltet man den Sample-Versand nicht ab, kann mitunter jede neu kompilierte Version eines Programms bei Microsoft landen – das gilt übrigens nicht nur für den Defender, sondern im Prinzip für jeden halbwegs modernen Virenwächter mit cloudgestützter Schutzfunktion.

Wer Programme entwickelt und vermeiden will, dass frischer Code automatisiert in fremde Hände gelangt, sollte die Funktion „Automatische Übermittlung von Beispielen“ daher ausschalten. Das geht in der App „Windows-Sicherheit“ unter „Viren- & Bedrohungsschutz/Einstellungen verwalten“. Für alle anderen empfiehlt es sich, die Funktion aktiv zu lassen.

Fazit

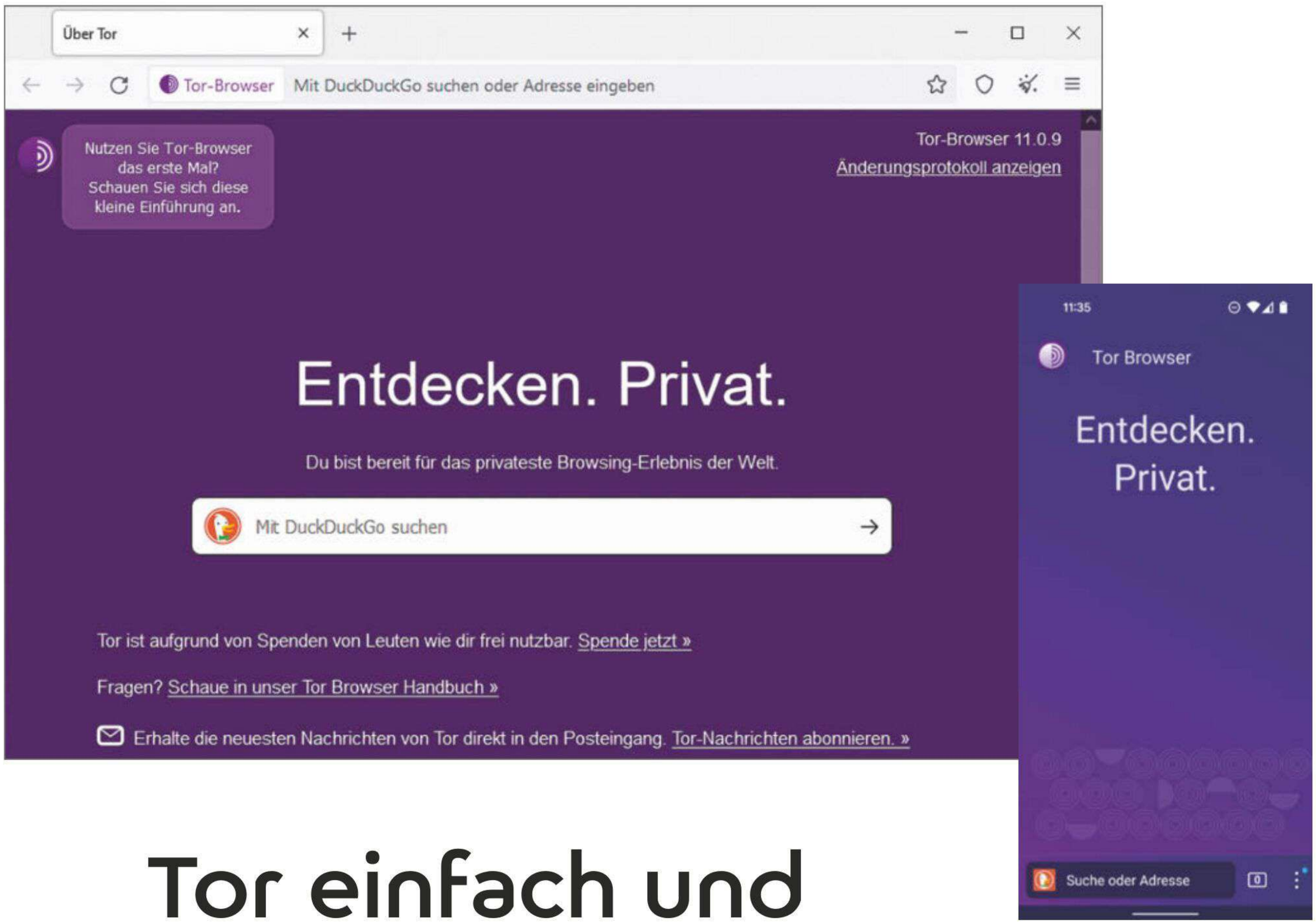
Auch bei Windows 11 erfordern viele wünschenswerte Einstellungen ein manuelles Eingreifen nach der Installation oder sogar Registry- und ähnliche Tricks. Erfreulicherweise funktionieren die von Windows 10 bekannten Handgriffe nach wie vor, sodass man sich als frischgebackener Windows-11-User nicht umstellen muss. (jss) c't

Literatur

[1] Axel Vahldiek, **Bitte einsteigen!**, Windows 11 installieren, c't 26/2021, S. 24

REG-Dateien

ct.de/wnk8



Tor einfach und sicher nutzen

Mit wenigen Klicks surfen Sie anonym über Tor im Netz – ganz gleich, ob unter Windows, Linux, macOS oder auf dem Smartphone. Doch es gilt ein paar Dinge zu beachten, damit Sie tatsächlich anonym bleiben.

Von **Ronald Eikenberg**

Der Einstieg in das Anonymisierungs-Netzwerk Tor ist schnell geschafft und nicht komplizierter als eine Browser-Installation. Der kostenlose Tor Browser bringt alles mit, was Sie brauchen. Es genügt ein Klick, um eine Verbindung mit dem Tor-Netz aufzubauen und anonym zu surfen – sowohl im öffentlichen Internet als auch im „Dark Web“. Die Einrichtung ist fast selbsterklärend, die Nutzung des Tor-Netzes birgt jedoch Risiken, die Sie kennen sollten, um Ihre Privatsphäre zu schützen. Dieser Artikel liefert Ihnen das nötige Wissen und begleitet Sie bei Ihren ersten Schritten.

Installation unter Windows …

Um sicherzustellen, dass Sie sich keine manipulierte Version einfangen, sollten Sie den Tor Browser ausschließlich auf **https://torproject.org** herunterladen. Vor der Installation können Sie die digitale Signatur der Datei überprüfen, um zu verifizieren, dass die Datei tatsächlich vom Tor-Projekt stammt und nicht verändert wurde (siehe ct.de/wupm).

Führen Sie die Installationsdatei anschließend aus und wählen Sie erneut „Deutsch“. Im nächsten Schritt fällt auf, dass der Installer standardmäßig den Ordner „Tor Browser“ auf dem Desktop als Installationsziel und nicht „Programme“ nutzt. Das liegt daran, dass es sich bei dem Tor Browser um eine portable Anwendung handelt. Sie können den Ordner also jederzeit an einen beliebigen Ort verschieben – sogar auf einen USB-Stick, um Tor mit anderen Rechnern zu nutzen. Klicken Sie auf „Installieren“, damit sich das Setup-Programm ans Werk macht und alle Dateien an ihr Ziel befördert.

Im letzten Schritt legt der Installer auf Wunsch eine Verknüpfung im Startmenü und auf dem Desktop an, damit Sie den Tor Browser künftig komfortabel starten können. Außerdem können Sie auswählen, dass Tor im Anschluss an die Installation direkt gestartet wird. Das war auch schon alles, Ihr Tor Browser ist jetzt einsatzbereit.

… Linux …

Unter Linux führt der schnellste Weg zum Tor Browser über den torbrowser-launcher (siehe ct.de/wupm), der allerdings nicht offiziell zum Tor-Projekt gehört. Der Launcher nimmt Ihnen alles ab: Ist Tor noch nicht vorhanden, lädt er die aktuelle Version in der passenden Sprache für Sie herunter, überprüft die digitale Signatur und legt eine Verknüpfung im Anwendungs-Launcher an, damit Sie Tor bequem starten können.

Im besten Fall können Sie den praktischen Helfer einfach als `torbrowser-launcher` über die Paketverwaltung Ihrer Linux-Distribution oder den Software-Katalog installieren. Klappt das nicht, bekommen Sie den Launcher als Flatpak-Paket. Stellen Sie zunächst sicher, dass `flatpak` installiert ist (siehe ct.de/wupm). Anschließend beziehen Sie das Paket mit dem folgenden Befehl: `flatpak install flathub com.github.micahflee.torbrowser-launcher -y`

Der sicherste, aber etwas aufwendigere Weg ist auch unter Linux die offizielle Website **torproject.org**. Ändern Sie oben rechts die Sprache auf Deutsch und



Die offizielle Website torproject.org ist die sicherste Quelle für aktuelle Versionen des Tor Browser.

laden Sie anschließend im Downloadbereich die Linux-Version herunter. Sie erhalten ein komprimiertes XZ-Dateiarchiv, das zum Beispiel wie folgt benannt ist: tor-browser-linux64-11.0.9_de.tar.xz. Auch hier können Sie die digitale Signatur überprüfen, um Manipulationen an der Datei auszuschließen (siehe ct.de/wupm).

Die anschließend nötigen Befehle erledigen Sie am besten übers Terminal, dieser Weg ist bei allen Linux-Distributionen gleich. Zunächst müssen Sie die Datei entpacken: `tar -xf tor-browser-linux64-11.0.9_de.tar.xz`. Anschließend wechseln Sie mit `cd` in den entpackten Ordner, der zum Beispiel tor-browser_de heißt. Danach stellen Sie sicher, dass das Startskript als ausführbar markiert ist: `chmod +x start-tor-browser.desktop`. Jetzt können Sie den Tor Browser einfach starten: `./start-tor-browser.desktop`

… und macOS

Auch Mac-Nutzer holen sich den Tor Browser am besten über torproject.org wie oben beschrieben. Der Knopf „Download für macOS“ liefert Ihnen ein Disk Image wie TorBrowser-11.0.9-osx64_de.dmg, dessen digitale Signatur Sie leicht überprüfen können, um Manipulationen auszuschließen (siehe ct.de/wupm). Um die Installation zu starten, klicken Sie einfach auf die DMG-Datei. Es öffnet sich ein kleines Fenster, in dem Sie den Tor Browser ein Stück nach rechts in das Appverzeichnis ziehen. Jetzt ist die Installation auch schon abgeschlossen und Sie können Tor starten. Falls Sie macOS beim Start des Browsers fragt, ob Sie diese App aus dem Inter-

Vertraue niemanden

Der Einstieg ins Tor-Netz ist schnell und einfach. Das sollte Sie allerdings nicht dazu verführen, fortan Ihren gesamten Internet-Verkehr durch das Anonymisierungsnetz zu schleusen. Das Tor-Netz ist offen und anonym, jeder kann daran teilnehmen. Sie wissen grundsätzlich nicht, mit wem Sie es zu tun haben und sollten stets ein angemessenes Maß an Misstrauen an den Tag legen.

Wenn Sie über Tor auf das normale Internet zugreifen, wird Ihr Verkehr aus dem Tor-Netz durch einen Exit Node dorthin geleitet. Dieser kennt Sie zwar nicht, er kann den Datenverkehr jedoch mitlesen und manipulieren. Alles, was nicht verschlüsselt ist, rauscht im Klartext vorbei. Meiden Sie daher HTTP-Adressen und rufen Sie stattdessen ausschließlich HTTPS-Adressen auf, damit die Daten in jedem Fall transportverschlüsselt zum Zielserver übertragen werden.

Geben Sie persönliche Daten wenn überhaupt nur auf HTTPS-Sites ein. Erscheint beim Aufruf der Site eine Zertifikatswarnung, sollten Sie kehrtmachen. Das kann ein Indiz dafür sein, dass jemand versucht, den verschlüsselten Datenverkehr mitzulesen. Halten Sie Tor stets auf dem aktuellen Stand, da insbesondere im Browser immer wieder Sicherheitslücken geschlossen werden.

net tatsächlich ausführen möchten, bestätigen Sie dies.

Der erste Start

Im Tor Browser finden sich Firefox-Nutzer sofort zurecht. Sie können jedoch noch nicht lossurfen, da der Browser von sich aus keine Verbindung mit dem Tor-Netz aufbaut. Wählen Sie „Immer automatisch verbinden“ aus und klicken Sie auf „Verbinden“, damit die Leitung künftig immer steht, sobald Sie den Tor Browser starten. Das ist sinnvoll, da Sie den Browser ohne Tor-Verbindung ohnehin nicht nutzen können.

Wenige Sekunden später sollte die Verbindung stehen und Sie können anonym surfen. Wenn Sie die deutschsprachige Version installiert haben, wird er Ihnen raten, die bevorzugte Sprache zum Abrufen von Websites auf Englisch zu ändern. Das dient vor allem der Anonymität, denn die angesteuerten Websites erfahren so nicht, dass Sie ein deutschsprachiger Nutzer sind. Entscheiden Sie individuell, ob Sie diesen Kompromiss eingehen möchten.

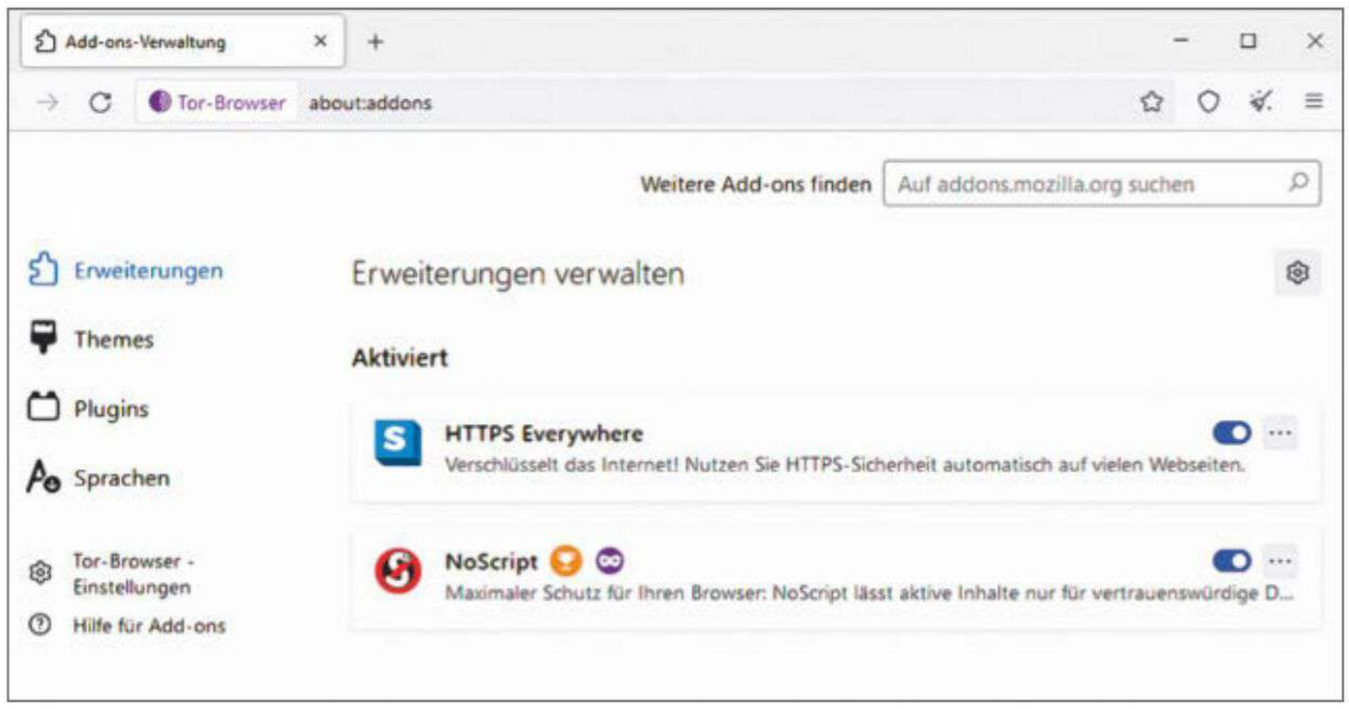
Wenn Sie jetzt zum Beispiel **https://heise.de** aufrufen, erfolgt der Abruf anonymisiert und verschlüsselt über das Tor-Netz. Die „letzte Meile“ vom Tor-Netz zum eigentlichen Server läuft über das reguläre Internet. Der Server heise.de sieht lediglich, dass der Abruf mit hoher Wahrscheinlichkeit von einem Tor-Ausgangsknoten (Exit Node) stammt, dort verläuft sich jedoch die Spur. Sie surfen mit der IP-Adresse des Exit Nodes, was Sie zum Beispiel über **https://check.torproject.org** oder **https://ct.de/ip** verifizieren können.

Onion Services nutzen

Den Weg durchs reguläre Internet auf der „letzten Meile“ fällt weg, wenn Sie Dienste nutzen, die ebenfalls am Tor-Netz teilnehmen, sogenannte Tor Onion Services. Diese erkennen Sie an der Endung .onion. Ein paar interessante Onion Services finden Sie beim Tor Project (siehe ct.de/wupm). Die Adresse der Deutschen Welle lautet zum Beispiel: **https://dwnewsgngmhlplxy6o2twtfgjnrnjxbegbwqx6wnotdhkzt562tszfid.onion**

Praktisch ist, dass Sie der Browser in der Adressleiste automatisch darauf hinweist, wenn die gerade besuchte, reguläre Website auch als Onion Service erreichbar ist. Klicken Sie in solchen Fällen einfach auf den lila Knopf „.onion verfügbar“, um ins Tor-Netz zu wechseln.

Im Tor-Netz gibt es viele dunkle Ecken, zum Beispiel Hackerforen und Shops, die verbotene Dinge im Sortiment führen. Lassen Sie sich vom Deckmantel der Anonymität nicht verleiten, gegen geltende Gesetze zu verstoßen, denn auch Tor ist kein rechtsfreier Raum. Zwar lassen sich Tor-Nutzer kaum anhand Ihrer Verbindungen identifizieren, sehr wohl aber anhand der Daten, die sie bei den Onion Services hinterlassen, wenn sie dort etwa einen Account anlegen oder eine Bestellung aufgeben.



Der Tor Browser bringt die essenziell wichtigen Erweiterungen HTTPS-Everywhere und NoScript mit.

Anonymität schützen

Der Tor Browser basiert auf Firefox ESR (Extended Support Release) und wurde umfangreich angepasst, damit Ihre Anonymität bestmöglich geschützt wird. So sind zum Beispiel die beiden Browser-Erweiterungen „HTTPS Everywhere“ und „NoScript“ vorinstalliert. HTTPS Everywhere versucht wann immer möglich eine transportverschlüsselte HTTPS-Verbindung zum Zielserver aufzubauen, NoScript schränkt die Ausführung von Skripten ein, da diese ein Risiko für Sicherheit und Privatsphäre darstellen können.

Darüber hinaus verhindert der Tor Browser effektiv das sogenannte Browser-Fingerprinting, bei dem Server individuelle Browser-Merkmale nutzen, um Nutzer wiederzuerkennen – ganz ohne Cookies. Ein solches Merkmal ist die Fenstergröße des Browsers, weshalb der Tor Browser den Inhaltsbereich stets auf bestimmte feste Größen skaliert, wenn Sie die Fenstergröße verändern. Am besten ist aber die empfohlene und beim Start des Browsers eingestellte Standardgröße, da sie bei sehr vielen Nutzern im Einsatz ist und Sie somit in der Masse untertauchen.

Interessant sind noch die ersten beiden Buttons rechts neben der Adressleiste: Über das Schutzschild können Sie die Sicherheitsstufe des Browers ändern. Mit der Stufe „Standard“ können Sie weitgehend ungehindert surfen, da alle Websites wie gewohnt funktionieren sollten. Auf „Sicherer“ zieht der Browser die Zügel an und blockiert etwa die Ausführung von JavaScript auf Websites, die nicht über HTTPS ausgeliefert werden. Eingebettete Mediendateien werden nicht mehr automatisch abgespielt, stattdessen müssen Sie zunächst draufklicken (Click-to-Play).

Die Sicherheitstufe „Am sichersten“ hält, was sie verspricht: Es sind nur statische Inhalte auf Websites erlaubt, Skripte werden auf allen Websites blockiert. Mediendateien und WebGL-Inhalte müssen Sie per Mausklick aktivieren, um sie nutzen zu können. Je höher Sie die Stufe setzen, desto häufiger müssen Sie mit Einschränkungen beim Surfen rechnen, dafür genießen Sie umso mehr Schutz.

Der Knopf mit dem Kehrbesen verschafft Ihnen per Klick eine neue Identität: Der Tor Browser vergisst daraufhin die aktuelle Sitzung und startet neu. Auch die Verbindung zum Tor-Netz wird neu aufgebaut, wodurch Sie wahrscheinlich einen neuen Exit Node erwischen und mit einer anderen externen IP-Adresse im Internet surfen.

Sauberer Rechner vorausgesetzt

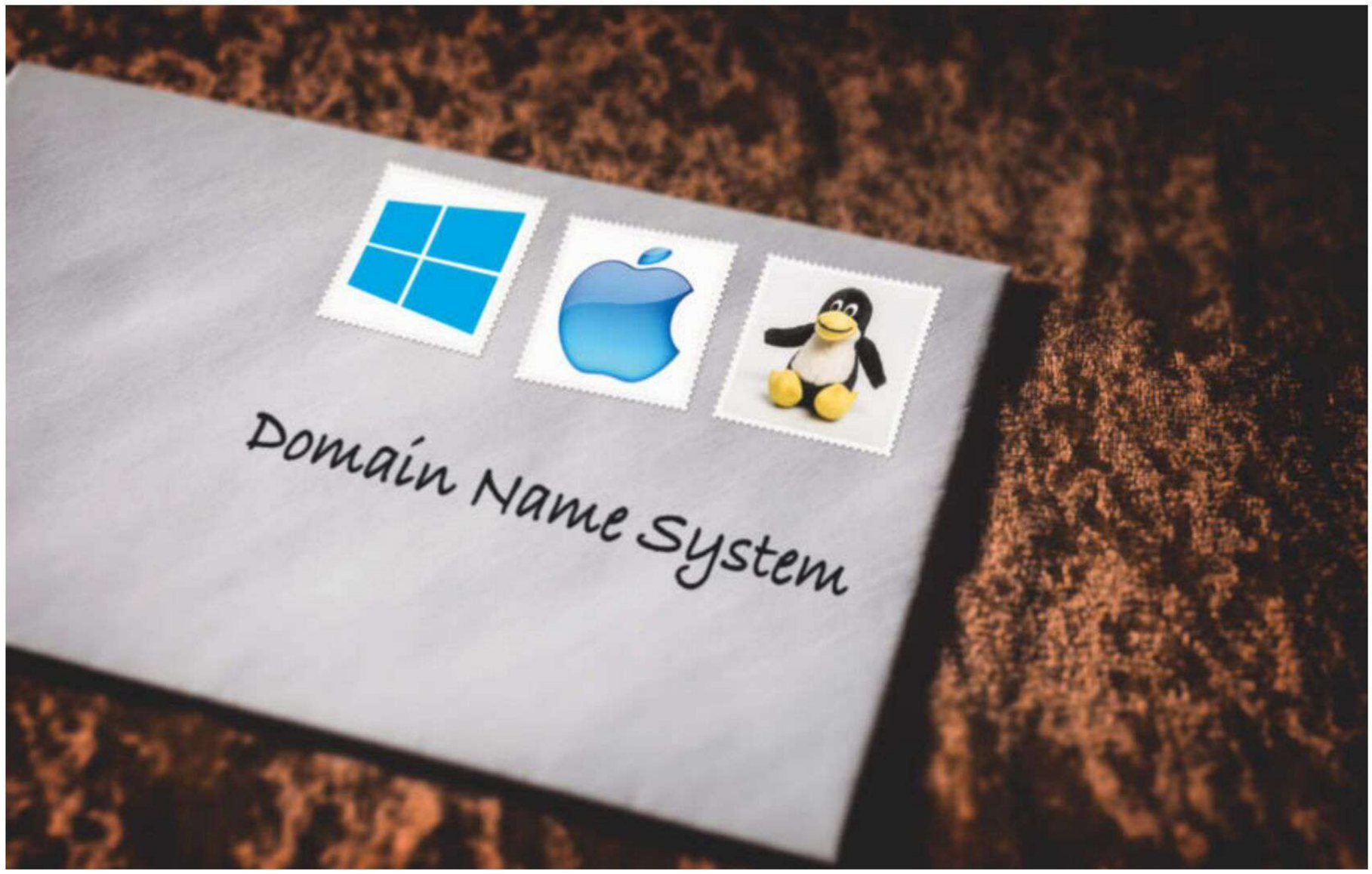
Der Tor Browser hat keinen Einfluss darauf, was um ihn herum auf Ihrem System passiert. Hat sich auf Ihrem Rechner eine Spionagesoftware eingenistet, kann Ihnen diese bei der Tor-Nutzung über die Schulter schauen. Wenn Sie auf Nummer sicher gehen wollen, booten Sie ein Live-Linux, das garantiert sauber ist und mit dem Herunterfahren sämtliche Eingaben und Änderungen am System vergisst. Für die Tor-Nutzung ist Tails ideal, das so vorkonfiguriert ist, dass es ausschließlich über das Tor-Netz mit dem Internet kommuniziert (siehe ct.de/wupm). Es bringt zudem einige Tools für Privatsphäre und gegen Zensur mit.

Tor to go

Der Tor Browser fühlt sich auch auf Ihrem Smartphone oder Tablet wohl. Für Android können Sie ihn entweder als APK-Datei von torproject.org beziehen oder über Google Play. Über F-Droid können Sie ihn ebenfalls installieren, nachdem Sie das Guardian-Repository hinzugefügt haben (siehe ct.de/wupm). Die Androidversion basiert auf Firefox und bedient sich ganz ähnlich wie die oben beschriebenen Desktopversionen. iOS-Nutzern empfiehlt das Tor-Projekt die App „Onion Browser“ von Mike Tigas, die Sie über den App Store installieren können (siehe ct.de/wupm). Die Sache hat allerdings einen Haken: Apple erlaubt unter iOS keine alternativen Browser-Engines, weshalb der Onion Browser die WebKit-Engine von iOS nutzen muss. Dadurch bietet er nicht das gleiche Maß an Anonymität. (rei) c't

Download und weitere Infos

ct.de/wupm



Privatsphärenschutz mit DNSCrypt-Proxy

Die Internet Engineering Task Force bereitet ein neues Protokoll für den Privatsphärenschutz vor, genauer, zur anonymen DNS-Kommunikation. Apple bietet auf dieser Basis einen kostenpflichtigen Dienst an. Doch den Schutz können Sie auch gratis bekommen, und zwar nicht nur für macOS, sondern auch für Linux und Windows.

Von **Dušan Živadinović**

Die Unternehmen Apple, Cloudflare und Fastly haben vor einiger Zeit ein Konzept zum Privatsphärenschutz aufgegriffen, das Paul Schmitt und weitere Mitarbeitende der Universität Princeton 2019 vorgestellt haben. Dabei geht es darum, die IP-Adressen von Nutzern bei der Kommunikation mit dem Domain Name System (DNS) zu verbergen. Netzwerkgeräte müssen nämlich vor jeder Verbindung Domainnamen zu IP-Adressen auflösen lassen und diesen Service bietet das DNS.

Wenn man aber das DNS nach IP-Adressen zu bestimmten Domains befragt, legt man offen, welche

Internet-Seiten man besucht. Das können Angreifer nutzen, um DNS-Antworten zu manipulieren, stille Mitleser aus reiner Neugierde oder für den Verkauf von Userprofilen an Werbetreibende oder als vorbereitende Maßnahme zur Industriespionage. Die DNS-Anfragen lassen sich an vielen Stellen im Internet leicht abgreifen, weil sie größtenteils unverschlüsselt sind.

Mittlerweile verbreiten sich verschlüsselnde Protokolle wie DNS-over-TLS und DNS-over-HTTPS, die die DNS-Kommunikation auf dem wichtigsten Teilstück, nämlich zwischen dem Benutzergerät und dem DNS-Resolver kryptografisch absichern. Der Resolver-Betreiber erfährt aber trotz Verschlüsselung, welcher Internetanschluss welche Domains ansteuert und kann so weiterhin Profile von Anwendern erstellen.

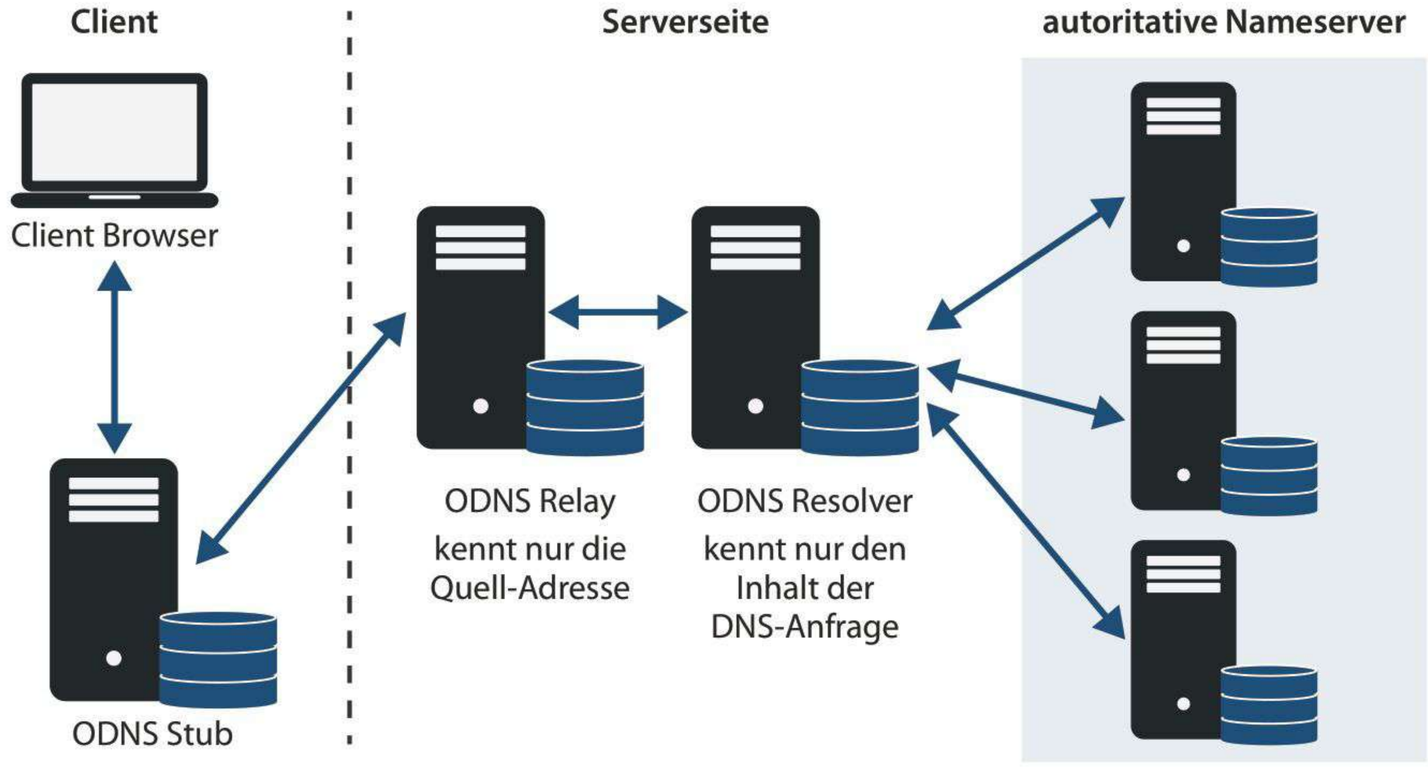
Stark verkürzt kann man sagen: Paul Schmitt und Kollegen schlagen eine zusätzliche Schicht in der DNS-Architektur vor, um die Nutzer-IP-Adressen vor dem Resolver-Betreiber zu verbergen. Apple, Cloudflare und Fastly haben dieses Konzept weiterentwickelt und definieren zurzeit einen herstellerübergreifenden Standard. Er gründet auf DNS-over-HTTPS und heißt Oblivious DoH, kurz ODoH. Apple bietet auf dieser Grundlage eine kostenpflichtige Funktion im Rahmen des Angebots „Private Relay“ an. Nutzer des Apple-Dienstes iCloud+ können es als Beta-Version in den Betriebssystemen iOS 15 und macOS 12 aktivieren.

Wenig bekannt ist, dass man Schmitts Konzept auf zahlreichen Betriebssystemen abseits des Apple-Universums nutzen kann. Eine Entwicklergruppe, die das quelloffene Protokoll DNSCrypt selbstständig vorantreibt, hat die Anonymisierung der DNS-Kommunikation in den eigenen Client DNSCrypt-Proxy implementiert. Die Software ist gratis für diverse Unix- und Linux-Plattformen sowie für Windows und macOS erhältlich (siehe ct.de/wxje).

So kann man etwa auch den beliebten DNS-Filter Pi-hole mit DNSCrypt-Proxy aufrüsten. Wie das geht, haben wir bereits gezeigt (ct.de/wxje). Um darauf

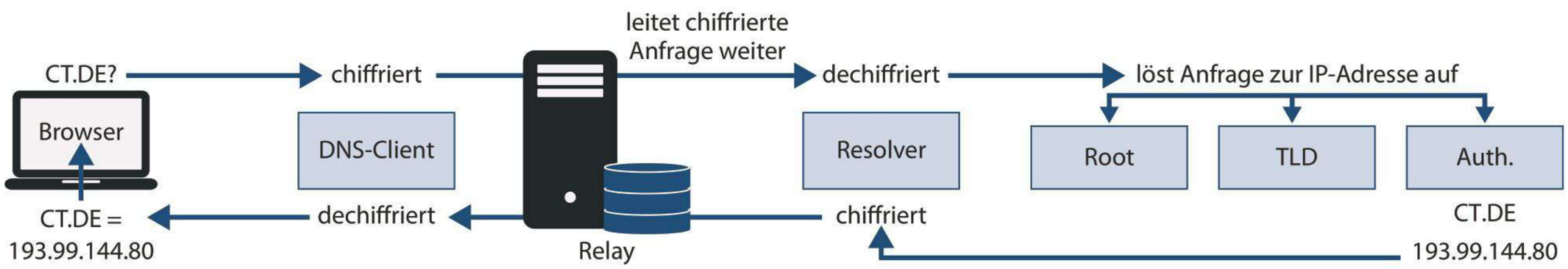
DNS-Hierarchie mit Anonymisierung

Eine zusätzliche Schicht in der DNS-Hierarchie verbirgt die Quell-IP-Adresse des Clients vor dem Resolver. Der Resolver-Betreiber kann so keine Nutzerprofile mehr erstellen. Voraussetzung dafür ist, dass Relay und Resolver verschiedene Institutionen oder Firmen betreiben.



Anonyme DNS-Auflösung

Die anonyme DNS-Auflösung setzt ein zusätzliches Relay voraus, an das ein Client seine Anfragen schickt. Das Relay kennt dann zwar die IP-Adresse des Clients, nicht aber den Inhalt der Anfrage. Es leitet sie an den Resolver weiter, der sie entschlüsselt. Damit kennt der Resolver den Inhalt, nicht aber den Absender.



die Anonymisierung zu aktivieren, muss man die in diesem Artikel vorgestellte Konfiguration auf den Pi-hole und DNSCrypt-Proxy aktualisieren.

Die Entwickler des DNSCrypt-Proxy wollen auch ODoH implementieren. Die IETF-Spezifikation ist aber noch nicht fertig, sodass Server und Relays noch nicht zuverlässig arbeiten. Deshalb klammern wir ODoH auf DNSCrypt-Proxy aus und beschreiben nur dessen eigene anonymisierende DNS-Technik.

Wie man den Anonymous-Mode konfiguriert, erklären wir im Weiteren anhand der DNSCrypt-Proxy-Version 2.1.0. Nach Redaktionsschluss erschien die Version 2.1.1, die im Wesentlichen ein Bugfix-Update ist. Unsere Anleitung gilt auch dafür.

Die Entwickler haben DNSCrypt-Proxy für alle unterstützten Plattformen übersetzt, sodass die Einrichtung wenig Aufwand erfordert. Für Raspbian OS und für andere Debian-basierte Distributionen ist die Software zwar über deren Paketverwaltungen erhältlich, aber nur in älteren 2.0.x-Versionen, weshalb wir den Download von der Entwickler-Webseite empfehlen. Auf dem Raspberry Pi haben wir das Programm mit Raspbian OS ausprobiert (7. Mai 2021, Kernel 5.10), auf Macs mit macOS (Big Sur 11.5.2). Windows haben wir in Version 10, Build-Nummer 20H2 (19042.1052) eingesetzt.

Im Prinzip läuft die Installation auf allen drei Systemen gleich ab: Zunächst lädt man die Software ins Download-Verzeichnis, dann testet man sie und tüftelt kurz an der Konfiguration. Anschließend verschiebt man den gesamten Ordner an den vorgesehenen Platz und richtet DNSCrypt-Proxy als Systemdienst ein.

Die konkreten Arbeitsschritte laufen unter Linux, macOS und Windows im Terminal ab; wir haben sie in der Tabelle aufgeführt. Im Weiteren erläutern wir die wesentlichen Schritte begleitend zur Tabelle. An einigen Stellen sind Benutzerpfade einzugeben. Wir setzen als Beispiel `ct` ein. Setzen Sie statt `ct` Ihren Benutzernamen ein.

DNSCrypt-Proxy einrichten

DNSCrypt-Proxy liest seine Konfiguration aus der Datei dnscrypt-proxy.toml. Über ct.de/wxje finden Sie ein Beispiel, das wir im Test erfolgreich verwendet haben. Falls Sie von Null anfangen möchten (empfehlenswert wegen Learning by Doing): Die Entwickler haben dem Archiv ein Beispiel beigefügt, das man nur noch passend benennen muss. Von dieser Ausgangssituation gehen wir bei den Befehlen in der Tabelle aus.

DNSCrypt-Proxy wurde ursprünglich für die einfache verschlüsselte DNS-Kommunikation ausgelegt. Deshalb ist das Einrichten der anonymisierten DNS-Kommunikation zweigeteilt. Im ersten Teil konfiguriert man einen oder mehrere Resolver, die DNSCrypt-Proxy befragen soll. Diese Parameter trägt man im Abschnitt „Global settings“ ein, der am Anfang der Datei steht.



DNSCrypt-Proxy bekommt man für macOS als fertige kompilierte Datei mitsamt einer Beispielkonfiguration. Den Start der Software muss man ausdrücklich genehmigen.

Dort finden Sie ein mit # auskommentiertes, also deaktiviertes Beispiel für die Resolver-Wahl. Entfernt man das Kommentarzeichen, befragt die Software die Resolver von Scaleway, Google, Yandex und Cloudflare. Diese eignen sich aber nicht für die anonyme DNS-Kommunikation. Geeignete Resolver finden Sie auf der Seite dnscrypt.info/public-servers.

Normalerweise würde man aus der Liste ein bis mehrere nahe gelegene Kandidaten auswählen, damit die DNS-Antworten möglichst schnell eingehen – also etwa Resolver in der Schweiz oder Österreich, wenn man dort ins Internet geht. Ein guter Kandidat für Surfer in Deutschland ist `dnscrypt-de-blahdns-ipv4`. Aber: Wenn man diesen Kandidaten als Laptop-Reisender verwendet, müsste man im Ausland in jedem neuen Land einen anderen suchen und konfigurieren.

Man kann daher Zeit sparen, wenn man von vornherein für häufig bereiste Länder oder Kontinente mehrere Resolver aussucht und einträgt – denn DNSCrypt-Proxy fragt sie alle direkt beim Start ab und sortiert sie in einer internen Tabelle nach der Antwortgeschwindigkeit.

Jedoch ist die Suche nach geeigneten Resolvern etwas umständlich, weil nicht jeder Resolver-Name mit einer Länderkennung gekennzeichnet ist. Es geht aber noch etwas einfacher: Manche Anbieter unterhalten nämlich viele gleichnamige Resolver in mehreren Ländern, einige gar auf fast allen Kontinenten. Man findet sie leicht anhand der Bezeichnung „anycast“. Trägt man solche Resolver ein, werden DNSCrypt-Pakete automatisch zur nächstgelegenen Instanz des gewählten Anbieters geroutet. In der Tabelle finden Sie das deaktivierte Beispiel und ein von uns beigesteuertes Beispiel mit einem Anycast- und zwei üblichen Anbietern. Tragen Sie es als eine Zeile unter das deaktivierte Beispiel ein, um es auszuprobieren.

Dabei steht `quad9-dnscrypt-ip4-nofilter-pri` für den Anycast-Dienst von Quad9, `dnscrypt.be` für das an der belgischen Universität Leuven stationierte Projekt des dortigen Administrators Sigfried Seldeslachts und `moulticast-de-ipv4` für das in Deutschland stationierte Non-Profit-Projekt des Schweizers Herve Rousseau.

Um andere Resolver einzustellen, öffnen Sie die Seite dnscrypt.info/public-servers und klicken auf die Spalte „Protocol“, sodass zuoberst alle Resolver aufgeführt werden, die sich für DNSCrypt eignen. Stellen Sie ganz unten in der Tabelle den Parameter „Rows per Page“ auf „All“, damit alle Kandidaten auf einer Seite aufgeführt werden.

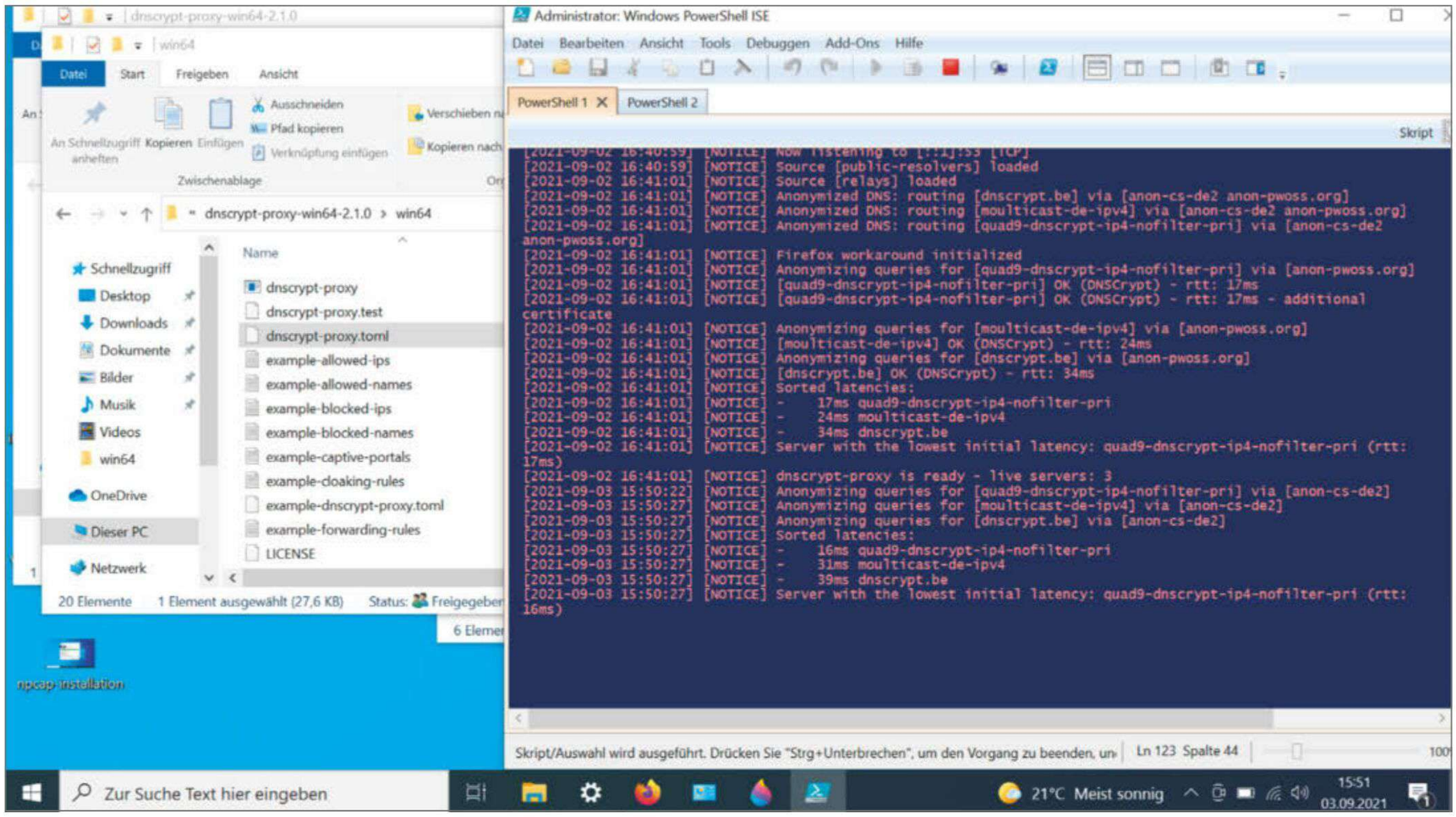
Nehmen Sie sich dann kurz Zeit und entscheiden Sie, ob die Resolver die Antworten gemäß DNSSEC auf Korrektheit und Vertrauenswürdigkeit prüfen sollen (das schützt DNSSEC-signierte Daten gegen Manipulation) und ob sie Anfragen nach Websites mit bekannt kriminellem Hintergrund oder pornografischem Inhalt filtern sollen. Meiden Sie aber die Resolver von Cisco, weil manche keine Anonymisierung unterstützen und teilweise sogar die anfragende Adresse an Dritte weitergeben.

Zu jedem Resolver ist auch aufgeführt, ob die Betreiber eine Protokollierung (logging) ausschließen oder nicht. Darauf müssen Sie keine Rücksicht nehmen, wenn Sie anonymisierendes DNSCrypt verwenden.

Die Einstellungen für anonyme DNS-Anfragen stehen fast am Ende der Datei im Abschnitt `[anonymized_dns]`. Dort trägt man einen oder mehrere Resolver und Relays ein. Mit einem Relay-Eintrag legt man fest, auf welchem Weg – über welche Relays – die DNSCrypt-Pakete zu einem bestimmten Resolver reisen. Man kann für einen Resolver ein oder mehrere Relays festlegen, denen DNSCrypt-Proxy seine Anfragen dann alternativ zuschickt.

Ein Muster mit einem Resolver und zwei Relays sieht wie folgt aus:

```
routes = [ { server_name='Resolver1',↵
↳ via=['Relay1', 'Relay2'] } ]
```



DNSCrypt-Proxy lief im Test auch auf Windows 10 reibungslos. Zur Prüfung der DNS-Anfragen kann man in der PowerShell einfach den Befehl `type` mit der Option `-wait` nutzen.

Eine Liste mit Relays finden Sie im DNSCrypt-Proxy-Ordner unter dem Namen `relays.md`. Der DNS-Client aktualisiert diese Datei bei jedem Start automatisch.

Bei der Auswahl wägt man die Antwortgeschwindigkeit (kürzestmögliche Latenz) gegen die Sicherheitsanforderungen ab. Wenn Sie größeren Wert auf den Schutz der Privatsphäre legen, konfigurieren Sie Resolver und Relays aus verschiedenen Ländern. Wenn Sie schnelle Antworten bevorzugen, tragen Sie Relays und Resolver aus dem Land ein, in dem auch Sie sich befinden.

DNSCrypt-Proxy akzeptiert mehrere Routen. Jedem Resolver lassen sich eigene Relays zuordnen:

```
routes = [ ⏎
↳{ server_name='Resolver1',⏎
↳ via=['Relay1', 'Relay2'] }, ⏎
↳{ server_name='Resolver2', ⏎
↳via=['Relay3', 'Relay4'] }, ⏎
↳{ server_name='Resolver3', ⏎
↳via=['Relay5', 'Relay6'] } ]
```

Wir haben der Einfachheit halber den drei weiter oben eingetragenen Resolvern jeweils die Relays `anon-cs-de2` und `anon-pwoss.org` zugeteilt. In der Tabelle finden Sie das Beispiel im „Abschnitt Anonymized DNS“. In diesem Fall könnte man anstatt jede Route einzeln aufzuführen in einer Zeile alle Resolver mit dem Zeichen `*` definieren:

```
routes = [ { server_name='*', ⏎
↳via=['Relay1', 'Relay2'] } ]
```

Alternativ könnte man Relays automatisch wählen lassen. DNSCrypt-Proxy sucht dann selbstständig

nach Relays, die nicht im selben Netzwerk stehen. Wir raten aber davon ab, weil man dann im Monitoring-Modus prüfen muss, ob die Auswahl tatsächlich den eigenen Vorstellungen entspricht, und gegebenenfalls korrigieren, was den Konfigurationsaufwand wieder erhöht.

Wenn Sie die gewünschten Resolver und Relays eingetragen haben, speichern Sie die Änderungen und starten Sie den DNS-Client wie in der Tabelle beschrieben. Der Proxy prüft beim Start, ob und wie schnell er die konfigurierten Resolver und Relays erreichen kann und gibt eine Reihenfolge wie folgende aus:

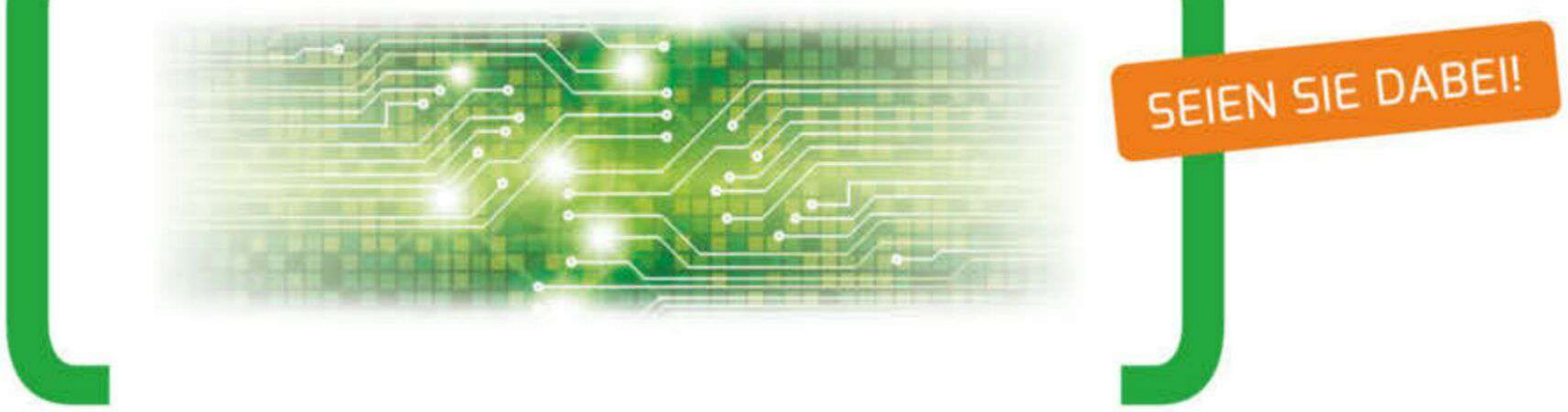
```
14ms quad9-dnscrypt-ip4-nofilter-pri
20ms moulticast-de-ipv4
40ms dnscrypt.be
```

In der letzten Zeile sollte stehen „dnscrypt-proxy is ready“ und die Anzahl der Resolver (servers), die er erreicht hat. Öffnen Sie ein zweites Terminal-Fenster im selben Verzeichnis und testen Sie die DNS-Auflösung wie in der Tabelle vorgeschlagen.

In der Antwort sollte 193.99.144.80 und 2a02:2e0:3fe:1001:302:: stehen sowie diverse weitere Auszüge aus der DNS-Datenbank des für ct.de zuständigen autoritativen DNS-Servers. Stoppen Sie nun den Proxy mit Strg + C und installieren Sie ihn so, dass er bei jedem Boot-Vorgang automatisch gestartet wird. Auf dem Raspi bietet es sich an, gleich auch den Ordnernamen besser kenntlich zu machen, weshalb wir dafür drei Schritte notiert haben.

Unter Windows schließen Sie zunächst das Explorer-Fenster, in welchem der Download-Ordner geöffnet ist. Andernfalls blockiert Windows das Verschieben des dnscrypt-proxy-Ordners.

Die Installation als Service erfolgt auf allen drei Systemen aus dem DNSCrypt-Proxy-Pfad heraus und sieht auch sonst sehr ähnlich aus. Prüfen Sie anschließend, ob der Dienst läuft. Auf allen drei Plattformen sollten dieselben Meldungen erscheinen, die das Programm schon beim manuellen Start



DNSCrypt-Proxy: Installation und Konfiguration auf Linux, macOS und Windows

Arbeitsschritt	Linux	macOS	Windows
DNSCrypt-Proxy laden über	ct.de/wxje	ct.de/wxje	ct.de/wxje
entpacken in Download-Ordner	/home/ct/Downloads	/Users/ct/Downloads	C:\Users\ct\Downloads
Terminal öffnen	distributionsspezifisch (Raspi: Menü/Zubehör/LX Terminal)	/Programme/Dienstprogramme/Terminal	PowerShell ISE mit Admin-Rechten
in DNSCrypt-Proxy-Ordner wechseln	cd /home/ct/linux-arm	cd /Users/ct/dnscrypt-proxy-macos_« »arm64-2.1.1	cd \Users\ct\Downloads\dnscrypt-« »proxy-win64-2.1.1\Win64
Konfigurationsdatei erzeugen	cp example-dnscrypt-proxy.toml « »dnscrypt-proxy.toml	cp example-dnscrypt-proxy.toml « »dnscrypt-proxy.toml	cp example-dnscrypt-proxy.toml « »dnscrypt-proxy.toml
Konfiguration editieren	nano dnscrypt-proxy.toml	nano dnscrypt-proxy.toml	PowerShell-Menü, „Datei/Öffnen“, zum OrdnerDNSCrypt-Proxy navigieren, Dateiauswahl auf „Alle Dateien“ umstellen, dnscrypt-proxy.toml doppelklicken
Abschnitt „Global settings“			
deaktivierte Resolver-Beispiele hinzufügen	# server_names = ['scaleway-fr', 'google', 'yandex', 'cloudflare']		
funktionierende Resolver-Beispiele hinzufügen	server_names = ['quad9-dnscrypt-ip4-nofilter-pri', 'dnscrypt.be', 'moulticast-de-ipv4']		
Abschnitt „Anonymized DNS“			
funktionierende Beispiel-Relays hinzufügen	routes = [{ server_name='quad9-dnscrypt-ip4-nofilter-pri', via=['anon-cs-de2', 'anon-pwoss.org'] }, { server_name='dnscrypt.be', via=['anon-cs-de2', 'anon-pwoss.org'] }, { server_name='moulticast-de-ipv4', via=['anon-cs-de2', 'anon-pwoss.org'] }]		
Konfiguration speichern	Strg + X,Y	Ctrl + X,Y	auf das Diskettensymbol klicken
DNS-Client starten	sudo ./dnscrypt-proxy	sudo ./dnscrypt-proxy	.\dnscrypt-proxy
Test der DNS-Auflösung in zweitem Terminal-Fenster	sudo ./dnscrypt-proxy -resolve ct.de	sudo ./dnscrypt-proxy -resolve ct.de	.\dnscrypt-proxy -resolve ct.de
Programmordner verschieben	cd /home/ct/Downloads	cd /Users/ct/Downloads	cd C:\Users\ct\Downloads
	sudo mv linux-arm dnscrypt-proxy-2.1.1	sudo mv dnscrypt-proxy-macos_arm64-« »2.1.1 /usr/local	mv .\dnscrypt-proxy-win64-2.1.1 « »'C:\Program Files'
	sudo mv dnscrypt-proxy-2.1.1 /usr/local	–	–
Installation als Dienst			
	sudo su	sudo su	cd 'C:\Program Files\dnscrypt-« »proxy-win64-2.1.0\Win64'
	cd /usr/local/dnscrypt-proxy-2.1.1	cd /usr/local/dnscrypt-proxy-2.1.1	.\dnscrypt-proxy -service install
	./dnscrypt-proxy -service install	./dnscrypt-proxy -service install	.\dnscrypt-proxy -service start
	./dnscrypt-proxy -service start	./dnscrypt-proxy -service start	–
	exit	exit	–
Läuft der Dienst?	sudo systemctl status dnscrypt-proxy	sudo tail -f /usr/local/var/log/« »dnscrypt-proxy.err.log	type -wait .\dnscrypt-proxy.log
DNS-Auflösung mitverfolgen			
Konfigurationsdatei öffnen	nano dnscrypt-proxy.toml	nano dnscrypt-proxy.toml	PowerShell-Menü, „Datei/Öffnen“, zum Ordner DNSCrypt-Proxy navigieren, Dateiauswahl auf „Alle Dateien“ umstellen, dnscrypt-proxy.toml doppelklicken
neue Zeile im Bereich „query_log“	file = '/usr/local/var/log/dnscrypt-proxy-query.log'		file = 'dnscrypt-proxy-query.log'
Änderungen speichern	Strg + X,Y	Ctrl + X,Y	auf das Diskettensymbol klicken
DNS-Client neu starten	sudo ./dnscrypt-proxy -service restart	sudo ./dnscrypt-proxy -service restart	.\dnscrypt-proxy -service restart
Log-Datei anzeigen	sudo tail -f /usr/local/var/log/« »dnscrypt-proxy-query.log	sudo tail -f /usr/local/var/log/« »dnscrypt-proxy-query.log	type -wait .\dnscrypt-proxy-query.log

ausgegeben hat, inklusive der ermittelten Laufzeiten und der Meldung „dnscrypt-proxy is ready“.

Um sich einen Überblick über die DNS-Auflösungen des Proxys zu verschaffen, fügen Sie dnscrypt-proxy.toml wie beschrieben eine Zeile im Bereich `query_log` hinzu, speichern Sie die Änderungen und starten Sie den Proxy neu. Dann legt das Programm die Datei dnscrypt-proxy-query.log an, das man je nach Betriebssystem mit `tail` oder `type` anzeigen lassen kann.

Im Query-Log notiert die Software zu jeder DNS-Anfrage, wie lang die Antwort gedauert hat und an wen sie geschickt wurde. So kommt man auch (sehr seltenen) Ausfällen von Resolvern auf die Spur. Dann notiert der Proxy „Network_Error“, die abgelaufene Frist für die Antwort (z. B. 5048 ms) und den Namen des Resolvers, der innerhalb der Frist nicht geantwortet hat. Wenn Sie mehr als einen konfiguriert haben, sollte der Proxy automatisch einen anderen befragen und dies eine Zeile später notieren. Wenn die Ausfälle zu häufig vorkommen, ersetzen Sie den unzuverlässigen Resolver durch einen anderen.

Generell gilt: Wenn Sie sich an den Logs sattgesehen haben, öffnen Sie wieder die Konfigurationsdatei und schalten Sie das Query-Log ab, um Rechenzeit und Speicherplatz zu sparen. Vergessen Sie nicht, DNSCrypt-Proxy neu zu starten.

Einen Raspi kann man nun als lokalen DNS-Proxy für das gesamte Heimnetz nutzen, indem man dessen IP-Adresse in die DHCP-Einstellungen des Routers einträgt. Sobald sich Netzwerkgeräte neu beim Router anmelden (etwa nach einem Neustart), verwenden sie den DNS-Server, den ihnen der DHCP-Server des Routers mitteilt – also etwa Ihren Raspi.

Einen Desktop-Mac kann man genauso als DNS-Proxy für sein Heimnetz konfigurieren. Wenn es sich um ein MacBook handelt, auf dem DNSCrypt-Proxy auch unterwegs laufen soll, empfiehlt es sich, macOS umzukonfigurieren. Öffnen Sie dazu die Systemeinstellungen und dort den Bereich Netzwerk. Klicken Sie auf die WLAN-Schnittstelle und dann nacheinander auf „weitere Optionen“ und „DNS“. Entfernen Sie alle Einträge in der Spalte „DNS-Server“, indem Sie auf das Minus-Symbol klicken. Klicken Sie auf „+“ und fügen Sie `::1` und in die nächste Zeile `127.0.0.1` ein. Damit befragen macOS sowie darauf eingerichtete Internet-Anwendungen die lokale Maschine; `::1` steht für localhost beim IPv6-Protokoll, `127.0.0.1` beim veralteten IPv4.

Wenn Sie sicherstellen wollen, dass der DNS-Dienst auch bei einem Ausfall von DNSCrypt-Proxy weiter funktioniert, tragen Sie in der dritten Zeile einen weiteren Resolver ein, beispielsweise `9.9.9.11` von Quad9. Dabei nutzt Ihr Mac weder die Verschlüsselung noch die Anonymisierung von Quad9, weil sich der von Apple eingebaute Stub-Resolver für beides nicht eignet. Aber falls DNSCrypt-Proxy mal ausfällt, haben Sie ein Fallback. Klicken Sie auf OK und dann auf Anwenden, damit der Mac die Einstellungen übernimmt.

In einem ausführlichen Test lief DNSCrypt-Proxy auf einem MacBook Pro mit Apples M1-Chip und Big Sur reibungslos – startete also automatisch, legte sich schlafen, wenn der Deckel zuklappte, und wachte umgehend auf, wenn man ihn öffnete, tage- und wochenlang.

Um Windows-Notebooks auf dieselbe Weise einzurichten, tippen Sie Windows+I und öffnen dann im Bereich „Netzwerk und Internet“ die Einstellungen für das WLAN-Interface. Klicken Sie dort auf „Adaptereinstellungen ändern“ und dann auf den betreffenden WLAN-Adapter sowie auf dessen Eigenschaften. Doppelklicken Sie dann auf „Internetprotokoll, Version 4...“ und schalten Sie um auf „Folgende DNS-Serveradressen verwenden“. Tragen Sie im Feld „Bevorzugter DNS-Server“ die IP-Adresse `127.0.0.1` ein. Im unteren Feld kann man einen Ersatz-Server wie `9.9.9.11` eintragen, falls DNSCrypt-Proxy mal ausfällt oder keiner der konfigurierten Server erreichbar ist. Im Bereich „Internetprotokoll, Version 6...“ tragen Sie `::1` ein, damit der lokale DNSCrypt-Proxy auch via IPv6 befragt werden kann. Als Fallback auf zum Beispiel Quad9 setzen Sie `2620:fe::11` ein.

Zu beachten ist, dass ein Laptop mit der hier beschriebenen Konfiguration nicht auf interne Server einer Firma zugreifen kann – externe Resolver kennen keine internen Server. Dafür schaltet man in den Laptop-Einstellungen hilfsweise auf die übliche DNS-Konfiguration zurück. Alternativ nutzt man den VPN-Zugang: Die VPN-Konfiguration enthält die für Firmenzugriffe erforderlichen DNS-Einstellungen grundsätzlich.

Schlussstrich

Anonyme DNS-Anfragen werden über ein zusätzliches Relay zum Resolver geschickt und sind daher etwas langsamer als übliche verschlüsselnde DNS-Anfragen und erst recht langsamer als die Klartext-DNS-Kommunikation. Der Zeitverlust war in unseren mehrwöchigen Tests aber nicht spürbar, auch nicht, als in einem Fall einer von drei konfigurierten Resolvern ausfiel. Um die Software auszuprobieren, genügt ein Stündchen, das Zugriffsprotokoll zeigt klar, wohin die DNS-Anfragen gehen.

Allerdings muss man den Relay-Betreibern vertrauen. Es gibt keinen Mechanismus, der verhindert, dass verschiedene Resolver- und Relay-Betreiber unter der Hand Daten austauschen und doch noch Userprofile erstellen. Es gibt aber etliche vertrauenswürdige Institutionen und auch Privatpersonen, die Relays und Resolver betreiben und sich glaubwürdig für den Privatsphärenschutz engagieren. (dz) c't

Downloads und Auswahllisten

ct.de/wxje

Schluss mit dem Passwort-Chaos

Bei der Menge an sensiblen Daten, die man Onlinediensten anvertraut, braucht es eine wasserdichte Login-Strategie. Wir geben Ihnen das Rüstzeug an die Hand, um Ihre Accounts mit sicheren Passwörtern und Zwei-Faktor-Authentifizierung abzusichern. Das ist einfacher als Sie vielleicht vermuten – und Sie können ohne Sorge um Ihre Online-Accounts entspannter surfen.

Von **Niklas Dierking**



Bild: Andreas Martini

Schluss mit dem Passwort-Chaos	48
Online-Accounts mit 2FA besser absichern	50
Passwort und zweiten Faktor einsetzen	56
Vorbeugen statt Frust bei 2FA-Verlust	64
FAQ Kennwörter, FIDO2 und TOTP	68

Hand aufs Herz: Ist jedes Ihrer Passwörter ausreichend lang? Benutzen Sie ein Passwort für mehrere Logins? Klebt ab und zu ein Post-it mit Zugangsdaten am Monitor? Speichern Sie manchmal Login-Informationen in einer Textdatei?

Bereits vor einigen Jahren hatte der durchschnittliche Internetnutzer schätzungsweise etwa 70 Accounts bei Onlinediensten, deren Zugänge alle verwaltet werden wollen. Inzwischen dürften es noch mehr geworden sein – und damit wächst auch das Unbehagen, denn laut einer im Februar 2022 durchgeführten Umfrage im Auftrag des E-Mail-Providers Web.de fürchtet sich über die Hälfte der Befragten vor Identitätsdiebstahl im Internet. Nutzer vertrauen Webdiensten sensible Daten an und viele von ihnen sind zum Bestreiten des Alltags unerlässlich geworden. Ein Angreifer, der sich Zugang verschafft, hat die Möglichkeit enormen finanziellen oder sozialen Schaden anrichten.

Zwei Verteidigungsringe

Lassen Sie sich von einem Passwortmanager unter die Arme greifen, um jedem Onlinezugang ein sicheres Passwort zu verleihen. Eine solche Software schützt gegen Wörterbuch- und Brute-Force-Attacken, indem sie lange, einzigartige Passwörter generiert und sicher speichert. Diese Passwörter können Angreifer mit herkömmlichen Methoden und verhältnismäßigem Aufwand nicht mehr knacken. Wie Sie Ihre Zugangsdaten mit einem Passwortmanager verwalten und Ihre Passwortdatenbank selbst vor neugierigen Blicken schützen, lesen Sie ab Seite 56.

Auch das beste Passwort schützt nicht in jedem Angriffsszenario, beispielsweise wenn Betrüger es mit einem Keylogger mitlesen oder man in eine Phishing-Falle tappt. Um sich für den Fall zu wappnen, dass Ihnen ein Angreifer das Geheimnis entlockt, müssen Sie Ihre Accounts mit einem zweiten Faktor absichern. Das Prinzip der Zwei-Faktor-Authentifizierung (2FA) dürfte vielen von TAN-Verfahren beim Onlinebanking geläufig sein oder wenn Sie sich von einem neuen Gerät in Ihren Google-Account einloggen. Zugänge werden dabei über einen zweiten Kanal abgesichert. Ein Cyberkrimineller müsste zusätzlich zu Ihrem Passwort auch diesen zweiten Kanal kompromittieren. Das macht es Angreifern deutlich schwerer.

Wer beginnt, sich über Möglichkeiten der Zwei-Faktor-Authentifizierung einzulesen, verliert schnell den Überblick. Gut möglich, dass Ihnen Begriffe wie TOTP, U2F und FIDO2 bereits über den Weg gelaufen sind. Unter dem Schlagwort 2FA tummeln sich eine Vielzahl von Verfahren, die sich sowohl in Funktionsweise, Sicherheit und Komfort unterscheiden. Der Artikel ab Seite 50 erklärt und vergleicht die gängigsten Verfahren, damit Sie die geeignete Methode für Ihren Anwendungsfall auswählen. Der Artikel ab Seite 56 hilft Ihnen dann, Ihren Accounts das zusätzliche Schloss zu verpassen. Sie finden heraus, welche 2FA-Optionen die Onlinedienste anbieten und wie Sie diese einrichten.

Ersatzschlüssel

Mit diesem zusätzlichen Gewinn an Sicherheit müssen Sie jedoch selbst vorsorgen, um sich nicht auszusperren, zum Beispiel wenn Sie Ihren Hardware-Sicherheitsschlüssel verbaseln. Außerdem sollten Sie einige Punkte zur Vor- und Nachsorge beachten, beispielsweise wie mit Sicherheitsfragen umzugehen ist. Diese Notfallpläne erläutert der Artikel ab Seite 64. Es gibt jedoch noch mehr Unwägbarkeiten: Ist es eigentlich sicherer, sich bei Diensten mit seinem Google-Konto anzumelden, statt überall einen eigenen Account zu registrieren? Antworten auf solche Fragen und weitere Login-Best-Practices lesen Sie in unserer FAQ ab Seite 68.



Welches Schloss darfs sein? Verfahren und Geräte, um Ihre Zugänge zu Webdiensten zusätzlich abzusichern, gibt es viele, zum Beispiel Sicherheitsschlüssel, TOTP-Apps und Hardware-Authentikatoren.

Loslegen

Beim Nachdenken über die eigene Passwortwirtschaft beschleicht viele ein mulmiges Gefühl. Das dürfte auch der Grund dafür sein, dass laut der eingangs erwähnten Umfrage mehr als die Hälfte der Befragten zusätzliche Schutzmaßnahmen für sinnvoll halten. Aber womit anfangen? Wir zeigen, auf welche Säulen Sie Ihre sichere Login-Strategie aufbauen müssen, wie Sie dem Passwort-Chaos Herr werden, Ihre Accounts mit einem zweiten Faktor verrammeln und Katastrophen vorbeugen. (ndi) c't

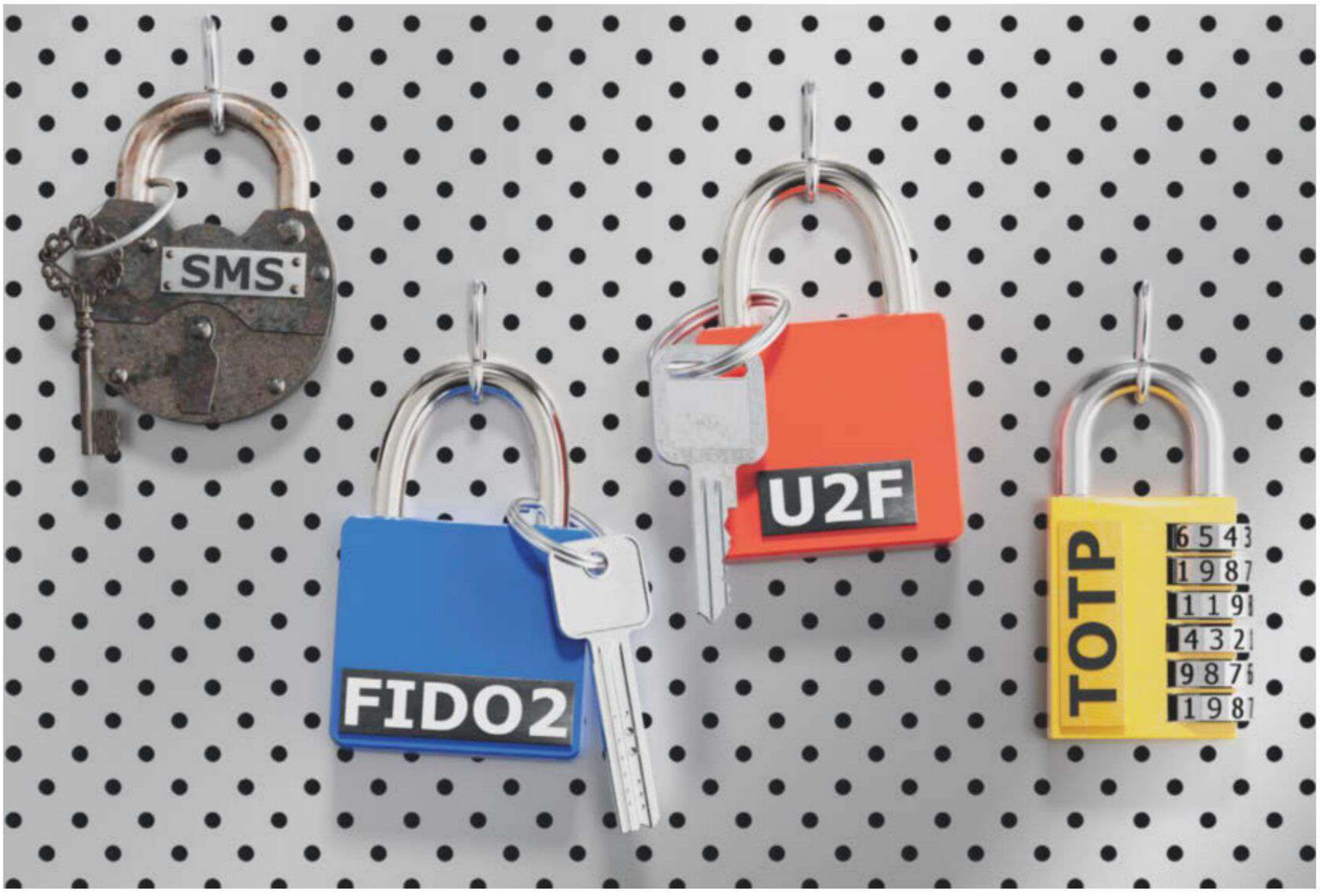


Bild: Andreas Martini

Online-Accounts mit 2FA besser absichern

Sie haben den Entschluss gefasst, sicherer zu leben, indem Sie mit dem Passwort-Chaos aufräumen und Ihre Login-Strategie optimieren? Dann stellt sich jetzt die Frage nach dem Wie. Dieser Leitfaden zeigt Ihnen die wichtigsten Hilfsmittel, mit denen Sie Ihre Accounts im Handumdrehen vor Hackern schützen.

Von **Niklas Dierking und Ronald Eikenberg**

Mit sicheren Passwörtern allein sind Ihre Online-Accounts noch nicht gut vor Hackern geschützt. Denn das Konzept des Passworts ist angesichts von Angriffstechniken wie Phishing, Keyloggern und Trojanern hoffnungslos veraltet.

Erst, wenn Sie eine Zwei-Faktor-Authentifizierung (2FA) eingerichtet haben, können Sie sich entspannt zurücklehnen. Die folgende Übersicht hilft Ihnen dabei, die passenden 2FA-Verfahren auszuwählen. Welche Methoden die Webdienste anbieten und

Ihr Weg zu sicheren Online-Accounts

Mit den folgenden Schritten können Sie Ihre Online-Accounts im Handumdrehen effektiv vor Hackern schützen. Starten Sie oben links und gehen Sie die drei Kästen **Vorbereitung, Account abriegeln und Nachsorge** der Reihe nach durch.



Vorbereitung

- Passwortmanager einrichten
- Zufälliges Kennwort setzen

(→ Seite 60)

Account abriegeln

- Herausfinden, welches 2FA-Verfahren verfügbar ist
- 2FA einrichten

(→ Seite 56)

Nachsorge

- Recovery einrichten
- Umgang mit Sicherheitsfragen

(→ Seite 64)

TOTP
(→ Seite 53)

entweder

TOTP-App
(z. B. Google)

oder

TOTP-Stick
(z. B. YubiKey)

oder

Generator
(z. B. Reiner SCT)

U2F
(→ Seite 54)

entweder

U2F-Stick
(z. B. YubiKey)

oder

FIDO2-Stick
(z. B. YubiKey)

FIDO2
(→ Seite 54)

entweder

FIDO2-Stick
(z. B. YubiKey)

oder

Geräte-Chip
(z. B. Android …)

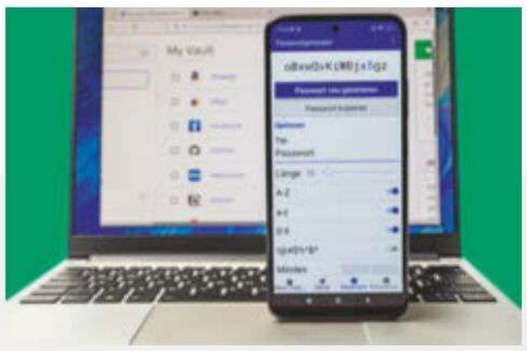
App
(→ Seite 53)

App des Dienstes

SMS
(→ Seite 52)

beliebiges Handy





Passwortmanager

Wer den Schutz seiner Online-Accounts ernst nimmt, muss für jeden Dienst ein anderes Passwort nutzen. Merken kann man sich die ganzen Passwörter natürlich nicht mehr, doch hier hilft ein Passwortmanager.

Die wichtigste Regel beim Umgang mit Passwörtern lautet: Nutzen Sie für jeden Account ein anderes! Fällt einem Hacker ein mehrfach genutztes Passwort in die Hände, hangelt er sich damit von Dienst zu Dienst und macht fette Beute. Doch leichter gesagt als getan: Inzwischen jongliert man nicht selten mit Dutzenden Accounts – und ständig werden es mehr. Hier kommt der Passwortmanager ins Spiel: Er nimmt Ihnen die Arbeit komplett ab, indem er sich alle Passwörter für Sie merkt und bei Bedarf auch neue, sichere generiert. Manche Passwortmanager speichern Ihre Zugangsdaten sicher verschlüsselt lokal, andere in der Cloud – im zweiten Fall bleibt der Passwort-Tresor auf allen Geräten automatisch auf dem aktuellen Stand.

Empfehlenswert unter den Passwortmanagern mit Synchronisierungsfunktion ist die Open-Source-Software Bitwarden, die viele Betriebssysteme und Browser unterstützt. Sie können ihn kostenlos nutzen und den Cloudserver dahinter sogar selbst betreiben, wenn Sie dem Hersteller nicht trauen. Wie Sie mit dem Passwortmanager loslegen, lesen Sie im Artikel ab Seite 56. Auch die integrierten Passwortmanager der Betriebssysteme und Browser leisten in vielen Fällen gute Dienste: Wer etwa im Apple-Universum heimisch ist, kann einfach den „Schlüsselbund“ nutzen, und Google kann Ihre Zugangsdaten zwischen Android, Chrome OS oder dem Chrome-Browser synchronisieren. Einen guten Job macht auch Mozilla Firefox.





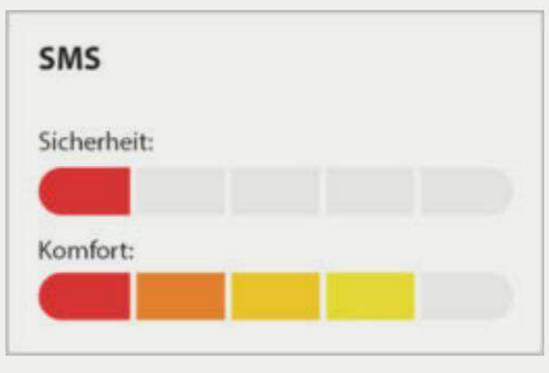
SMS

Vor rund 30 Jahren war die SMS eine echte Innovation, heute gilt das Verfahren nicht gerade als sicher. Dennoch kommt es ausgerechnet bei der Zwei-Faktor-Authentifizierung immer noch zum Einsatz.

Der große Vorteil von SMS als zweitem Faktor ist, dass es jeder versteht und nutzen kann – es erfordert weder eine komplizierte Einrichtung noch spezielle Hardware oder Apps. Beim Login bekommt der Nutzer eine SMS aufs Handy, die einen Zahlencode enthält. Diesen muss der Nutzer anschließend abtippen, um sich erfolgreich einloggen zu können.

Das SMS-Verfahren ist zwar einfach, aber nicht mehr zeitgemäß, da es unverschlüsselt und nicht an ein Gerät gekoppelt ist. Gefährlich ist vor allem das sogenannte SIM-Swapping: Kriminelle bestellen beim Mobilfunkprovider im Namen des Nutzers eine weitere SIM-Karte zur Rufnummer und können so die SMS-Nachrichten mit den 2FA-Codes abfangen. Aufgrund des niedrigen Schutzniveaus sind TAN-SMS beim Online-Banking im Aussterben begriffen.

Zudem ist ein Wechsel der Rufnummer mit großem Aufwand verbunden, da man bei sämtlichen Online-Accounts rechtzeitig sicherstellen muss, dass die neue Rufnummer hinterlegt ist. Vergisst man einen Account, sperrt man sich schlimmstenfalls dauerhaft aus, sobald die alte Rufnummer nicht mehr funktioniert. Das SMS-Verfahren ist zwar besser, als gar keinen zweiten Faktor einzurichten. Bevorzugen Sie jedoch immer ein moderneres und sichereres 2FA-Verfahren wie TOTP, U2F oder FIDO2, wenn Sie die Wahl haben. Falls ein Webdienst kein anderes 2FA-Verfahren anbietet und Sie daher um SMS nicht herumkommen, sollten Sie den Anbieter darauf aufmerksam machen, dass dies nicht mehr zeitgemäß ist. Steter Tropfen höhlt bekanntlich den Stein.





Time-based One-Time Passwords (TOTP)

TOTP ist ein simples Verfahren zur Zwei-Faktor-Authentifizierung, das wenige Voraussetzungen verlangt. Die allermeisten Webdienste, die 2FA anbieten, haben TOTP in ihrem Login-Portfolio: ein guter Einstieg in die Welt der zweiten Faktoren.

Für TOTP als zweiten Faktor brauchen Sie eine Gegenstelle, meist Authenticator genannt, die ein Geheimnis hütet und für Sie Einmalkennwörter generiert. Der Authenticator operiert idealerweise unabhängig von dem Gerät, mit dem Sie sich anmelden wollen. Am gängigsten sind Apps wie der Google- und Microsoft-Authenticator, Authy oder die Open-Source-Apps andOTP und FreeOTP. Auch einige Passwortmanager und der Schlüsselbund in iOS integrieren TOTP. Die sind allesamt kostenlos.

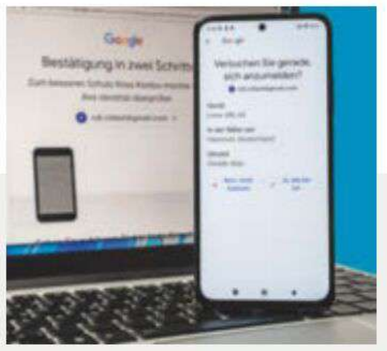
Sie können auch einige Hardware-Sicherheitsschlüssel in Verbindung mit der Authenticator-App des Herstellers nutzen, um TOTP-Codes zu erzeugen. Das ist sicherer, weil der Sicherheitsschlüssel das Geheimnis auf einem geschützten Chip speichert, wo es nicht ausgelesen werden kann. Als dedizierte Hardwarelösung hat sich der Reiner SCT Authenticator bewährt. Der ist nicht aus dem Internet erreichbar, was die Angriffsfläche reduziert. Sperren Sie Ihren Authenticator wenn möglich mit einer PIN oder dem Fingerabdruck, um Ihre Einmalpasswörter vor neugierigen Augen zu schützen. Bei einem Smartphone übernimmt diese Rolle sonst die Anmeldesperre des Geräts, die unbedingt aktiviert sein sollte.

Sie flößen dem Authenticator das Geheimnis meist ein, indem Sie einen QR-Code scannen oder eine Zeichenfolge abtippen. Aus dem Geheimnis und der aktuellen Zeit errechnet der Authenticator einen kryptografischen Hash-Wert. Daraus speist sich das Einmalpasswort, das in der Regel 30 Sekunden lang gültig ist.

Time-based One-Time Password (TOTP)

Sicherheit:

Komfort:



Zweistufige Anmeldung via Push-Benachrichtigung

Statt offene und dokumentierte 2FA-Standards zu nutzen, integrieren viele Webdienste eigene Apps in ihren Anmeldeprozess. Das ist sicherer als ein Passwort allein, hat aber Nachteile gegenüber etablierten Lösungen.

„Wir müssen kurz verifizieren, dass Sie es sind.“ So einen Dialog bekommen Sie als Nutzer oft zu Gesicht, wenn Sie sich von einem bisher unbekannten Gerät bei einem Onlinedienst anmelden. Was folgt, ist die Frage danach, auf welchem Wege man dem Dienst die eigene Identität glaubhaft machen möchte.

Neben Einmalpasswörtern via SMS und TOTP können Sie meistens die App des Dienstes selbst zur Bestätigung nutzen. Das Prinzip dürfte vielen Nutzern beispielsweise von Apple, Google, Facebook, PayPal, Microsoft oder Steam bekannt sein. In der Regel müssen Sie auf eine Push-Benachrichtigung der App am Smartphone oder Tablet reagieren, vorausgesetzt das Gerät ist dem Dienst bereits bekannt. Je nach Umsetzung müssen Sie anschließend eine angezeigte Zahlenfolge oder ein Symbol abgleichen. Oft genügt es, die Anmeldung plump über eine Schaltfläche zu bestätigen.

Grundsätzlich ist diese zweistufige Anmeldung ein Gewinn an Sicherheit gegenüber der einstufigen Anmeldung mit Nutzername und Passwort. Der Nachteil gegenüber Verfahren wie TOTP, U2F oder FIDO2 ist jedoch, dass Sie in der Regel nicht nachvollziehen können, mit welchen Verfahren der Dienst hinter den Kulissen arbeitet und ob diese Ihren Sicherheitsanforderungen genügen. Bleiben Sie bei diesem und allen anderen 2FA-Verfahren skeptisch gegenüber unplausiblen Aufforderungen, Logins zu bestätigen. Nutzer gewöhnen sich schnell daran, auf „Ja“ zu klicken, wodurch schon mal ein Fremdzugriff durchrutschen kann.

Zweistufige Anmeldung via Push-Benachrichtigung

Sicherheit:

Komfort:



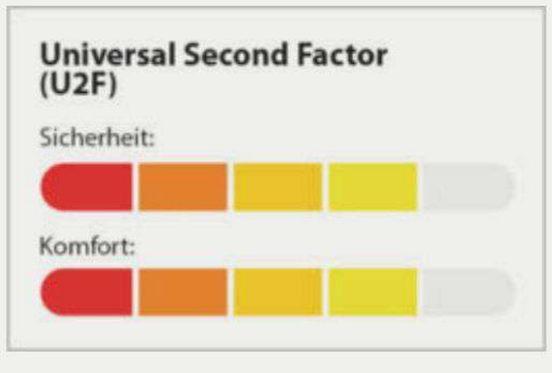
Universal Second Factor (U2F)

Anders als der Nachfolger FIDO2, der auch ganz ohne Passwort auskommen kann, dient das U2F-Verfahren als eine Ergänzung dazu. Das Verfahren ist sehr verbreitet, sicher und komfortabel. Passende U2F-Sticks gibt es in vielen Farben und Formen.

Mit einem U2F-Stick können Sie viele Accounts effektiv vor Hackern schützen. Das U2F-Verfahren ist nicht nur komfortabel und sicher, sondern auch sehr verbreitet, weil der Standard bereits 2014 veröffentlicht wurde. Einige U2F-Geräte (auch Sicherheitsschlüssel oder Hardware-Token genannt) bieten auch Bluetooth oder eine NFC-Schnittstelle, um ohne Adapter mit Smartphones zu kommunizieren. Wenn Sie noch kein U2F-Gerät besitzen, greifen Sie am besten gleich zu einem FIDO2-Sicherheitsschlüssel, da diese abwärtskompatibel zu U2F sind.

Nach der Einrichtung des Verfahrens kümmert sich der Browser um die Kommunikation mit dem Hardware-Token und wickelt die Anmeldung beim Dienst über ein Challenge-Response-Verfahren ab. Das Schlüsselpaar aus öffentlichem und privatem Schlüssel wird für jeden Dienst individuell generiert, wodurch U2F automatisch vor Phishing schützt. Selbst wenn die Phishing-Seite dem Original perfekt nachempfunden wäre, würde der U2F-Stick beim Phishing-Versuch einen individuellen Schlüssel nutzen, der keinen Zugriff auf die Originalseite erlaubt.

Um sich mit einem U2F-Gerät anzumelden, müssen Sie eine Aktion direkt am Gerät ausführen. Meist genügt ein Druck auf eine Taste am Stick, einige Hardware-Token sichern diesen Schritt mit PIN oder Fingerabdruck ab. Praktisch: Neben der Absicherung Ihrer Online-Accounts können Sie U2F- und FIDO-Sticks auch anderweitig nutzen, etwa um sich Systemverwalterrechte auf der Linux-Kommandozeile einzuräumen.





FIDO2

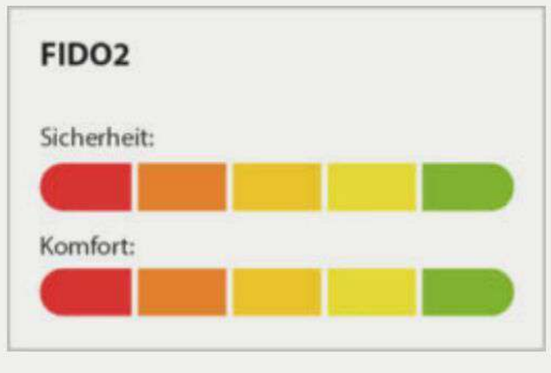
Das moderne FIDO2-Verfahren dient nicht nur als zweiter Faktor, Sie können sich damit sogar ohne Passwort einloggen. Es nutzt einen Sicherheits-Chip, der schon jetzt in den meisten Geräten steckt.

Bei FIDO2 authentifizieren Sie sich mit einem Sicherheitsschlüssel gegenüber den Diensten, die Sie nutzen möchten. Der Schlüssel ist entweder ein spezieller USB-Stick oder ein Krypto-Chip, der mit hoher Wahrscheinlichkeit bereits in Ihrem Rechner, Smartphone und Tablet steckt. Sie müssen ihn nur noch benutzen.

Beim Einloggen greift der genutzte Webdienst auf den Sicherheitsschlüssel zu, um zu verifizieren, dass Sie ihn tatsächlich besitzen. Der Dienst akzeptiert nur bestimmte Schlüssel, die zuvor mit dem Account gekoppelt wurden. Für einen Cyber-Schurken ist das eine unüberwindbare Hürde: Wenn er Ihre Zugangsdaten geklaut hat, kann er sich damit nicht einloggen, weil ihm der FIDO2-Schlüssel fehlt. Die Schlüssel sind kryptografisch abgesichert und nicht kopierbar.

FIDO2 ist sehr flexibel und wird bei den Webdiensten, die es bereits anbieten, zumeist als zweiter Faktor eingesetzt – also als zusätzliche Schutzschicht neben dem Passwort. Der Dienst kann allerdings auch auf Benutzername und Passwort verzichten, dann reicht der FIDO2-Schlüssel zum Einloggen. Das klappt beispielsweise schon bei Microsoft und Nextcloud.

Die folgenden Betriebssysteme unterstützen FIDO2 ohne Extra-Hardware: Windows 10 und 11, macOS ab Mojave, iOS ab Version 13.3 sowie Android ab Version 7. FIDO2-Sticks gibts unter anderem von SoloKeys, Yubico und Nitrokey ab 20 Euro aufwärts. Mit den abwärtskompatiblen Sticks sind Sie dann auch gleich für den FIDO2-Vorgänger U2F gerüstet.



wie Sie diese einrichten, lesen Sie im Artikel ab Seite 56.

Passwörter und PINs gehören in die Kategorie „geheimes Wissen“ und sind nach wie vor allgegenwärtig. Die meisten anderen Anmeldefaktoren kann man unter dem Schlagwort „Besitz“ zusammenfassen. Darunter fallen beispielsweise Krypto-Token in Form von USB-Sticks oder auch das Smartphone. Gerade bei Onlinediensten ist es sinnvoll, den Account an den Besitz einer bestimmten Sache zu koppeln. Denn Hacker können zwar Ihr Passwort stehlen, jedoch nicht Ihr Smartphone oder das Hardware-Token an Ihrem Schlüsselbund.

Trotzdem bleibt das Passwort der erste Baustein einer sicheren Login-Strategie. Deshalb lautet die wichtigste Regel im Umgang damit: Verwenden Sie für jeden Dienst ein anderes! Greifen Sie lieber direkt zum Passwortmanager, der sichere Passwörter generiert, sie in einer verschlüsselten Datenbank speichert und optional über mehrere Geräte synchronisiert. Der Passwortmanager verwaltet alle Ihre Passwörter, halten Sie also das System, auf dem Sie die Software installieren, sauber und aktuell.

Extraschloss

In unserer Infografik finden Sie die gängigsten Verfahren für mehr Sicherheit, die wir auf den folgenden Seiten vorstellen und vergleichen. Das Smartphone kann oft die Rolle des zweiten Kanals übernehmen, beispielsweise wenn Sie über eine App sogenannte „Time-based One-Time-Passwords“ (TOTP) generieren. Dabei handelt es sich um sechsstellige Zahlenfolgen, die Sie zum Beispiel mit dem Google Authenticator generieren.

Auch die iOS- und Android-Apps großer Plattformen wie Google, Facebook, Steam oder PayPal können als zweiter Faktor arbeiten, allerdings nur für den jeweiligen Dienst. Etwas in die Jahre gekommen ist die SMS als zweiter Faktor. Ein geschickter Angreifer kann die Einmalcodes potenziell abfangen, wenn er sich für Sie ausgibt.

Mit modernen 2FA-Verfahren wie U2F oder FIDO2 genießen Sie den besten Schutz bei wenig Komfortverlust. Das Herz dieser Verfahren ist ein kryptografisch geschützter Sicherheitschip, der mit den Accounts gekoppelt wird. Geeignete Chips für das ältere Verfahren U2F stecken auf vielen USB-Sticks, die man als Sicherheitsschlüssel oder Authenticator bezeichnet. Für das neuere FIDO2-Verfahren können Sie auf so einen Stick prinzipiell sogar oft verzichten. Wahrscheinlich besitzen Sie schon einen passenden Sicherheitschip: In modernen Smartphones steckt ein „Secure Element“, aktuelle PCs enthalten ein „Trusted Platform Module“ (TPM).

Wägen Sie stets ab, welche Anforderungen Sie an Sicherheit und Komfort haben, wenn Sie sich für ein angebotenes 2FA-Verfahren bei einem Dienst entscheiden. Mit der folgenden Grafik und den Kurzbeschreibungen der Verfahren verschaffen Sie sich einen Überblick über die Säulen, auf die Sie Ihre sichere Login-Strategie bauen können. Danach wird es praktisch: Welche der hier vorgestellten Extraschlösser populäre Dienste anbieten und wie Sie damit Ihre Accounts abschließen, lesen Sie im nächsten Artikel ab Seite 56. (ndi) c't



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

heise Shop

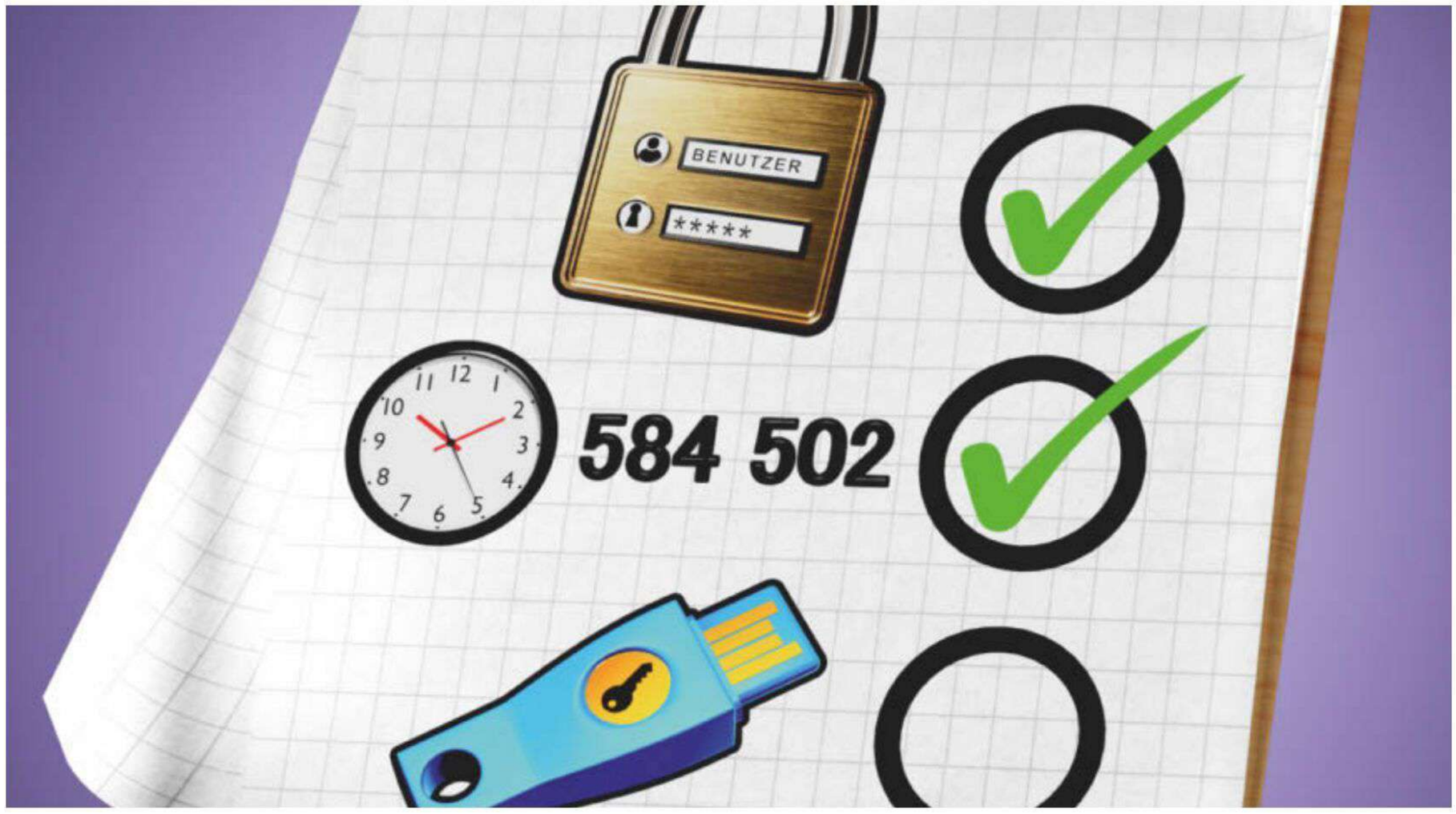


Bild: Andreas Martini

Passwort und zweiten Faktor einsetzen

Eine Zwei-Faktor-Authentifizierung ist bei Onlinediensten in wenigen Schritten eingerichtet. Leider unterstützt jeder Dienst andere Verfahren und benennt die zweiten Faktoren unterschiedlich oder versteckt sie mitunter: ein Wegweiser durch die Einstellungen.

Von **Keywan Tonekaboni, Niklas Dierking**

Auch das beste Passwort schützt ein Konto nur mäßig, wie die Recherchen zu diesem Artikel uns noch mal vor Augen führten. Eigentlich wollten wir diesen Artikel mit der üblichen Warnung vor geleakten Kennwörtern, vor Keyloggern und Phishern beginnen. Aber die Deutsche Bahn bescherte uns eine noch greifbarere Gefahr: Zum Test riefen wir von einer bewusst nicht mit unserem Account verknüpften Telefonnummer beim Support an und wollten die Login-Daten zu unserem bahn.de-Account zurücksetzen. Nach nur fünf Minuten in der Warteschleife und etwas gespielter langer Leitung unserseits hatten wir den Zugang zu dem Konto.

Dafür reichte es in dem kurzen Telefonat, lediglich die Fragen nach dem Benutzernamen und der hinterlegten Postleitzahl zu beantworten. Als wir nach der bisher zum Fahrkartenkauf genutzten E-Mail-Adresse gefragt wurden, stellten wir uns unwissend. Trotzdem nannte uns der hilfsbereite Hotline-Mitarbeiter

ein neues Passwort noch am Telefon. In diesem Fall war es der eigene Account, aber das Experiment zeigt, wie leicht ein Angreifer den Passwortschutz hätte aushebeln können.

Damit Ihre Konten nicht so blank liegen, zeigen wir Ihnen, wie Sie die Zwei-Faktor-Authentifizierung (2FA) einrichten und wie Sie damit verbundene Probleme vermeiden oder bewältigen. Auf den folgenden Seiten geben wir zudem Tipps, wie Sie selbst herausfinden, wie es bei den von Ihnen genutzten Angeboten um die 2FA steht.

Aber vor der Einrichtung des zweiten Faktors sollte man den ersten Faktor, das Kennwort, nicht aus dem Blick verlieren. Auf Seite 60 erfahren Sie, wie Sie mit dem Passwortmanager Bitwarden bessere Passwörter erzeugen und verwalten – andere Passwortmanager arbeiten ähnlich.

Babylon trotz Standards

Eine Zwei-Faktor-Authentifizierung richtet man nach dem immer gleichen Schema ein: In den Einstellungen des Onlinekontos wählt man aus, welches Verfahren man verwenden möchte: Typische Formulierungen in den Oberflächen sind etwa Sicherheitsstick, Authenticator-App oder SMS-Code. Bevor dieser zweite Faktor mit dem Konto verknüpft wird, muss man das eingerichtete Verfahren einmal benutzen, also einen Code eingeben oder den Stick einstecken. Zum Schluss erhält man häufig noch einen oder mehrere Einmalcodes zum Ausdrucken als Backup. Das ist die letzte Rettung, falls man den Zugriff auf die Zusatzfaktoren mal verliert.

Doch die zahlreichen Onlinedienste haben die Zwei-Faktor-Authentifizierung sehr unterschiedlich implementiert. Oft bieten sie nur wenige der möglichen Verfahren an. Nach unserer Zählung kommt am häufigsten der Versand eines Einmalcode per SMS zum Einsatz, auf Platz 2 liegt TOTP, also ein mit einer App generierter zeitbasierter Code, der nur 30 Sekunden lang gültig ist. Sogar per E-Mail versandte Einmalcodes kommen vor, sind aber noch unsicherer als SMS.

Häufig, aber leider nicht immer, kann man mehrere Verfahren parallel einrichten. Bei einigen Diensten kann man zum Beispiel nur eine Handynummer hinterlegen oder maximal einen Sicherheitsstick anlernen. Mehr zur Funktionsweise der zweiten Faktoren und zu möglichen Hardware-Anschaffungen lesen Sie ab Seite 50.

Es gibt aber auch kuriose Einschränkungen: Bei Instagram kann man die Zwei-Faktor-Authentifizierung per TOTP nur in der mobilen App aktivieren. Im Browser ist die Funktion ausgegraut. Wikipedia bietet 2FA nur für bestimmte Nutzergruppen wie Administratoren an. Bei der Bahn muss man sich zwischen SMS und TOTP entscheiden. Beides gleichzeitig geht nicht – unverständlich, da die Bahn keine Backup-Codes ausstellt.

Manchmal schützt der zweite Faktor auch nur bestimmte Funktionen. So kann man bei Instagram die Bestätigung per App als zusätzlichen Faktor einrichten, aber die greift nur, wenn man sich auf einem anderen Gerät mit der Instagram-App anmelden möchte, die Anmeldung im Browser bleibt davon unberührt. Bei der Fritzbox schützt TOTP nur bestimmte Änderungen, wie die Einrichtung von Rufumleitungen, aber nicht die Anmeldung selbst. Die Online-Funktion MyFritz erlaubt wiederum, neben TOTP auch mehrere FIDO2-Geräte zu koppeln und erzeugt einen Backup-Code.



Große Tech-Firmen wie Microsoft bieten viele 2FA-Optionen an, andere Onlinedienste meist nur SMS oder TOTP.



Richtet man in Instagram die 2FA per App ein, erscheint für eine neu eingerichtete App eine Warnung, aber für Anmeldeversuche per Webseite nicht.

Zwei-Faktor-Authentifizierung finden

Die größte Hürde ist herauszufinden, wo die Anbieter im Webinterface oder in der App die Einstellungen zur Zwei-Faktor-Authentifizierung versteckt haben. Es kursieren verschiedene Begriffe: Zwei-Faktor-Authentifizierung, 2FA, „Zweistufige Authentifizierung“, „Zweistufige Überprüfung“, „Bestätigung in zwei Schritten“, „Zusätzlicher Schutz“ oder MFA (Multi-Faktor-Authentifizierung). Manchmal heißt es auch nur „Bestätigung über Google Authenticator App“, wenn eigentlich TOTP gemeint ist. Googles App ist eine TOTP-Implementierung, aber bei Weitem nicht die einzige (siehe S. 62).

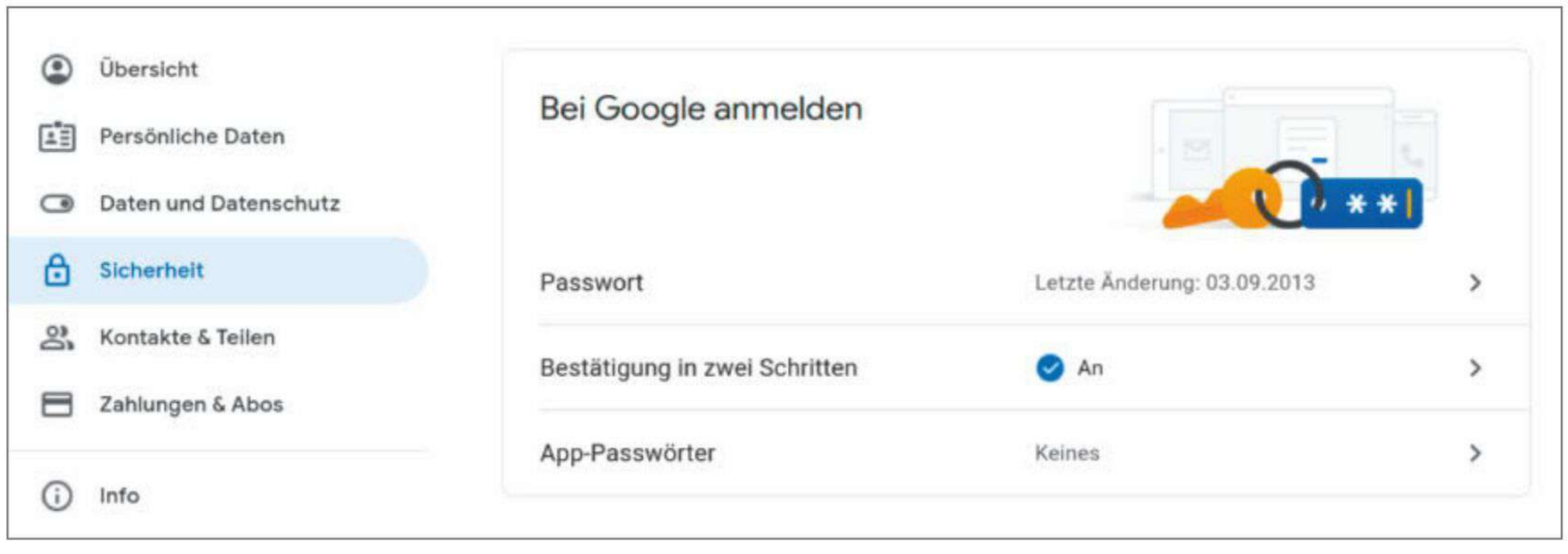
Suchen Sie nach diesen Schlagwörtern in den Einstellungen. Meist werden Sie fündig in Rubriken wie (Erweiterte) Sicherheit, Datenschutz, Account-Zugriff, Privatsphäre, Benutzereinstellungen oder Kontoeinstellungen. Mal sind es nur zwei Klicks, aber nicht selten ist die Funktion in den Untermenüs vergraben. Bei manchen Diensten muss man, um TOTP oder U2F/FIDO2 verwenden zu können, vorher eine Telefonnummer für SMS hinterlegen oder 2FA über SMS einrichten. Vermutlich dient das als Backup, falls man keinen Zugriff mehr auf die Authenticator-App oder den FIDO-Stick hat. Solche Einschränkungen sind unschön, weil ausgerechnet SMS-Codes aus Sicherheitsperspektive nicht mit dem technisch sehr sicheren FIDO2 mithalten können.

Zum Verwechseln ähnlich benannt sind manchmal die Optionen zur Absicherung des Passwort-Resets („Passwort vergessen“). Bevor Onlinedienste einen Passwort-Zurücksetzen-Link verschicken, fragen manche von ihnen nach einem per SMS versandten Code oder nach einer vorher eingerichteten Frage („Wie lautet der Geburtsname Ihrer Mutter?“). Achten Sie also genau darauf, was der zweite Faktor tatsächlich schützt (siehe Instagram-App).

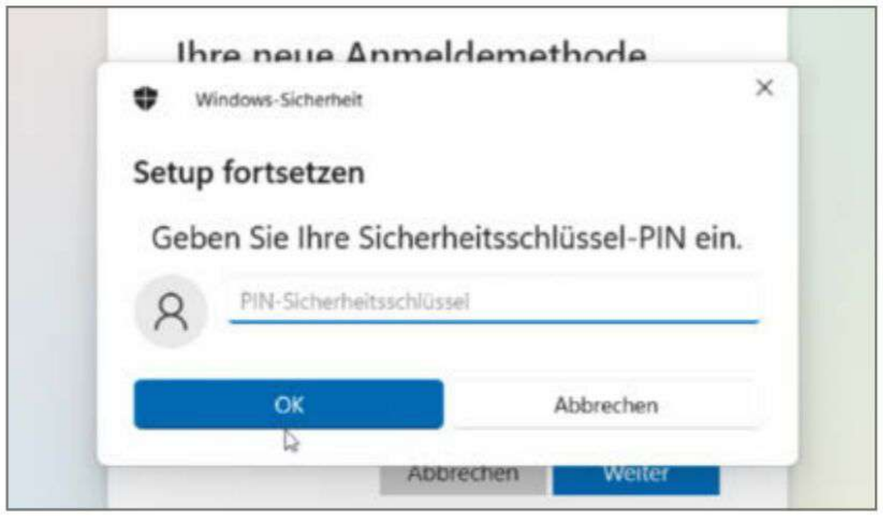
Bei Microsoft ist der Übergang zwischen den Funktionen „Schutz des Kennwort-Resets“ und „2FA“ fließend. Dort legen Sie erst fest, womit Sie Ihre Identität nachweisen wollen und aktivieren dann die „Zweistufige Überprüfung“.

2FA-Datenbank und FIDO2 ausprobieren

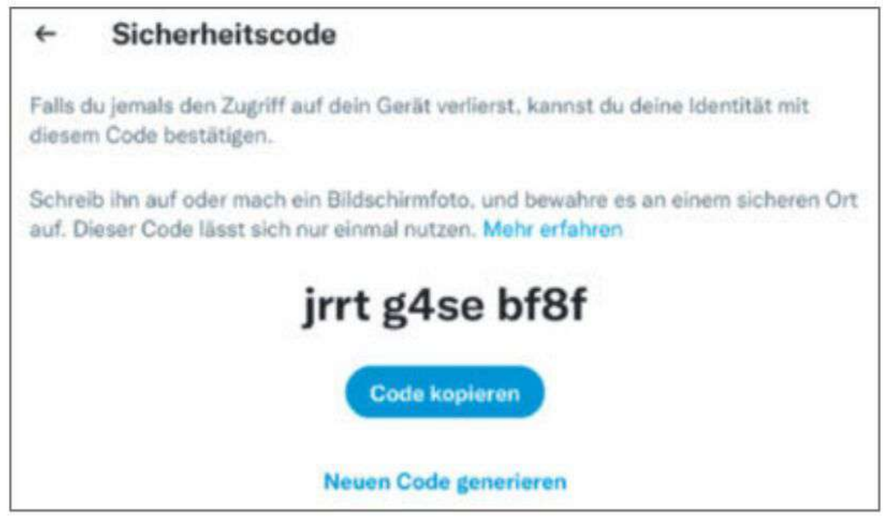
Leider geben viele Dienste außerhalb der Einstellungsdialoge keine präzise Auskunft, welche Verfahren sie verwenden. Eine gute Quelle, die solche



Zwei-Faktor-Authentifizierung richtet man über die Kontoeinstellungen ein. Dort findet man oft unter einem Menüpunkt wie „Sicherheit“ eine eigene Rubrik. Bei Google heißt sie „Bestätigung in zwei Schritten“.



Manche Dienste verlangen, dass der FIDO2-Sicherheitsschlüssel per PIN oder Fingerabruck abgesichert ist.



Verwahren Sie den angezeigten Backup-Code unbedingt gut. Mal ist es eine einfache Zeichenkette, oft ähnelt es einer TAN-Liste mit einem Dutzend Zahlencodes.

Informationen stets aktuell und übersichtlich bereitstellt, ist die als Open-Source-Projekt gepflegte Datenbank „2FA Directory“. Unter der Adresse 2fa.directory (siehe ct.de/whw3) erfahren Sie, ob Ihr Anbieter Zwei-Faktor-Authentifizierung unterstützt und finden auch Links zu den jeweiligen Hilfeseiten.

Leider funktioniert auch nicht jede Kombination aus FIDO2-, U2F-Stick oder Geräte-Chip, Betriebssystem, Browser und Onlinedienst. So verweigert Microsoft den passwortfreien Login mit FIDO2-Stick unter Linux mit Firefox, aber mit Chromium klappt es anstandslos. Wenn Sie testen wollen, ob Ihr Computer, Smartphone und Sicherheitsstick mit FIDO2 zurechtkommt, empfehlen wir die Demoseite webauthn.io. Dort sehen Sie in der Regel, welche Verfahren Ihr Browser unterstützt und welche Geräte er erkennt – eingebaut oder extern.

Änderungen kontrollieren

Ganz gleich, wie Sie vorgehen und für welches Verfahren Sie sich entscheiden: Loggen Sie sich nach der Veränderung der Zwei-Faktor-Einstellungen nicht aus. Öffnen Sie eine neue Browser-Sitzung, am besten auf einem anderen Computer, mit einem anderen Browser oder zumindest als Privat- oder Inkognito-Fenster. Ein neuer Tab reicht nicht. Versuchen Sie, sich dort anzumelden. Wird der zweite Faktor abgefragt? Klappt die Anmeldung per TOTP-Code, Sicherheits-Stick oder Geräte-Anmeldung? Funktioniert die Anmeldung auch auf anderen Geräten und in Anwendungen, die Sie benötigen?

Solange Sie in einer Sitzung angemeldet sind, haben Sie noch einen Fuß in der virtuellen Tür. So können Sie die Einstellungen korrigieren und verhindern, dass Sie sich schlimmstenfalls aussperren. Insbesondere später, wenn Sie einen zweiten Faktor entfernen oder andere 2FA-Optionen anpassen, sollten Sie vorm Abmelden prüfen, ob Sie immer noch Zugang haben.

Notieren Sie sich auch angezeigte Backups-Codes oder erzeugen Sie diese, soweit es angeboten wird. Kontrollieren Sie auch, ob der angezeigte Backup-Code mit dem notierten übereinstimmt. Gemein: Viele Dienste erzeugen jedes Mal einen neuen Backup-Code, wenn Sie sich diesen anzeigen lassen, verraten das aber nicht.

Einfach loslegen

Hat man einmal angefangen einen zweiten Faktor einzurichten, ist die größte Hürde auch schon genommen. Jedes weitere Konto ist ratzfatz abgesichert. Damit es noch einfacher wird, sollten aber manche Onlinedienste ihre Implementierungen dringend überdenken. Dazu sollten sie unbedingt mehr als einen zweiten Faktor anbieten, TOTP und FIDO2 unterstützen und proaktiv ihre Nutzer auffordern, mit Zwei-Faktor-Authentifizierung ihre Konten abzusichern.

Als Nutzer sollte man, damit sich die gewonnene erhöhte Sicherheit nicht als Bumerang ausweist, mehrere Zusatzfaktoren einrichten und die Backup-Codes gut aufbewahren. Wie man am besten verhindert, sich selbst durch verlorene oder defekte Geräte auszusperren, erklärt der folgende Artikel. Dann steht sicherem und entspanntem Anmelden nichts mehr im Weg. (ktn) c't

Literatur

[1] Jan Schüßler und Marvin Strathmann, **Ich kaufe ein ****, 25 Passwortmanager für PC und Smartphone, c’t 5/2021, S. 16

[2] Niklas Dierking, **Geheimniskrämer**, Der Raspberry Pi als Passwort-Server, c’t 9/2021, S. 18

Links zu 2FA-Datenbank und FIDO2-Testseite

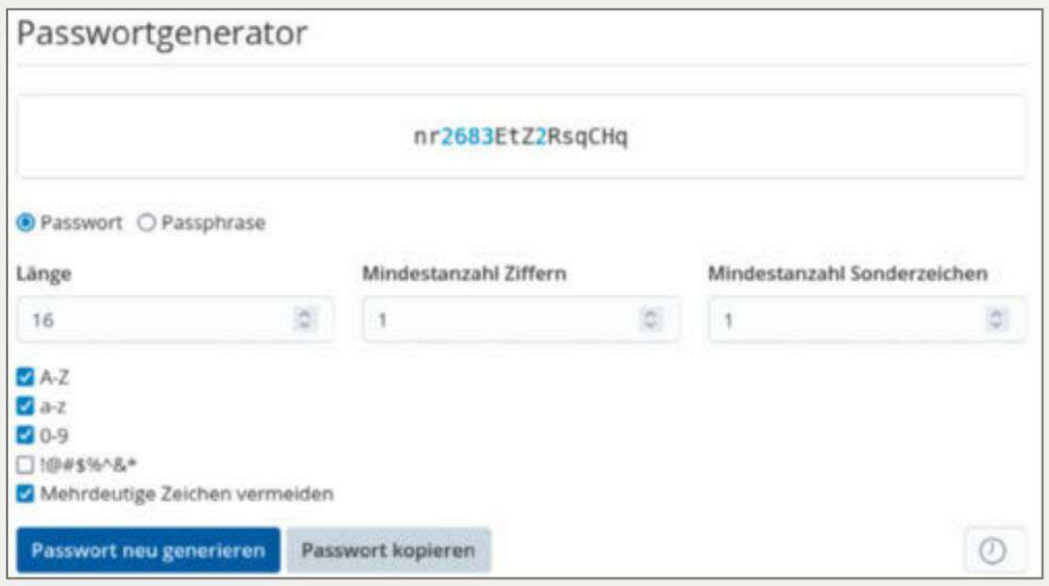
ct.de/whw3

Passwortmanager: 1-Faktor hegen und pflegen

Passwortmanager helfen, die Sicherheit Ihrer Onlinekonten zu steigern. Vergangenes Jahr haben wir 25 Passwortmanager getestet [1]. Gute Erfahrungen haben wir mit Bitwarden und KeePassXC gemacht. Letzterer eignet sich eher für den lokalen Betrieb. Es ist aber grundsätzlich möglich, die verschlüsselte Passwortdatenbankdatei etwa mit Clouddiensten zwischen mehreren Geräten zu synchronisieren. Bei Bitwarden ist diese Funktion eingebaut. Beide Programme sind Open Source und kostenlos nutzbar. Bitwarden verlangt für einige optionale Features 10 Euro im Jahr. Wer über etwas Know-how verfügt, kann mit Vaultwarden einen eigenen Passwortserver betreiben, der zu den offiziellen Bitwarden-Anwendungen kompatibel bleibt [2]. Bitwarden-Clients gibt es für Windows, Linux, macOS, Android und iOS. Den Passworttresor können Sie auch im Browser aufrufen.

Registrieren Sie zunächst einen Account auf vault.bitwarden.com. Dazu müssen Sie einen Nutzernamen und Ihre Mailadresse angeben und ein Masterpasswort setzen. Das dient fortan als Generalschlüssel Ihrer Passwortsammlung, es sollte also so sicher wie möglich sein. Ein langes Passwort ist wichtiger als viele Sonderzeichen. Denken Sie daran, dass Sie sich das Passwort merken und es höchstwahrscheinlich auch mal außerhalb des Rechners eintippen müssen. Den Zugang zu Ihrem Tresor sollten Sie außerdem mit einem zweiten Faktor versehen. In der kostenlosen Variante steht bei Bitwarden dafür das TOTP-Verfahren zur Verfügung. Sie aktivieren TOTP in den Einstellungen unter dem Menüpunkt „Zwei-Faktor-Authentifizierung“. Um sich nicht auszusperren, sollten Sie sich auch die Wiederherstellungscodes anzeigen lassen und sie im Anschluss sicher aufbewahren. Mehr dazu im Artikel auf Seite 64. Wenn Sie die App auf dem Smartphone nutzen, empfiehlt sich die Entsperrung per Fingerabdruck.

Der (Web-)Tresor listet alle Ihre Accounts auf. Hier herrscht zunächst noch gähnende Leere. Es gilt nun, Ihre Accounts samt Zugangsdaten anzulegen. Das können Sie in einer großen Hau-Ruck-Aktion manuell erledigen oder Sie installieren die Bitwarden-Browsererweiterung und erledigen den Umzug Schritt für Schritt. Die Erweiterung fragt Sie beim Login auf Webseiten, für die noch keine Zugangsdaten im Tresor liegen, ob Nutzername und Passwort gespeichert werden sollen. Das sollten Sie bestätigen und bei der Gelegenheit direkt prüfen, ob das aktuell genutzte Passwort sicher genug ist. Wenn nicht, schmeißen Sie den Passwortgenerator an, der in allen Bitwarden-Anwendungen zur Verfügung steht. Dabei können Sie zwischen Passwörtern und Passphrasen wählen und diverse Parameter setzen, zum



Schluss mit Kopfzerbrechen und Eselsbrücken: Der Passwortgenerator nimmt Ihnen die Denkarbeit beim Erstellen starker Passwörter ab.

Beispiel die Passwortlänge oder ob es Sonderzeichen, Ziffern und Groß- und Kleinbuchstaben enthalten soll. Darauf, ob das Passwort gut zu merken ist, müssen Sie keine Rücksicht mehr nehmen, darum kümmert sich ab jetzt die Software. Sie müssen lediglich das Masterpasswort im Kopf behalten. Mit dem Werkzeug „Bericht über wiederverwendete Passwörter“ warnt Bitwarden, wenn Sie entgegen der ausdrücklichen Empfehlung für mehrere Dienste das gleiche Passwort nutzen.

Ersetzen Sie jetzt Ihr altes Passwort bei dem Onlinedienst durch das sichere Passwort aus dem Generator und melden sich erneut an. Die Browsererweiterung bietet nun an, das Passwort im Tresor zu aktualisieren. Dem stimmen Sie zu. Falls bei diesem Vorgang mal etwas schiefläuft und Sie ein bombensicheres, nicht merkbares Passwort beim Dienst gesetzt haben, ohne dass es in Ihren Tresor gewandert ist, haben Sie sich nicht endgültig ausgesperrt. Sie können das Passwort immer noch über die herkömmliche „Passwort vergessen?“-Funktion des Dienstes zurücksetzen. In solchen Fällen hilft auch ein Blick in die Passworthistorie des Generators. Sie listet die letzten generierten Passwörter, egal ob sie in den Tresor gewandert sind oder nicht.

Sobald Nutzername und Passwort eines Dienstes im Tresor gelandet sind, füllt Bitwarden dessen Login-Formulare im Browser automatisch aus, wenn Sie auf das Icon der Bitwarden-Browsererweiterung klicken oder die Tastenkombination Cmd- oder Windows-Taste + Umschalt + L betätigen. Mit den grundlegenden Funktionen sind Sie nun vertraut und Ihre Accounts durch starke Passwörter ein gutes Stück sicherer.

U2F und FIDO2

Aus Nutzersicht unterscheidet sich die Einrichtung von U2F und FIDO2 nicht. Wählen Sie in den Zwei-Faktor-Einstellungen als Typ „Sicherheitsschlüssel“, U2F, FIDO2 oder ähnliches aus, soweit verfügbar. Dann fragt der Browser, ob Sie der Webseite den Zugriff auf das Sicherheitsgerät gestatten. Beim älteren U2F-Verfahren sind es ausschließlich externe USB-Sticks.

Bei FIDO2 können Sie je nach Betriebssystem und Browser den Sicherheitsstick auch per NFC oder Bluetooth koppeln oder den in PC, Tablet oder Handy eingebauten Sicherheitschip (Trusted Platform Module, TPM, oder Secure Element) verwenden. Bei Android heißt die Option verklausuliert „Displaysperre“. Unter macOS dienen der Fingerabdrucksensor, unter iOS je nach Gerät Fingerabdrucksensor oder Gesichtserkennung zum Entsperren des Chips. Unter Windows drängelt sich zunächst Windows Hello vor. Bestätigen Sie den Vorgang so, wie Sie auch die Displaysperre aufheben, also per PIN, Fingerabdruck oder Hello-Kamera.

Wenn Sie stattdessen den Dialog abbrechen, können Sie einen angeschlossenen Sicherheitsstick verwenden. Der Stick blinkt und Sie bestätigen den Kopplungsvorgang per Druck auf die Taste oder Kontaktfläche des Sticks. Manche Dienste verlangen zusätzlich, dass der Sicherheitsstick per PIN gesichert wird. Falls Sie für Ihren Sicherheitsstick noch keine zugewiesen haben, können Sie eine neue PIN festlegen. Anschließend dürfen Sie bei vielen Anbietern für den neuen Eintrag einen Namen vergeben, damit Sie Ihre jeweiligen FIDO-Geräte später auseinanderhalten können.

Einige wenige Dienste wie Microsoft und eBay bieten an, mit FIDO2 ganz aufs Passwort zu verzichten, aber die überwiegende Mehrheit beschränkt sich auf die Funktion als zweiter Faktor.

Unter anderem vorhanden bei: AWS, Facebook, GitHub, GitLab, Google, Microsoft, Twitter



Erkennt Ihr System den eingebauten Sicherheitschip, dürfen Sie auch diesen auswählen, sonst müssen Sie ein externes Gerät wie einen FIDO2-USB-Stick verwenden.

Anbieter-App

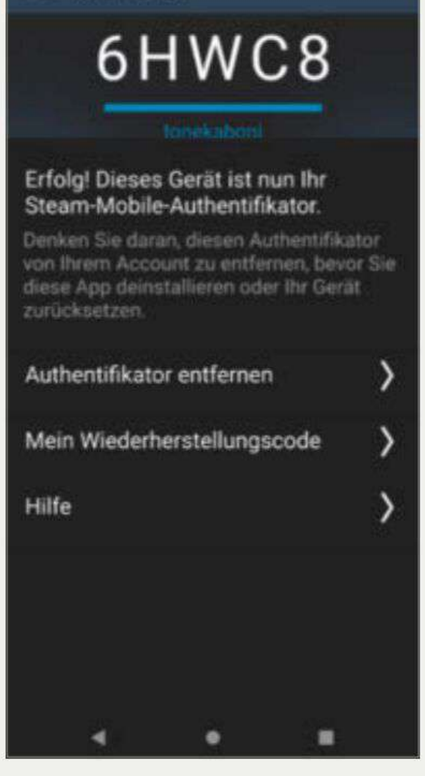
Auch eine anbieterspezifische App kann einen komfortablen zweiten Faktor abgeben. Manch ein Dienst wie Google oder Dropbox richtet das auch automatisch ein, sobald Sie auf einem anderen Gerät angemeldet sind. Ansonsten finden Sie es als eine weitere Option in den Zwei-Faktor-Einstellungen, etwa unter der Bezeichnung „App verwenden“. Teilweise heißt es auch ganz anders, wie bei Steam, wo 2FA auf den Namen „Steam Guard“ hört.

Die Einrichtung und Arbeitsweise der App ist je nach Dienst unterschiedlich, wird aber meist gut erklärt. Bei Steam müssen Sie einen per SMS zugesandten Code hinzufügen, bei Microsoft einen QR-Code einscannen. Letzteres ähnelt dem TOTP-Verfahren. Microsoft versucht so, alle an TOTP Interessierten zu seinem eigenen Verfahren zu locken.

Bei manchen Apps reicht es einfach, nur auf dem Handy oder Tablet den Login zu bestätigen. Andere Apps zeigen wie bei TOTP einen Code an, den man im Browser angeben muss.

Unter anderem verfügbar bei: Dropbox, eBay, Instagram, Microsoft, PayPal, Steam

Steam Guard arbeitet ähnlich wie TOTP, aber man ist auf die Steam-App festgelegt.



TOTP (Authenticator App)

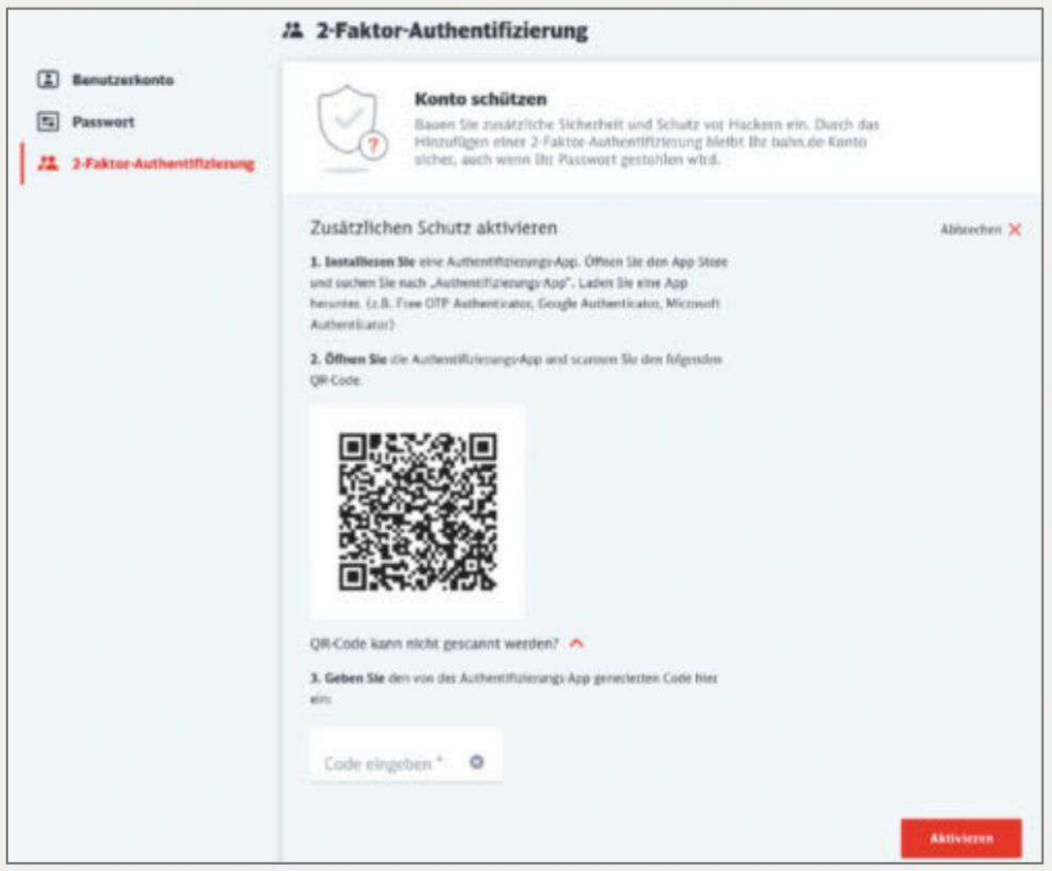
In den Zwei-Faktor-Einstellungen heißt TOTP oft „Bestätigung per Authentifizierungs-App“, irgendwas mit „Google Authenticator“ oder „(zeitbasiertes) Einmalkennwort“. Sie werden zunächst aufgefordert, die App herunterzuladen und einzurichten. Auch wenn viele Dienste den Google Authenticator empfehlen, können Sie die Codes auch in einer anderen App wie andOTP oder Authy, einem Passwortmanager oder einem Hardwaregerät verwalten. Obacht: Microsoft versucht einem zunächst ein proprietäres nicht kompatibles Verfahren anzudrehen, aber man kann eine beliebige TOTP-App nutzen und auch Microsofts App spricht TOTP.

Wenn Ihnen der QR-Code angezeigt wird, scannen Sie diesen mit Ihrer App oder dem Lesegerät ein. Auf dem Smartphone starten Sie die TOTP-App und wählen „QR-Code scannen“. Lesen Sie den Code ruhig mit mehreren Geräten ein. Die Desktop-App „Yubico Authenticator“ sucht auf Wunsch den sichtbaren Bildschirmbereich nach QR-Codes ab.

Alternativ zum QR-Code können Sie sich auch eine Zeichenkette anzeigen lassen, wenn Sie auf einen Satz wie „Ich kann den QR-Code nicht scannen“ klicken. Die Zeichenkette können Sie kopieren und manuell als TOTP-Geheimnis hinterlegen, etwa im Passwortmanager oder einer TOTP-App. Die Leerzeichen spielen keine Rolle. Manche Dienste wie Sipgate erzeugen aber jedes Mal ein neues Geheimnis, wenn Sie die Ansicht wechseln. Überprüfen Sie, ob alle Geräte das gleiche Ergebnis anzeigen.

Nachdem Sie den Code gescannt haben, wird Ihnen in Ihrem TOTP-Gerät ein sechsstelliger Code angezeigt, der alle 30 Sekunden wechselt. Klicken Sie auf der Webseite auf „Weiter“ und bestätigen Sie mit dem Zifferncode. TOTP wird als zweiter Faktor in der Regel erst dann aktiv, wenn Sie mit einem Code die Einrichtung abgeschlossen haben.

Unter anderem vorhanden bei: DB, Fritzbox, Hetzner, IONOS, LinkedIn, Reddit, Sipgate, Slack, WISO Steuer, Xing

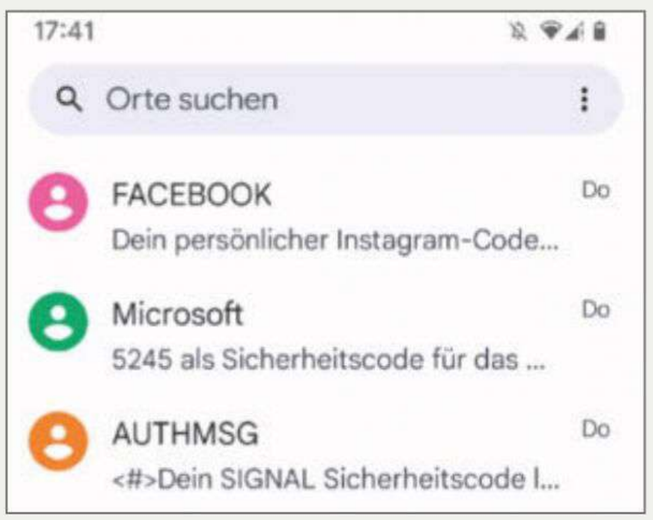


Um die Einrichtung von TOTP abzuschließen, müssen Sie den QR-Code einscannen und dann den im Authenticator angezeigten Zahlencode eingeben.

SMS

Relativ einfach ist die Einrichtung von SMS als zweiter Faktor und funktioniert ähnlich wie die mTAN beim Onlinebanking, krankt aber an den gleichen Problemen. Dazu geben Sie unter den Zwei-Faktor-Einstellungen Ihre Rufnummer an. Kurze Zeit später sollten Sie eine SMS mit einem Code erhalten. Bestätigen Sie die Einrichtung mit Eingabe des Codes. Falls keine SMS kommt, versuchen Sie sich erneut eine SMS zuschicken zu lassen oder schauen Sie im Spam-Bereich Ihrer SMS-App.

Indem sie 2FA-Codes nur per SMS schicken, machen es sich viele Dienste einfach.



Ein Veranstaltungsformat der Make:
make-magazin.de

3,- EUR Rabatt je Ticket
mit dem Code **CTW226MF**
SCHNELL SEIN LOHNT SICH.
Gilt nur für die ersten 100 Bestellungen!

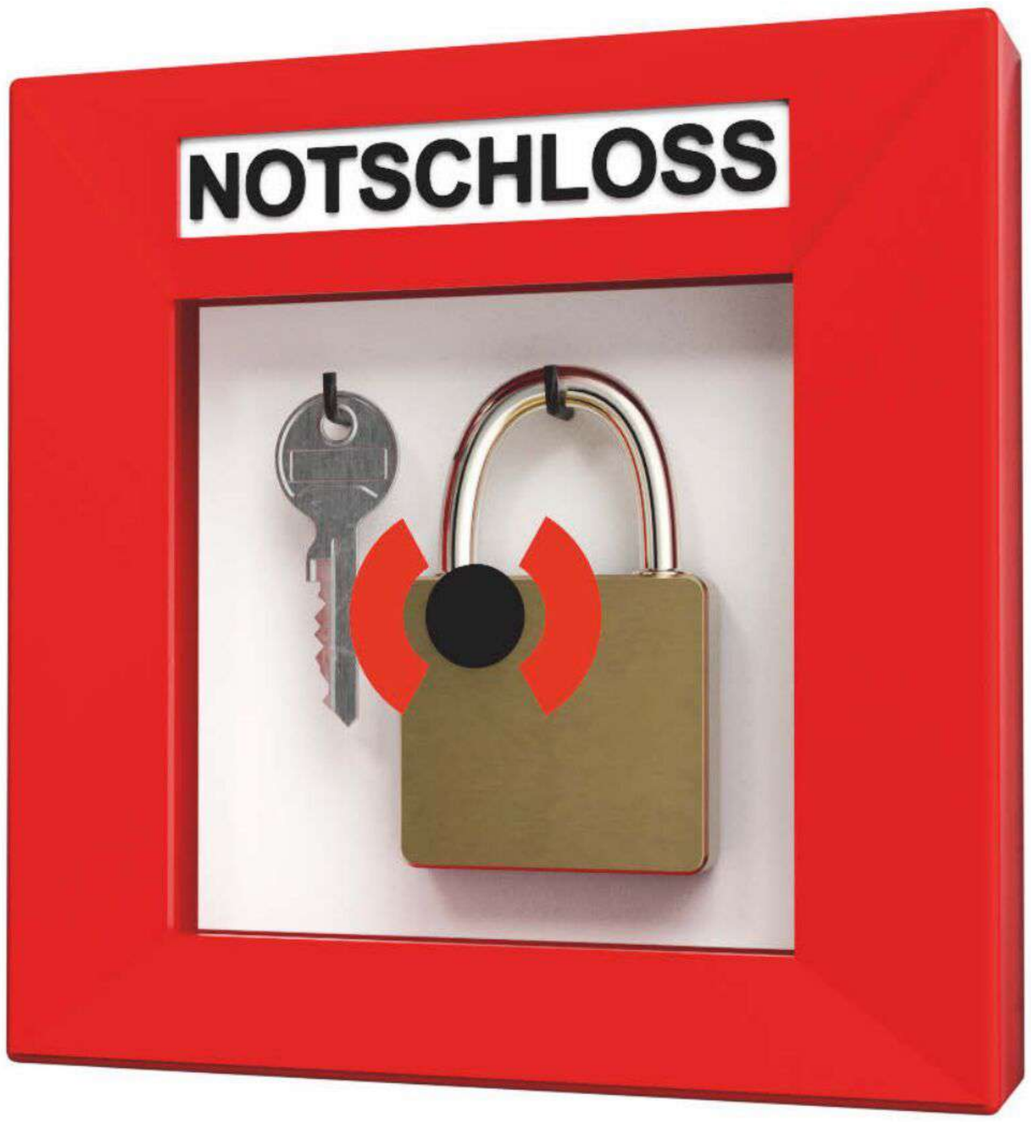
Hannover Maker Faire®

Das Format für Innovation und Macherkultur

10.–11. Sept.

Hannover Congress Centrum

maker-faire.de/hannover



Vorbeugen statt Frust bei 2FA-Verlust

Der zweite Faktor sollte Angreifer aussperren, Sie aber keinesfalls. Auch dann nicht, wenn Sie das Handgepäck verlieren oder zu Hause eingebrochen wurde. Mit unseren Tipps für eine systematische Bestandsaufnahme vermeiden Sie Login-Katastrophen.

Von **Jan Mahn**

Sie haben bereits für alle Dienste einen zweiten Faktor aktiviert, authentifizieren sich mit SMS-Codes, FIDO2-Sticks und TOTP-Apps und fühlen sich rundum sicher? Dann hätten wir noch eine Frage, die Sie beunruhigen könnte: Haben Sie auch an Backups Ihrer zweiten Faktoren gedacht? Bei Dateien hat es sich bereits herumgesprochen: Backups sind unersetzlich, denn allzu schnell haben sich Emotet oder andere Verschlüsselungstrojaner Ihrer Daten bemächtigt. Hat man ein Backup, sollte man sich auch Gedanken machen, wie man an die Daten kommt, wenn die Wohnung unter Wasser steht – ein sogenanntes Offsite-Backup (am besten verschlüsselt) in der Cloud oder bei Freunden muss her. Glei-

ches gilt für die Sicherungen Ihrer zweiten Faktoren, damit Sie sich im Ernstfall nicht bei wichtigen Diensten aussperren.

Vorab direkt die schlechte Nachricht: Wenn Sie bei einem Dienst einen zweiten Faktor eingerichtet haben und auf diesen aus welchem Grund auch immer nicht mehr zugreifen können, brauchen Sie nicht auf die Hilfe der Dienstanbieter zu hoffen: Bei Facebook, Twitter, Google & Co. können Sie sich in dem Moment innerlich von Ihrem Account verabschieden, in dem Sie den zweiten Faktor unrettbar verloren haben. Der Support wird sich mit Ihrem Problem sicher nicht im erhofften Maße beschäftigen – irgendwie auch zu Recht, denn sonst könnten ja auch Angreifer mit netten Mails an den Support und hübschen Geschichten an Ihren Account gelangen. Eine Chance haben Sie beim Support oft nur, wenn Sie dort eine bestätigte postalische Adresse hinterlegt haben.

Damit es nie so weit kommt, dass Sie verzweifelt den Support kontaktieren müssen, gilt: Zweite Faktoren sind Rudeltiere, keine Einzelgänger: Die allermeisten Dienste, die einen zweiten Faktor anbieten, kennen die Option, mehrere Verfahren und auch dort jeweils mehrere Geräte zu nutzen – also zum Beispiel mehrere FIDO-Sticks und mehrere TOTP-Apps. Machen Sie davon reichlich Gebrauch. Nur wenige erlauben nur einen einzigen zweiten Faktor.

Was kann schon schiefgehen?

Zu einer sinnvollen Zwei-Faktor-Strategie gehört deshalb eine Backup-Strategie und deren Ausarbeitung darf ruhig einen regnerischen Nachmittag in Anspruch nehmen. Nehmen Sie am besten Zettel und Stift oder eine Tabellenkalkulationssoftware zur Hand und verschaffen sich zunächst einen Überblick, was bei Ihnen alles als zweiter Faktor herhält: Handy mit Apps und SMS, FIDO-Stick, das TPM in Desktop und Notebook, externer TOTP-Generator. Der Artikel ab Seite 50 beschreibt konkret, wo bei den einzelnen Verfahren das schützenswerte Geheimnis abgelegt wird.

Im zweiten Schritt bietet sich eine simple Tabelle an – in die Spalten nebeneinander kommen die genutzten zweiten Faktoren, in die Zeilen untereinander alle Dienste, bei denen Sie Konten haben. Im Passwortmanager des Vertrauens, den Sie als ersten Schritt zur Absicherung Ihrer Logins eingerichtet haben, bekommen Sie den besten Überblick, bei welchen Diensten noch Accounts existieren. Sind Spalten und Zeilen vorbereitet, setzt man Häkchen überall dort, wo der zweite Faktor eingerichtet ist.

Dabei lohnt es sich, bei jedem Dienst direkt die Einstellungsseiten zu besuchen und möglichst viele zweite Faktoren einzurichten, damit sich die Tabelle mit Häkchen füllt. Unten sehen Sie, wie eine solche Tabelle aussehen kann. Außerdem kann man bei der Gelegenheit noch einmal sicherstellen, dass alle Kennwörter zufällig generiert und möglichst lang sind. Im gleichen Schritt schadet es nicht, bei den Diensten die Wiederherstellungscodes, sofern angeboten, abzurufen. Das sind Zweitschlüssel für den Notfall, dass alle anderen zweiten Faktoren nicht mehr zur Verfügung stehen. Accounts, die Sie nicht mehr brauchen, sollten Sie direkt löschen.

Am Ende der mühsamen Prozedur haben Sie eine bestenfalls gut mit Häkchen gefüllte Tabelle als Arbeitsgrundlage für die nächsten Schritte. Herausfiltern können Sie zunächst alle Dienste, die keinen zweiten Faktor unterstützen. Das sind offene Baustellen für später. Sofern Sie dort ein einmaliges und langes Kennwort einsetzen, haben Sie Ihre Schuldigkeit getan.

Mit den verbliebenen Zeilen in der Tabelle können Sie jetzt verschiedene Szenarien durchspielen, indem Sie einzelne oder mehrere Spalten abdecken oder ausblenden. Was passiert zum Beispiel, wenn im Zug der Rucksack mit Handy, Laptop und FIDO2-Stick abhandenkommt? Sofern dann in einer Zeile,

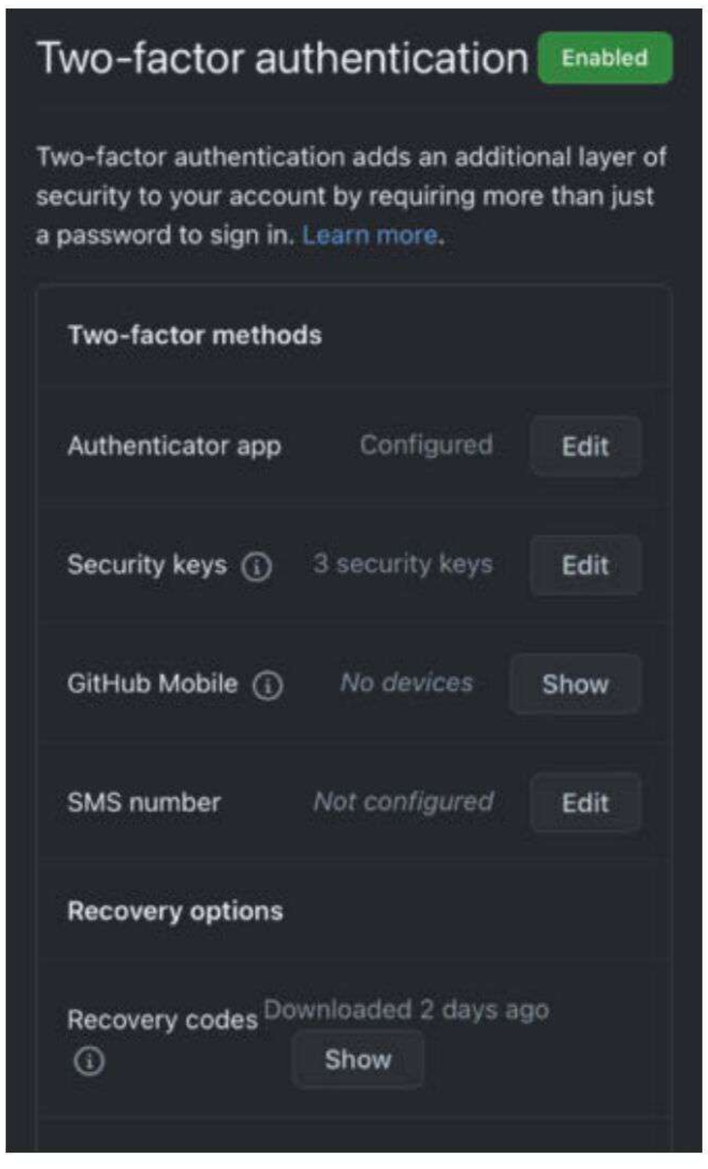
Zwei-Faktor-Strategie: Eine Beispieltabelle

Dienst	SMS	USB-C-FIDO-Stick	FIDO2 im Notebook	FIDO2 im Smartphone	TOTP-App	Probleme bei
GitHub		✓	✓	✓	✓	
Amazon	✓				✓	Verlust des Smartphones
Google	✓	✓	✓	✓		

also bei einem Dienst, kein Häkchen mehr übrig bleibt, besteht Handlungsbedarf.

Was tun?

Sobald Sie problematische Zeilen ausgemacht haben, müssen Sie nachlegen und möglicherweise neue Spalten, also zusätzliche Faktoren, anlegen. Zunächst sollten Sie aber überlegen, ob Sie schon alle Optionen ausgeschöpft haben, die Ihnen zur Verfügung stehen. Macs, Windows-PCs, iOS- und Android-Telefone mit TPM arbeiten zum Beispiel sehr komfortabel als FIDO2-Authenticator, ganz ohne Investition in einen FIDO2-Stick – das sollten Sie nutzen, mehr dazu ab Seite 50. Wer bereit ist, das Geld auszugeben, kann zusätzlich in einen FIDO2-Stick als Backup investieren, der (mit PIN gesichert) bei vertrauenswürdigen Freunden, Verwandten oder im Bankschließfach landet.



Viel hilft viel: GitHub zeigt in den Einstellungen eine ausführliche Übersicht über die eingerichteten Faktoren.

Eine kostenlose Alternative ist ein Open-Source-Passwortmanager wie KeePassXC, der unter Windows, Linux und macOS läuft. Er legt seine Kennwortdatenbank verschlüsselt in einer Datei ab. Andere Passwortmanager, die so arbeiten, eignen sich ebenfalls als letzte Reserve. Speichern können Sie in den meisten Passworttresoren nicht nur Kennwörter, sondern sämtliche Geheimnisse in Form von „Notizen“ oder „Anmerkungen“. Legen Sie sich also eine Backup-Datenbank im Passwortmanager an und füllen die mit allem, was die Dienste hergeben, etwa mit sämtlichen Wiederherstellungscodes. Hinzu kommen Geheimnisse, die beim Einrichten von TOTP zusätzlich zum QR-Code angezeigt werden. Damit können Sie zusammen mit Account- und Dienstname später im Notfall eine frische TOTP-App einrichten.

Zu guter Letzt speichern Sie die Antworten auf die leidigen Sicherheitsfragen, die einige Dienste bis heute stellen, ebenfalls in der Datei. Weil diesen Fragen ein völlig antiquiertes Konzept zugrunde liegt, beantworten Sie die Frage nach dem Namen Ihrer Großmutter nicht wahrheitsgemäß, sondern generieren mit dem Passwortmanager eine Zufallszeichenkette als Antwort – dann haben auch Angreifer keine Chance, die eine solche Information mit wenig Aufwand zum Beispiel aus den sozialen Netzwerken oder durch Nachfragen bei Ihnen oder Verwandten herausfinden könnten.

Wenn Ihre Datenbank für alle Notfälle gefüllt ist und Sie die wichtigen Lücken in der Tabelle schließen konnten, verschließen Sie die Geheimnisdatenbank mit einem wirklich sicheren Kennwort. Die Datenbankdatei lagern Sie dann zum Beispiel auf zwei USB-Sticks, einer bleibt zu Hause und einer liegt außer Haus. Für das Kennwort überlegen Sie sich einen anderen sicheren Ort, oder verwenden direkt den ersten Satz Ihres Lieblingsbuchs. Das lässt sich auch beschaffen, wenn die Wohnung unter Wasser steht.

Muss ich sperren?

Trotz Backup-Strategie ist der Verlust der zweiten Faktoren ein Problem: Ein Dieb oder unehrlicher Finder Ihres Rucksacks mit allerhand Faktoren darin könnte versuchen, auch Ihre digitale Identität zu übernehmen. Anders als bei einem verlorenen Portemonnaie und dem Verlust von Bank- sowie Kreditkarten müssen Sie aber nicht direkt die Kartensperrhotline (116 116) anrufen. Für zweite Faktoren gibt es die bisher auch nicht – eine häufige Kritik am

FIDO-Standard. Doch ganz so einfach ist es für den Finder ohnehin nicht.

Zunächst ein Blick auf alle Geräte, an denen Sie sich anmelden müssen, also Telefone, Laptops und Tablets: Wenn dort das TPM als Hort für Geheimnisse genutzt wird, ist dieses mit Kennwort, PIN oder Fingerabdruck verriegelt. Bei vielen TOTP-Apps etwa reicht es nicht mal, wenn das Telefon entsperrt ist – zum Nutzen der App muss man sich erneut mit Fingerabdruck oder PIN ausweisen. Wer die PIN zu oft falsch eintippt, der sperrt sich endgültig aus. Der Verlust des Laptops in der Bahn bleibt damit ärgerlich, wird aber nicht zum Sicherheitsdesaster. Es reicht, in Ruhe zu Hause zu einem der Backups zu greifen, sich bei allen Diensten anzumelden und die verlorenen zweiten Faktoren zu löschen. Es wäre zweifelsohne schön, wenn mal jemand einen Standard erfinden könnte, damit das automatisiert gelingt.

Einen genaueren Blick wert sind Codes per SMS. Ist das Mobiltelefon so eingestellt, dass es Textnachrichten im Sperrbildschirm vor der PIN-Abfrage einblendet, könnten Finder damit durchaus Schaden anrichten. Wenn Sie SMS-Codes als zweiten Faktor nutzen, schalten Sie diese Funktion im Telefon aus.

Bei FIDO-Sticks hängt die Schwere des Problems davon ab, wie Sie diese eingerichtet haben. Am bequemsten im Alltag ist es, auf eine PIN-Eingabe zu verzichten. Für einen Finder ist die Hürde dennoch vergleichsweise hoch – er müsste erst mal wissen, für welche Accounts der gefundene Stick eingerichtet ist. Dann bräuchte er immer noch Ihr sicheres Kennwort. Wenn Sie etwas Komfortverlust in Kauf nehmen, sichern Sie ihn per PIN. Gibt ein Finder die fünf Mal falsch ein, kann er den Stick nur noch zurücksetzen.

Lohnt sich das?

Eine gute Zwei-Faktor-Strategie ist wie eine Backup-Strategie für Daten mühsam. Bewähren kann sie sich aber schneller, als man hofft. Es muss nicht immer der größte anzunehmende Unfall sein – es reicht, dass ein Handy den Geist aufgibt. Dann schnell wieder arbeiten zu können, ist die Mühe allemal wert.

(jam) c't

Sicherer Einsatz von Microsoft 365

Online-Workshop am 6. Juli 2022

iX Workshop

In diesem Workshop zeigen wir Ihnen auf, wie Sie den Einsatz von Microsoft 365 sicher gestalten können, genauso wie notwendige Maßnahmen in Bezug auf den Datenschutz und die Informationssicherheit.

Die Inhalte
- Datenschutz und Microsoft 365
- Informationssicherheit
- Security auf der Microsoft Plattform
- Compliance-Vorgaben

Jetzt FRÜHBUCHER-RABATT sichern!



heise-events.de/workshops/sicherer-einsatz-von-m365

Kennwörter, FIDO2 und TOTP



In der Theorie sind zweite Faktoren einfach: Zusätzlich zum Kennwort in Kopf oder Passwortmanager muss man beim Anmelden beweisen, dass man etwas besitzt, das ein Geheimnis enthält. In der praktischen Umsetzung tauchen aber diverse Fragen auf – die häufigsten haben wir zusammengetragen.

Von **Niklas Dierking und Jan Mahn**

? Es heißt immer, das Risiko sei groß, dass Webdiensten Kennwortdatenbanken abhandenkommen und man deswegen unbedingt für jeden Dienst ein eigenes Kennwort benutzen soll. Ist das wirklich so wahrscheinlich oder wird die Gefahr übertrieben dargestellt?

! Unbestritten gibt es viele Anbieter, die sehr verantwortungsvoll mit den Kennwörtern ihrer Nutzer umgehen, sie mit einem sogenannten Salt versehen sowie als Hash und nicht im Klartext abspeichern – mit einer solchen Kennwortdatenbank kann ein Angreifer, der es geschafft hat, in einen Server einzubrechen, sehr wenig anfangen. Ein kleiner Anteil der Anbieter dagegen hat die Security-Empfehlungen der letzten 20 Jahre verpennt, schlampt zusätzlich mit Updates und lässt sich unverschlüsselte Kennwortlisten megabyteweise klauen. Wenn man Konten bei diversen Webshops und Foren hat, ist die Wahrscheinlichkeit daher sehr hoch, dass ein schwarzes Schaf dabei ist.

Wer wissen will, ob Benutzername/Kennwort-Datensätze für eigene Accounts bereits im Umlauf sind, kann die Suche auf haveibeenpwned.com bemühen und dort seine Mailadresse eintippen, die ja bei den meisten Diensten als Benutzername herhält. Die Seite wird von einem Freiwilligen ohne kommerzielles Interesse betrieben und verwahrt Datensätze aus bekannten Leaks, deren Daten meist schon in dunklen Kreisen gehandelt werden. Nach Angaben des Betreibers hat er bereits 11 Milliarden kompromittierte Accounts in seiner Datensammlung. Das sollte auch den letzten Fan von vermeintlich sicheren Universalkennwörtern überzeugen, für jeden Dienst unbedingt ein eigenes zu vergeben. Eine deutschsprachige Alternative ist die vom Hasso-Plattner-Institut betriebene Seite sec.hpi.de/ilc.

? Ist es sicher, wenn ich mich bei Onlinediensten mit meinem Google-, Facebook- oder GitHub-Account einlogge?

! Das Angebot, sich über den Account eines Anbieters anzumelden, findet man im Internet häufig. Auf immer mehr Websites gibt es Buttons wie „Login mit Facebook oder Google“. Die vermittelnden Anbieter sind in der Lage, Ihre Anmeldungen sehr sicher zu gestalten – sicherer womöglich als ein kleiner Webshop-Betreiber, der darauf angewiesen ist, dass sein IT-Dienstleister regelmäßig die Webshop-Software aktuell hält. Wer gelegentlich in unterschiedlichen kleinen Shops einkauft, ist zum Beispiel mit einem „Check out über Amazon“ oft sicherer unterwegs als mit einem neuen Kundenkonto.

Andererseits werden die großen Dienste damit auch zu einem „Single Point of Failure“ und für Angreifer wird es reizvoller, solche Accounts zu erbeuten. Deshalb sollte man solche Funktionen nur nutzen, wenn man den Account beim großen Anbieter mit allen zur Verfügung stehenden Mitteln vernagelt hat. Ein anderes Problem kann man nicht lösen: Google, Facebook & Co. bieten diesen Dienst nicht

aus purer Nächstenliebe an. Im Gegenzug für die Dienstleistung sammeln sie durch Tracking Nutzungsdaten, merken sich also zum Beispiel, in welchen Shops man sich rumtreibt. Solche Informationen können dann in personalisierte Werbung einfließen.

FIDO2 und Kryptografie

? Mal lese ich von FIDO2, mal von Webauthn. Wie heißt das denn jetzt?

! Hinter beiden Begriffen steckt die FIDO-Alliance, bei der Branchengrößen wie Apple, Amazon, Google, Intel und Microsoft Mitglied sind. Für eine FIDO2-Anmeldung braucht man zwei Komponenten: Auf der einen Seite muss der Browser mitspielen, per JavaScript Bescheid bekommen, dass eine Anmeldung über FIDO2-Hardware stattfindet, und den Auftrag an die Hardware übergeben. Dieser Teil ist im Webstandard mit dem Namen Webauthn (kurz für Web Authentication) geregelt, der vom World Wide Web Consortium (W3C) verwaltet wird. Die zweite Komponente ist die Hardware selbst (als Stick oder über das in Geräten eingebaute TPM oder Secure Element). Der Standard dafür heißt „Client to Authenticator Protocol“ (CTAP) und wird von der FIDO Alliance betreut.



? Bei FIDO2 und U2F gibt es ein Geheimnis, das in der Hardware liegt. Wird das beim Anmelden übertragen? Dann wären die Verfahren ja genauso unsicher und anfällig gegen Man-in-the-Middle-Angriffe wie Kennwörter.

! Das kryptografische Geheimnis verlässt den FIDO2-Stick oder das TPM niemals. Zum Einsatz kommt ein Challenge-Response-Verfahren, also asymmetrische Kryptografie: Der Server schickt eine Zeichenkette, im Krypto-Chip wird diese kryptografisch signiert und zurückgeschickt (der Browser vermittelt zwischen Server und Chip). Der Server kann anhand der Signatur überprüfen, dass Sie im Besitz des Geheimnisses sind, ohne dass das Geheimnis selbst verschickt wird. Nach demselben Prinzip funktionieren auch viele andere asymmetrische Verfahren wie die Zertifikatsanmeldung bei SSH-Verbindungen oder eine digitale Unterschrift.

Schafft es ein Angreifer, sich in den Verkehr zwischen Ihrem Browser und dem Server einzuklinken, kann er dort wenig Schaden anrichten. Wenn er nur den Verkehr mitliest, sieht er keine Geheimnisse. Schafft er es, den Verkehr zu manipulieren, kann er schlimmstenfalls dafür sorgen, dass eine Anmeldung scheitert. Er kann dennoch keine Geheimnisse entführen. Was genau bei einer Webauthn-Anmeldung im Hintergrund passiert und wie man die Funktion in Webseiten einbaut, haben wir in einem Artikel für Entwickler ausführlich beschrieben [1].

? Ich verstehe immer noch nicht, warum das Geheimnis im Krypto-Chip unter keinen Umständen ausgelesen werden kann. Wenn es da reinkommt, muss man es doch auslesen können.

! Die Krypto-Chips im TPM und in FIDO2-Sticks wurden eigens für diesen Zweck entworfen, daher konnte man auch genau bestimmen, welche Funktionen sie haben. Einen Befehl, der das Geheimnis herausrückt, gibt es nicht. Außerdem wird das Geheimnis nicht auf dem PC von einer Software generiert und dem Chip übergeben, sondern direkt in diesem ausgewürfelt und gespeichert. Immer wenn man einen FIDO-Stick auf Werkseinstellungen zurücksetzt, erzeugt er ein neues Geheimnis.



Bild: www.freepik.com

? Ist es klug, einen FIDO2-Stick im Rechner stecken zu lassen oder sollte ich ihn immer abziehen, um es Angreifern nicht zu leicht zu machen?

! Bei Notebooks gibt es zunächst eine ganz direkte Gefahr: Der Stick könnte unterwegs geklaut werden, wenn man den Rechner mal kurz allein lässt. Dann gibt es noch eine theoretische Gefahr aus der Ferne. Angreifer könnten probieren, dem Stick massenhaft Challenges zu schicken, die er signieren soll. Mit ausreichend signierten Zeichenketten könnten sie möglicherweise auf den Schlüssel schließen. Das ist aber ein hypothetischer Angriff, den bisher noch niemand umgesetzt hat. Praktisch im Weg steht außerdem die Forderung im Standard nach „User Presence“. Der Benutzer muss bei jedem Login einen Hardware-Knopf betätigen. Besonders schützenswerte Dienste können auch „User verification“ (per PIN oder Biometrie) verlangen. Beides können Angreifer nicht für massenhaftes Signieren umgehen.

Wer ganz sicher gehen will, zieht den Stick immer ab und legt ihn weg, besonders wenn man ihn so konfiguriert hat, dass er neben seiner Arbeit als FIDO2-Authenticator auch als Tastatur-Emulator arbeitet und eine lange Passphrase auf Knopfdruck ausgibt. Nach unserer Langzeiterfahrung überleben alle Sticks, die aus einer durchgehenden Platine bestehen (wie die SoloKeys und YubiKeys) auch jahrelang am Schlüsselbund.

? Ich möchte FIDO2 ungern bei mehreren Diensten nutzen, weil ich Angst habe, damit meine Anonymität aufzugeben. Weil die Dienste ja beim Registrieren einen öffentlichen Schlüssel meines FIDO2-Sticks speichern, könnten sie sich untereinander austauschen, wo ich noch alles Accounts habe, oder stimmt das nicht?

! Genau das haben die FIDO2-Erfinder bedacht und verhindert: Die Sticks und auch die TPMs nutzen ihr Geheimnis, um für jeden Dienst einen eigenen Schlüssel abzuleiten – dafür verarbeiten sie die URL des Dienstes. Jeder Betreiber bekommt also einen eigenen öffentlichen Schlüssel zu sehen, Rückschlüsse auf Accounts bei anderen Anbietern sind nicht möglich.

2FA Implementieren

? Mein Arbeitgeber wünscht von mir als Entwickler, dass wir eine von uns entwickelte Anwendung mit einem zweiten Faktor absichern. Was sollte ich beachten, wo fange ich an?

! Am besten beschränken Sie sich auf TOTP und FIDO2. Damit erreichen Sie viele Anwender und haben sichere Verfahren. Für SMS-Codes braucht man einen SMS-Dienstleister und zahlt bei großen Nutzerzahlen recht viel Geld für ein vergleichsweise unsicheres Verfahren. Bevor Sie loslegen und FIDO2 und TOTP in die eigene Anwendung einbauen, sollten Sie überlegen, ob nicht auch ein vorgeschalteter Authentifizierungsdienst infrage kommt. Wie Sie mit der Open-Source-Software Authelia Webanwendungen ohne Programmieren mit zweitem Faktor sichern, haben wir bereits beschrieben [2].

Wenn Sie die Funktion selbst integrieren wollen, fangen Sie nicht bei null an – bei kryptografischen Funktionen sollte man immer auf erprobte und von einer großen Gemeinschaft geprüfte Bibliotheken setzen. TOTP- und Webauthn-Bibliotheken gibt es in vielen Programmiersprachen.

Machen Sie beim Design des Backends nicht den Fehler, nur einen zweiten Faktor pro Benutzer zu erlauben. In einer relationalen Datenbank sollte es eine eigene Tabelle mit einem Eintrag pro eingerichtetem Gerät geben. Im Frontend sollte es eine übersichtliche Einstellungsseite geben, in der man alte Faktoren auch löschen kann. Nur dann kann der Nutzer eine für ihn geeignete Backupstrategie umsetzen. Am besten gibt man ihm auch die Möglichkeit, jedem Gerät einen Namen zu geben.

Um Supportanfragen bei verlorenen Geräten zu reduzieren, erinnern Sie Nutzer, die nur eine Methode zur Zwei-Faktor-Authentifizierung eingerichtet haben, regelmäßig daran, dass das nicht unbedingt geschickt ist. (jam) c't

Literatur

[1] Jan Mahn, **Anmelde-Baukasten**, Logins für Websites mit Web-Authn, c't 18/2019, S. 26

[2] Niklas Dierking, **Geschlossene Gesellschaft**, Webanwendungen schützen mit Authelia, c't 21/2021, S. 140

IIoT Conference

Die Heise-Konferenz für Industrial IoT in Kooperation mit der automatica

23. Juni 2022 · Messe München

Jetzt Tickets sichern!

Brücke zwischen Automatisierung und Softwareentwicklung

- W3C-Standard Web of Things
- Open Source im IIoT
- Deep Dive MQTT 5
- Digitaler Zwilling
- Robot Operating System (ROS)

www.iiot-conference.de

Zusätzlicher Workshop am 22. Juni zu MQTT 5

Veranstalter

iX Magazin für professionelle Informationstechnik · heise Developer · dpunkt.verlag

Datenlöcher bei Android stopfen

Smartphones plappern fortwährend mit dem Hersteller und mit Google, Werbetreibende destillieren aus dem Benutzerverhalten ein Persönlichkeitsprofil, Apps kratzen alle auffindbaren Informationen zusammen. Manche dieser Datenabflüsse nerven nur, aber hinter anderen drohen Sicherheitsrisiken. Wir zeigen, wohin die Daten fließen und welche Maßnahmen Ihnen zu mehr Privatsphäre verhelfen.

Von **Jörg Wirtgen**



Bild: Rudolf A. Blaha

Datenlöcher bei Android stopfen	72
Android und Apps datensparsam nutzen	78
Custom-ROMs für Android im Vergleich	86
Android-Apps selbst auf Tracker prüfen	94

Es bleibt im Dunkeln, was mit den ganzen Daten passiert, die von den Smartphones an die Gerätehersteller, die App-Entwickler, die Werbenetzwerke und Google ausposaunt werden – selbst wenn man die hundert Seiten Datenschutzinformationen wirklich lesen würde, falls sie denn vorhanden sind und stimmen. Können chinesische oder US-Firmen ihre Server wirklich nach DSGVO abgesichert in der EU betreiben oder müssen sie ihren Behörden Zugriff gewähren? Wissen die Werbenetzwerke nur, dass ich ein männlicher Europäer mit seltsamem Musikgeschmack bin, oder rühren sie weitere Interessen, politische Ansichten oder finanzielle Möglichkeiten hinein? Fließt etwas davon in die mir angezeigten Angebote der Preissuchmaschinen ein? Verkaufen solche Datensammler nur an Werbetreibende oder kumulieren sich gefährlichere Angreifer daraus etwas zusammen? Welche hinterlistigen Schlüsse könnten aus für Entwickler sogar nützlichen Debug-Logs gezogen werden?

Manche dieser Risiken mag man aktuell für harmlos halten, auch weil man glaubt, nichts verbergen zu müssen. Doch die Datenoffenheit schadet indirekt denen, die eine andere Einstellung zur Privatsphäre haben, indem sie einem gesellschaftlichen Veröffentlichungsdruck zumindest nicht widerspricht. Zudem passieren schon bei weit harmloseren Auswertungen unzählige Fehler: Möglicherweise wird man selbst mit etwas in Verbindung gebracht, was andere nicht privat gehalten haben. Und nicht zuletzt zeigt die aktuelle krisengebeutelte Zeit brutal, wie schnell manche Gewissheit kippt. Die wirksamste Antwort auf diese Probleme bleibt, solche kritischen Daten gar nicht erst in die Welt zu funken.

In diesem Artikel erklären wir, wo Android Daten abfließen lässt und was dagegen hilft. Grob gibt es drei Maßnahmen: Erstens durchforsten Sie Ihr Smartphone nach Einstellmöglichkeiten bezüglich Privacy. Zweitens ersetzen Sie vorinstallierte Apps durch andere und ergänzen spezielle Software etwa zum Blockieren von Werbetrackern. Der Artikel ab Seite 78 erklärt diese beiden Wege.

Der dritte Weg ist steiniger: Sie spielen eine alternative Android-Distribution auf Ihr Smartphone, auch Custom-ROM genannt. Im Artikel ab Seite 86 zeigen wir, wie Sie ein passendes Custom-ROM finden, installieren und in der Praxis nutzen. Idealerweise treffen Sie die Entscheidung für ein Custom-ROM schon vor dem Smartphone-Kauf, denn ein gewünschtes Custom-ROM lässt sich auf einige Modelle innerhalb weniger Minuten aufspielen, auf andere nur mit erheblichem Aufwand – und auf die meisten gar nicht. Als weitere Alternative verkaufen einige Custom-ROM-Anbieter inzwischen Smartphones mit vorinstalliertem Custom-ROM.

Hochfahr-Vergleich

Als Erstes haben wir untersucht, welche Daten ein Smartphone schon beim Hochfahren ausposaunt. Dazu haben wir ein Samsung S10 und ein Xiaomi Mi 10T jeweils im Auslieferungszustand untersucht sowie Smartphones mit den im Artikel ab Seite 86 getesteten Custom-ROMs (Calyx, Graphene, /e/, iodé, Lineage und Volla).

Das Samsung S10 transferierte bei jedem Booten um 2 MByte in weit über 100 Verbindungen und rief dabei nie benutzte Apps auf wie Spotify und Facebook. Ähnlich verhielt sich das Xiaomi. Zum Vergleich: Selbst das geschwätzigste Custom-ROM (Calyx) baute nur 20 Verbindungen auf und transferierte knappe 60 KByte.

Ein Großteil der Daten geht auf Google-Dienste zurück. Die anderen Apps kontaktieren hauptsächlich eigene Server oder Cloud-Dienstleister etwa für Diagnosedaten, Updates und Ähnliches – genauer hineinschauen kann man in die Kommunikation nicht, da sie größtenteils verschlüsselt abläuft. Insgesamt handelt es sich also nicht um böswillige Datenabflüsse, sondern um schlimmstenfalls überflüssige, aber oft halbwegs nützliche Verbindungen – sofern man denn die Apps und Dienste nutzen mag. Genau diese Wahl, Unerwünschtes abzuschalten, lassen einem die Gerätehersteller und Google allerdings nicht.

Kontenpflege

Am hungrigsten knurrt offenbar Googles Datenmagen. Ohne den Account läuft so gut wie nichts, am liebsten hätte Google einen Standortverlauf, die komplette Browserhistorie aller verknüpften Geräte, alle Kontakte, Termine, Aufgaben, Dateien und Fotos, und kaufen soll man dann auch noch per Google Pay.

Einiges davon können Sie einfach abschalten – mehr dazu ab Seite 78 – oder Sie nutzen es einfach nicht. Suchen Sie sich für Mails, Kalender und Adressbuch andere Dienste [1], speichern Sie Fotos [2] und Daten [3] in anderen Clouds. Zahlen Sie per Smartwatch [4] oder klassisch per Karte oder Bargeld. Ihrem Google-Konto fügen Sie so wenige persönliche Daten wie nötig hinzu.

Ähnlich sieht es bei den Konten aus, zu denen viele Gerätehersteller Sie drängeln: Wenn Sie nicht



Den DNS-Server kann man schon beim Standard-Android auf einen der öffentlichen Server mit eingebautem AdBlocker umstellen. Einige Custom-ROMs vereinfachen das.



Die Firewall Blokada zeigt an, welche Verbindungen zu Tracker-Servern sie abgeblockt hat.

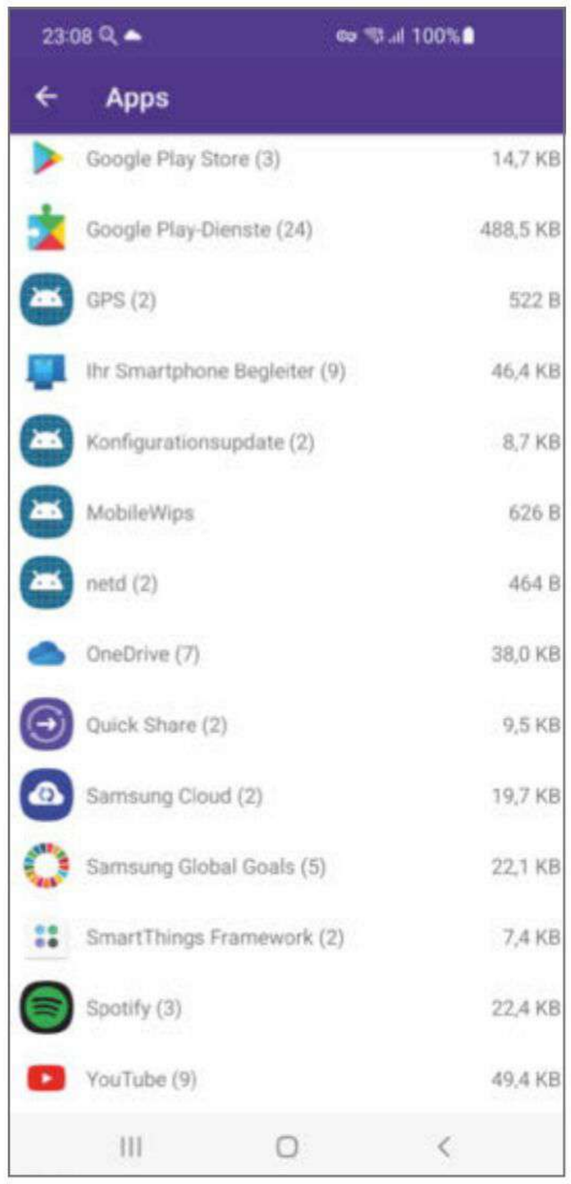
darauf eingehen, rücken die meisten Hersteller keine Updates der eigenen Apps heraus – unverschämt. Richten Sie also sinnvollerweise ein Konto mit möglichst wenigen oder Fantasiedaten ein. Gehen Sie sorgfältig alle Einstellungen durch und schalten Sie so viel wie möglich ab.

Ein schöner Nebeneffekt: Sie binden sich weniger an Google und einen bestimmten Hersteller. Umso leichter fällt dann der Wechsel zu einem anderen Hersteller oder auch mal zu einem iPhone.

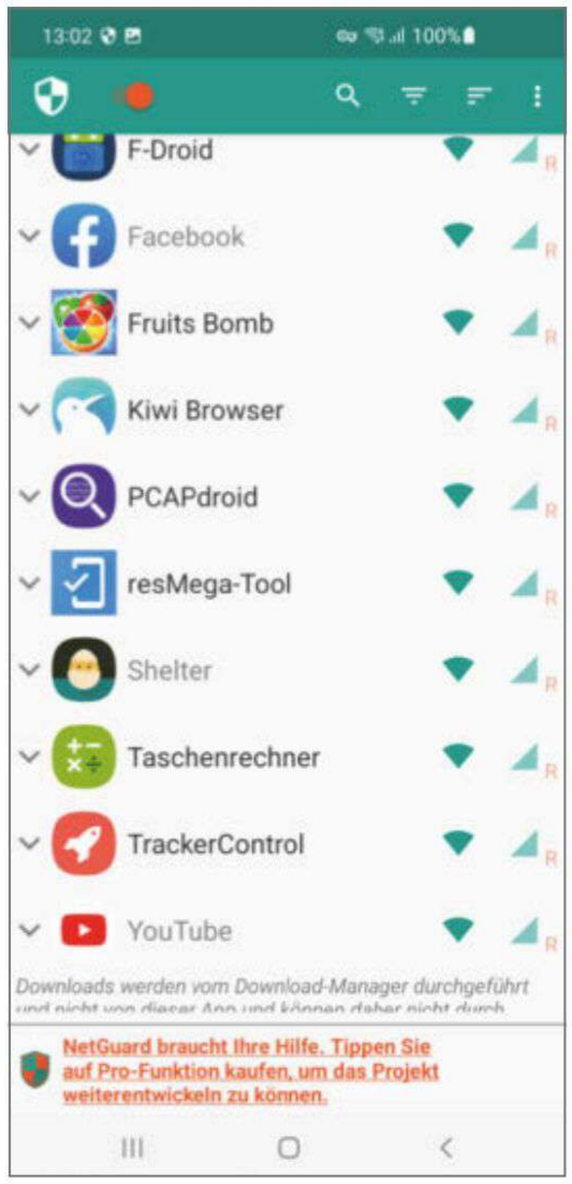
Nutzlose Apps

Wollen Sie ungenutzte Apps deinstallieren, stoßen Sie auf ein Problem: Das klappt lange nicht bei allen vorinstallierten Apps. Ärgerlich daran ist nicht nur, dass zumindest ihre Updates Platz fressen, sondern dass einige von ihnen bei jedem Hochfahren starten, auch wenn man kein App-Konto hinterlegt hat. Allzu brisante Daten können sie dann eigentlich nicht sammeln, aber ein ungutes Gefühl bleibt. Samsung-Handys beispielsweise lassen Facebook, Spotify und YouTube ans Ruder, ohne dass man diese Apps jemals aufgerufen hätte. Einiges lässt sich deinstallieren (bei Samsung beispielsweise Spotify, aber nicht Facebook oder OneDrive). Falls nicht, sollten Sie die App deaktivieren, sie sollte dann beim Gerätestart nicht mehr aufgerufen werden. Selbst das Deaktivieren erlauben die Gerätehersteller aber nicht bei jeder App – ein Unding. Löschen Sie dann wenigstens in den App-Einstellungen alle Daten. Die bei einigen Apps angebotene Option, die Updates zu löschen, spart zwar auf den ersten Blick ein paar Megabyte, doch bei nächster Gelegenheit ziehen sich die Store-Apps das Update wieder herunter.

Ein weiterer Trick, um unerwünschte Apps loszuwerden, soll nicht unerwähnt bleiben: Im Entwicklermodus per Android Debug Bridge (adb) von einem



Samsung-Smartphones laden Dutzende Apps beim Booten, auch wenn man sie gar nicht nutzt und keine Konten hinterlegt hat.



Die Firewall NetGuard kann Apps das Internet abdrehen – getrennt nach WLAN, Mobilfunk und Roaming.

PC aus können Sie auch System-Apps deinstallieren. Achtung: Sie zerschießen sich damit leicht Ihr System – Details und wichtige Vorsichtsmaßnahmen dazu in [5]. Der durch die Deinstallation freigeschaufelte Platz liegt übrigens auf einer Systempartition und ist nicht etwa für neue Apps nutzbar.

Näher gehen wir in diesem Artikel nicht auf diese Methode ein, weil sie zumindest in unserem Testfeld wenig brachte. Tatsächlich zerstörte schon der erste Versuch (com.xiaomi.finddevice und com.xiaomi.payment) das System und erforderte einen zeitfressenden Recovery-Vorgang samt kompletter Neuinstallation.

Boot-Diät

Nach dem manuellen Deinstallieren und Deaktivieren aller Apps transferierte das Samsung S10 beim Booten immerhin nur noch um 1,5 MByte in 60 Verbindungen. Einige ungenutzte Dienste wie „Ihr Smartphone-Begleiter“, „Quick Share“ und das „SmartThings Framework“ waren weiter dabei. Beim Xiaomi-Smartphone führte unsere Diät zu rund 850 KByte in 90 Verbindungen; auch starteten einige Apps trotz ausgeschalteter Synchronisation.

Um einen gewissen Datenaustausch mit Google kommt man nicht herum, wenn man den Play Store samt Infrastruktur nutzen will. Letztlich bekommt man die Datenflüsse an Google und den Gerätehersteller nur durch ein Custom-ROM ausgetrocknet – siehe Seite 86.

Doch selbst einige Custom-ROMs kontaktieren noch Google: als Uhrzeit-Server (NTP), als Connection-Test und als Default-DNS, falls kein anderer zu ermitteln ist. Wer gar keine Spuren bei Google hinterlassen möchte, muss darauf achten, dass das Custom-ROM diese Google-Verweise umbaut (siehe Tabelle auf Seite 93); einige aktualisieren ihre Uhr

beispielsweise über pool.ntp.org. Die Graphene-Entwickler wiederum erklären, explizit keinen anderen Default-DNS zu nutzen, weil darüber ein Fingerprinting von anderer Stelle her möglich wäre – wichtig, falls man dem lokalen Netz oder Provider noch weniger vertrauen möchte als Google oder den trackenden Apps.

Werbung und Tracker

Die nächste Datensenke sind Werbebanner und Tracker auf Webseiten und in Apps. Werbung möchten die meisten Nutzer nicht angezeigt bekommen und den (Mobilfunk-)Traffic sparen, selbst wenn sie dem einen oder anderen Anbieter vielleicht sogar die Werbeeinnahmen gönnen. Noch kritischer sind Techniken für Native Advertising und Werbeprofile.

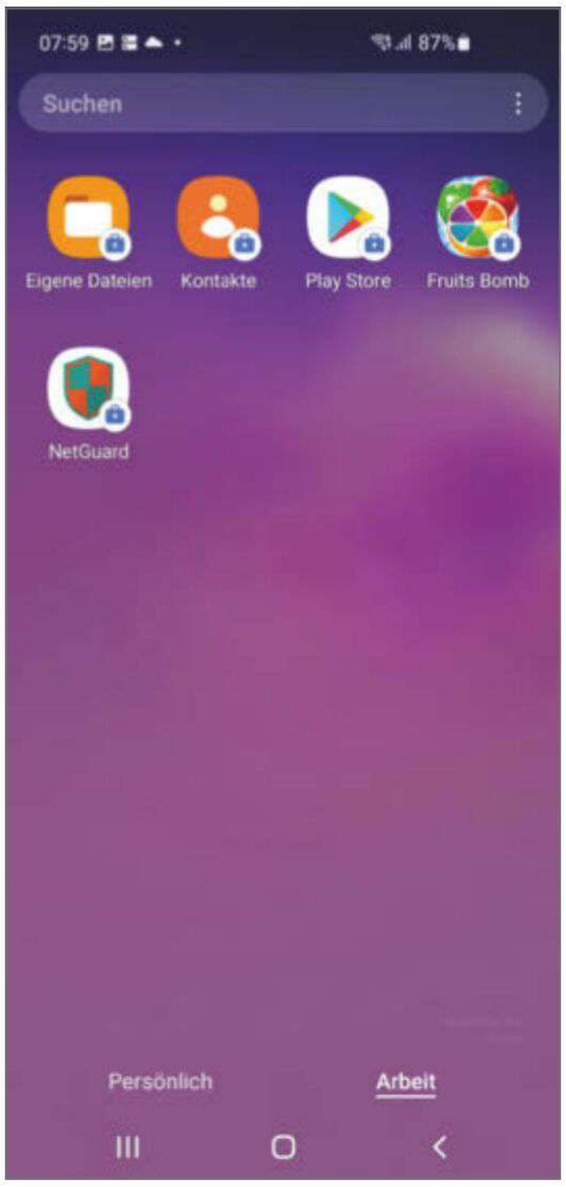
Trifft ein Browser keine weiteren Vorkehrungen und scrollt man eine typische News-Seite bis zum Ende, haben wir 200 bis 400 Internetverbindungen gezählt – nicht nur wie zu erwarten beim Samsung- und Xiaomi-Smartphone, sondern auch bei den drei Custom-ROMs Lineage, Volla und Graphene. Hingegen kommen die drei anderen Custom-ROMs Calyx, /e/ und iodé mit ein paar Dutzend bis knapp 100 Verbindungen hin: Das sind nicht entdeckte Tracker, aber vor allem weiterer Nutzwert der Seite, beispielsweise die nachgeladenen Bilder, die ein Browser erst anfordert, wenn man sie ins Display scrollt.

Um auf einen hohen Schutzlevel zu kommen, brauchen Sie kein Custom-ROM: Mit einem datenschutzfreundlichen Browser oder entsprechenden Einstellungen erreichen Samsung und Xiaomi denselben Datenschutz – Tipps dazu im folgenden Artikel. Bei Xiaomi war sogar der hauseigene „Mi Browser“ praktisch genauso sparsam, wenn man den eingebauten Werbeblocker in dessen Einstellungen aktiviert.

Die Browser der Custom-ROMs Graphene (Vanadium), Lineage und Volla (Fennec) erfordern hingegen Nacharbeit. Fennec beispielsweise: Ergänzt man bei diesem für jedes Android-Gerät erhältlichen Browser wie im folgenden Artikel beschrieben die Add-ons NoScript und uBlock Origin, ist er datensparsamer als alle Custom-ROMs im Test.

Apps bändigen

Werbung und Tracker in Apps lassen sich hingegen nicht so einfach unterbinden. Ein Standard-Android hat dem nichts entgegenzusetzen, außer dass man statt dem vom WLAN oder Mobilfunkprovider zugewiesenen DNS einen Blocker-DNS wie dnsforge.de oder dns.adguard.com fest einträgt. Dann filtert der DNS, nicht das Smartphone.



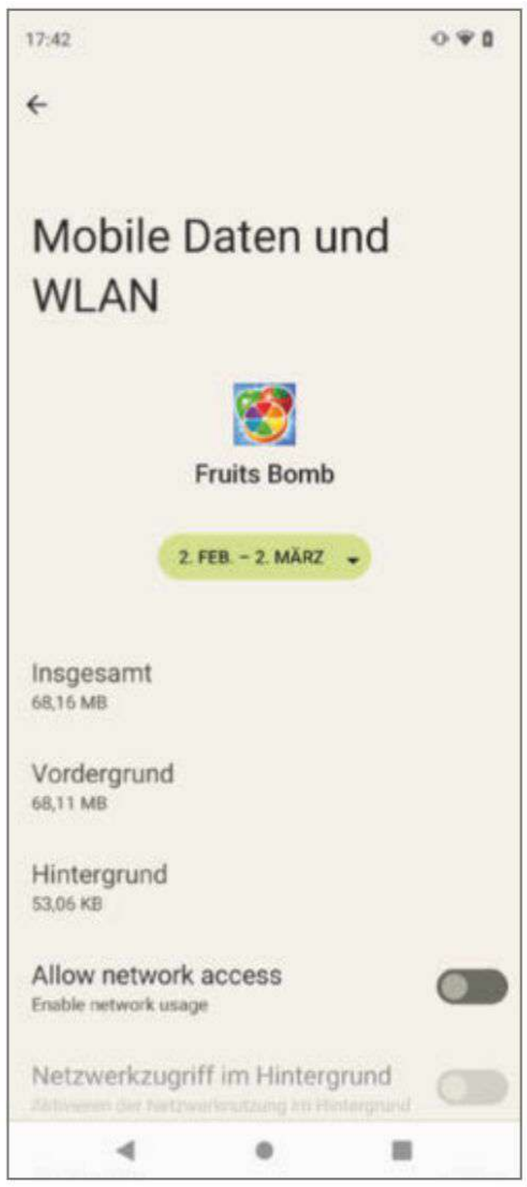
Shelter und Island legen einen Arbeitsbereich an. Die Apps findet man dann in einem separaten Bereich der App-Übersicht, hier bei Samsung beispielsweise unten umzuschalten, bei Xiaomi oben.

Die Alternative sind lokale Adblocker, beispielsweise Blokada (siehe der folgende Artikel). Sie geben sich Android gegenüber als VPN aus. Ihre größten Nachteile sind, dass sie ein wenig CPU-Last erzeugen, also die Laufzeit geringfügig verringern. Und dass man sie nicht zusammen mit einem echten VPN oder WireGuard nutzen kann. Das Custom-ROM iodé springt mit einem ins System integrierten Adblocker in diese Bresche.

Wir haben die drei Methoden auf ein tracker- und werbeintensives Spiel losgelassen: Auf unvorbereiteten Systemen lud es beim Start je nach Displayauflösung 8 bis 25 MByte Daten herunter und baute 150 bis 220 Verbindungen auf. Das iodé-Smartphone und die per Blokada oder Adblocker-DNS geschützten Systeme kriegen es gezähmt auf unter 100 KByte und rund ein Dutzend Verbindungen. Die Methoden wirken also im Großen und Ganzen gleich gut.

Auf den ersten Blick machen diese Blocker die oben beschriebenen datensparsamen Browser über-

Android selbst kann einer App das Internet nicht abdrehen. Dazu benötigt man ein Custom-ROM (dann geht das in den App-Einstellungen) oder eine Firewall-App.



flüssig, da sie Tracker und Werbung ebenfalls aus dem Browserverkehr ausfiltern. Doch die Datensparsamkeit des Browsers umfasst weitere Aspekte, etwa im Umgang mit Cookies, bleibt also wichtig.

Apps einsperren

Mancher App mag man lieber die Verbindung zum Internet komplett sperren, statt einzelne Verbindungen zu blockieren. Das beherrscht Android nicht, obwohl eine Berechtigung „Internet“ vorhanden ist. Auch die Adblocker können keine Apps einsperren. Abhilfe schafft beispielsweise die Firewall NetGuard, sie kann einzelnen Apps das Internet abdrehen. Auch die meisten Custom-ROMs haben diese Möglichkeit.

All das geht einen weiteren Datenabfluss nicht an: Gewährt man einer App Zugriff auf Dateien, Adressbuch und Terminkalender, weiß man nicht, was sie damit anstellt. Ärgerlich vor allem, wenn man die App benötigt und sie ohne diese Berechtigungen nicht vernünftig läuft.

Eine Abhilfe sind die Tools Island und Shelter, die im Play Store und bei F-Droid (dort der Island-Fork Insular) erhältlich sind. Sie öffnen das „Arbeitsprofil“ von Android auch auf Geräten ohne die eigentlich dafür nötige Firmen-Infrastruktur. Das Arbeitsprofil ist eine Art zweite Umgebung mit eigenem Dateisystem, Kalender, Adressbuch – mehr dazu im folgenden Artikel.

Zum Schluss sei noch eine weitere Methode erwähnt, die Datenhoheit wiederzugewinnen: das Rooten des Smartphones. Dabei bleibt das Hersteller-ROM erhalten, man verschafft sich aber Vollzugriff, üblicherweise durch eine Sicherheitslücke. Danach können Sie systemnahe Tools installieren, darunter Tracker- und Werbeblockierer, die ohne den VPN-Trick auskommen, ähnlich dem in iodé eingebauten; beispielsweise AdAway. Als weiteren Vorteil behalten Sie die paar wichtigen Hersteller-Apps, allen voran die Kamera. Sie erkaufen sich das allerdings mit einer größeren Verantwortung für die Systemsicherheit und einer ähnlich komplizierten und Garantie verwirkenden Installation wie beim Custom-ROM. Zudem funktionieren nicht alle Apps, vor allem Banking-Apps misstrauen gerooteten Handys. Mehr dazu finden Sie auf dem Blog des Sicherheitsexperten Mike Kuketz (siehe ct.de/wwag).

Fazit

Es muss nicht direkt ein Custom-ROM sein: Gegen Browser-Tracking helfen datensparsame Browser, gegen zu geschwätzige Apps Tools wie Blokada und NetGuard, und Ihre Daten transferieren Sie in eine andere als die Google-Cloud.

Custom-ROMs benötigt man vor allem, um sich vom Tracking-Hunger Googles und des Geräteherstellers zu befreien. Zudem können die meisten einzelne Apps komplett vom Netzzugriff abschotten, ohne den VPN-Trick zu bemühen. Darüber hinaus hat iodé einen eingebauten Adblocker, und Graphene ist stärker gehärtet gegenüber böswilligen Apps, die Bugs im Betriebssystem suchen.

Die Island/Shelter-Methode wiederum benötigen Sie sowieso, um besonders verdächtige Apps einzusperren oder um Ihre Adressen, Termine und Dateien vor solchen Apps zu schützen.

Auch über Werbe- und Tracker-Blocker müssen Sie sowohl mit Custom- als auch mit Hersteller-ROM nachdenken. Ob man lieber per App lokal blockt oder durch einen öffentlichen DNS-Server, ist eine komplexe Entscheidung. Letzterer ist schnell eingerichtet und spart lokale Ressourcen, aber nur wenige erlauben individuelle Einstellungen; zudem muss man dem Serverbetreiber trauen. (jow) c't

Literatur

[1] Jörg Wirtgen, **Die Cloudchenfrage**, Apps und Dienste für Mail, Kalender, Kontakte, Aufgaben und Notizen ohne Google, c't 4/2017, S. 82

[2] André Kramer, **Teile und herrsche**, Fotoclouddienste für Android und iOS, c't 21/2021, S. 98

[3] Robin Brand, Michael Link, Stefan Porteck, **Passend gemacht**, Alternativen für Google-Apps und -Dienste, c't 7/2020, S. 22

[4] Stefan Porteck, Jörg Wirtgen, **Gute Karten**, Drahtloses Bezahlen mit Handys und Uhren, c't 9/2021, S. 58

[5] Ronald Eikenberg, **Schlanker Roboter**, Android-Smartphones ohne Rooten von vorinstallierten Apps befreien, c't 26/2018, S. 144

Mehr zu Raspi, Wireshark und Rooten

ct.de/wwag



Bild: Rudolf A. Blaha

Android und Apps datensparsam nutzen

Einerseits erheben Android-Handys unzählige Daten und übertragen sie an Hersteller sowie Werbenetzwerke. Andererseits bieten sie auch viele Optionen, um den Datenstrom einzudämmen. Wenn die nicht reichen, helfen wichtige Tools zum Datensparen aus dem Google Play Store weiter.

Von **Stefan Porteck und Jörg Wirtgen**

Auf modernen Smartphones fließen Daten über unterschiedliche Wege zu verschiedenen Unternehmen ab – und leider in größerem Maß, als man glauben würde. Zum einen überträgt Android Telemetrie- und Nutzungsdaten an Google. Einiges davon dient der Bereitstellung personalisierter Werbung, anderes der Produktverbesserung, und mancher Transfer ist zwingend nötig, damit einzelne Google-Dienste überhaupt funktionieren.

Zum anderen erheben Apps Daten ihrer Nutzer. Einiges hilft den App-Entwicklern bei der Produktver-

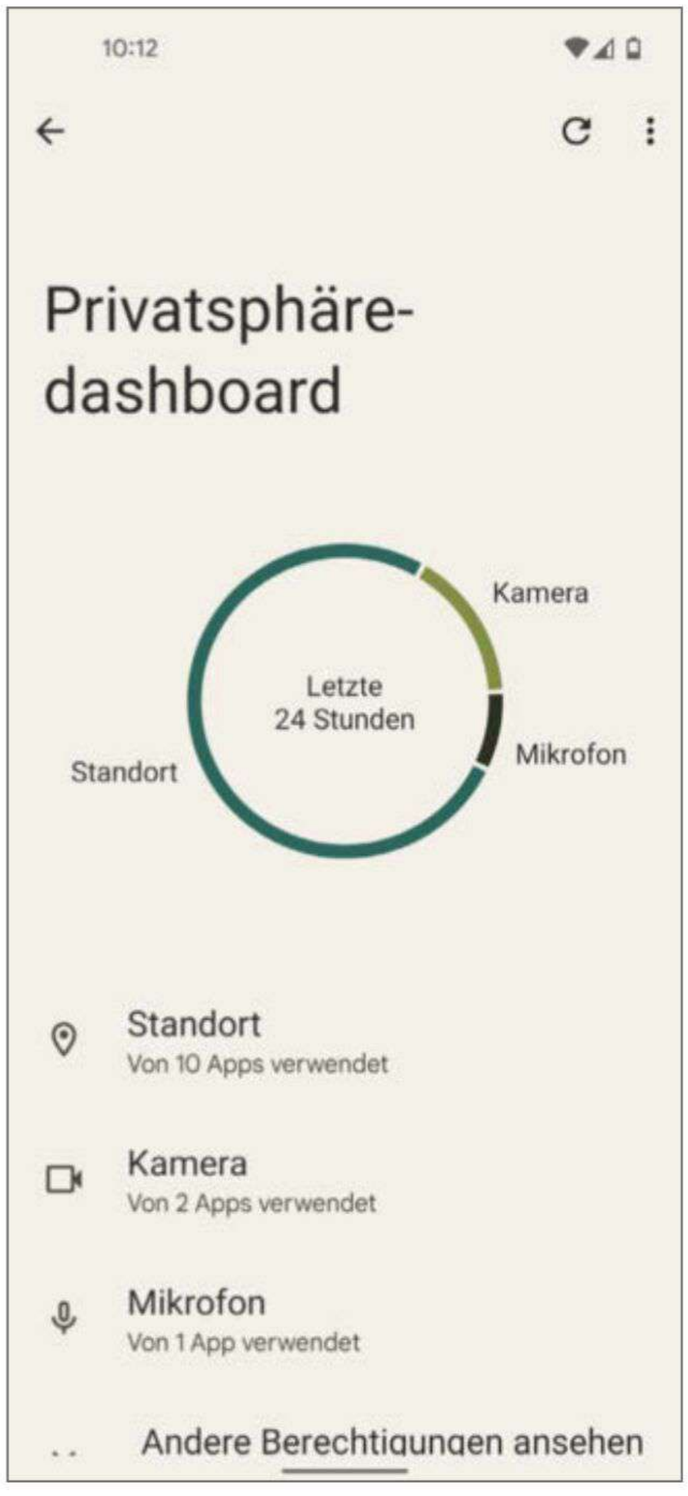
besserung, etwa der Google-Tracker Firebase Crashlytics, der Absturzberichte versendet. Die meisten kostenlosen und werbefinanzierten Apps haben Tracker, die Nutzungsdaten an Werbedienstleister schicken. Diese Netzwerke verknüpfen die Daten mehrerer Apps zu einem Nutzerprofil mit dem Zweck, auf einzelne Zielgruppen optimierte, personalisierte Werbung auszuspielen. In welchem Umfang die Daten abfließen, wo die potenziellen Gefahren liegen und welche Schutzmechanismen generell helfen, beschreibt der vorige Artikel ab Seite 72.

Im Folgenden zeigen wir, wie Sie Ihr Smartphone mit Einstellungen in Apps und Betriebssystem möglichst datensparsam benutzen. Da man den Apps nicht ansieht, welche Tracker sie mitbringen und was diese versenden, stellen wir zu den vielen vorinstallierten Apps Alternativen mit weniger Trackern vor. Zudem erklären wir, wie Sie Tracker erkennen und mit welchen Tools aus dem Play Store Sie sie zum Schweigen bringen. Puristen wird das nicht reichen, sie schwören darauf, ihr Smartphone mit einem Custom-ROM im Idealfall komplett frei von Google- und Hersteller-Apps zu halten – mehr dazu im folgenden Artikel ab Seite 86.

Andere Apps, gleiche Funktionen

Ein guter Anfang beim Datensparen ist die Google-Such-App, die sich als Suchleiste auf dem Homescreen des Handys breit macht: Google erfährt darüber, was Sie suchen, und speichert das in Ihrem Suchverlauf in der Cloud. Wenn Sie darüber Apps starten, erfährt Google sogar davon. Eine gute Alternative ist die in der Testversion kostenlose App Sesame Search: Sie durchsucht das Telefon nach Apps, Audio- und Videodateien, Bildern und Kontakten. Darüber hinaus gibt sie Suchanfragen auch an andere Apps weiter. So kann man etwa einen Suchbegriff an den Browser übergeben, der die Websuche beispielsweise mit DuckDuckGo ausführt, in Spotify direkt nach Songs und Interpreten durchforsten, die Suchanfrage in einen App-Store schicken oder nach Chats in Signal oder WhatsApp fahnden. Wer mit Sesame Search warm geworden ist, wird nach dem Ende der 14-tägigen Probezeit kaum zögern, die paar Euro für die Vollversion ohne Nag-Screens auszugeben – auch weil die Suche so gut funktioniert, wie man sich das eigentlich von der Google-Suche wünschen würde.

Auf den meisten Android-Smartphones ist die Softwaretastatur GBoard voreingestellt. Auch sie erhebt Nutzerdaten – wenn auch zum eigentlich gewünschten Zweck, passende Vorschläge fürs nächste Wort zu präsentieren. Die vielleicht sogar bessere Alternative kommt von einem anderen Softwareriesen: Microsofts kostenlose Tastatur Swiftkey bietet eine sehr gute Rechtschreibkorrektur, erlaubt die Texteingabe mittels Tippen und Wischen, hat eine eigene Zwischenablage mit mehreren Speicherplätzen und unterstützt Themes und die nicht nur fürs Chatten gängigen Spielereien wie Sticker, GIFs und Emojis. Wer Microsoft ein paar Daten anvertrauen mag, meldet sich mit seinem MS-Konto an, um Einstellungen und persönliche Wörterbücher auf



In jeder Version lernt Android ein paar neue Funktionen zur Privatsphäre. Sie sind aber teils in den Einstellungen verteilt und lange nicht ausreichend.

mehreren Geräten zu synchronisieren. Doch selbst bei abgeschalteter Synchronisation sammelt Microsoft Telemetriedaten; datensparsamer arbeiten beispielsweise die Tastatur-Apps Open Board oder AnySoftKeyboard.

Ein weiterer großer Datenquell ist der Google-Kalender. Gerade dort zeigt sich das Abwägen zwischen Komfort und Datenschutz sehr deutlich: Klar ist es praktisch, wenn das Smart Display oder die Wear-OS-Smartwatch anhand der aktuellen Verkehrslage rechtzeitig daran erinnert, dass man so langsam zum Arzttermin aufbrechen sollte – im Gegenzug weiß Google dann aber auch von der Darmspiegelung oder anderen Wehwehchen …

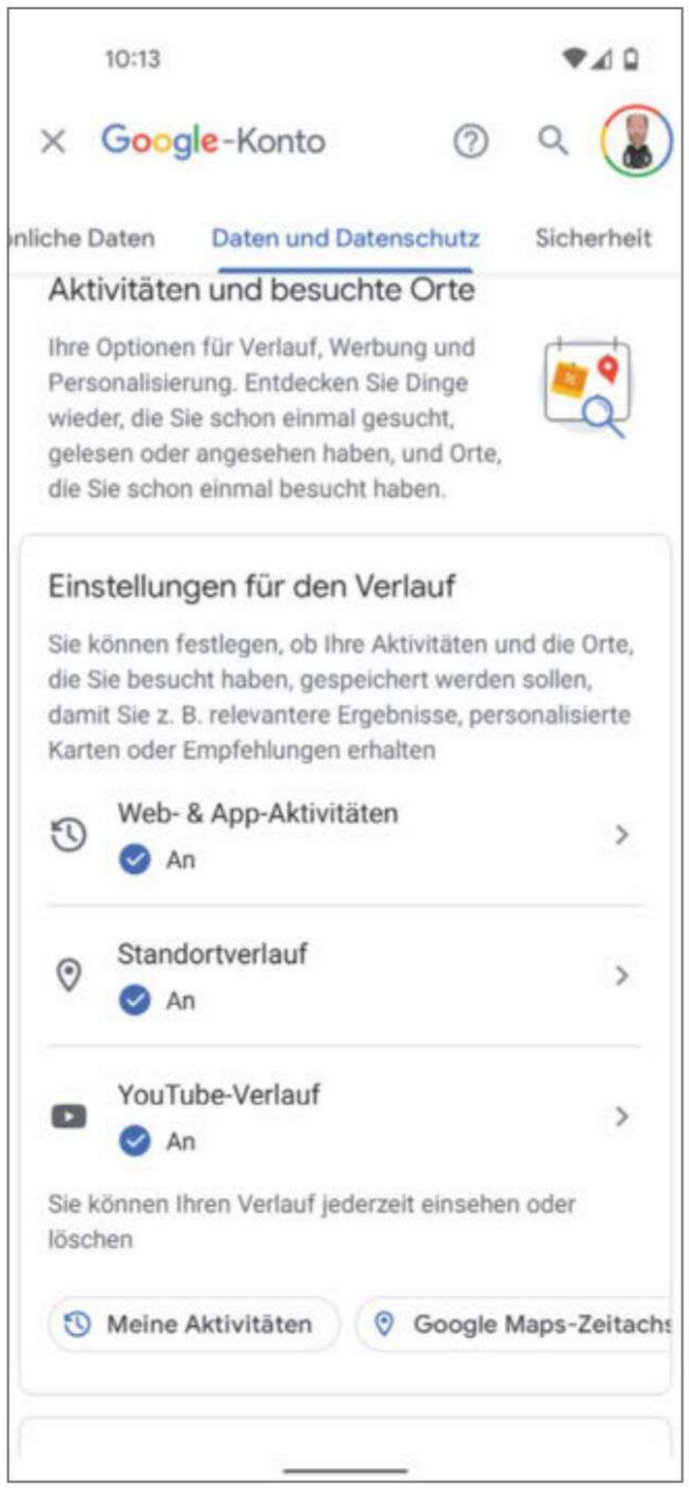
Besser speichert man seine Termine also bei einem anderen Dienst. Eingebaut ist die Synchronisation mit Exchange-Konten und kompatiblen Diensten. NextCloud-Kalender erfordern das CalDAV/CardDAV-Protokoll, was CalDAV-Sync (kostenlos) und DAVx5 (5 Euro im Play Store, kostenlos bei F-Droid) nachrüsten – der ehemalige Geheimtipp von Blackberry ist mittlerweile aus den Stores verschwunden. Die so über andere Clouds synchronisierten Termine zeigt die Google-App anstandslos an und es gibt keine Hinweise, dass sie etwas davon an Google sendet.

Wer ihr trotzdem nicht traut, findet zahlreiche alternative Kalender-Apps, teils sogar mit größerem Funktionsumfang und besserer Bedienung. Darf die App ein paar Euro kosten, lohnt sich ein Blick auf aCalendar+: Sie legt auf Wunsch lokale Kalender an, die das Smartphone nicht verlassen, erinnert an Geburtstage der Kontakte und bindet Wochennummern, Feiertage und Ferien ein. Abgerundet wird das Ganze von praktischen Widgets für den Homescreen und umfangreichen Konfigurationsmöglichkeiten.

Anders browsen

Die vielleicht größte Datenquelle für Google ist der vorinstallierte Chrome-Browser. Er überträgt jede Eingabe in der Adressleiste und jede besuchte Webseite zu Google, wenn man das nicht abstellt. Man kann Google dabei nicht nur Eigennutz unterstellen, die Daten werden auch zum Wohle der Nutzer erhoben: etwa um vor Phishing oder Webseiten mit Viren und Trojanern zu schützen. Das Synchronisieren des Verlaufs bewirkt, dass man eine vom Handy angesurfte Webseite am Desktop-PC wiederfindet. Auch wenn einige Daten nur verschlüsselt und für Google selbst nicht einsehbar im eigenen Account gespeichert werden, erzeugt der Datenhunger bei etlichen Nutzern ein mulmiges Gefühl.

Die Lösung ist leicht: Statt Chrome installiert man einen datensparsamen Browser. Dazu gehören der freie Browser Firefox oder besser gleich den nicht bei Google Play, aber im F-Droid-Store erhältlichen Fork namens Fennec. Letzterer wird aus dem gleichen Open-Source-Code kompiliert, vorher aber von einigen Trackern befreit, die Telemetriedaten an Mozilla senden. Vom Funktionsumfang unterscheiden sich Fennec und Firefox nicht. Sogar das Anmelden mit einem Mozilla-Account funktioniert einwandfrei, sodass man (ebenfalls verschlüsselt) Passwörter, Verlauf, Bookmarks und offene Tabs über verschie-



Auch die Privatsphären-Einstellungen des eigenen Google-Kontos sollte man sich genau anschauen, vor allem bezüglich des Suchverlaufs und der Standortermittlung.

dene Geräte synchronisieren kann. Beide lassen sich aber auch vollständig anonym nutzen.

Eine Alternative ist der auf Chromium aufbauende Browser Kiwi. Firefox, Fennec und Kiwi unterstützen anders als der Android-Chrome die Installation von Add-ons. Reichert man die drei beispielsweise mit uBlock, NoScript und Privacy Badger an, schützen sie vor Malware und blockieren viele Trackingdienste und Werbenetzwerke der aufgerufenen Webseiten. Wer es schlanker möchte, installiert den Browser DuckDuckGo, der auf Android WebView aufbaut, einen guten integrierten Trackerschutz hat, aber wenige Einstellmöglichkeiten bietet.

Mit diesen einfachen Änderungen hinterlässt man schon deutlich weniger Datenspuren. Theoretisch ließe sich die Liste der Alternativen nahezu beliebig weiter verlängern. Doch die Umstiege etwa von Twitter auf Mastodon, von Google Maps zu Open Street Map oder von Drive zu Nextcloud erfordern mehr Aufwand, als nur eine neue App zu installieren.

Zentrale Anlaufstellen

Einen großen Einfluss auf die eigene Datenspur hat auch die Art, wie man die Apps nutzt. Android bietet seit Version 11 einige praktische Funktionen, wie man die Freizügigkeit von Apps und auch des Betriebssystems selbst einschränkt.

Wichtige Optionen finden Sie in den Android-Einstellungen unter „Google-Konto“ und dort unter „Daten und Datenschutz“. Im darauf geöffneten Dialog schalten Sie den Verlauf für „Web & App-Aktivitäten“ sowie für den Standort und für YouTube ab. Der bisherige Verlauf lässt sich dort ebenfalls von den Google-Servern entfernen. Weiter unten legen Sie fest, ob ein Werbeprofil für Sie angelegt werden soll. Darunter findet sich der Schalter, der die Anzeige persönliche Daten anderer Google-Dienste in der Google-Suche erlaubt, wofür unter anderem Informationen aus Maps verknüpft werden.

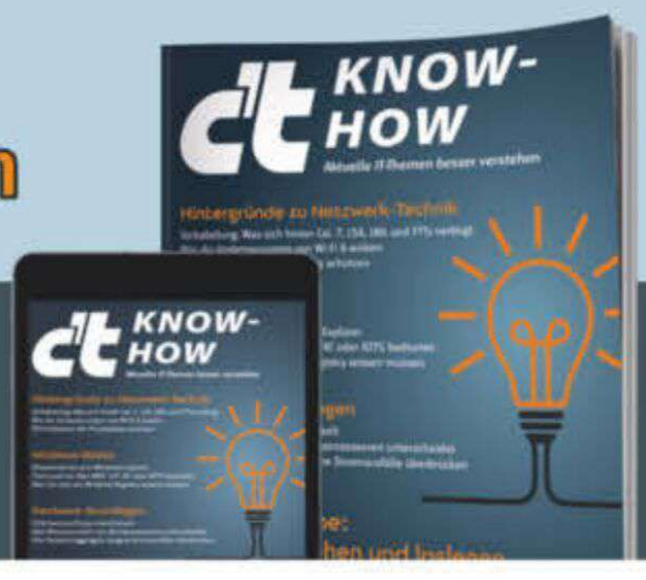
Etwas weiter unten finden Sie die Einstellungen, welche weiteren Anbieter Zugriff auf Ihr Konto haben, beispielsweise Fitness-Dienste wie Strava, die auf Google Fit zugreifen. Wenn man viele Apps ausprobiert, sammelt sich dort über die Zeit einiges an. Es lohnt sich, regelmäßig auszumisten.

Nachdem Sie so die wichtigsten Löcher von Android gestopft haben, sollten Sie sich um einzelne Apps kümmern. Dazu bieten aktuelle Android-Versionen mittlerweile viele Bordmittel. Eines davon ist das Privacy-Center, das man in den Systemeinstellungen unter „Datenschutz“ und „Privatsphäre-Dashboard“ erreicht. Dort listet Android alle Apps, die in den vergangenen 24 Stunden auf die Kamera, das Mikrofon oder die Standortdaten zugegriffen haben. Mit wenigen Fingertipps können Sie einzelnen Apps die Rechte entziehen. Sofern eine App eine widerrufene Berechtigung zwingend benötigt, fordert Sie sie beim nächsten Start erneut an.

Standortfragen

Besonders den Standortzugriff sollte man großzügig einschränken: Android unterscheidet mittlerweile zwischen dem ungefähren Standort mit einer Genauigkeit von einigen Kilometern und dem auf wenige Meter genauem Standort. Letzteren benötigen nur wenige Apps etwa zur Routenführung. Anderen Apps reicht die Information, in welcher Stadt man sich aufhält. Wieder andere Apps funktionieren ohne Standortermittlung ganz gut, überraschenderweise auch Google Maps. Sie können Routen planen und

Mehr wissen – besser verstehen



- Docker verstehen und richtig loslegen
- Mikrocontroller versus Mikroprozessoren
- Windows-Basics: Explorer, Dateisysteme, Registry
- Das eigene Netzwerk richtig ausrüsten

Heft + PDF mit 29 % Rabatt

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €

shop.heise.de/ct-knowhow22

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

heise Shop

sich die Umgebung gewohnt anschauen – müssen aber manuell zu Ihrem Standort hinzoomen und können sich nicht navigieren lassen.

In den Android-Einstellungen unter „Standort“ wählen Sie, was Google zu sehen bekommt: Der Google-Standortverlauf speichert in der Cloud alle Bewegungen des Smartphones, die Google-Standortfreigabe ermöglicht darüber hinaus, den aktuellen Standort anderen Nutzern freizugeben.

An dieser Stelle können Sie auch zentral die Standortermittlung des Geräts abschalten. Bis Android 10 funktioniert dann allerdings die Risikoermittlung der Corona-Warn-App nicht mehr. Ab Android 11 darf das zugrundeliegende API auch ohne Standortzugriff die Bluetooth-Geräte der Umgebung scannen, was für die Funktion der Warn-App reicht; den echten Standort benötigt sie gar nicht [1]. Offenbar implementieren das aber nicht alle Hersteller richtig, jedenfalls beharrte die App auf einem Xiaomi-Smartphone trotz Android 11 weiterhin auf den Ortsdatenzugriff.

Browser statt App

Durch das gezielte Entziehen von Rechten schränken Sie effektiv ein, welche Daten eine App überhaupt erheben darf. Doch das Rechtemanagement ist für eine vollständige Kontrolle nicht engmaschig genug. Apps haben beispielsweise stets die Möglichkeit, den Handytyp, die Speichergröße, die Nutzungsdauer und andere Daten abzufragen. Oft ist es deshalb ratsam, eine App gar nicht erst zu installieren, sondern das Webinterface des jeweiligen Dienstes zu nutzen, sofern es zur Verfügung steht. Komfortabel ist es allerdings nicht, für jeden Check der Twitter-Timeline den Browser zu öffnen und die Webseite händisch aufzurufen. Abhilfe schaffen Progressive Web Apps (PWA). Viele Dienste, aufgerufen im mobilen Chrome-Browser, bietet in einem Pop-up-Hinweis an, sich als PWA zu installieren.

Eine PWA ist eine nur wenige Kilobyte große Webseiten-Verknüpfung, die sich wie eine reguläre App im App-Menü einnistet, auf dem Homescreen platzieren lässt und übers App-Menü wieder zu deinstallieren ist. Sie brauchen weniger Speicher und laufen nicht (heimlich) im Hintergrund. Sobald man sie startet, öffnet sich der gewünschte Inhalt in einem Chrome-Custom-Tab – also einem verschlankten Fenster, dem man nicht ansieht, dass es sich in Wirklichkeit um ein Browserfenster handelt.

Leider hat die Sache den Schönheitsfehler, dass Android die Daten von PWAs nicht von denen des Chrome-Browsers trennt. Nutzt man beispielsweise Facebook oder Instagram als PWA, schneidet der Mutterkonzern Meta praktisch das gesamte Surfverhalten mit, da man im Browser als angemeldet gilt und die auf fast jeder Seite eingebetteten Like- und Share-Buttons die Seitenaufrufe zu Meta schicken. Eine Lösung wäre, Chrome nicht zu nutzen, sondern die genannten datensparsamen Browser. Dann sehen sich die PWAs nur untereinander.

Eine andere Lösung bietet die kostenpflichtige App Hermit. Sie ist ein auf den ersten Blick wilder Mix aus alternativem Browser und App-Launcher. Webdienste speichert man darin als Verknüpfung;



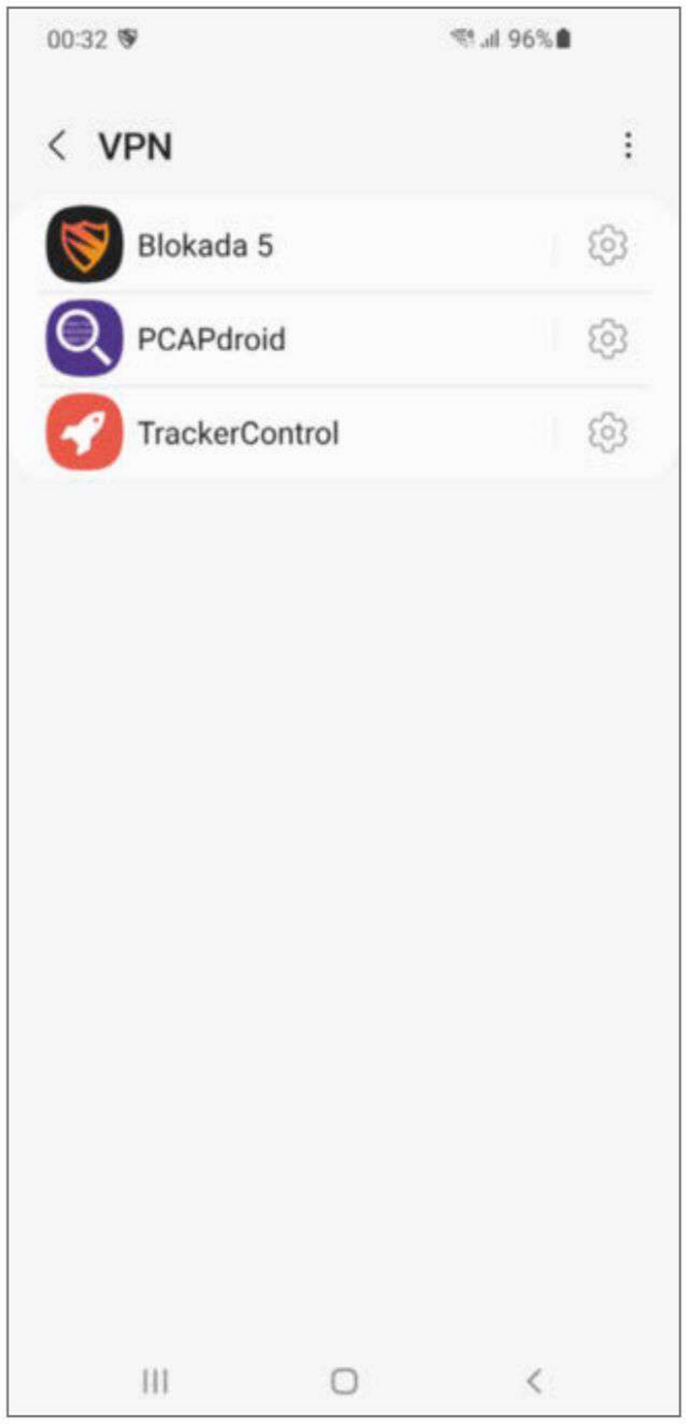
Dass eine App auf den Standort zugreift, zeigt Android in der Statuszeile. Inzwischen sind auch Symbole für Kamera- und Mikrofonzugriff hinzugekommen.

beim Start öffnet Hermit sie im Vollbild ohne Adressleiste und in einer Browser-Sandbox mit getrennten Cookies und Werbeblocker. Anders als eine einfach per Bookmark aufgerufene Seite registriert Hermit die Web-Apps aber als Ziel für „Teilen mit“ und „Senden an“, sodass Sie beispielsweise Fotos aus der Galerie an die Web-App schicken können. Nur wenige Dienste bieten allerdings per Web die gleichen Funktionen wie per nativer App.

Kontrolliert und eingebremst

Wichtig ist es daher, normalen Apps auf die Finger schauen zu können und ihren Traffic zu beschneiden. Wollen Sie sich einen Überblick verschaffen, welche Spy- und Werbe-Tracker in einer App stecken, bietet sich der auf Seite 94 beschriebene APK Library Scanner an.

Für den Alltag gibt es praktikablere Tools. Die Open-Source-App Blokada beispielsweise implementiert einen Trackerschutz und Werbeblocker direkt auf dem Gerät. Aufgrund der Hausregeln von Google findet man im Play Store nur die abgespeckte Version Blokada Slim, empfehlenswert ist die Vollversion von F-Droid oder blokada.org. Die Vollversion lädt konfigurierbare Blocklisten mit Schwerpunkt auf Werbetracker, Spam oder Phishing. Blokada fängt dann alle DNS-Abfragen ab und sperrt diejenigen an Server von diesen Listen. Sie baut dazu ein lokales VPN auf. Einzelne Apps und auch einzelne Server lassen sich von der Blockade ausnehmen. In den vergangenen Jahren wurde Blokada stetig weiterentwickelt und auf ein Freemium-Modell umgestellt. Für bestimmte Funktionen und einen externen VPN-Dienst, der Tracking filtert, ist ein kleiner Obolus fällig.



Die per VPN-Trick arbeitenden Firewalls und Adblocker tauchen in der VPN-Liste in den Android-Einstellungen auf. Hier stellt man ein, dass sie beim Systemstart aktiviert werden sollen.



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

heise Shop

Eine schlanke und kostenlose Alternative ist die ebenfalls bei F-Droid erhältliche App Tracker Control. Das unter dem Dach der University of Oxford entwickelte Tool arbeitet nach dem gleichen VPN-Prinzip wie Blokada. Darüber hinaus hat Tracker Control eine Analysefunktion, die den Code von Apps gezielt auf Tracker untersucht. Zudem kann man den Internetzugang einzelner Apps komplett sperren.

Wer sich tiefer einarbeiten möchte, installiert NetGuard, eine ausgewachsene Firewall [2]. Sie nutzt ebenfalls den VPN-Trick. Für jede App lässt sich einzeln einstellen, ob sie immer, nur bei eingeschaltetem Display oder nie Internetzugriff bekommt und ob sie durch die Firewall muss – getrennt nach WLAN- und Mobilfunkverbindungen. NetGuard blockiert dabei sämtlichen Traffic. Um nur Werbung und Tracker auszufiltern, muss man selbst DNS-Listen in der App anlegen und sie permanent aktuell halten – viel Aufwand.

Alle drei Apps lassen sich direkt beim Booten starten – dank VPN-Trick, denn so kann man die Tools als Always-on-VPN konfigurieren, was ab Android 7 funktioniert. Dazu sucht man in den Android-Einstellungen den Eintrag VPN – auf den meisten Geräten irgendwo unter „Verbindungen“ zu finden –, tippt auf den dortigen Eintrag von Blokada, NetGuard oder Tracker Control und schaltet „Durchgehend aktives VPN“ und „Verbindungen ohne VPN blockieren“ ein. Fehlt die App in der VPN-Liste, muss man sie in der App einmal manuell aktivieren.

Getrennte Bereiche

Wichtig für den Datenschutz ist auch, seine Kontakte, Dateien und Termine vor einzelnen Apps zu schützen – oder anders herum nur einzelnen Apps Vollzugriff zu geben. Android hat zu diesem Zweck eine Profilverwaltung ähnlich den Desktop-Systemen: Man loggt sich aus und mit einem anderen Profil wieder ein. Das implementieren allerdings nur wenige Smartphones. Praktischer wäre zudem, wenn beide Profile gleichzeitig aktiv sind, etwa um Messenger-Nachrichten an das Hauptprofil auch dann zu empfangen, wenn man im zweiten Profil arbeitet.

Samsung und Xiaomi haben das in ihre Android-Versionen integriert. Xiaomis „Zweitprofil“ ist in den Einstellungen unter „Spezielle Funktionen“ zu finden, Samsungs „Sicherer Ordner“ unter „Biometrische Daten und Sicherheit“.

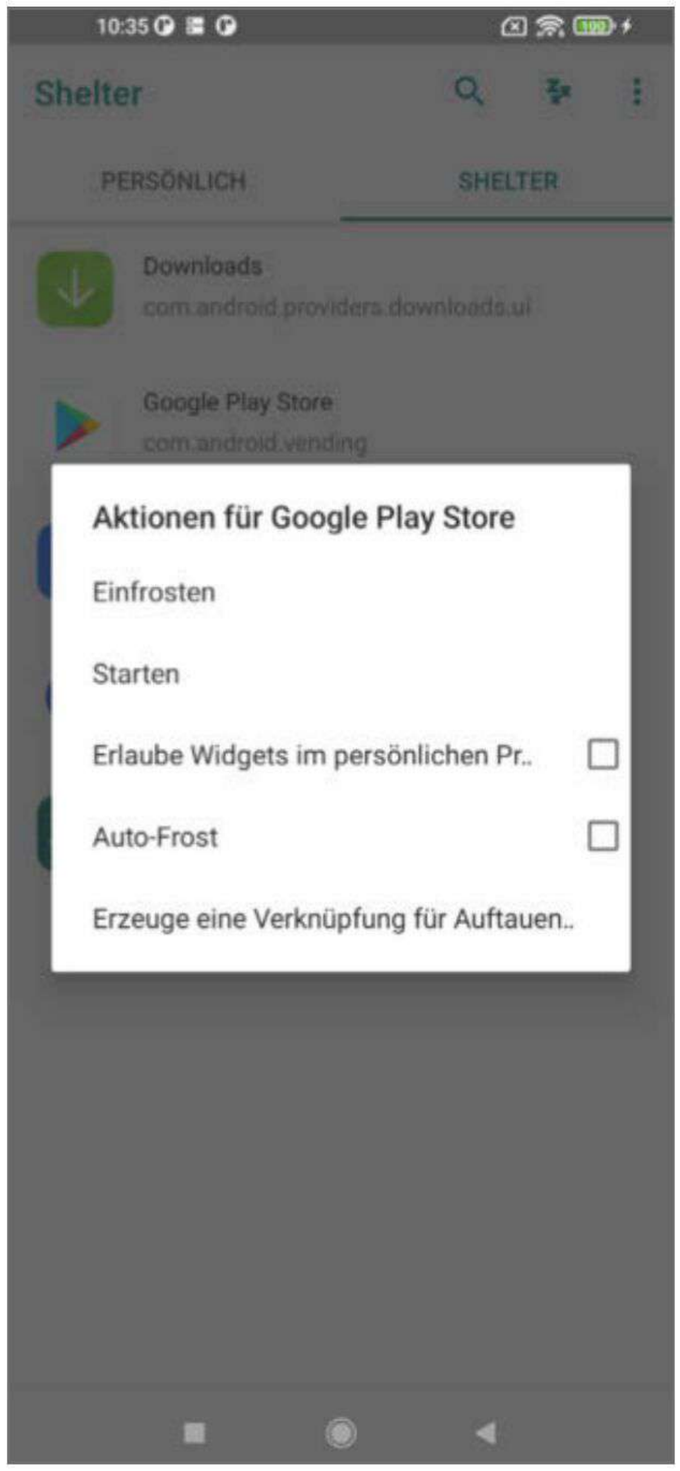
Google selbst hat sich die funktionsgleichen „Arbeitsprofile“ ausgedacht, die allerdings nur in einer gewissen Firmeninfrastruktur aktivierbar sind.



Tracker Control ist nicht nur eine Firewall, die Tracker und Werbung blockiert. Die App analysiert auch die installierten APKs anderer Apps auf bekannte Tracker-Bibliotheken.

Findige Entwickler haben aber einen einfachen Weg gefunden, die Arbeitsprofile auf jedem Smartphone zu öffnen, und zwar mithilfe der App Island, zu finden im Play Store. Es folgten die Open-Source-Varianten Insular auf F-Droid vom selben Entwickler und Shelter. In unserem Test haben sich Shelter, Island, Insular sowie die Lösungen von Samsung und Xiaomi als gleich effektiv erwiesen, wenn auch jeweils etwas anders zu bedienen.

Ihr Prinzip ist gleich: Im zweiten Profil kann man andere Konten für Adressen und Termine anlegen, und somit auch ein anderes (oder kein) Google-



Per Shelter ins Arbeitsprofil eingesperrte Apps kann man einfrieren – nützlich für selten genutzte Apps, die nichts im Hintergrund sammeln sollen.

Konto. Die Apps bekommen also keinen Zugriff aufs Haupt-Adressbuch und -Terminverzeichnis. Auch die Dateien bleiben getrennt, das Zweitprofil bekommt einen eigenen „internen gemeinsamen Speicher" – das Gemeinsame daran bezieht sich darauf, dass alle Apps des Profils darauf zugreifen können.

Auch wirken sich VPN-Verbindungen und somit darüber realisierte Adblocker nur aufs gestartete Profil aus. Ein Autostart ist vorgesehen; sobald man das VPN-Tool erstmals im Zweitprofil startet, wird es separat in der Liste der VPNs eingetragen. Es startet dann allerdings schon beim Hochfahren des Smartphones und nicht erst beim ersten Start einer App im Zweitprofil. Für gelegentliche Nutzung dürfte es daher sinnvoller sein, das Zweitprofil-VPN manuell zu starten. Andere Funktionen teilen sich die Profile, beispielsweise die Mobilfunk- und WLAN-Anbindung.

Im Hauptprofil installierte Apps kann man ins Zweitprofil klonen; das erledigt man bei Island/Shelter in den Apps und bei Samsung/Xiaomi in den Android-Einstellungen. Die Apps bekommen im Zweitprofil einen separaten Konfigurationssatz, sodass man sich mit einem anderen Konto etwa bei WhatsApp oder Facebook anmelden kann. Nicht geklonte Apps erscheinen im Zweitprofil nicht. Zusätzlich kann man neue Apps im Zweitprofil installieren. Die Apps im Zweitprofil lassen sich dann auf den Homescreen holen, man erkennt sie an einem kleinen Symbol unten am Start-Icon. Mehrfache Arbeitsprofile sind nicht vorgesehen, aber Samsungs Sicherer Ordner und Xiaomis Zweitprofil laufen parallel zu Island/Shelter und erlauben dann sozusagen ein Drittprofil.

Eine weitere nützliche Funktion von Island/Shelter ist das Einfrieren von Apps im Zweitprofil. Sie laufen dann nicht im Hintergrund, fressen keine Ressourcen und sammeln keine Daten. Das geht bei Shelter und Island manuell. Ein automatischer Freeze ist bei Shelter eingebaut und bei Island über die App Greenify nachrüstbar, funktioniert aber nicht unter allen Bedingungen zuverlässig. Vor allem muss man Shelter und Island dazu von den Stromsparmechanismen von Android ausnehmen.

Fazit

Die vorgestellten Tools helfen Ihnen dabei, Ihre Daten halbwegs unter Kontrolle zu haben. Getrennte Arbeitsbereiche, Firewalls und datensparsame Browser werden auch bei zukünftigen Android-Versionen notwendig bleiben. Denn zwar lernt Android in jeder Version mehr Datenschutz, die Optionen liegen aber verstreut in den Einstellungen, als hätte Google sie absichtlich versteckt.

Aber dass einige grundlegende Privatsphäre-Funktionen fehlen und dass Google sich selbst einen dicken Datenhappen genehmigt, schürt Misstrauen. Einen Adblocker braucht man von Google nicht zu erhoffen, aber schön wäre schon, wenn eine künftige Android-Version zumindest ein echtes Firewall-API bekommt, sodass gleichzeitig dazu ein VPN nutzbar ist. Wer aber Google inklusive aller Apps und zusätzlich auch alle Apps des Geräteherstellers los werden möchte, liest im nächsten Artikel über Custom-ROMs weiter. (jow) c't

Literatur

[1] Jörg Wirtgen, **Location-Berechtigung für Kopfhörer?**, c't 3/2020, S. 172

[2] Ronald Eikenberg, **Netzwerk-Kontroletti**, Android-Firewall NetGuard, c't 11/2020, S. 84



Bild: Rudolf A. Blaha

Custom-ROMs für Android im Vergleich

Ein Custom-ROM ist der Königsweg, um Google den Datenhahn trotz Android-Handy zuzudrehen. Doch schon die Installation kann steinig sein. Wir haben uns sechs alternative Androids angeschaut, die mit langen Updates und guter Bedienbarkeit auch ohne Google punkten – es zeigte sich schnell, was klappt und was nicht.

Von **Robin Brand, Steffen Herget und Jörg Wirtgen**

Zu viel Bloatware, zu wenig Datenschutz, keine Updates mehr: Es gibt viele Gründe, vom regulären Android eines Allerwelts-Smartphones auf ein alternatives Android umzusteigen, ein Custom-ROM. Ob das aus Privacy-Gründen überhaupt sinnvoll ist, haben wir im Einleitungsartikel ab Seite 72 geklärt. Manchmal reicht es auch aus – bequemer ist es immer –, Google mit Bordmitteln plus einigen Tools den Datenhahn zuzudrehen (siehe Seite 78).

Custom-ROMs entwickeln im Allgemeinen die freie Android-Variante AOSP – oder ein anderes Custom-ROM – so weiter, dass sie auf konkreten Smartphones bootet; die Maintainer ergänzen Treiber,

implementieren eigene Konzepte und packen ausgesuchte Apps dazu. Die Hersteller-Apps fehlen daher komplett. Mit der Installation eines Custom-ROMs lässt man sich auf eine oftmals rege Community ohne offiziellen Support ein.

In diesem Artikel schauen wir auf den Funktionsumfang der im Einleitungsartikel vorgestellten Custom-ROMs, deren Installation und geben Tipps, woher man Apps bekommt, wenn der Play Store als Bezugsquelle entfällt.

Vor allem steht die Aufgabe, das gewünschte Custom-ROM aufs Smartphone zu schaufeln. Nur wenige Maintainer liefern Smartphones direkt mit dem Custom-ROM aus. Dazu gehört im Testfeld das Volla Phone. Auch die eFoundation vertreibt diverse Neugeräte sowie aufbereitete Smartphones mit vorinstalliertem /e/OS, ebenso iodé. Doch in der Regel heißt es selbst Hand anlegen. Welche Smartphones für welches Custom-ROM passen, verrät ein Blick auf die Seiten der Entwickler.

Aufs Smartphone gebracht

Die Installation läuft bei allen Custom-ROMs ähnlich ab; wie kompliziert sie ist, hängt weniger vom Custom-ROM ab als vom Smartphone. Zuerst muss man den Bootloader entsperren, dann das ROM irgendwie aufs Gerät kopieren, meist im Fastboot-Modus. Wenn möglich, sperrt man dann den Bootloader wieder zu, und schließlich kann man ins Custom-ROM booten und mit der Konfiguration loslegen. Für einige der Schritte muss man das Smartphone per USB an einen Rechner hängen und dort die Google-Tools adb und fastboot installieren.

Auf Pixel-Phones ist das mit wenigen Handgriffen erledigt. Calyx macht es einfach: Man lädt sich ein Hilfsprogramm herunter, das alle benötigten Tools und ROMs automatisch nachlädt, installiert und dabei am PC-Bildschirm informiert, wann man welche Tasten auf dem Smartphone zu drücken hat. Graphene nutzt noch komfortabler das WebUSB-Interface: Die Installation läuft aus dem Browser heraus.

Etwas schwerer tat sich LineageOS mit dem Pixel 5. Der Hinweis, dass Android 11 installiert sein muss, schien ernst gemeint: Auf unserem war jedenfalls schon Android 12 aufgespielt, und nach der Lineage-Installation bootete es nicht mehr. Auch das Einspielen eines Android-11-Images von Google klappte danach nicht mehr, wir bekamen das Pixel nur noch per Android-12-Image zum Laufen.

Samsung, Xiaomi und andere werfen den Kunden mehr Knüppel zwischen die Beine. Auf den Webseiten der Custom-ROMs finden sich dazu mal bessere, mal arg knappe Anleitungen. Vor allem Lineage und /e/ pflegen dank aktiver Community ausführliche Beschreibungen, und auch bei YouTube wird man fündig.

Ein Sonderfall sind Samsung-Smartphones, da sie nicht den normalen Fastboot-Modus benutzen, sondern das Spezial-Tool Odin. Diese für die Installation von Custom-ROMs und die Samsung-eigene Firmware notwendige Software rückt Samsung nicht offiziell heraus. Stattdessen muss man sie sich irgendwo suchen oder auf die freie Alternative Heimdall zurückgreifen. Doch die läuft offenbar auf modernen PCs nicht immer rund, auch weil sie sehr spezielle USB-Treiber mitbringt – die übrigens nur recht kompliziert wieder zu entfernen sind, wenn man sie nicht mehr braucht. Uns ist es nicht gelungen, ein Custom-ROM auf ein Galaxy S10 zu spielen, obwohl wir Heimdall unter Windows 10, Windows 11 und macOS 12.2 ausprobiert haben.

Auch an einem Xiaomi Mi 10T sind wir gescheitert: Zum Entsperren des Bootloaders muss man ein Xiaomi-Konto anlegen, es mit einer Telefonnummer verknüpfen, eine SIM einlegen, eine bestimmte Seite zwingend per Mobilfunk aufrufen, dort eine Freischaltung beantragen und diese dann in einer Windows-Software durchführen. Doch auch nach Tagen erschien unsere beantragte Freischaltung nicht in der Windows-Software.

Das Einspielen des Custom-ROMs per Fastboot ist nicht auf allen Smartphones möglich. Daher müssen diejenigen Custom-ROMs, die nicht nur auf Pixels laufen, einen anderen Weg wählen: Lineage, /e/ und iodé. Im Allgemeinen installiert man ein kleines Recovery-Image, bootet dort hinein, sucht einen meist „Sideload“ genannten Punkt und überträgt dann das eigentliche Image per adb vom Rechner. Möchte man auf dem Gerät vielleicht mit mehreren Custom-ROMs experimentieren, könnte sich das universelle und um einige Funktionen erweiterte Recovery-Image TWRP lohnen.

Ein wenig Geduld und Hartnäckigkeit sind also bei allen Smartphones – auch den Pixels – vonnöten. Manche Dokumentation liest sich, als hätte der Autor auch erst im -zigsten Versuch Erfolg gehabt und sich nicht ganz genau gemerkt, was er nun anders gemacht hat als in den Versuchen zuvor. Welche Tasten in welcher Reihenfolge? Mit oder ohne eingestecktem USB-Kabel? Was sind die wesentlichen Rahmenbedingungen? Manches werden Sie ausprobieren müssen. Auch ist Fingerspitzengefühl vonnöten: Um in den Recovery- und Fastboot-Modus zu booten,

muss man bei ausgeschaltetem Gerät bestimmte Tastenkombinationen drücken. Die sind zwar ganz gut dokumentiert, aber man erkennt nicht immer zweifelsfrei, ob das Gerät ausgeschaltet ist. Denn viele Smartphones zeigen nach dem Herunterfahren eine Ladestandsanzeige oder andere Animationen an – und zwar meist dieselbe wie beim Einschalten.

Groß sind sie geworden

Einmal installiert, zeigen sich die Custom-ROMs überraschend erwachsen. Grundlegende Funktionen laufen ohne Nacharbeiten. Besonders einsteigerfreundlich ist das optisch an iOS angelehnte Android /e/ – optional mit eigenen Cloudservices. Damit muss man auf den von Google gewohnten Komfort inklusive Synchronisation von Fotos, Kontakten und Notizen über mehrere Geräte nicht verzichten, die Daten lagern auf Servern in der EU.

Mehr Umgewöhnung erfordert das Volla Phone, die Entwickler haben ganze Arbeit geleistet und das gesamte Bedienkonzept auf links gedreht. Hat man sich erst einmal eingearbeitet, muss man den Homescreen kaum mehr verlassen. Alle häufig verwendeten Apps sind mit einem Daumenwisch erreichbar, Nachrichten versenden oder Webseiten aufrufen kann man über ein Textfeld auf dem Homescreen. Mehr oder weniger an das klassische Stock-Android in der Version 11 respektive 12 erinnern die anderen alternativen Betriebssysteme. Allen ROMs ist eine Sache gemein: Kommt man mit der Bedienung nicht zurecht, kann man sich auch einfach durch die Installation einer Launcher-App das gewohnte Konzept nachbauen [1].

Was läuft, was nicht

Mehr Aufwand müssen die Custom-ROM-Entwickler treiben, um die zahlreichen Komfort-Funktionen nachzubauen, die man sich unter einem offiziellen Android mit einer Datenspende an Google erkauft. Nicht wenige Schnittstellen hat Google nämlich aus dem Betriebssystem gelöst und in die Google-Play-Dienste ausgelagert, ein prominentes Beispiel ist die Standortbestimmung. Das kann sogar so weit gehen, dass Apps von Drittanbietern ganz oder teilweise nicht mehr funktionieren, wenn man sie unter einem Custom-ROM statt einem kommerziellen Android verwenden möchte. Wir haben uns angeschaut, was bei den Custom-ROMs ohne Nacharbeiten funktioniert. Auf einigen ist microG vorinstalliert, ein Projekt, um Google-APIs möglichst datenzahm nachzubauen.

Eine der zuverlässigsten Quellen für kommerzielle Apps ist der Aurora-Store, den wir auf allen Custom-ROMs herangezogen haben. Dieser App-Store kann ein Google-Konto simulieren und auf diese Weise die Installation der Apps ermöglichen, die so ein Konto brauchen. Einen gut gefüllten eigenen Store bringt /e/ mit – Informationen über die in den Anwendungen enthaltenen Tracker inklusive. Ausschließlich quelloffene Anwendungen stehen im alternativen Store F-Droid zur Auswahl. Alle drei Stores lassen sich ohne Konto benutzen, und sie halten die darüber installierten Apps mithilfe eines eigenen Aktualisierungsdiensts auf Stand.

Eine gelungene Installation allein ist jedoch keine Garantie, dass eine Anwendung auch läuft. Zahlreiche Streaming-Apps für Musik und Video vertrauen dem Google-Dienst SafetyNet. Dessen Aufgabe ist die Überprüfung der Integrität des Android-Geräts. Zwar haben die microG-Dienste eine eigene Version von SafetyNet eingebaut, die solche Apps lauffähig halten soll, sicher ist das aber nicht. Schlaue Köpfe bei Google drehen stets an den entsprechenden Rädchen im System, um Android-Versionen ohne echte Zertifizierung von SafetyNet auszusperren.

Im Test sind wir immer wieder auf teils kleine, teils größere Probleme gestoßen. Beim Pixel 5 mit GrapheneOS etwa ließ sich der Fingerabdruck nicht anlernen. Immer wieder beschwerte sich das Gerät über einen angeblich verschmutzten Sensor.

Google Pay funktionierte auf keinem unserer Custom-ROMs. Kauft man gerne per Smartphone ein, ist Googles Zahlmeister also außen vor. Auch andere Bezahl-Apps und Anwendungen mit In-App-Käufen können zicken, mit PayPal und – stellvertretend für Banking-Apps ausgewählt – ING konnten wir allerdings problemlos Geld hin und her schieben. Mit den großen Streaming-Apps Netflix, Spotify und Amazon Prime hatten wir ebenfalls keinerlei Schwierigkeiten. Manchmal ist die Lösung irgendwo im System vergraben: So konnten wir uns auf unserem iodé-Smartphone beim Streaming-Dienst Tidal erst einloggen, nachdem wir die App aus der Blockliste der in iodé eingebauten Tracker-Firewall genommen hatten. Einiges mag man mit dem eigentlich als Root-Verstecker gedachten Tool Magisk zum Laufen bringen [2].

Google-Apps wie Maps funktionierten auf allen unseren Testgeräten, beschwerten sich aber mitunter über fehlende Google-Dienste, was die Bedie-



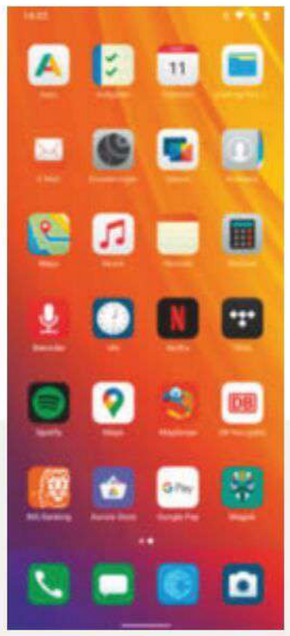
CalyxOS

CalyxOS ist eines der jüngsten Custom-ROMs, im Sommer 2022 feiert es erst seinen zweiten Geburtstag. Mit eingebauter Datura-Firewall, VPN und Cloudflare DNS verspricht Calyx mehr Sicherheit als manch anderes mobiles System. Praktisch: Wer ein Calyx-Smartphone als Hotspot verwendet, kann die Verbindung mit dessen VPN- oder Tor-Zugang absichern. Verified Boot, das automatische Abschalten von WLAN und Bluetooth und monatliche Sicherheitsupdates sind weitere Pluspunkte. Sicherheitsaktualisierungen liefert Calyx etwas länger als Google für das jeweilige Pixel-Smartphone und macht auf der Website genaue Angaben zu jedem Gerät.

Dabei merkt man Calyx diese Sicherheitsfeatures in der täglichen Benutzung kaum an, das System bedient sich wie ein normales Android. Die Google-Ersatzdienste von microG gehören bei CalyxOS zum Standard, ebenso die App-Stores von Aurora und F-Droid. Mit Android 12 als Unterbau ist CalyxOS auf dem aktuellen Stand. Backups landen entweder lokal per USB auf dem Rechner oder per Nextcloud, auf Wunsch auch automatisch.

Die Geräteauswahl bei CalyxOS ist beschränkt auf Googles Pixel-Smartphones ab dem Pixel 3 sowie ein Xiaomi-Handy. Vorinstalliert kann man CalyxOS derzeit nur auf einem Google Pixel 4a kaufen – zum horrenden Preis von 700 Dollar und wenn man der mit jährlichen Kosten verbundenen Calyx-Membership beitritt.

- **einfache Installation**
- **viele nützliche Apps vorinstalliert**
- **wenige Geräte unterstützt**



/e/OS

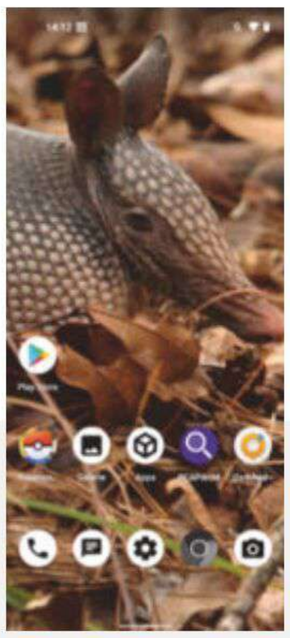
Beim ersten Blick auf das frisch installierte Android /e/OS dachten wir fast, wir hätten iOS installiert, so hemmungslos haben die Macher von /e/ bei Apple abgekupfert. In einer Fußleiste sind Kamera-, Telefon-, Nachrichten- und Browser-App hinterlegt, die weiteren Apps legt das System auf dem Homescreen ab, einen App-Drawer gibt es nicht. Hält man eine App lange gedrückt, fangen alle App-Icons wie bei iOS an zu wackeln und man kann ein Icon auf ein anderes ziehen, damit sie in einem gemeinsamen Ordner landen.

Ein gut gefüllter eigener App-Store hält viele populäre Anwendungen wie Spotify, Netflix, PayPal oder WhatsApp bereit. Die Apps bezieht die eFoundation aus dem Angebot von Cleanapk.org und informiert vor dem Download, welche Tracker eine Anwendung nutzt und welche Berechtigungen sie einfordert. Das Betriebssystem lässt sich komplett ohne Konto verwenden. Richtet man eines ein, lassen sich diverse Daten geräteübergreifend synchron halten – in der kostenlosen Variante gibt es 1 GByte Cloudspeicher auf einem Server in der EU. Wer sich eine Synchronisation von Kalender und Adressbuch wünscht, kann die Daten statt in der /e/-Cloud auch einfach in einer selbst gehosteten Nextcloud ablegen. Im System sind die quelloffenen microG-Dienste integriert, die die Funktionen und APIs der Google-Play-Dienste ersetzen. Mit Ausnahme von Google Pay liefen die von uns getesteten Apps problemlos.

- **zahlreiche Apps vorinstalliert**
- **eigene Cloud-Funktionen**
- **vorinstallierte Modelle im Shop**

nung etwas frustrierend machte. Probleme machte bei einigen ROMs der Login ins Google-Konto innerhalb einer Google-App: Teils schlug er einfach fehl, teils meldete das Smartphone zwar einen Fehler, irgendwie angemeldet war man aber doch, nur um in der nächsten App erneut vor verschlossener Tür zu stehen. Es läuft allerdings auch dem Grundgedanken eines Betriebssystems, das weniger Daten an Google senden soll, zuwider, sich auf eben diese Dienste zu stürzen, es gibt schließlich genügend Alternativen [3]. Um den Datenabfluss einzuschränken, bieten mit Ausnahme von VollaOS alle ROMs die Möglichkeit, einzelnen Apps komplett die Internetnutzung zu verbieten, GrapheneOS kann Apps zudem den Zugriff auf die Sensoren im Smartphone entziehen.

GrapheneOS



GrapheneOS ist eine Weiterentwicklung von CopperheadOS. Der Fokus liegt auf Sicherheit und Datenschutz, weshalb sich Graphene ausschließlich auf Google-Pixel-Smartphones, die Verified Boot unterstützen, installieren lässt. Damit einher geht die Entscheidung der Entwickler, GrapheneOS nur solange zu unterstützen, wie Google die Firmware des jeweiligen Gerätes auf Stand hält. Beim Pixel 6 ist das bis Oktober 2026, beim 5er Pixel ist schon drei Jahre früher Schluss. Das nicht mit Graphene verbundene Unternehmen Nitro verkauft Pixel-Smartphones mit vorinstalliertem Graphene – und für einen happigen Aufpreis kann man diverse Sensoren oder Kameras entfernen lassen, wenn man denn will. Die Installation von GrapheneOS gelingt recht einfach: Sie läuft über ein WebUSB-Interface aus dem Browser heraus.

GrapheneOS wird ohne microG-Dienste ausgeliefert, stattdessen laufen die Google-Apps und -Dienste in einer abgesicherten Umgebung und erhalten keinen Zugriff auf Systemebene. GrapheneOS verzichtet fast auf jegliche vorinstallierten Apps. Wie beispielsweise auch bei Lineage kann man die Ziffern für die Eingabe des Entsperrcodes zufällig anordnen lassen, um heimliches Ausspähen zu erschweren. Die integrierte Backup-Lösung Seedvault ermöglicht Ende-zu-Ende-verschlüsselte Komplett-Backups, etwa auf USB-Speicher oder in die selbst gehostete NextCloud.

- **gehärteter Android-Kern**
- **Google-Dienste in Sandbox**
- **läuft nur auf Google Pixel**

iodéOS



iodéOS ist ein Custom ROM auf bekannter Basis, nämlich LineageOS. Daraus macht der Anbieter auch kein Geheimnis, schon bei der Installation grüßt das Lineage-Logo. Die Optik des Systems unterscheidet sich dann auch kaum von LineageOS, alles wirkt aufgeräumt, klar strukturiert und nicht weit weg vom normalen Android.

Die App-Stores Aurora und F-Droid sind ebenso vorinstalliert wie die Open-Source-Tastatur OpenBoard und einige weitere quelloffene Alternativen zu gängigen Programmen. Herzstück von iodéOS ist die schlicht „iodé“ genannte App. Die arbeitet ähnlich wie Blokada, filtert den Netzwerktraffic, zeigt Statistiken über blockierte Anfragen an und bietet verschiedene Schutzmechanismen. Man kann einfach eigene Blocklisten für unbeliebte Schnüffler anlegen und für jede App die Schutzklasse definieren.

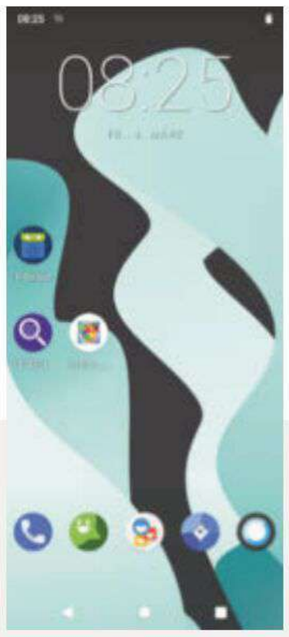
iodéOS gibt es entweder zum Download und Selbst-Installieren oder direkt auf Smartphones. Im Online-Shop von iodé finden sich zwei fabrikneue Geräte mit dem Betriebssystem (Fairphone 3 und Teracube 2E) sowie gut zehn refurbished Smartphones von Samsung, Sony und Xiaomi. Die Preise sind jedoch teils happig, das fünf Jahre alte Samsung Galaxy A5 soll noch 239 Euro kosten. Wer selbst installiert, spart kräftig: Ein Galaxy A5 ist gebraucht bereits für deutlich unter 100 Euro zu haben (Stand: April 2022). Marktgerechter sind die rund 300 Euro fürs Galaxy S9.

- **integrierter Werbeblocker**
- **vorinstallierte Modelle im Shop**
- **viele Apps vorinstalliert**

Blind auf ihren Augen

Die Freiheit von den Fesseln, die Google, OnePlus & Co. Android anlegen, hat an anderer Stelle ihren Preis. Eine davon betrifft die Kameras der Smartphones, denn mit der Installation eines Custom-ROM geht in aller Regel der Verzicht auf die Kamerasoftware einher, die der Hersteller dem Smartphone mit auf die Reise gibt. Die meisten Custom-ROMs setzen auf quelloffene Kamera-Apps wie Open Camera [4]. Die haben aber mit modernen Multi-Kamera-Smartphones ihre liebe Müh’ und Not.

Über die Hauptkamera und die Selfie-Cam hinausgehende Objektive, etwa der Ultraweitwinkel des Google Pixel oder das Tele des OnePlus 7T, ließen sich im Test nicht ansteuern, was die kreativen



LineageOS

LineageOS, hervorgegangen aus dem 2009 begründeten CyanogenMod, ist eines der bekanntesten und am längsten bewährten Custom-ROMs, und das merkt man auch. Das System nimmt AOSP als Grundlage und wirkt sehr nah an Googles Android. Durch das Internet surft man mit dem Jelly Browser recht komfortabel, Apps kommen aus den – selbst zu installierenden – Stores von F-Droid und Aurora, navigiert wird mit dem zwar nicht allzu hübschen, aber alltagstauglichen OsmAnd, also mit Karten von OpenStreetMap. Wer sich mit gängigen Android-Smartphones auskennt, findet sich schnell zurecht. Es finden sich Builds für etliche Smartphone-Modelle.

Der Bedienkomfort geht jedoch ein wenig zulasten der Sicherheit. LineageOS verzichtet auf eine Möglichkeit, den Bootloader zu verschließen. Das macht das System an dieser Stelle anfälliger als solche, die nur mit signierten Paketen starten, etwa Graphene und Calyx. Einen eingebauten Schutz vor Trackern gibt es weder systemweit noch im Browser, auch eine Firewall fehlt im Standardumfang.

Kurz vor Redaktionsschluss erreichte LineageOS 19.1 mit Android 12 als Unterbau unser Google Pixel 4. Zuvor war es auf Version 18.1 mit Android 11 als Basis gelaufen. Den Support von LineageOS 17.1 hat das Team gerade eingestellt, Android 10 ist dort also bereits auf dem Abstellgleis gelandet.

- **sehr viele Modelle unterstützt**
- **rege Community auch für Updates**
- **wenige Privacy-Verbesserungen**



Volla OS

Volla OS gibt es nicht zum Download, sondern nur vorinstalliert vom Händler. Die Firma Hallo Welt Systeme verkauft derzeit zwei Varianten des Volla Phone: Die eine ist ein Outdoor-Smartphone, bei der anderen handelt es sich um ein angepasstes Gigaset GS290, weitere sollen folgen. Das GS290 ist seit 2019 auf dem Markt und war zwischenzeitlich für rund 100 Euro im Abverkauf – und man merkt ihm sein Alter an. Die Kamera ist nur mit gutem Willen schnappschusstauglich, ressourcenhungrige Anwendungen bringen das Gerät an seine Grenzen. Der aufgerufene Preis von 360 Euro ist für die gebotene Hardware zu hoch angesetzt.

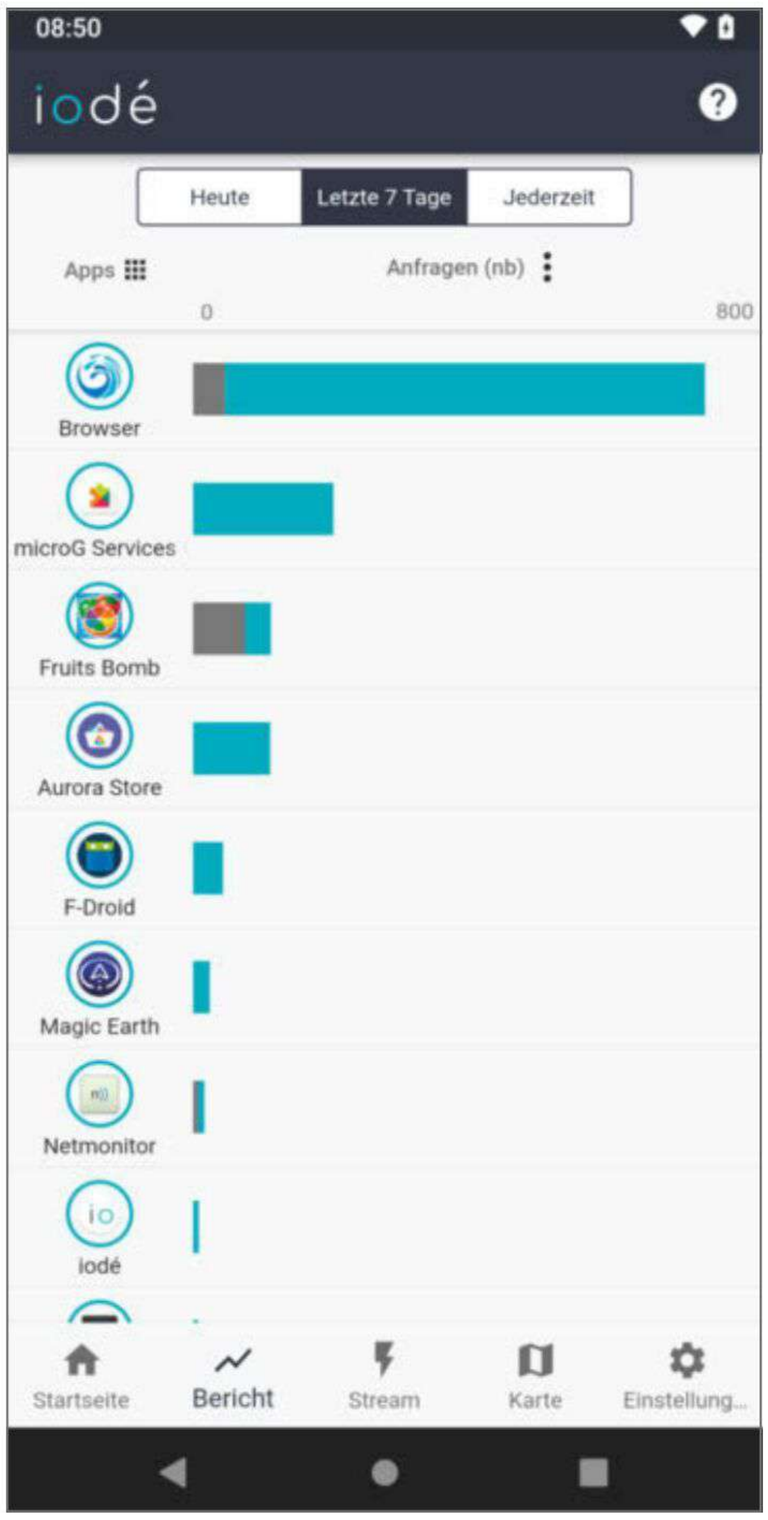
Das Volla Phone punktet mit seiner Software. Das Bedienkonzept ist einzigartig und benötigt eine kurze Eingewöhnung. Dann allerdings navigiert man sich schnell durch die Menüs, alle häufig verwendeten Apps sind mit einem Wisch erreichbar. In einem „Sprungbrett“ getauften Feld kann man Text tippen und direkt per Messenger oder Mail an einen Kontakt versenden, als Notiz speichern oder im Browser nach dem Begriff suchen. Ein Tipper auf einen roten „Schnellstart“-Punkt auf dem Homescreen öffnet Verknüpfungen zu häufig verwendeten Anwendungen. Links des Homescreens sind alle installierten Apps einsortiert, links daneben findet sich ein Einstellungsmenü. Positiv: Beim Booten kommuniziert das Volla Phone nur mit einem Updateserver.

- **originelles Bedienkonzept**
- **keine Download-Version**
- **nur zwei ältere Modelle unterstützt**

Möglichkeiten deutlich einschränkt. Softwarehelfer wie Nacht-, Portrait- oder Astromodus fehlen Open Camera ebenfalls.

Betrachtet man ohne und mit Custom-ROM aufgenommene Fotos, wird am Beispiel des Google Pixel 6 deutlich: Die Bilder sind ohne Googles Fotosoftware zwei Klassen schlechter. Die Hauptkamera des Pixel 6 zählt mit der Originalsoftware derzeit zu den besten Kameras auf dem Markt, mit der Kamera-App von CalyxOS reicht es nicht einmal fürs gehobene Mittelfeld.

Leider ist es auch keine allzu einfache Option, Googles Kamera-App nachträglich zu installieren. Auf dem Pixel 5 mit Lineage versagte diese uns nach der Installation den Start. Auf dem Pixel 6 ließ sich das Programm zwar starten und wir konnten auch Fotos



Die iodé-App zeigt auf einen Blick, welche Apps geblockte Verbindungen verursachen. Mit einem Tipp sieht man dann, welche Server sie anfunken. Man kann dann einzelne Server freischalten und sperren sowie Apps komplett den Mund verbieten.

knipsen. Umschalten auf Ultraweitwinkel bei Fotos führte aber ebenso verlässlich zum Absturz der App wie Zoomen oder die Verwendung des Portraitmodus.

Updates für alle

Der Nachhaltigkeitsgedanke ist in der Custom-ROM-Szene tief verwurzelt. Nicht zuletzt, weil etliche Hersteller eigentlich voll funktionsfähige Smartphones nach wenigen Jahren nicht mehr mit Updates versorgen, wechseln viele Nutzer auf ein alternatives Android. Selbst für fast zehn Jahre alte Smartphones wie das Samsung Galaxy S4 finden sich noch halbwegs aktuelle Lineage-Builds.

Wer sein Gerät lange mit Updates versorgt wissen will, sollte genau hinsehen. Es wäre ein Trugschluss zu glauben, ein Custom-ROM gehe automatisch mit langer Update-Versorgung einher. Bei Lineage ist eine rege Community für ein Gerät ein guter Indikator, dass man noch lange auf Updates hoffen darf. Bei Systemtreibern gerät aber auch die Community nach offiziellem Support-Ende an ihre Grenzen. So bekommt etwa das Google Pixel 1 immer noch regelmäßige Updates für das Custom-ROM */e/*, dessen Betriebssystemkern verharrt aber auf Android 9.

Handys mit Graphene werden dagegen nur für den Zeitraum unterstützt, in dem der Smartphone-Hersteller, das heißt Google, Firmware- und Kernel-Updates liefert. In dem Fall kann sich der Aufpreis für die neueren, teureren Geräte lohnen. Während die 6er Pixel Updates bis Oktober 2026 erhalten werden, lässt Google den Support für das 4a im August 2023 auslaufen.

Auch Calyx orientiert sich am Support der Smartphones durch Google selbst, geht allerdings ein wenig darüber hinaus. Die 4er Pixel erhalten beispielsweise bis August 2023 Sicherheitsaktualisierungen, während Google den Support im Oktober 2022 auslaufen lassen wird. Updates für proprietäre Firmware oder den Bootloader erhalten die Geräte nach dem Support-Ende durch Google nicht mehr.

Für iodé-Geräte mit LineageOS-18-Unterbau wollen die Entwickler mindestens drei Jahre Sicherheits-Updates liefern und mindestens vier Jahre für Version 19. Ziel sei es allerdings, darüber hinaus Sicherheitspatches zu liefern, hieß es auf unsere Anfrage.

Auch der Pariser Entwickler von */e/*, Gael Duval, schrieb uns, dass die Geräte wie das bereits vier Jahre alte Samsung Galaxy S9, das das Unternehmen aufbereitet selbst verkauft, noch viele Jahre Updates erhalten werde. Das sei allerdings ein großer Entwicklungsaufwand – und den stecken Duval und sein Team in die Pflege der Builds für Geräte, die sie auch selbst verkaufen. Neben Galaxy-Smartphones sind das Fairphone 3 und 4 und das Gigaset GS290. Man begrüße aber Maintainer für andere Geräte, so Duval. Doch selbst wer nicht direkt bei der eFoundation kauft, sondern das OS selbst installiert, dürfte mit den vorgenannten Modellen beste Chancen auf lange Updates haben – schließ-

Literatur

[1] Robin Brand, Stefan Porteck, **Des Kaisers neue Kleider: Acht Android-Launcher im Vergleich**, c't 23/2020, S. 154

[2] Stefan Porteck, **Root ohne Reue?** Mit dem Tool Magisk den Rootzugriff vor Google und Apps verstecken, c't 6/2020, S. 124

[3] Robin Brand, Michael Link, Stefan Porteck, **Passend gemacht: Alternativen für Google-Apps und -Dienste**, c't 7/2020, S. 22

[4] Steffen Herget, **Knipsware: Was Open Camera kann – und was nicht**, c't 19/2020, S. 140

Custom-ROMs

System	CalyxOS	/e/OS	GrapheneOS	iodéOS	LineageOS	Volla OS
URL	calyxos.org	e.foundation	grapheneos.os	iode.tech	lineageos.org	volla.online
installiert auf	Pixel 6	OnePlus 7T	Pixel 5	Fairphone 3	Pixel 4	Volla Phone
Ausstattung						
Android-Version	Android 12	Android 11	Android 12	Android 11	Android 12	Android 10
aktuelles Update	April 2022	März 2022	April 2022	März 2022	April 2022	Februar 2022
Lock Bootloader möglich	✓	–	✓	✓	–	✓
Permission Internet / Sensoren	✓ / –	✓ / –	✓ / ✓	✓ / –	✓ / –	– / –
Indikator Location / Kamera / Mikro	✓ / ✓ / ✓	✓ / – / –	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –	✓ / – / –
WLAN- / Bluetooth-Auto-Aus	✓ / ✓	– / –	✓ / ✓	– / –	– / –	– / –
Trackerschutz im OS / Browser	– / ✓	– / ✓	– / –	✓ / ✓	– / –	– / –
Stores	Aurora, F-Droid	App Lounge	Google Play Sandbox	Aurora, F-Droid	–	Aurora, F-Droid
Google-Dienste	microG Services Core	microG Services Core	–	microG Services Core	–	–
Launcher	Quickstep	Bliss Starter	GrapheneOS Launcher	Trebuchet	Trebuchet	Volla Launcher
Tastatur	Android AOSP	Android AOSP	Android AOSP	OpenBoard	Android AOSP	Android AOSP
Mail	K-9 Mail	E-Mail AOSP	–	p=p (K-9 mit PGP)	–	E-Mail AOSP
Kamera	Android Camera 2.0.002	OpenCamera-Fork 1.48.1	GrapheneOS Camera	OpenCamera 1.49.2	LineageOS Snap	Kamera 1.1.60030
Karte und Navigation	Organic Maps	Magic Earth	–	Magic Earth	–	OsmAnd
Browser	Chromium, DuckDuckGo	/e/ (Chromium-Fork)	Vanadium	iodé Browser (Mozilla)	LineageOS	Fennec F-Droid
Bewertungen						
Funktionsumfang	⊕	⊕	⊕⊕	⊕	⊕	○
Geräteunterstützung	○	⊕	○	○	⊕⊕	⊖
Bedienbarkeit / Einsteigerfreundlichkeit	⊕ / ⊕	⊕ / ⊕⊕	⊕ / ○	⊕ / ⊕⊕	⊕ / ⊕	⊕⊕ / ○

✓ vorhanden – nicht vorhanden ⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht

lich zeichnet hier die eFoundation selbst verantwortlich.

Das Volla Phone wird laut Geschäftsführer Dr. Jörg Wurzer mindestens für den Garantiezeitraum mit Updates versorgt: „Das bedeutet, dass wir mindestens zwei Jahre nach dem Verkauf des letzten Volla Phones Aktualisierungen garantieren“, so Wurzer. Ziel sei aber eine deutlich längere Unterstützung. Für Aktualisierungen des Basisbetriebssystems habe man den Quellcode an die Aktualisierungen und Patches des Android-Open-Source-Projektes gekoppelt. Außerdem hat das Unternehmen den Quellcode von Volla OS veröffentlicht, sodass auch eine Developer Community zu einer Weiterentwicklung und Aktualisierung beitragen kann.

Fazit

Custom-ROMs bieten eine Menge Vielfalt und Optionen, bei denen das normale Android nicht mithält: Lineage setzt auf breite Geräteunterstützung, Calyx legt mit Verified Boot den Fokus auf Sicherheit. Graphene dreht das Security-Rad noch viele Umdrehungen weiter und packt zusätzlich die echten Google-Dienste in einer Sandbox dazu. iodé schützt besonders durch die eingebaute Firewall die Privatsphäre. Volla macht auch optisch einiges anders als Google. /e/ kann mit eigener Cloud und eigenem App-Store punkten und ist besonders einsteigerfreundlich.

Auf einige Geräte lassen sich die Custom-ROMs – falls unterstützt – besonders einfach installieren: Google Pixel, Fairphone, OnePlus vor allem. Im Test zickten Smartphones von Samsung und Xiaomi; den Beschreibungen nach dürften aber auch andere Hersteller massiv nerven. Wer auf Hardware abseits von Google, Fairphone und OnePlus steht, sollte sich in den Shops von /e/ und iodé umsehen, zumal man mit den dort angebotenen Refurbished-Geräten auch der Nachhaltigkeit dient – und selbst als Note-Stift-Fan wird man fündig. Mit dem Aufpreis unterstützt man nicht nur die Maintainer, sondern spart auch eine Menge Zeit und Nerven. (rbr) c't



Bild: Thorsten Hübner

Android-Apps selbst auf Tracker prüfen

Mit dem APK Library Scanner lassen sich in Android-Apps missliebige Tracking-Spionagefunktionen aufspüren. Wir beschreiben, was das Tool besser macht als Analyse-Websites und was Nutzer und Programmierer davon haben, die eingesetzten Programmiermodule damit zu prüfen.

Von **Andreas Itzchak Rehberg und Michael Link**

Vor ein paar Jahren schreckte eine Untersuchung der Yale-Universität auf, die besagte, dass drei Viertel aller Apps Schnüffelmodule enthalten, die unbefugt Nutzerdaten erfassen. Mit der hier beschriebenen Lösung können App-Nutzer ihre Android-Apps – beziehungsweise deren Applikationspakete, die APK-Dateien (engl. Android Package Kits) – auf Signaturen untersuchen. Auch Programmierern kann diese Methode helfen, unkoschere Programm-Module zu erkennen. Wir schauen uns

zuerst an, warum Analyse-Websites bei diesem Problem eher selten weiterhelfen und erklären dann, wie Sie mit dem APK Library Scanner Apktool erfahren, was Sie wissen müssen.

Bekanntlich müssen Programmierer längst nicht mehr jede Zeile ihrer Codes selbst stricken – Programmbibliotheken gibt es schon ewig lange und man spart viel Zeit damit, bestimmte Funktionen einfach als löffelfertige Module einzubauen. Das ganze Drumherum einer App wird damit zur Nebensache und als Programmierer kann man sich zeitsparend auf den Punkt konzentrieren, weshalb man die App überhaupt entwickelt. Wenn man beispielsweise Geschäfte auf einer Karte in der App einblenden will, findet man über die Google-Maps-Plattform eine Programmierschnittstelle (Application Programming Interface, API) dafür, die man lediglich mit einigen Parametern bestücken muss, damit sie das tut, was sie soll. Aber die vorgefertigten Module für Google Maps sind nicht privatsphärenfreundlich. Nicht jeder kennt die Möglichkeit, stattdessen für mehr Datensparsamkeit OpenStreetMap einzubinden.

Nicht nur Google-Baukästen, sondern auch viele andere Programmierbausteine, die spezielle Fähigkeiten wie Datenbankinteraktionen, Bedienoberflächen, Dateioperationen und so weiter zuliefern, enthalten proprietäre Module, deren Quellcode sich nicht einsehen lässt – und deren Tätigkeit sich somit nicht einschätzen lässt.

Danaer, die Geschenke bringen

Schon Vergils Priester Laokoon in der Aeneis sagte, dass er die Danaer fürchte, auch wenn sie Geschenke tragen. Dass der Spruch auch heute noch gilt, weil so manche Apps in Googles Play Store trojanische Pferde sind – wer hätte das gedacht? Etwa die bei Google topbewerteten Apps von Cheetah Mobile. Das Mobilsicher-Blog von Mike Kuketz schaute genauer hin und kritisierte, dass die Antivirus-App aus diesem Stall im Hintergrund Traffic für Porno-Sites erzeugt. Eine weitere des gleichen Anbieters bringt durch Umleitungen Entwickler um Werbeeinnahmen.

Als Laie kann man das alles nicht erkennen, und App-Reviews auf etablierten Portalen gehen mit wenigen Ausnahmen nur auf Oberflächliches ein: grafische Gestaltung, Funktionsumfang und wie gut eine App funktioniert. Wie es um die Sicherheit der eigenen Daten bestellt ist, erfährt man selten. Und selbst wenn: Mit dem nächsten Update kann der Anbieter einen Datenschnüffler in die App eingeschleust haben, absichtlich oder aus Unwissenheit des Programmierers. Es gibt etliche Ansätze zur statischen Analyse von APK-Dateien. Sie ist wenig aufwendig, weil man dabei nicht die tatsächlichen Datenabflüsse mühselig durch Auswertung von Datenmitschnitten prüft, sondern schaut, welche Bibliotheken eine App nutzt.

Gefahrenzone: Tracker inside!

Wie findet man aber heraus, welche Module in einer App stecken? Da gäbe es zunächst einige Websites mit Analysefunktionen wie Exodus Privacy, AppBrain und Mobilsicher. Doch warum nicht da beginnen, wo man Apps kauft? Schon da gibt es eine (oder keine) Überraschung: Der Play Store von Google enthält gar keine Informationen über Tracker oder proprietäre Module in den angebotenen Apps. Anders etwa der alternative App-Store F-Droid, der das aber eher implizit macht: Seine Betreiber bezeichnen solche Eigenschaften als Anti-Features und bieten übergriffigen Apps erst gar kein warmes Plätzchen.

Auf den ersten Blick scheint die Website AppBrain.com mehr hilfreiche Infos über Tracker zu bieten. Sie listet für etliche Apps die verwendeten Bibliotheken auf, unterscheidet darin aber nicht nach guten und privatsphärenschädlichen Modulen. Sie werden zwar in Kategorien wie „Werbenetzwerke“, „Soziale Netze“ und „Entwicklungs-Tools“ eingeteilt, Tracking-Module werden aber nicht explizit als solche ausgewiesen. Man muss sich schon ziemlich gut auskennen, um das reichlich datenhungrige Facebook-



Einige Apps, die die Analyse-Website Exodus Privacy untersucht hat, weisen mehr als 50 Tracker auf, so diese Beauty-App.

SDK im Bereich „Soziale Netze“ als übergriffig zu identifizieren. Ähnliches gilt für Flurry, ein sehr übergriffiger Analysedienst, der harmlos unter „Entwicklungs-Tools“ einsortiert ist. Dem Urteil ist also nicht zu trauen, auch deswegen nicht, weil die Website eigentlich dazu gedacht ist, die Monetarisierung von Apps zu fördern.

Besser sieht es da bei der Website von Exodus Privacy aus: Exodus Privacy ist ein Dienst, der sich dem Aufspüren von Tracking-Modulen in Android Apps verschrieben hat [1]. Darin finden sich Apps, die mehr als 50 Tracking-Module enthalten. Zu den jeweiligen Modulen sind außerdem teilweise recht umfangreiche Informationen hinterlegt. Apps, die dem Dienst noch nicht bekannt sind, kann man zur Analyse einreichen.

Klar, man könnte sich selbst auf die Suche nach Trackern machen, aber die schiere Größe heutiger Apps macht das immer schwieriger. Nannte man anno Schnee Apps mit mehr als 100 Kilobyte ziemlich groß, so bläht Ballast aller Art – darunter laut Exodus Privacy auch 25 Tracker – schon eine simple, aber topbewertete Wecker-App wie Alarmy auf satte 248 Megabyte auf.

Schaut man sich an, von wem die meisten Tracking-Module in Apps stammen, enthält die Statistik von Exodus Privacy als Top-10 ausschließlich Module von Google und Facebook. Erst mit weitem Abstand folgen Schnüffelmodule anderer Firmen.

Exodus berücksichtigt in seinen Reports nur, ob eine App Signaturen enthält, die bekanntermaßen Trackern zugeordnet werden können. Es kann nicht erkennen, ob die Module in der App aktiv genutzt werden. Exodus Privacy ist auch blind für andere proprietäre Bestandteile von Apps. Proprietär heißt, dass der Quellcode nicht öffentlich einsehbar ist. Wer als Programmierer solche Fremdmodule ohne Einblick in den Quelltext verwendet, muss schon viel Vertrauen in die Entwickler haben. Als Nutzer ist man ihnen ebenso ausgeliefert.

Exodus Privacy untersucht nur kostenlose Apps, die im Google Play Store oder bei F-Droid zu finden sind. Das spendenfinanzierte Projekt kann sich nicht leisten, auch kostenpflichtige oder nur in bestimmten Ländern verfügbare Apps zu untersuchen. Auch APK-Dateien, also Android-Programmpakete, die man aus anderer Quelle heruntergeladen oder als Programmierer selbst erstellt hat, untersucht Exodus Privacy leider nicht.

Einen ähnlichen Fokus hat auch die Website appcheck.mobilsicher.de. Auf ihr sind zahlreiche Apps zu finden, die durch einen automatischen Analysepro-



Die Top Ten der von der Website Exodus Privacy im Play Store gefundenen Tracker werden komplett durch Module von Facebook und Google abgedeckt.

zess geschleust und von Experten kritisch seziert wurden – etwa bezüglich ihrer Hintergrundaktivitäten und auf ihre Datenzugriffe und -übertragung, ob diese verschlüsselt werden und mehr. Auch der Appcheck berücksichtigt nur Apps aus F-Droid und aus dem Google Play Store.

Was soll man aber tun, wenn man die App als APK aus einer anderen Quelle hat, etwa von der Entwickler-Website? Und was kann ein Entwickler tun, um ein Modul, das er in einer App einsetzen will, auf potenzielle Schädlinge abzuklopfen? LibRadar, ein Python-Tool dafür, wird leider seit 2018 nicht mehr weiterentwickelt. Androguard ist das Mittel der Wahl bei Exodus und auch bei F-Droid. Classyshark wird ebenfalls von vielen Tools als Grundlage verwendet.

Praxis: Library Scanner to the rescue

Im Folgenden stellen wir die Arbeit mit dem Library-Scanner Apktool vor. Er ist vergleichsweise einfach zu installieren und verbreitet, etwa im IssueBot von F-Droid. Wie vergleichbare Werkzeuge nimmt er APK-Dateien zunächst so weit auseinander, dass man ihre Bestandteile erkennen kann. Um bestimmte Fremdmodule wiederzuerkennen, benötigt man dann noch eine Datenbank mit Library-Spezifikationen. APKs bekommt man zum Beispiel aus Quellen

wie der Website APKMirror.com oder direkt vom Entwickler. Mit einigen von Google nicht gern gesehenen Tricks kann man Apps auch als APK aus dem Google Play Store herunterladen.

Apktool steckt in einer JAR-Datei und benötigt zum Ausführen eine Java-Runtime. Man muss nicht unbedingt einen Linux-Rechner benutzen, es gestaltet sich aber bequemer. Da Apktool problemlos in einer virtuellen Umgebung wie VirtualBox mit einer geeigneten Linux-Distribution läuft, sollte man sich das selbst dann antun, wenn man ansonsten lieber auf anderen Betriebssystemen unterwegs ist. Mit der WSL-Umgebung von Windows könnte man ebenfalls arbeiten, wenn man mit den Eigenheiten vertraut ist; eine virtuelle Maschine ist bequemer.

Java sollte zumindest als Runtime-Version vorhanden sein. Notfalls installiert man Java nach Aufruf der Konsole mit `sudo apt install -y default-jdk` nach. Auch danach bewegt man sich auf der Kommandozeile. Mit `mkdir test` erstellen Sie einen Ordner und wechseln mit `cd test` dorthin. Mit

```
wget https://github.com/iBotPeaches/↵
↳Apktool/releases/download/v2.6.0/↵
↳apktool_2.6.0.jar
```

und

```
wget https://github.com/iBotPeaches/↵
↳Apktool/raw/master/scripts/linux/↵
↳apktool
```

laden Sie das Handwerkszeug. Mit `chmod u+x apktool` setzt man die Zugriffsrechte und das Kommando `ln -s apktool_2.6.0.jar apktool.jar` erzeugt einen Link.

Eine APK-Datei, die unters Mikroskop soll, muss nur noch in den eingangs angelegten Ordner kopiert werden und nach Eingabe von `apktool d APKName.apk` – wobei `APKName` durch den Namen der APK ersetzt wird – erhält man nach einigen Sekunden Wartezeit ein Verzeichnis mit dem Namen der APK-Datei. Darin befindet sich unter anderem das Ver-

Literatur

[1] Michael Link, Andreas Itzchak Rehberg, **Trackerentdecker**, Tracker in Android Apps finden, c't 11/2019, S. 182

Internetausfälle kompensieren:

Multi-Access-Netze für KMU | Termine: 14.06.2022, 08.11.2022

c't WORKSHOP



Heutzutage ist jede Firma auf eine funktionierende Internetanbindung angewiesen. E-Mails, der Zugriff auf Partnernetzwerke, Recherchen, die eigene Standortvernetzung. Fällt die Internetanbindung aus, und sei es nur für wenige Stunden, „steht" oftmals der ganze Betrieb.

Der Workshop vermittelt einen Überblick über **aktuelle Techniken zu redundanten Internet-Anbindungen** von Firmenstandorten.

- Vorstellung unterschiedlicher Access-Technologien
- Unterschiede IPv4/IPv6
- Redundanzverfahren
- Konvergenzzeiten

heise-events.de/workshops/multi-access-netze

zeichnis „smali“. Darüber lassen sich die in der App verwendeten Bibliotheken ermitteln. Benutzt eine App beispielsweise Google Mobile Services, gibt es ein Verzeichnis namens APKName/smali/com/google/android/gms.

Es deutet sich an, dass es ganz schön mühsam wäre, jeden der Smali-Ordner durchzuklicken und auszuwerten. Denn man müsste ja auch wissen, wie die Pakete heißen, nach denen man suchen muss. Das lässt sich mithilfe von Library-Definitionen erledigen. Sie ordnen den jeweiligen Pfaden Modulnamen und weitere Details zu.

Mit Library-Definitionen das Leben erleichtern

Eine Sammlung von Library-Definitionen sowie ein Wrapper-Skript, das die Ausgaben im Smali-Ordner damit abgleicht, finden sich im nachfolgend genannten GitLab-Repository. Das Skript selbst setzt eine Kommandozeilenversion von PHP einschließlich des zugehörigen JSON-Paketes voraus. Die bekommen Sie mit `sudo apt install php-cli php-json`. Man kann natürlich genauso gut auch einfach mit `sudo apt-get install php` eine Komplettinstallation auf die Maschine packen.

Die Library-Definitionen werden im Schnitt ein- bis zweimal monatlich aktualisiert. Um sie einfach auf dem aktuellen Stand halten zu können empfiehlt es sich, das Repo zu klonen:

```
git clone https://gitlab.com/↵
↳IzzyOnDroid/repo.git
```

Danach erstellen Sie mit `mkdir -p repo/lib/radar/tool` einen Ordner und verschieben das Apktool mit `mv test/apktool* repo/lib/radar/tool` hinein. Mit einem Alias wird der Aufruf noch etwas bequemer, weil man sich damit wiederholtes Tastaturgeklimper spart.

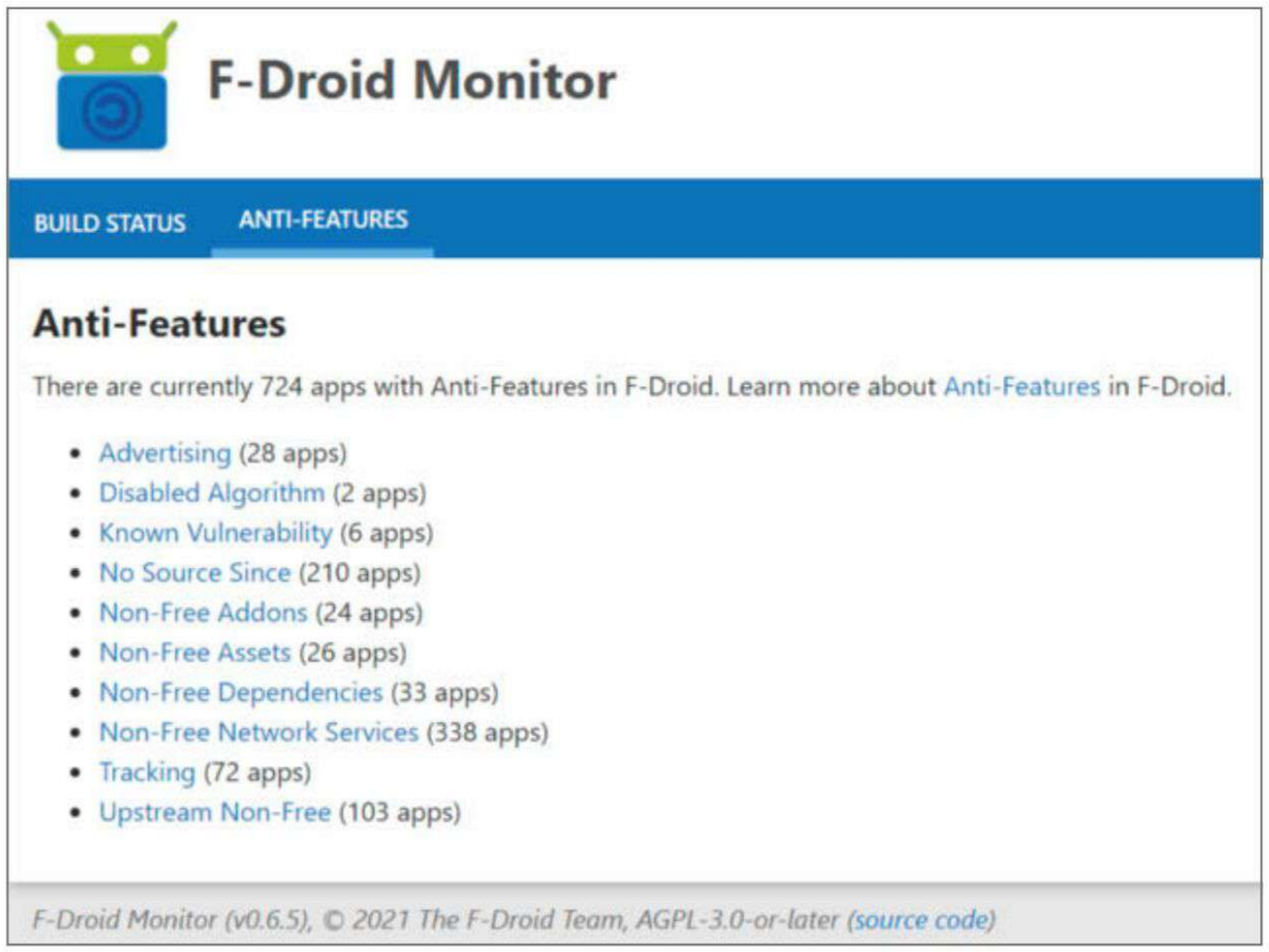
```
alias scanapk=↵
↳$(pwd)/repo/bin/scanapk.php
```

Eine Android-App als APK lässt sich nun ganz einfach abklopfen, wie dieses Beispiel illustriert:

```
No libsmali.txt entry for /com/shaded/fasterxml/jackson, this library will be ignored.
Libraries detected:
------------------
* Android Design Support Library (/android/support/design): Utility
* Android Support v4 (/android/support/v4): Development Framework
* Android Support v7 (/android/support/v7): Development Framework
* Androidx Core (/androidx/core): Utility
* Media (/androidx/media): Utility
* Butter Knife (/butterknife): Utility
* Material Dialogs (/com/afollestad/materialdialogs): UI Component
* Glide (/com/bumptech/glide): Utility
* Google Ads (/com/google/ads): Advertisement Ads
* FlexboxLayout (/com/google/android/flexbox): Utility
* Google Mobile Services (/com/google/android/gms): Development Framework NonFreeDep
* Firebase (/com/google/firebase): Utility NonFreeNet,NonFreeDep
* Firebase Analytics (/com/google/firebase/analytics): Mobile Analytics Tracking
* Google Gson (/com/google/gson): Utility
* SnappySmoothScroller (/com/nshmura/snappysmoothscroller): UI Component
* ShineButton (/com/sackcentury/shinebuttonlib): UI Component
* RecyclerView-FastScroll (/com/simplecityapps/recyclerview_fastscroll): UI Component
* Android Sliding Up Panel (/com/sothree/slidinguppanel): UI Component
* OkHttp (/com/squareup/okhttp): Utility
* Android Image Cropper (/com/theartofdev/edmodo/cropper): Utility
* AVLoadingIndicatorView (/com/wang/avi): UI Component
* MaterialProgressBar (/me/zhanghai/android/materialprogressbar): UI Component
* jsoup (/org/jsoup): Utility
* Calligraphy (/uk/co/chrisjenx/calligraphy): Utility Offending libs:
---------------
* Google Ads (/com/google/ads): Ads
* Google Mobile Services (/com/google/android/gms): NonFreeDep
* Firebase (/com/google/firebase): NonFreeNet,NonFreeDep
* Firebase Analytics (/com/google/firebase/analytics): Tracking

4 offenders.
```

Das Wrapper-Skript liefert eine Ausgabe der gefundenen Tracker und wie sie zu klassifizieren sind.



F-Droid führt Statistiken über seine Apps mit unerwünschten „Anti-Features“. Auch die Beschreibungen der Apps enthalten Hinweise darauf.

```
scanapk com.bhandari.music_190.apk
```

Das Skript zerpflückt in einem Rutsch die APK-Datei mithilfe des Apktools und klassifiziert die enthaltenen Komponenten. Als Ausgabe erzeugt es eine ausführliche Ausgabe mit einer Liste aller identifizierten Bibliotheken und Module; als kritisch bekannte werden am Ende nochmals zusammengefasst. Die Abkürzungen am Zeilenende erklären, warum sie die Alarmglocken auslösen.

Die Kürzel werden ganz ähnlich auch im alternativen App-Store F-Droid verwendet, um Apps mit sogenannten Anti-Features, also unerwünschten Eigenschaften zu markieren. Leicht abweichend von der dortigen Beschreibung bedeutet das Kürzel „NonFreeDep“ in der Auswertung des Library Scanners jedoch, dass das entsprechende Modul selbst „unfrei“ ist – was bei den Bibliotheken Google Mobile Services sowie Firebase unmittelbar einleuchtet.

Details zu den aufgespürten Modulen lassen sich übrigens in der Datei lib/libinfo.txt finden, wenn man dort nach `"id": "<PaketName>"` sucht, also beispielsweise nach `"id": "/com/google/firebase"`.

Ausblick

Mit dem Library Scanner können Benutzer Informationen darüber gewinnen, ob suspekte Bibliotheken in einer App stecken. Und das kann das Tool auch mit Apps tun, bei denen herkömmliche Analyse-Websites in der Regel blind sind: bei kostenpflichtigen Apps und Apps, die nicht im Google Play Store angeboten werden. Auch Programmierer kann ein Library Scan davor schützen, vielleicht unwissentlich ihren Apps Spionagefunktionen zu verpassen und später deswegen einen Shitstorm zu ernten. Zwar ist nicht gesagt, dass bei den gefundenen Bibliotheken die Schnüffelei tatsächlich aktiv ist, doch immerhin wird klar, womit man rechnen muss. Noch schöner wäre es freilich, wenn man das ohne Aufwand im Google Store sehen könnte. (mil) c't



Mit Matrix selbst Chatserver betreiben

Ein eigener Chatserver bietet viele Vorteile, von schicken Benutzernamen mit der eigenen Domain bis zur Unabhängigkeit von Messenger-Anbietern und deren zweifelhaften Datenschutzversprechen. Das Matrix-System lässt kaum Wünsche offen und mit den richtigen Hilfsmitteln kommt man schnell zum voll einsatzbereiten Server.

Von **Sylvester Tremmel**

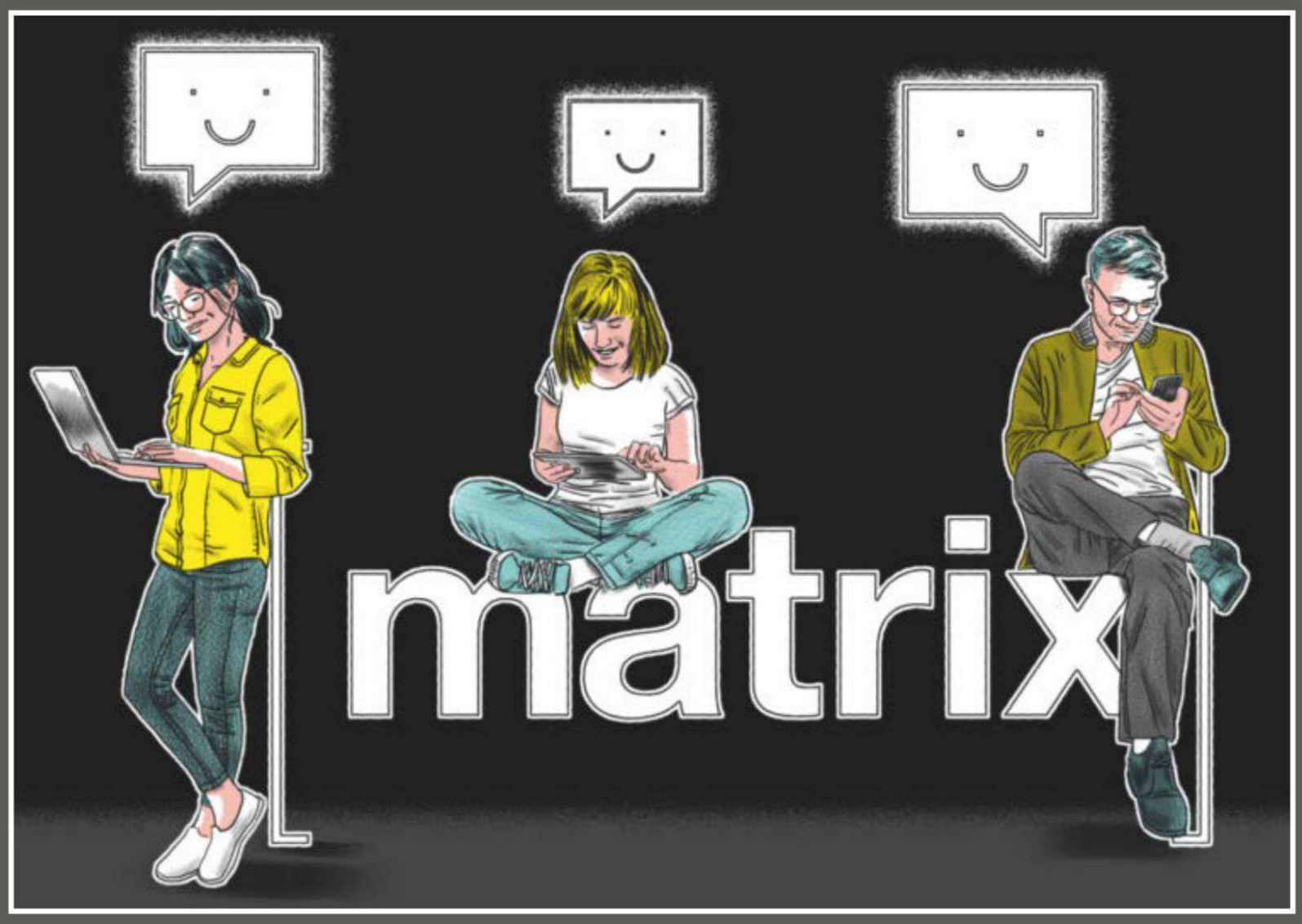


Bild: Thomas Kühlenbeck

Mit Matrix selbst Chatserver betreiben	100
Andere Messenger an Matrix anbinden	108

Das Messaging-Protokoll Matrix bietet den typischen Funktionsumfang von Instant Messengern wie WhatsApp, Signal oder Telegram. Dazu gehören Ende-zu-Ende-Verschlüsselung, Individual- und Gruppenchats sowie Sprach- und Videoanrufe. Anders als bei den meisten Alternativen kann man mit Matrix aber eigene Chatserver betreiben – und ist auf diesen keineswegs isoliert. Denn Matrix-Server föderieren, das heißt, Nutzer beim Anbieter A können auch mit Nutzern vom Anbieter B sprechen, wie bei der guten alten E-Mail.

Wer Matrix einfach nur benutzen will, braucht lediglich eine Client-App (die am weitesten verbreitete heißt Element) und einen Account bei einem offenen Matrix-Server wie matrix.org. Wer stattdessen ohne großen Aufwand einen eigenen Server haben will, kann sich an spezialisierte Hoster wenden, die alles von der kleinen Lösung für Familie und Freunde bis zum On-Premise-Hosting für große Unternehmen offerieren.

Günstiger, datenschutzfreundlicher und vor allem interessanter ist es aber, Matrix selbst auf einem Server zu installieren. Die Referenzimplementierung des Protokolls heißt Synapse, eine Python-Applikation.

Installationsvielfalt

Synapse findet sich in den Repositorys zahlreicher Linux-Distributionen, für Debian und Ubuntu stellen die Entwickler auch ein Repo mit eigenen – aktuelleren – Paketen zur Verfügung. Alternativ dazu gibt es Docker-Images, und sogar als Python-Modul aus dem Python Package Index (PyPI) kann man die Software installieren.

Besonders gut gefallen hat uns aber ein vom Entwickler Slavi Pantaleev ins Leben gerufenes Ansible-Playbook, auf das auch die offizielle Synapse-Dokumentation verweist (alle Links unter ct.de/waef). Das Konfigurationsmanagement- und Softwareverteilungssystem Ansible haben wir in c't 7/2021 ausführlich erklärt [1, 2], aber um das Playbook zu benutzen, sind keine nennenswerten Kenntnisse darüber erforderlich. Pantaleevs Playbook nutzt Docker-Images, bietet gegenüber der manuellen Installation aber einen ganz entscheidenden Vorteil: Es kümmert sich um sämtliches Drumherum.

Damit ein Matrix-Server gut läuft, braucht man nämlich mehr als nur Synapse. Fast zwingend nötig ist zum Beispiel eine PostgreSQL-Datenbank, in der Synapse seine Daten verwaltet. Der ins Programm eingebaute Notnagel SQLite dient nur zum Testen. Ein Webserver als Reverse-Proxy wird ebenfalls empfohlen, wie auch ein STUN- und TURN-Server und einiges mehr.

All das lässt sich von Hand installieren, aber vor allem die Konfiguration der Komponenten wird schnell aufwendig. Das Ansible-Playbook bringt dagegen alle nötigen Dienste mit. Standardmäßig installiert das Playbook Folgendes:

- den eigentlichen Matrix-Server **Synapse**;
- **PostgreSQL** als Datenbank für Synapse;
- den TURN- und STUN-Server **coturn**, der hilft, die Tücken der Netzwerkadressübersetzung (NAT) zu umgehen und so zuverlässige Audio- und Videotelefonate ermöglicht;
- die Web-Version des Matrix-Clients **Element**, damit man direkt im Browser drauflos chatten kann;
- **SSL/TLS-Zertifikate** von Let's Encrypt, um die Verbindungen zu Synapse und Element abzusichern;
- den Mailserver **Exim**, der sich um Bestätigungsmails und dergleichen kümmert;
- den Webserver **Nginx**, der als Reverse-Proxy anderen Services vorgelagert wird.

Diese Dienste packt das Playbook in Docker-Container und konfiguriert sie passend. Daneben können Sie noch Dutzende weitere Services aus dem Matrix-Umfeld einrichten, eine Liste finden Sie im GitHub-Projekt des Playbooks. Wer so einen weiteren Service nutzen will, muss in der Regel nur ein paar Playbook-Optionen setzen, um ihn einzurichten. Genauso kann man die Standarddienste abschalten, zum Beispiel, weil man bereits einen Webserver hat, der als Reverse-Proxy fungieren soll.

Voraussetzungen

Um Synapse mit dem Playbook zu installieren, benötigen Sie einen Linux-Server mit installiertem Python 3. Auf den Server sollten Sie SSH-Zugriff haben, entweder mit dem Benutzer „root" oder mit einem Benutzer, der per `sudo` Root-Rechte erlangen kann.

Um auch größere Chaträume zu bewältigen, raten die Playbook-Autoren zu mindestens zwei Gigabyte RAM, vier sind besser. Zur Not tut es aber sogar ein Raspberry Pi, der allerdings schnell an seine Grenzen kommen kann. Das Playbook kommt mit den Distributionen CentOS 7, Debian 10 oder neuer, Ubuntu 18.04 oder neuer sowie Arch Linux klar.

Ansible installieren Sie idealerweise auf dem eigenen PC. Dort führen Sie das Playbook aus, das sich dann per SSH mit dem Server verbindet und

darauf Matrix einrichtet. Windows-Nutzer können entweder Ansible im Windows Subsystem for Linux (WSL) einrichten oder Ansible stattdessen direkt auf dem Server installieren, den es dann lokal konfiguriert. Letzteres ist eventuell auch eine Option, wenn man nicht per SSH an den Server kommt.

Außerdem brauchen Sie eine Domain, deren DNS-Einträge Sie konfigurieren können, damit der Server darüber erreichbar ist. Das bedarf etwas Vorüberlegung, denn die Domain können Sie später nicht einfach anpassen. Die Benutzernamen von Matrix-Accounts sind ganz ähnlich wie Mailadressen aufgebaut: Ein Teil identifiziert den Nutzer, der andere Teil den Server, zu dem der Account gehört. Nur das Format von Matrix-Namen unterscheidet sich von Mailadressen:

```
@benutzername:example.com
```

Die Benutzernamen vergeben Sie später nach Belieben, aber wie und unter welcher Domain Ihr Matrix-Server erreichbar sein soll, müssen Sie vorher festlegen. Unter Ihrer Domain ist häufig bereits ein anderer Dienst erreichbar – etwa ein klassischer Webserver, der die eigene Homepage ausliefert. Damit sich dieser Dienst und Matrix nicht ins Gehege kommen, weicht man dann in der Regel auf eine Subdomain wie matrix.example.com aus oder nutzt eine ganz andere Domain. Man kann trotzdem dafür sorgen, dass die Account-Namen auf die Hauptdomain enden. Damit das klappt, müssen Sie aber beide Domains und auch den Server hinter der Hauptdomain konfigurieren dürfen.

Alternativ dazu können Sie eine dedizierte Domain für Ihren Server und die Account-Namen nutzen (à la example-matrix.org) oder eben in Kauf nehmen, dass die Subdomain auch in den Account-Namen auftaucht (à la @benutzername:matrix.example.com).

In jedem Fall müssen Sie für die gewählte Domain einen A-Record setzen, sodass sie auf die IPv4-Adresse Ihres Servers auflöst; IPv6 unterstützt das Playbook noch nicht. Für manche optionalen Zusatzdienste müssen Sie außerdem eigene Subdomains mit CNAME-Records konfigurieren. Ein Beispiel dafür beschreiben wir weiter unten.

Buch herunterladen

Anschließend können Sie sich das Ansible-Playbook herunterladen und konfigurieren. Am besten erledigen Sie das über das Versionsverwaltungssystem Git mit folgendem Befehl:

```
git clone https://github.com/spantaleev/↵
  ↳matrix-docker-ansible-deploy.git
```

Diese Methode bietet den Vorteil, dass Sie sich dann über `git pull` immer die aktuellste Version des Playbooks besorgen können, was bei Updates hilft. Ohne Git können Sie das Playbook auch einfach als Zip-Datei herunterladen und entpacken.

Beide Wege führen zu einem neuen Verzeichnis, das Sie in einem Terminal öffnen. Alle folgenden Befehle werden aus diesem Verzeichnis heraus abgesetzt.

Wer sich ein wenig umschauen will: Im Unterverzeichnis roles befindet sich ein Ordner für jeden Service, den das Playbook konfigurieren kann. Innerhalb dieser Ordner befindet sich jeweils eine Datei defaults/main.yml mit einer kommentierten Standardkonfiguration für den jeweiligen Service. So lernt man schnell den Funktionsumfang des Playbooks kennen. Interessant ist zum Beispiel die Datei matrix-base/defaults/main.yml, die einige allgemeine Standardeinstellungen festlegt. Eine Einstiegshilfe für die diversen Services bietet die Dokumentation des Playbooks, die Sie als Markdown-Dateien im Ordner docs finden.

Die Einstellungen in den main.yml-Dateien haben nur den einzelnen Service im Auge. Das Playbook selbst überschreibt sie daher teilweise mit Werten, die für das Zusammenspiel der Services geeigneter sind. Das geschieht in der Datei group_vars/marix_servers. Die deaktiviert auch einen Großteil der Services, sodass sie standardmäßig nicht installiert werden.

In einem dritten Schritt wertet Ansible eine benutzerspezifische Konfigurationsdatei aus, sodass Sie die Vorgaben des Playbooks überschreiben können. Diese Konfigurationsdatei müssen Sie anlegen, indem Sie im Verzeichnis inventory/host_vars einen Ordner erstellen, den Sie nach Ihrer Domain benennen. Anschließend kopieren Sie eine Beispielkonfiguration als Startpunkt in den Ordner:

```
mkdir inventory/host_vars/matrix.example.com
cp examples/vars.yml ↵
  ↳inventory/host_vars/matrix.example.com/
```

Buch konfigurieren

Die Kopie von vars.yml können Sie jetzt in einem beliebigen Editor öffnen und anpassen. Sie enthält ausführliche Kommentare (Zeilen, die mit einer Raute beginnen), aber lediglich fünf Optionen:

```
matrix_domain:
matrix_homeserver_implementation:
matrix_homeserver_generic_secret_key:
matrix_ssl_lets_encrypt_support_email:
matrix_postgres_connection_password:
```

Die `matrix_homeserver_implementation` können Sie ignorieren, da die Option bereits Synapse als Server-Software definiert. Die anderen Optionen müssen Sie anpassen, alles Weitere hängt von Ihren Wünschen ab. Zentral ist die erste Einstellung, `matrix_domain`, mit der Sie den Domainnamen festlegen, der Ihre Matrix-Accounts identifiziert. Achtung, das Playbook leitet standardmäßig weitere Domainnamen daraus ab, indem es Subdomains ergänzt. Wenn Sie also beispielsweise „example.com“ angeben, weil Sie Benutzernamen wie „@benutzer:example.com“ haben möchten, dann geht das Playbook davon aus, dass der Matrix-Server unter „matrix.example.com“ erreichbar sein soll. Wenn das nicht stimmt (etwa weil Sie eine Domain exklusiv für Matrix nutzen oder weil Sie die volle Subdomain auch in den Benutzernamen haben möchten), dann müssen Sie lediglich die Server-Domain zusätzlich angeben, indem Sie eine Option ergänzen:

```
matrix_server_fqn_matrix: example.com
```

Solche Optionen mit „server_fqn“ (fully-qualified name) gibt es auch für andere Dienste, für die das Playbook standardmäßig Subdomains annimmt. Eine Liste dieser Optionen finden Sie in der erwähnten Datei roles/matrix-base/defaults/main.yml.

Die Option `matrix_ssl_lets_encrypt_support_email` benutzt das Playbook, wenn es SSL/TLS-Zertifikate von Let’s Encrypt ausstellen lässt. Falls dabei (oder bei einer späteren Zertifikatsverlängerung) etwas schiefgeht, kann Let’s Encrypt Sie über die angegebene Mailadresse informieren. Sie sollten also eine Adresse angeben, unter der Sie auch erreichbar sind, sie erscheint nicht öffentlich einsehbar im Zertifikat.

Wer Let’s Encrypt nicht nutzen möchte, setzt die Option `matrix_ssl_retrieval_method` auf den Wert `manually-managed` und beschafft die Zertifikatsdateien anderweitig. Die Datei docs/configuring-playbook-ssl-certificates.md erklärt die Details. Diese Option gestattet außerdem den Wert `none`, damit sich das Playbook überhaupt nicht um SSL/TLS kümmert, und den Wert `self-signed`. Bei letzterem generiert das Playbook eigene Zertifikate, die mangels Signatur durch eine vertrauenswürdige Stammzertifizierungsstelle aber nur für den nicht-öffentlichen Gebrauch taugen.

Die verbleibenden zwei Optionen enden auf „secret_key“ und „password“. Es handelt sich um Werte, die die Kommunikation zwischen den verschiedenen Services absichern. Die Werte können Sie frei festlegen, aber Sie sollten nicht irgendwas eintragen, sondern sichere Passwörter. Die können Sie zum Beispiel mit einem Passwortmanager generieren, das Playbook rät zu Werten, die aus 64 zufälligen Zeichen bestehen.

Alles kann, nichts muss

Damit haben Sie die notwendige Konfiguration abgeschlossen, alles Weitere ist optional. Wenn auf dem Server zum Beispiel Docker bereits installiert ist, verhindert `matrix_docker_installation_enabled: false`, dass das Playbook eine weitere Instanz installiert.

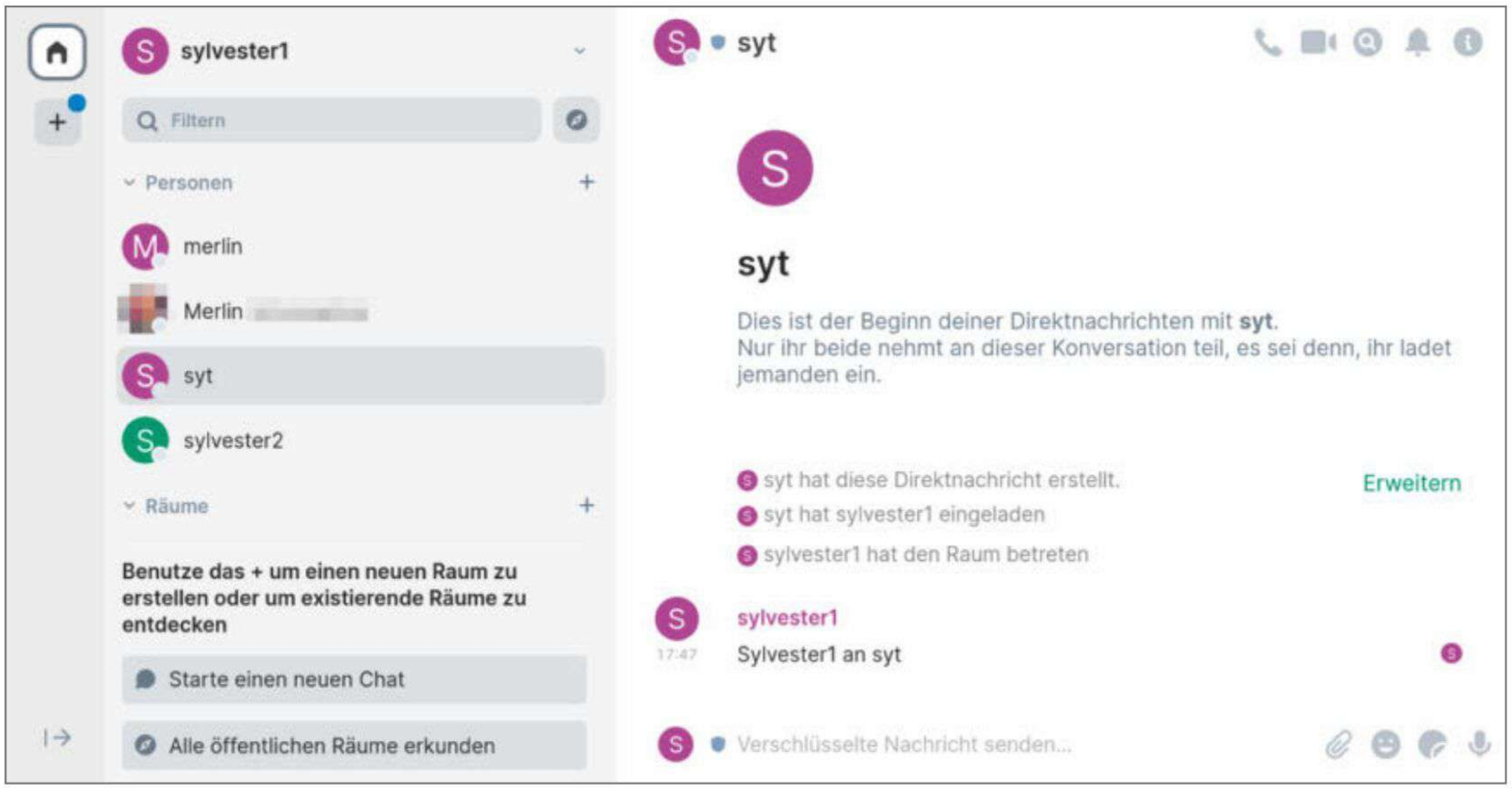
Falls Sie keinen Wert auf den Element-Webclient legen, können Sie ihn per `matrix_client_element_enabled: false` abschalten. Wenn Sie das nicht tun, versucht das Playbook, den Client unter der Subdomain „element“ bereitzustellen. Damit das klappt, sollten Sie einen CNAME-Eintrag im DNS vornehmen, der diese Subdomain auf Ihren Matrix-Server umleitet, sodass zum Beispiel element.example.com auf matrix.example.com zeigt.

Falls Sie Element unter einer anderen Domain betreiben wollen, geben Sie die einfach in der Option `matrix_server_fqn_element` an. Zu so einer Domaintrennung raten die Synapse-Entwickler; sie hilft, Cross-Site-Scripting-Attacken zu verhindern.

Für Server mit mehr als einer Handvoll Accounts kann es sinnvoll sein, ein Web-UI zur Account-Verwaltung zu aktivieren. Setzen Sie dafür einfach die Option `matrix_synapse_admin_enabled` auf `true`.

Falls Sie Ihren Server nur für interne Chats verwenden wollen, schalten Sie die Föderation per `matrix_synapse_federation_enabled: false` ab. Nutzer Ihres Servers können dann nicht mit Nutzern anderer Matrix-Server chatten.

Außerdem müssen Sie sich überlegen, ob Sie einen Identity-Server betreiben wollen. Das Playbook kann dafür eine Anwendung namens ma1sd installieren. Identity-Server dienen dazu, dass Matrix-Nutzer Mailadressen oder Telefonnummern über ihre Clients in ihrem Account hinterlegen können. Anhand dieser Information finden Freunde die Nutzer dann, ohne den Matrix-Accountnamen zu kennen. Wenn Sie daran Bedarf haben, aktivieren Sie



Auf Wunsch installiert das Playbook auch einen Webclient für Matrix.

ma1sd per `matrix_ma1sd_enabled: true`. Details zu ma1sd finden Sie in der Datei docs/configuring-playbook-ma1sd.md.

Matrix starten

Wenn Sie das Playbook nach Gusto konfiguriert haben, ist es Zeit, die Einrichtung auf dem Server anzustoßen. Kopieren Sie dafür die Datei examples/hosts nach inventory/hosts und öffnen Sie die Kopie in einem Editor. Über inventory/hosts teilen Sie dem Playbook mit, auf welchem Server es Matrix einrichten soll. Das geschieht in der letzten Zeile der Datei, der Rest ist erklärender Kommentar. Ersetzen Sie dort „matrix.<your-domain>“ durch die Domain Ihres Matrix-Servers und „<your-server's external IP address>“ durch die IP-Adresse des Servers:

```
matrix.example.com ansible_host=123.234.123.234 ↵
  ↳ansible_ssh_user=root
```

Falls Sie sich per SSH nicht direkt als root einloggen können, ersetzen Sie `ansible_ssh_user=root` durch `ansible_ssh_user=BENUTZER become=true become_user=root`. Statt `BENUTZER` müssen Sie einen Usernamen angeben, der per `sudo` Root-Rechte erlangen kann. Wenn Sie das Ansible-Playbook nicht auf einem PC, sondern auf dem Server selbst ausführen, sollten Sie noch die Option `ansible_connection=local` an die Zeile anhängen.

Anschließend können Sie das Playbook mit folgenden Befehl ausführen:

```
ansible-playbook -i inventory/hosts ↵
  ↳setup.yml --tags=setup-all
```

Wenn Sie Ihre SSH-Verbindung per Passwort absichern, sollten Sie beim obigen Befehl noch die Option `--ask-pass` ergänzen. Und wenn Sie sich nicht direkt als root verbinden, die Option `--ask-become-pass`, um das Passwort für `sudo` abzufragen.

Das Playbook installiert und konfiguriert nun alles Gewünschte, ein Vorgang, der durchaus ein paar Minuten dauert. Am Ende steht hoffentlich eine Zeile, die diverse Tasks als „ok“ oder „changed“ ausweist und keine als „unreachable“ oder „failed“. Eine hohe Zahl an „skipped“-Tasks ist normal, schließlich sind viele Services standardmäßig abgeschaltet.

Falls etwas schiefgeht, generiert das Playbook in der Regel aussagekräftige Meldungen, die bei der Fehlersuche helfen. Wenn Sie den Fehler behoben haben, führen Sie den obigen Befehl einfach noch mal aus. Das können Sie ohnehin jederzeit tun, zum Beispiel, nachdem Sie die Konfiguration geändert haben. Mit einem neuen Durchlauf sorgt das Playbook dann dafür, dass die Server-Installation wieder mit der Konfiguration übereinstimmt. So können Sie auch leicht mit einem eher minimalen Matrix-Server anfangen und nach und nach weitere Services hinzufügen.

Wenn die Installation (oder Umkonfiguration) erfolgreich verlief, starten Sie über Ansible alle Services:

```
ansible-playbook -i inventory/hosts ↵
  ↳setup.yml --tags=start
```

Nacharbeiten

Im Grunde ist der Matrix-Server jetzt fertig. Um ihn zu benutzen, müssen sie aber zumindest einen (Admin-)Account einrichten. Auch das geht per Playbook:

```
ansible-playbook -i inventory/hosts ↵
  ↳setup.yml --extra-vars='username=↵
  ↳BENUTZER password=PASSWORT ↵
  ↳admin=yes' --tags=register-user
```

`BENUTZER` und `PASSWORT` müssen Sie natürlich gegen den gewünschten Benutzernamen und Passwort austauschen.

Mit obigem Befehl können Sie auch weitere Nutzer einrichten, per `admin=no` auch ohne Admin-Rechte. Wenn Sie das Web-UI zur Accountverwaltung eingerichtet haben, geht das allerdings bequemer im Browser über https://matrix.example.com/synapse-admin/. Dort können Sie sich mit Ihrem Admin-Account anmelden und alle weiteren Benutzer über die grafische Oberfläche anlegen.

Außerdem müssen Sie sich noch um eine Weiterleitung kümmern, falls die Domain Ihres Servers eine andere ist als die, die in den Accountnamen steht. Wenn also zum Beispiel der Server unter „matrix.example.com“ läuft, aber Benutzernamen aussehen wie „@benutzer:example.com“. Ohne so eine Weiterleitung kontaktieren Matrix-Clients und föderierende Server example.com, finden dort keinen Matrix-Server und wissen nicht, dass sie unter matrix.example.com nachsehen müssen. Wenn sich die Domains in Ihrem Fall nicht unterscheiden, können Sie die nächsten beiden Absätze ignorieren.

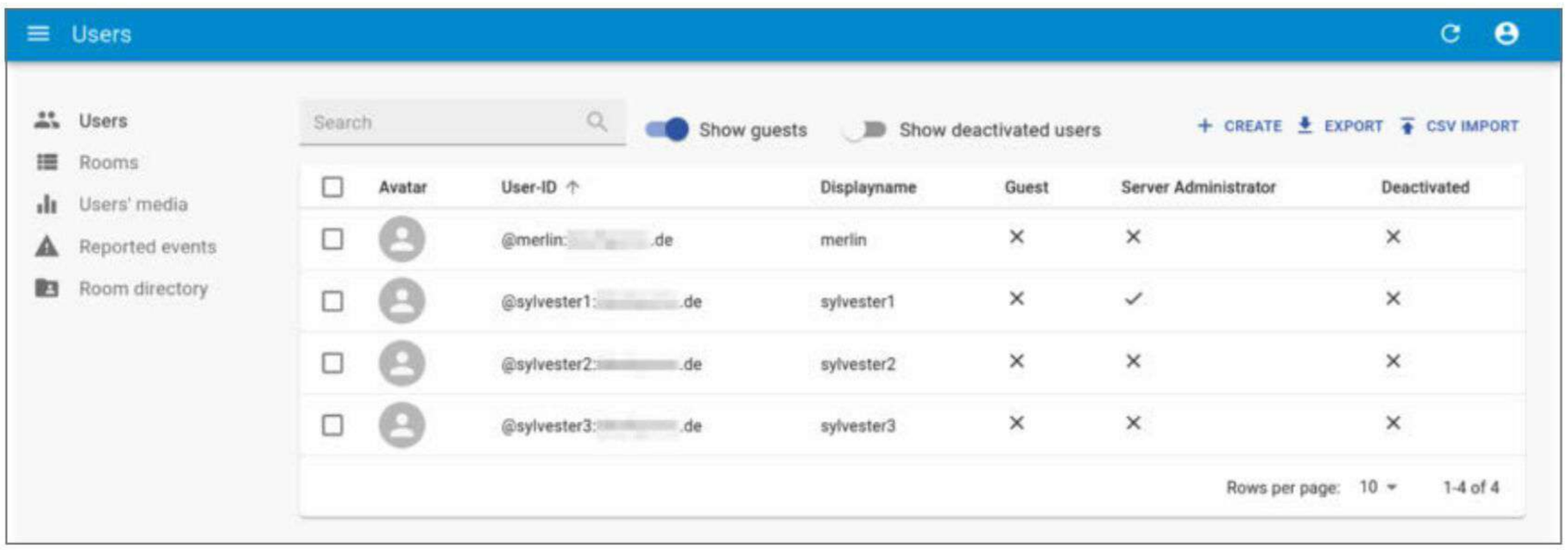
Am einfachsten erfolgt die Weiterleitung über zwei .well-known-Dateien, die unter der Account-Domain erreichbar sein müssen, im Beispiel also unter https://example.com/.well-known/matrix/. Die Dateien heißen client und server und enthalten die nötigen Informationen für Matrix-Clients und föderierende Server. Das Playbook generiert automatisch zwei passende Dateien im Verzeichnis /matrix/static-files/.well-known/matrix.

Kopieren Sie die beiden Dateien auf den Webserver, der sich um die Domain in Ihren Accountnamen kümmert, sodass sie dort wie beschrieben erreichbar sind. Alternativ können Sie den dortigen Webserver auch als Reverse-Proxy konfigurieren, sodass er die Dateien automatisch vom Matrix-Server lädt und weiterleitet. Die Datei docs/configuring-well-known.md enthält Konfigurationsbeispiele für gängige Web- und Proxyserver. (Die Datei docs/howto-server-delegation.md beschreibt eine Alternative zu .well-known-Dateien, wenn es etwa keinen Server hinter der Accountnamen-Domain gibt.)

Systemcheck

Ob alles funktioniert können Sie unter anderem mit folgendem Befehl überprüfen:

```
ansible-playbook -i inventory/hosts ↵
  ↳setup.yml --tags=self-check
```



Das optionale Web-UI macht die Account-Verwaltung leicht und liefert unter anderem auch Informationen zu Chaträumen.

Wenn alle Tasks „ok“ oder „skipped“ sind, ist alles in Ordnung. Andernfalls sollten Sie die angezeigten Fehler beheben, die Konfiguration neu einspielen und die Services wieder starten. Ob Ihr Server korrekt föderiert, können Sie außerdem über die Website https://federationtester.matrix.org prüfen. Geben Sie im Formular einfach die Domain aus Ihren Accountnamen an und klicken Sie auf „Go“.

Ausprobieren können Sie Ihren Matrix-Server über einen Client wie Element, dessen Webversion Sie eventuell ohnehin installiert haben. Melden Sie sich mit Ihrem Admin-Account an und chatten Sie los. Für einen ersten Test reicht ein zweiter Client mit einem zweiten Account, über den Sie mit sich selbst chatten und telefonieren. Oder Sie kennen bereits jemanden mit einem Matrix-Account auf einem anderen Server. Zur Not eignet sich zum Test auch ein Bot wie @mauping:t2bot.io. Wenn Sie diesen Account mit „!echo Was auch immer“ anschreiben, antwortet er umgehend mit „Was auch immer“.

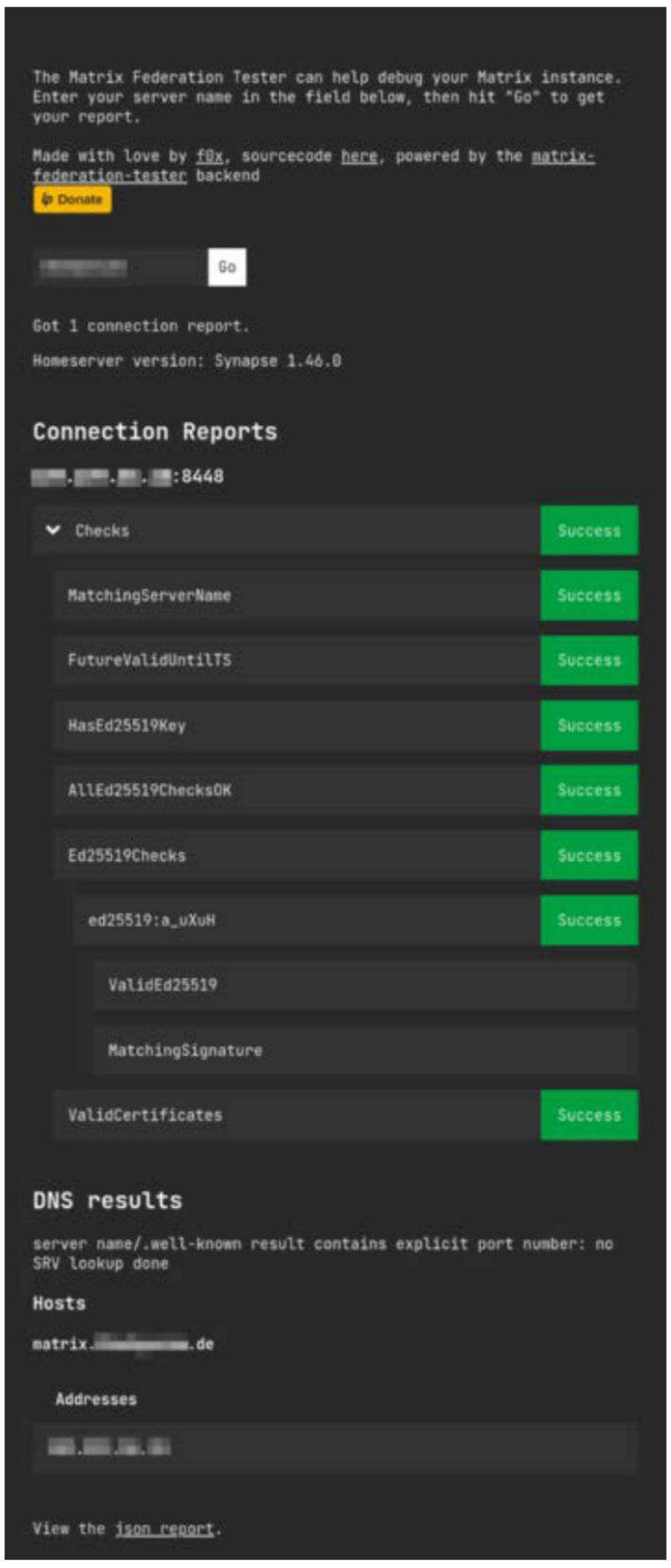
Wenn Sie den Server dauerhaft betreiben wollen, müssen Sie sich regelmäßig um Updates kümmern. Mit dem Ansible-Playbook ist das zum Glück nicht weiter schwer. Im Grunde brauchen Sie nur die aktuelle Version des Playbooks, denn die Entwickler aktualisieren es, wenn es beispielsweise eine neue Version eines Matrix-Dienstes gibt.

Stellen Sie für ein Update also sicher, dass Sie die aktuelle Version des Playbooks haben. Führen Sie dafür `git pull` aus. Wenn Sie das Playbook als Zip-Datei heruntergeladen haben, müssen Sie es erneut herunterladen und die Dateien inventory/host_vars/matrix.example.com/vars.yml und inventory/hosts in die neue Version übertragen.

Anschließend öffnen Sie die Datei CHANGELOG.md und lesen sich durch, was die neuesten Änderungen beinhalten und ob Sie irgendwelche zusätzlichen Maßnahmen ergreifen müssen. Wenn alles passt, können Sie einfach über die bekannten Befehle Ihren Matrix-Server an die aktuelle Playbook-Version anpassen und die Dienste wieder starten:

```
ansible-playbook -i inventory/hosts ↵
  ↳setup.yml --tags=setup-all
ansible-playbook -i inventory/hosts ↵
  ↳setup.yml --tags=start
```

Außerdem sollten Sie sich die Dokumentation zur Wartung des Servers ansehen. Die finden Sie im Ordner docs/ in den Dateien, deren Namen mit „maintenance-“ beginnen.



Alles grün: Der Federation-Tester ist mit dem Setup zufrieden und der .well-known-Verweis funktioniert auch.

Ausblick

Die Möglichkeiten von Matrix und auch des Playbooks gehen noch weit über das hier Beschriebene hinaus. Zum Beispiel kann man weitere Dienste wie die Videokonferenzsoftware Jitsi einbinden. Das Playbook erlaubt auch, sogenannte Bridges zu installieren. Bridges integrieren viele andere Messenger (im weitesten Sinne) in Matrix, etwa WhatsApp, Signal oder Twitter. Dann kann man auch Freunde ohne Matrix-Account via Matrix erreichen. Wie das geht, erklärt der folgende Artikel. (syt) c't

Literatur

[1] Götz Rieger, **Formgebung**, Grundlagen zur Automatisierung mit Ansible, c't 7/2021, S. 150

[2] Peter Siering, **Ansible-Strap**, Schnellstart ins Konfigurationsmanagementsystem Ansible, c't 7/2021, S. 156

Synapse- und Playbook-Dokumentation

ct.de/waef

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@ct.de oder xxx@ct.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: Jobst-H. Kehrhahn (keh)
(verantwortlich für den Textteil)

Konzeption: Holger Bleich (hob)

Koordination: Pia Ehrhardt (piae), Angela Meyer (anm)

Redaktion: Ernst Ahlers (ea), Holger Bleich (hob), Robin Brand (rbr), Niklas Dierking (ndi), Ronald Eikenberg (rei), Steffen Herget (sht), Michael Link (mil), Jan Mahn (jam), Angela Meyer (anm), Stefan Porteck (spo), Jan Schüßler (jss), Peter Siering (ps), Keywan Tonekaboni (ktn), Sylvester Tremmel (syt), Jörg Wirtgen (jow), Dušan Živadinović (dz)

Mitarbeiter dieser Ausgabe: Andreas Itzchak Rehberg, Holger Zuleger

Assistenz: Susanne Cölle (suc), Tim Rittmeier (tir), Christopher Tränkmann (cht), Martin Triadan (mat)

DTP-Produktion: Lara Bögner, Beatrix Dedek, Madlen Grunert, Lisa Hemmerling, Cathrin Kapell, Paula Krause, Kirsten Last, Martina Lübke, Steffi Martens, Marei Stade, Matthias Timm

Digitale Produktion: Christine Kreye (Ltg.), Melanie Becker, Kevin Harte, Thomas Kaltschmidt, Martin Kreft, Pascal Wissner

Fotografie: Andreas Wodrich, Melissa Ramson

Illustration: Rudolf A. Blaha, Frankfurt am Main; Thorsten Hübner, Berlin; Andreas Martini, Wettin; Thomas Kühlenbeck, Münster; www.freepik.com

Titel: Steffi Martens, Bild: Andreas Martini

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: Andre 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: 24.05.2022

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlags in irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Hergestellt und produziert mit Xpublisher:
www.xpublisher.com

Printed in Germany.

Alle Rechte vorbehalten.

© Copyright 2022 by
Heise Medien GmbH & Co. KG



Bild: Thomas Kuhlenbeck

Andere Messenger an Matrix anbinden

Wer einen Matrix-Server betreibt, nennt einen vollwertigen Messaging-Dienst sein Eigen. Über „Bridges“ lassen sich sogar andere Dienste einbinden, sodass man per Matrix-Client mit WhatsApp-Nutzern spricht oder Twitter-Nachrichten verschickt. Wir erklären, wie das mit vertretbarem Aufwand funktioniert.

Von **Sylvester Tremmel**

Einen Matrix-Server aufzusetzen ist nicht sonderlich schwer, besonders wenn man den ab Seite 100 beschriebenen Weg über ein Ansible-Playbook des Entwicklers Slavi Pantaleev geht. Man muss zwar mit passendem Server und Domainnamen ein paar Voraussetzungen schaffen, aber das Playbook übernimmt die Installation und den Großteil der Konfiguration aller Komponenten. Im Nu ist man stolzer Betreiber eines Chatservers, der es durchaus mit WhatsApp, Signal & Co. aufnimmt.

In einigen Bereichen bietet Matrix sogar deutlich mehr als diese Konkurrenten: Matrix-Server können föderieren, sich also mit anderen Matrix-Servern verknüpfen. Matrix-Nutzer Ihres Servers chatten dadurch automatisch und problemlos mit den Nutzern anderer Server. Die meisten anderen Messaging-Dienste beherrschen Föderation nicht oder nur bedingt – oder erlauben ohnehin keine Server neben dem des Betreibers. (Eine rühmliche Ausnahme stellt das altehrwürdige XMPP dar.)

Diese Limitierung anderer Chatsysteme umgehen Matrix-Bridges. Das sind kleine Server, die zwischen Matrix-Nutzern und Nutzern eines anderen Dienstes übersetzen – wohlgemerkt in der Regel, ohne dass

es dafür eine Unterstützung durch diesen anderen Dienst gäbe. Mit Bridges kann man verschiedenste Dienste an Matrix anbinden, allerdings gibt es dabei diverse Einschränkungen zu beachten. Die folgen teilweise daraus, dass andere Dienste schlicht andere Funktionen als Matrix bieten, und teilweise daraus, dass Bridges eine einseitig erzwungene Verbindung sind.

Brückenarchitekturen

Nutzer sollten es im Grunde gar nicht merken, wenn sie über eine Bridge kommunizieren. Ein Beispiel: Der Matrix-Nutzer Max schreibt in einem Matrix-Chat eine Nachricht an den Signal-Nutzer Siggi, der die Nachricht in einem Signal-Chat liest. De facto bekommt Siggi die Nachricht von der Bridge und nicht von Max' Gerät.

Im einfachsten Fall einer „Bridgebot-basierten" Brücke sieht man das deutlich; in Signal wird dann als Absender der Nachricht nicht Max angezeigt, sondern ein Bot-Account (ein sogenannter Bridgebot oder Relaybot). Der Bot kann die Nachricht ergänzen und ihr beispielsweise „von Max:" voranstellen, aber komfortabel ist diese Variante nicht. Metadaten wie der reale Absender gehen verloren und Siggi sieht alle Matrix-Nutzer als denselben Account, eben den des Bots.

Schöner sind „Puppeted Bridges". Damit bezeichnet man Brücken, die sich als Nutzerclient beim externen Dienst anmelden. Für den externen Dienst, also beispielsweise wieder Signal, sieht es so aus, als ob sich Max mit einem Signal-Client anmeldet und chattet. In Wahrheit meldet sich die Bridge mit Max' Signal-Account an und leitet alle Nachrichten weiter, die Max mit seinem Matrix-Client schreibt. Es gibt also eine Art Marionetten-Account in Signal, der all das tut, was Max mit seinem Matrix-Account in Matrix tut. Von diesen Marionetten leitet sich die Bezeichnung Puppeted Bridge ab.

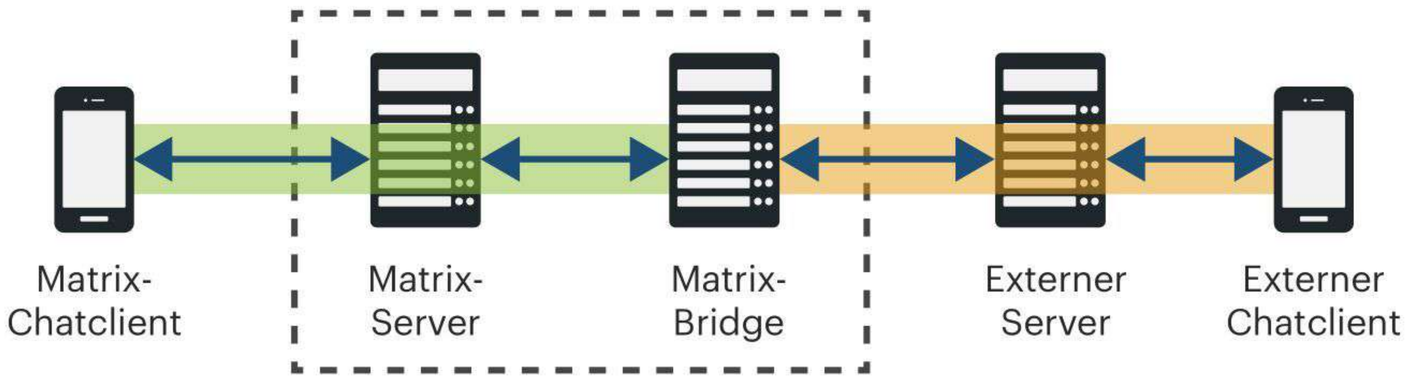
Puppeted Bridges setzen voraus, dass Nutzer Accounts bei den externen Diensten haben oder anlegen. Dabei gelten die üblichen Anforderungen: Wenn ein Service zum Beispiel Accounts an Telefonnummern bindet, kann man dieser Anforderung mit einer Puppeted Bridge nicht entgehen. Die letzte Ausbaustufe sind Double-Puppeted Bridges, die auch umgekehrt Marionetten-Accounts in die Matrix-Chats schleusen, um das Verhalten von Nutzern der externen Dienste im Matrix-Chat nachzuahmen. Daneben gibt es noch eine Reihe weiterer Möglichkeiten, Bridges zu realisieren. Die spielen in der Praxis aber geringere Rollen; eine Übersicht finden Sie in der Matrix-Dokumentation (siehe ct.de/wjhq).

Sicherheitsbedenken

So eine Double-Puppeted Bridge muss die Accounts ihrer Nutzer auf beiden Seiten steuern können und braucht daher Zugriff auf ebendiese Accounts. Schon

Brückenkonfiguration

Über Bridges lassen sich externe (Messenger-)Systeme in Matrix-Chats einbinden. Die Brücke schaltet sich dafür zwischen die beiden Systeme und übersetzt zwischen dem externen Server und einem Matrix-Server. Der Brücke muss man vertrauen, eventuelle Ende-zu-Ende-Verschlüsselungen reichen auf beiden Seiten nur noch bis dorthin und werden zu Ende-zu-Brücke-Verschlüsselungen. Matrix-Server und -Brücken können auf derselben Maschine laufen – müssen das aber nicht.



daraus ergibt sich, dass man der Bridge und dem Bridge-Betreiber mindestens so sehr vertrauen muss wie den Betreibern der beteiligten Chatserver. „Mindestens“ deshalb, weil Bridges außerdem Ende-zu-Ende-Verschlüsselungen unmöglich machen. Das spielt natürlich keine Rolle, wenn der betroffene externe Dienst oder der Matrix-Raum gar nicht Ende-zu-Ende verschlüsseln. Falls sie es jedoch tun, werden daraus zwei Ende-zu-Brücke-Verschlüsselungen und die Betreiber der Bridge haben – im Unterschied zu den Betreibern der Chatserver – Zugriff auf die Nachrichteninhalte im Klartext.

Hinzu kommt, dass Bridges möglicherweise Sicherheitsmaßnahmen der externen Chatanbieter unterlaufen. Beispielsweise speichert Signal keine Nachrichten dauerhaft auf seinen Servern; einmal zugestellt, wird auch das Chiffrat von den Signal-Servern gelöscht. Matrix hingegen speichert Chatinhalte auf dem Server und führt damit eine potenzielle Angriffs- oder Fehlerquelle ein.

Relevant sind diese Überlegungen insbesondere dann, wenn man Server und Bridges nutzt, die man nicht selbst betreibt, denn manche Matrix-Hoster, etwa „Element Matrix Services“, bieten auch Bridges an. Der Anbieter Beeper fokussiert sich sogar explizit auf dieses Feature.

Brücken bauen

Wer dagegen Matrix-Bridges selbst betreibt, hat zwar mehr Arbeit, muss sich aber keine Gedanken um die Vertrauenswürdigkeit des Bridge-Betreibers machen. Kombiniert mit einem eigenen Matrix-Server ist auch die Verschlüsselung vom Matrix-Client zur Brücke weniger relevant, schließlich liegt dazwischen nur der eigene Server. Dem vertraut man wohl genauso sehr wie der eigenen Matrix-Brücke.

Bridges für über zwei Dutzend Services listet die Webseite matrix.org/bridges auf, oft gibt es mehrere alternative Implementierungen pro Service. Das Angebot reicht von hierzulande üblichen Messengern (etwa WhatsApp, Signal oder Telegram) über Exotischeres (Tencent QQ oder Tox) zu Chat-fernen Systemen wie RSS oder E-Mail. Unter den hierzulande populären Chatdiensten fehlt Threema, allerdings steht ein entsprechendes Projekt bereits in den Startlöchern (siehe ct.de/wjhq).

Recht weite Verbreitung haben die Brücken des Projektes „mautrix“ gefunden. Sie decken diverse Services ab, sind relativ gut dokumentiert und funktionieren alle ähnlich, was die parallele Benutzung mehrerer Brücken bequemer macht. Ebenfalls verbreitet sind Brücken, die auf der Bibliothek mx-puppet-bridge aufbauen. In diesem Artikel beschreiben wir exemplarisch die Einrichtung von drei Mautrix-Brücken für Signal, WhatsApp und Twitter. Das machen wir wieder anhand des erwähnten Ansible-Playbooks (siehe S. 100), weil es den praktischen Konfigurationsaufwand massiv reduziert.

Authentifizierung

Wie erwähnt, muss eine Bridge auf der einen Seite mit einem Matrix-Server und auf der anderen Seite mit einem externen Dienst kommunizieren. Auf Matrix-Seite nutzen die Brücken das Application Service API, eine Programmierschnittstelle, die die Matrix-Spezifikation unter anderem für solche Zwecke definiert.

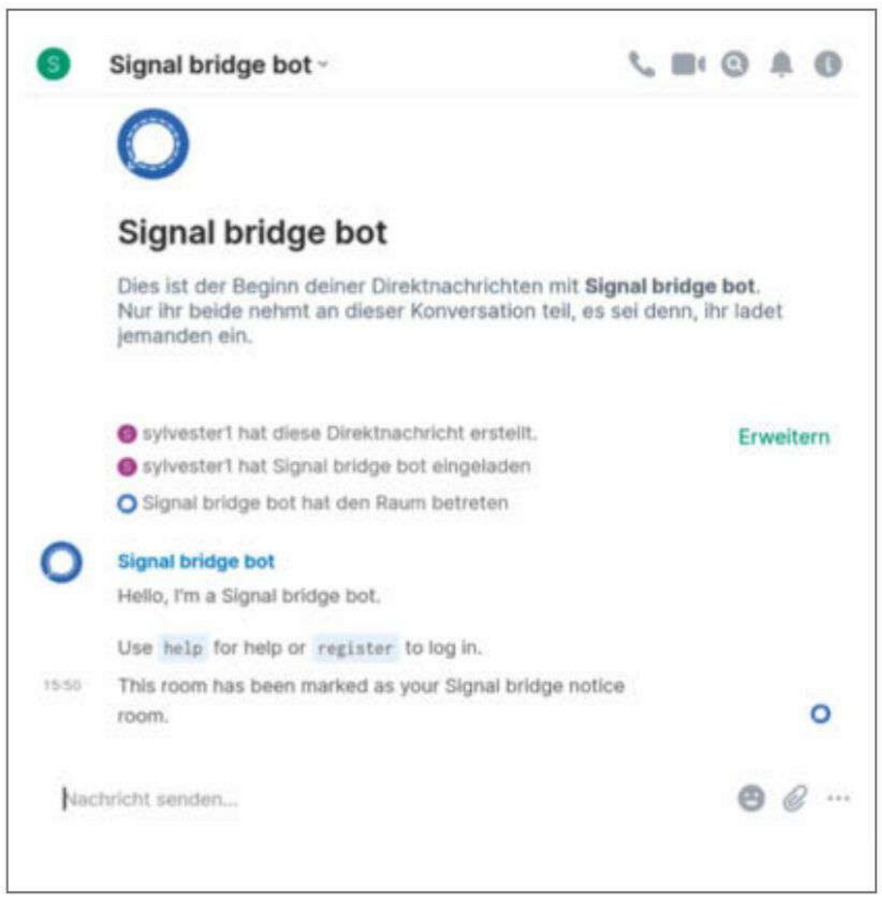
Anders als normale Clients können Application Services alle Nutzer-IDs in einem Namespace kontrollieren und unterliegen keiner Durchsatzbegrenzung. Bridges nutzen das, um beispielsweise für jeden Signal-Nutzer einen Marionetten-Account auf dem Matrix-Server anzulegen, dessen (interner) Name mit „@signal_“ beginnt und mit der Domain des Matrix-Servers endet. Solche Accounts kann die Brücke kontrollieren und als verschiedene Nutzer auftreten.

Damit solche erweiterten Rechte keine Sicherheitslücke in den Matrix-Server reißen, können sich Application Services nicht einfach beim Server melden. Stattdessen muss man eine zugehörige Registrierungsdatei in der Konfiguration des Servers hinterlegen. Diese Datei beschreibt unter anderem, welche Accounts die Brücke kontrollieren kann, und etabliert Geheimnisse, über die sich Brücke und Matrix-Server gegenseitig authentifizieren. Nur Administratoren mit Zugriff auf die Konfiguration des Matrix-Servers können so eine Datei hinterlegen.

Die Registrierungsdatei wird in der Markup-Sprache YAML verfasst, aber man muss sie nicht manuell erstellen. Mautrix-Bridges enthalten Skripte, um die Datei zu erzeugen, aber nicht einmal das ist nötig: Wer seinen Matrix-Server mit dem Playbook angelegt hat, spart sich nämlich die manuelle Installation und das Konfigurationsprozedere.

Signal

Das Playbook unterstützt eine ganze Reihe von Mautrix-, mx-puppet- und anderen Bridges. Um damit beispielsweise eine Signal-Bridge in Betrieb zu nehmen, reicht es grundsätzlich, in der Konfigura-



Einmal eingerichtet steuert man die Bridges, indem man mit Bot-Accounts chattet.

tionsdatei inventory/host_vars/matrix.example.com/vars.yml folgende Zeile einzufügen:

```
matrix_mautrix_signal_enabled: true
```

Nach den obligatorischen Befehlen, um die neue Konfiguration anzuwenden und die verschiedenen Services neu zu starten, steht die Signal-Brücke zur Verfügung:

```
ansible-playbook -i inventory/hosts ↵
  ↳setup.yml --tags=setup-all
ansible-playbook -i inventory/hosts ↵
  ↳setup.yml --tags=start
```

Im Hintergrund hat das Playbook sowohl die eigentliche Brücke installiert als auch signald, einen inoffiziellen Signal-Daemon, den die Brücke für die Kommunikation mit Signals Servern benutzt. Außerdem hat das Playbook die Komponenten passend konfiguriert und die Brücke wie beschrieben beim Matrix-Server registriert.

Um eine Bridge zu benutzen, muss man in Matrix eine Konversation mit ihrem Bot-Account aufbauen. Die Signal-Bridge können Sie unter „@signalbot:example.com“ erreichen, wobei Sie „example.com“ durch die Domain ersetzen müssen, die Ihr Matrix-Server für Account-Namen nutzt. Schicken Sie dem Bot testweise die Nachricht `help`. Er antwortet darauf mit einer Liste der von ihm unterstützten Befehle.

Marionettentheater

Im Chat mit dem Signalbot müssen Sie der Bridge nun Zugang zu Ihrem Signal-Account verschaffen. Dafür eignen sich die „gekoppelten Geräte“ gut, mit denen man normalerweise die Signal-Apps für Desktops oder Tablets mit dem eigenen Account verknüpft. Öffnen Sie die Liste der gekoppelten Geräte in den Einstellungen Ihrer Signal-App und fügen Sie ein neues hinzu. Die App will nun einen QR-Code scannen, um das Gerät zu verknüpfen.

Senden Sie die Nachricht `link` in Matrix an den Signalbot. Der antwortet darauf mit dem QR-Code, den Sie mit der Signal-App scannen. Nun ist die Brücke mit Ihrem Signal-Account verknüpft und kann die Marionette steuern.

Falls Sie die Signal-App weder haben noch haben wollen, gibt es auch die Option, die Brücke als primäres Gerät für einen neuen Signal-Account anzumelden. Das kann jedoch etwas komplizierter werden, weil Signal den Erstellungsprozess mit Verifizierungs-SMS und eventuell Captchas absichert. Die Dokumentation der Signal-Brücke beschreibt das nötige Vorgehen (siehe ct.de/wjhq).

Im nächsten Schritt aktivieren Sie den Rückweg, mit dem Sie der Brücke erlauben, Ihren Matrix-Account als Marionette zu steuern. Dafür benötigt sie Zugang zum Account. Der komplizierte – aber zum Verständnis wichtige – Weg dafür ist, der Brücke ein Authentifizierungstoken für Ihren Matrix-Account zur Verfügung zu stellen. Das Token können Sie unter der URL https://matrix.example.com/_matrix/client/r0/login abrufen, wenn Sie sich dort anmelden. Das geht zum Beispiel mit dem Kommandozeilentool curl [1]. Legen Sie dazu zuerst eine JSON-Datei mit dem folgenden Inhalt an:

```
{
  "identifier": {
    "type": "m.id.user",
    "user": "BENUTZER"
  },
  "password": "PASSWORT",
  "type": "m.login.password",
  "device_id": "Mautrix-Signal",
  "initial_device_display_name": "Mautrix-Signal"
}
```

`BENUTZER` und `PASSWORT` müssen Sie durch die Anmeldedaten Ihres Matrix-Accounts ersetzen. Anschließend senden Sie die Anfrage per curl an Ihren Matrix-Server:

```
curl --data @DATEINAME \
https://matrix.example.com/_matrix/client/r0/login
```

Statt `DATEINAME` müssen Sie den Namen der eben erstellten Datei angeben. Sofern Benutzername und Passwort stimmen, antwortet der Server mit einem JSON-String, dessen zweiter Wert das gesuchte `access_token` ist. Kopieren Sie den Wert und stellen Sie ihn der Bridge zur Verfügung, indem Sie eine solche Nachricht an den Signalbot schicken: `login-matrix TOKEN` Statt `TOKEN` geben Sie Ihren Access-Token an. Ab jetzt können Sie Konversationen über die Bridge führen (siehe Überschrift „Brücken begehen“), aber vorher lohnt sich noch der Blick auf eine Vereinfachung und die anderen Beispielbrücken.

Passwort-Provider

Wie schon angedeutet, ist das beschriebene Vorgehen relativ kompliziert und außerdem eher fragil: Wenn das Token seine Gültigkeit verliert, etwa weil man die Bridge versehentlich abmeldet, bricht das Double-Puppeting zusammen. Einfacher und verlässlicher ist es, das Passwort-Provider-Modul „Shared Secret Authenticator“ für den Matrix-Server Synapse zu nutzen.

Dieses Modul erlaubt externen Systemen (wie Matrix-Bridges), automatisch Zugriffsberechtigungen für beliebige Accounts eines Matrix-Servers zu erhalten – wenn sie ein mit dem Server gemeinsames Geheimnis kennen. Auch dieses Modul wird vom Playbook unterstützt, das wiederum die lästige Installations- und Konfigurationsarbeit abnimmt. Sie müssen lediglich Folgendes in der erwähnten Datei vars.yml ergänzen:

```
matrix_synapse_ext_password_provider_↲
  ↳shared_secret_auth_enabled: true
matrix_synapse_ext_password_provider_↲
  ↳shared_secret_auth_shared_secret: SHARED_SECRET
```

Statt `SHARED_SECRET` geben Sie eine zufällige Zeichenkette an, die das Playbook dem Synapse-Modul und der Bridge zur Verfügung stellt, damit diese einander authentifizieren können. Nutzen Sie ruhig einen langen Wert, das Playbook rät zu Geheimnissen aus 64 zufälligen Zeichen.

Nach der üblichen Konfigurationsübernahme und einem Neustart der Services mit den oben genannten Befehlen steht der Passwort-Provider zur Verfügung. Zumindest auf der Matrix-Seite verschaffen sich Bridges jetzt automatisch Zugang zu den Marionetten-Accounts. An der manuellen, von Service zu Service unterschiedlichen Authentifizierung auf der externen Seite der Brücke führt kein Weg vorbei.

WhatsApp

Die WhatsApp-Brücke funktioniert weitgehend identisch zur Signal-Bridge. Als Pendant zu signald kommt whatsmeow zum Einsatz, eine Bibliothek, um mit dem Web-API von WhatsApp zu sprechen. Sie aktivieren die Brücke, indem Sie in der vars.yml diesen Wert hinterlegen:

```
matrix_mautrix_whatsapp_enabled: true
```

Vergessen Sie nicht, die Konfiguration anzuwenden und die Services neu zu starten. Anschließend kommunizieren Sie mit der Brücke in Ihrem Matrix-Client, indem Sie „@whatsappbot:example.com“ kontaktieren. Schicken Sie `login` an den Bot, um einen QR-Code zu erzeugen. Öffnen Sie nun die Einstellungen des WhatsApp-Clients auf Ihrem Smartphone und fügen Sie unter „Verknüpfte Geräte“ die Brücke hinzu, indem Sie den Code scannen.

Eine Möglichkeit wie bei Signal, die Matrix-Bridge als primäres WhatsApp-Gerät zu nutzen, gibt es nicht. Wer partout kein WhatsApp auf seinem Handy installieren will, kann versuchen, mit einer Android-VM zu arbeiten. Die kann nach ihrer Einrichtung auch „headless“, also ohne Benutzeroberfläche, auf dem Server laufen. Die Einrichtung ist allerdings nicht trivial und sprengt den Rahmen dieses Artikels. Details erklärt die Dokumentation der Brücke (siehe ct.de/wjhq), die allerdings auch vor dem Vorgehen warnt: Solche Umwege erhöhen das Risiko, dass WhatsApp den Account blockiert.

Im Unterschied zu Signal kann WhatsApp auch bereits vergangene Konversationen nachträglich auf verknüpfte Geräte übertragen. Die Unterstützung dafür ist in Synapse allerdings noch als experimentell gekennzeichnet und standardmäßig deaktiviert. Wir raten davon ab, das Feature zu nutzen.

Twitter

Als drittes und letztes Beispiel soll die Mautrix-Twitter-Bridge eingerichtet werden, über die man Twitter-Direktnachrichten mit Matrix senden und empfangen kann. Wie gehabt ist die Einrichtung der Bridge



Die Anmeldung der Bridge bei Twitter ist umständlich, man muss Access-Token aus dem Browser pulen.

im Playbook trivial, fügen Sie einfach `matrix_mautrix_twitter_enabled: true` in vars.yml ein, übertragen Sie die Konfiguration und starten Sie die Services neu.

Anschließend können Sie in Matrix mit „@twitterbot:example.com“ Kontakt aufnehmen und dem Bot die Nachricht `login-cookie` schicken. Twitter sieht keine per QR-Code verknüpften Geräte vor, Brücken müssen sich hier anders authentifizieren. Es gibt eine Brücke auf Basis von mx-puppet-bridge, die das App-API von Twitter nutzt. Allerdings muss man sich dafür unter anderem bei Twitter als Entwickler anmelden. Die Twitter-Bridge von mautrix geht einen anderen Weg. Das Verfahren gleicht der manuellen Authentifizierung auf Matrix-Seite, man loggt sich anderweitig ein und übergibt der Brücke dann einen Access-Token:

1. Öffnen Sie ein privates Browserfenster und loggen Sie sich bei Twitter ein.
2. Öffnen Sie die Entwicklerwerkzeuge des Browsers, indem Sie F12 drücken.
3. In den Werkzeugen öffnen Sie in Chrome das Tab „App“ beziehungsweise in Firefox das Tab „Web-Speicher“.
4. Klappen Sie in der Seitenleiste den Punkt „Cookies“ auf und wählen „https://twitter.com“ an.
5. In der Cookie-Tabelle suchen Sie die Zeile mit dem Namen „auth_token“, kopieren den zugehörigen Wert und senden ihn per Matrix-Nachricht an den Twitterbot.
6. Anschließend kopieren Sie den Wert von „ct0“ und schicken auch diesen dem Twitterbot.

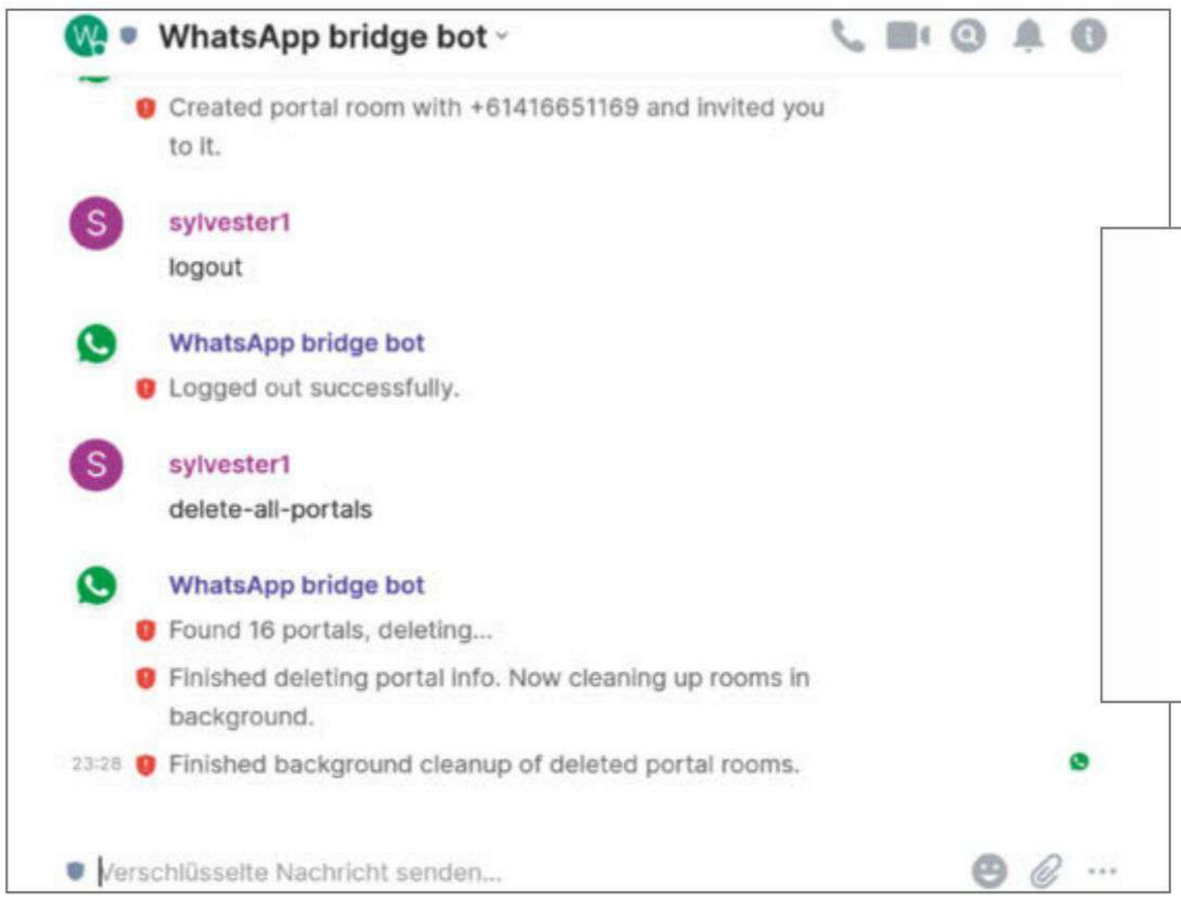
Anschließend ist die Brücke mit Ihrem Twitter-Account angemeldet und kann ihn steuern.

Brücken begehen

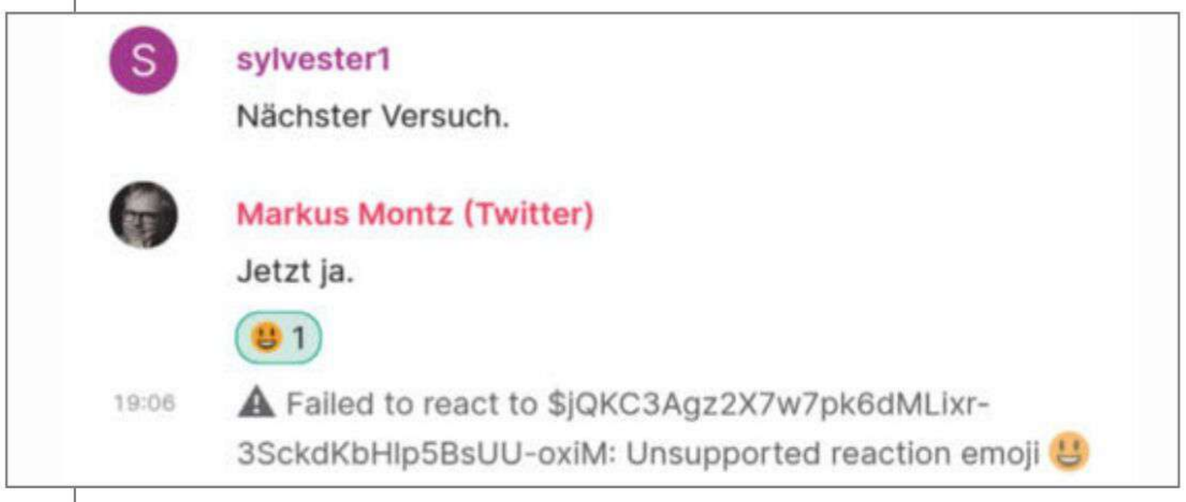
Einmal aktiviert und angemeldet, erstellen die Brücken automatisch passende Accounts und Chats („Portale“) in Matrix, um neue und, je nach Bridge, auch bestehende Konversationen bei den externen Diensten abzubilden. So einen Chat können Sie fortan wie jeden anderen benutzen; die Brücke spiegelt Ihre Aktionen auf den externen Dienst und überträgt die Antworten Ihrer Gesprächspartner zurück. Auch wenn Sie selbst den externen Dienst direkt benutzen, spiegelt die Brücke Ihre Nachrichten, sodass beide Systeme immer auf demselben Stand sind.

Bei manchen Brücken, etwa Signal und WhatsApp, können Sie auch direkt aus Matrix heraus neue Konversationen beginnen, indem Sie dem passenden Bridgebot einen Befehl senden. In den beiden genannten Fällen etwa den Befehl `pm` (für „private message“) gefolgt von einer Telefonnummer, schließlich identifizieren WhatsApp und Signal ihre Accounts über Telefonnummern.

In Konversationen, die über Brücken laufen, können Sie auch direkt mit der zuständigen Bridge kommunizieren, indem Sie Nachrichten ein passendes Präfix voranstellen. Für die gezeigten Brücken sind das `!signal`, `!wa` und `!tw`. Als Test eignet sich wieder der Befehl `help` beispielsweise als `!wa help` in einem Chat über die WhatsApp-Brücke. Studieren Sie ruhig, welche Fähigkeiten die einzelnen Brücken als Antwort auf `help` rapportieren; was genau der Bridgebot kann, ist von Brücke zu Brücke verschieden. Einige Brücken bieten beispielsweise eine „Relay bot“-Funktion, mit der sie für einzelne Matrix-Räume als Relay-Brücke agieren und die Nachrichten aller Matrix-Nutzer – ohne Puppeting – an den externen Service durchstellen.



Brücken kann man auch wieder abbauen, hier schließt der WhatsApp-Bot sämtliche „Portale“ und räumt auf.



Ein lachendes Emoji ist keine Reaktion, die es auf Twitter gibt. Es kann daher von der Brücke nicht gespiegelt werden.

Ebenfalls von Brücke zu Brücke verschieden ist, was genau übertragen wird: Wenn ein externer Service zum Beispiel keine dieser „Nutzer X schreibt gerade“-Informationen kennt, dann kann eine Brücke diese auch nicht übertragen. Und wer in Matrix eine Reaktion mit einem Emoji anzeigt, das es auf Twitter nicht als Reaktions-Emoji gibt, erhält eine Fehlermeldung.

Wer eine Brücke produktiv nutzen will, sollte sich eingehend damit beschäftigen, was die Bridge kann, wie sie zwischen Matrix und dem externen Dienst übersetzt und welche Konfigurationsoptionen sie bietet. Im Playbook findet man letztere in den Dateien roles/matrix-bridge-[...]/defaults/main.yml. Die dortigen Optionen kann man in die Datei vars.yml übernehmen, um zum Beispiel zu überschreiben, auf welchen Namen ein Bridgebot hört oder ob die Relay-Bot-Funktion aktiviert ist.

Außerdem lohnt sich ein Blick auf die Dateien roles/matrix-bridge-[...]/templates/config.yaml.j2. Wer etwas an den dortigen Einstellungen verändern will, ergänzt am besten passende ..._configuration_extension_yaml-Werte in der Datei vars.yml. Die folgenden Einträge aktivieren beispielsweise die Ende-zu-Brücke-Verschlüsselungen für die drei beschriebenen Brücken:

```
matrix_mautrix_signal_configuration_extension_yaml: |
  bridge:
    encryption:
      allow: true
      default: true

matrix_mautrix_twitter_configuration_extension_yaml: |
  bridge:
    encryption:
      allow: true
      default: true

matrix_mautrix_whatsapp_configuration_extension_yaml: |
  bridge:
    encryption:
      allow: true
      default: true
```

Fazit

Verschiedenste Services ohne deren Kooperation mit dem Matrix-Protokoll zu verkoppeln, ist kein leichtes Unterfangen. Nicht alle Funktionen der beteiligten Protokolle sind kompatibel und die externen Anbieter achten eher nicht darauf, ob eine Änderung eine Matrix-Bridge stört. Umso beeindruckender ist, wie gut die Bridges im Allgemeinen funktionieren und wie viel sie können. Es lohnt sich jedenfalls, damit zu experimentieren. Diverse – eigentlich inkompatible – Messenger mit einer App zu bedienen ist praktisch, macht Spaß und verleiht Kontrolle über die eigene Kommunikations-Infrastruktur. (syt) c't

Literatur

[1] Tim Schürmann, **Angebissen**, Mit Curl Webseiten anzapfen und Dateien herunterladen, c't 13/2021, S. 142

Dokumentation

ct.de/wjhq

Von Hackern lernen!

Heft + PDF mit 29 % Rabatt



Schützen Sie sich vor Angriffen! Das c't-Sonderheft zeigt Ihnen, wie Sie Netzwerk, PC, Smartphone und Online-Accounts absichern:

- ► Hacking-Tools als Problemlöser einsetzen
- ► Daten in Servern und Webanwendungen absichern
- ► Seriösen und sicheren VPN-Anbieter finden
- ► Aktuelle Hardware für 2-Faktor-Authentifizierung

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €

shop.heise.de/ct-securitytipps21

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

heise Shop

WIR MACHEN
KEINE WERBUNG.
WIR MACHEN EUCH
EIN ANGEBOT.

c't

ct.de/angebot

Jetzt gleich bestellen:
ct.de/angebot
+49 541/80 009 120
leserservice@heise.de

ICH KAUF MIR DIE c't NICHT. ICH ABONNIER SIE.

Ich möchte c't 3 Monate lang mit 35 % Neukunden-Rabatt testen.
Ich lese 6 Ausgaben als Heft oder digital in der App, als PDF oder direkt im Browser.

**Als Willkommensgeschenk erhalte ich eine Prämie nach Wahl,
z. B. einen RC-Quadrocopter.**

