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.

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.

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.

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.

ZUM HEFT

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

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

Lesen Sie mehr in c't Sicher ins Netz 2022

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

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.

Loslegen

Lesen Sie mehr in c't Sicher ins Netz 2022

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

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 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.

Lesen Sie mehr in c't Sicher ins Netz 2022

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**

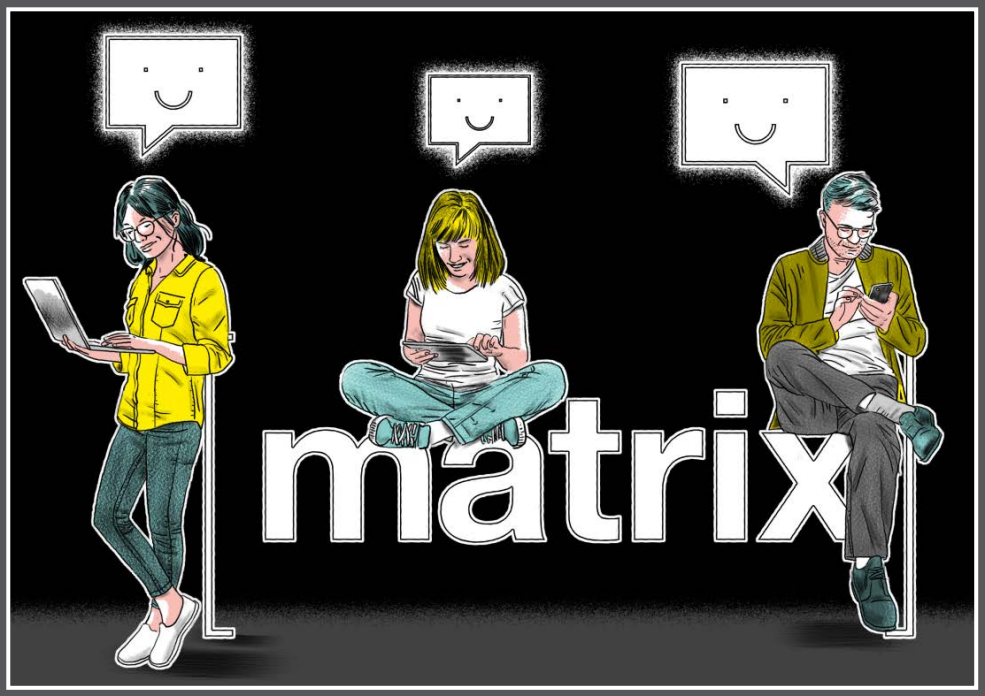

Bild: Thomas Kuhlenbeck

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 aus-

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