2020

c't Daten schützen

So bleiben Ihre Daten im Netz sicher und privat

Privatsphäre sichern

Social Media aufräumen • Spuren in Fotos verwischen
Daten richtig anonymisieren

Spione enttarnen

c't-Raspion einrichten
Datenlecks im Haushalt identifizieren

Verfolger abschütteln

Inkognito im Netz • Tracking aushebeln
Google entkommen • Maulkorb für Windows

Daten verschlüsseln

Sicher mailen mit PGP und S/MIME
Dateien & System mit Bitlocker und VeraCrypt sichern

Die 13 wichtigsten Privacy-Checklisten

Mehr Schutz für PC, Smartphone, Homeoffice & Social Media

4 196982 312906 02

c't Daten schützen

Heise

Liebe Leserin, lieber Leser,

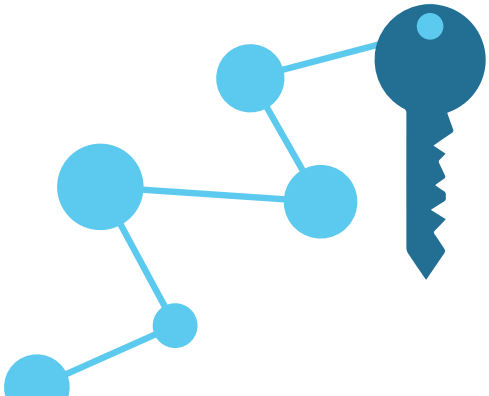
Sie kennen dieses unheimliche Phänomen sicherlich: Kaum haben Sie im Online-Shop Ihrer Wahl nach einer neuen Waschmaschine gesucht, werden Sie quer durchs Web mit Reklame für Waschmaschinen penetriert. Daran erkennen Sie, dass jemand Ihre Daten sammelt und Ihr Verhalten auswertet. Dieses sogenannte „Retargeting“ ist nur die Spitze des Eisbergs: Ob Website-Besuche, E-Mails oder Ortsangaben – sowohl für datengetriebene Unternehmen als auch für Behörden sind all Ihre digitalen Spuren wertvoll. Sie greifen sie, wo immer möglich, ab, ohne dass Sie es mitbekommen.

Wehren Sie sich gegen das hinterlistige Tracking! Es ist gar nicht so schwierig, wie Sie vielleicht denken. Wir liefern Ihnen auf den folgenden Seiten das nötige Rüstzeug. Sie erfahren, wie und wo US-Konzerne, allen voran Google, ihre digitalen Wanzen einsetzen und wie Sie dem begegnen. Unsere umfangreiche Sammlung von Checklisten hilft Ihnen dabei, den Schutz Ihrer Privatsphäre deutlich zu verbessern. Dazu müssen Sie kein IT-Profi sein: Es genügt meist, an wenigen Stellschrauben in Standard-Software wie Webbrowser, E-Mail-Programm oder Messenger zu drehen. Wenn Sie nun noch Ihre Social-Media-Accounts durchfeudeln und Ihre Kommunikation verschlüsseln, entziehen Sie sich der Beobachtung bereits wirksam.

Wir gehen noch einen Schritt weiter und laden Sie dazu ein, die Spione zu enttarnen. Nutzen Sie dazu unser Projekt c’t-Raspion. Mit der kleinen Hardware-Box analysieren Sie Traffic und entdecken ungewollten Abfluss von privaten Daten, beispielsweise von smarten TV-Geräten oder billigen IP-Kameras. Als Käufer dieses Sonderhefts erhalten Sie ein Hardware-Set für den c’t-Raspion in unserem Shop zum reduzierten Preis.

Viel Spaß beim Lesen und Basteln wünscht Ihnen

Holger Bleich



Inhalt

Tracking verstehen und vermeiden

Privatsphäre sichern

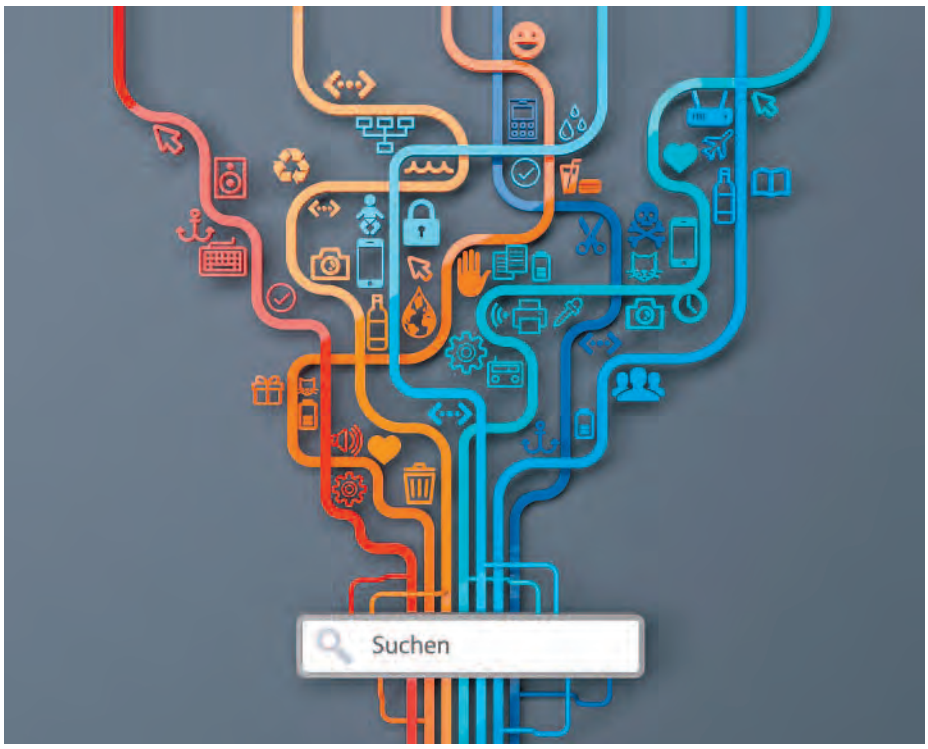
Social-Media-Accounts aufräumen

Daten verschlüsseln

Spione enttarnen

Datenschutzrecht anwenden

Zum Heft



Vertrackt

Wie Google das Leben von Milliarden Menschen erfasst

Von Torsten Kleinz

Vom ersten Griff zum Smartphone am Morgen über die Joggingrunde bis zum abendlichen Abschalten des Lichts im Smart-Home: Bei vielen Menschen kennt Google den Tagesablauf im Detail. Sich der Neugier des Datenkonzerns zu entziehen, ist gar nicht so einfach. Eine Bestandsaufnahme der konstanten Datenerfassung.

Sie mögen Geheimnisse vor ihren Eltern, vor ihren Kindern, Ihrem Arzt und sogar vor Ihrem persönlichen Trainer haben können – aber es erfordert enorme Mühen, Ihre Gedanken vor Google zu verbergen", polterte der britische Premierminister Boris Johnson 2019 in seiner Rede über zukünftige Technologien vor der UN-Generalversammlung. „Und wenn das heute schon so ist, gibt es in der Zukunft vielleicht keinen Platz mehr, wo man sich verstecken könnte."

Viele Politiker und Bürgerrechtsorganisation haben Google auf dem Radar, weil das Unternehmen wie kein zweites für die Ausbeutung der Ressource „Nutzerdaten" steht. Die Suchmaschine, das Mobilbetriebssystem Android, der Videodienst YouTube: Google ist in vielen Bereichen Marktführer und nutzt seine Plattformen intensiv, um Nutzerdaten zu ernten.

So verwundert es nicht, dass das Bundeskartellamt, die Europäische Kommission und das US-Justizministerium der Frage nachgehen, wie sie dem Datenkonzern Einhalt gebieten könnten. Daneben sind diverse Verfahren zum Geschäftsgebaren Googles anhängig.

Google hingegen beteuert den verantwortungsvollen Umgang mit den Daten seiner Kunden, die man nur in deren und im allgemeinen Interesse erfasse und verarbeite. So präsentierte das Unternehmen in der Corona-Krise Statistiken zu Bewegungsmustern der Bevölkerung, damit Politiker die Wirkung der Kontakteinschränkungen besser einschätzen konnten.

Ein Account für alles

Viele Nutzer geben Google ihre Daten gerne, denn sie erhalten dafür oft einen enormen Gegenwert. Gibt der Anwender zum Beispiel seinen Standort auf dem Smartphone frei, erhält er eine hochwertige und kostenlose Navigation. Verrät er dazu noch Wohnort und Arbeitsplatz, warnt Google Maps ihn rechtzeitig, wenn ein Stau auf dem Weg zur Arbeit die rechtzeitige Ankunft gefährdet.

Wer ein Android-Handy mit sich führt, per Gmail mailt und ein Thermostat der Google-Tochter Nest installiert, übermittelt mehr Daten als jemand, der ein iPhone benutzt und sich dem Smart-Home-Trend verweigert. Sich der Google-Datenerfassung komplett zu entziehen, ist indes kaum möglich. Nur wer Googles Datenhunger versteht, kann überhaupt Gegenmaßnahmen ergreifen. Daher haben wir diesen Überblick zusammengestellt.

Ein Blick in die Datenschutzerklärung

Welche Daten Google erfasst, lässt sich ziemlich detailliert anhand der Datenschutzerklärung nachvollziehen - grundsätzlich. Hand auf Herz: Haben Sie das Dokument durchgelesen? Falls nicht, dürften Sie zur Mehrheit der Anwender zählen, die AGBs und Datenschutzerklärungen gewohnheitsmäßig abnicken, wenn sie damit konfontiert werden.

2012 hatte der Konzern die bis dahin 60 verschiedenen Datenschutzerklärungen zu einem Text zusammengeführt. Wer den Text durchlesen und im Detail verstehen will, der muss viel Zeit mitbringen. Die deutsche Version der PDF-Datei umfasste im Mai 2020 34 Seiten.

Obwohl der Text in verständlicher Sprache gehalten ist und kaum juristischen Fachjargon enthält, dauert es rund eine Stunde, um ihn im Detail zu verstehen. Dabei sollte man sehr darauf achten, welche konkreten Aussagen Google macht und wo der Konzern nur einige

harmlose Beispiele wählt, um Datenverarbeitung generell zu rechtfertigen.

Google teilt die erfassten Daten in drei Kategorien ein:

- Google-Apps, -Websites und -Geräte, wie die Google-Suche, YouTube und Google Home
- Plattformen wie der Chrome-Browser und das Android-Betriebssystem
- Produkte, die in Apps und Websites von Drittanbietern integriert sind, wie Werbeanzeigen und das eingebettete Google Maps

Alleine bei der Nutzung von Google-Apps und -Websites fallen riesige Datenmengen an. Das gilt sogar dann, wenn der Anwender sie ohne Anmeldung nutzt, was in vielen Fällen grundsätzlich möglich ist. Auch bei solchen Nutzern legt Google eine ausführliches Profil an, wie die Datenschutzerklärung verrät.

Unbekannte Nutzer bekommen über Cookies eine eindeutige Kennung zugewiesen, die teilweise über Jahre erhalten bleibt, solange der Nutzer sie nicht explizit löscht. Auf Mobilgeräten oder einem Smart-TV lässt sich Google sogar zubilligen, Gerätedaten abfragen zu dürfen, um Nutzer eindeutig zu identifizieren.

Eingeloggte Anwender von Google-Diensten müssen damit rechnen, dass der Konzern ihre Daten bis ins Kleinste analysiert. Bis 2017 scannte Google Mail die Inhalte einer jeden empfangenen Mail, um entsprechend angepasste Werbung einzublenden.

Wer seine Smartphone-Fotos wie voreingestellt zu Google Fotos hochlädt, eröffnet Google einen intimen Einblick in das Sozialleben. Mit der Funktion „Ähnliche Gesichter gruppieren“ erfasst Google Fotos alle abgebildeten Personen. Auf der einen Seite ist das praktisch – sucht man Bilder einer Person, zeigt Google Fotos diese mit einem Klick an. Auf der anderen Seite ist dieses Vorgehen auch sehr invasiv.

Damit das Sortieren funktionieren kann, legt Google automatisch ein Verzeichnis der biometrischen Merkmale aller abgebildeten Personen an. Aus dem Schnappschuss-Archiv in der Cloud wird so eine mächtige biometrische Datenbank. Nutzer werden sogar ermuntert, den einzelnen Gesichtern Namen zuzuordnen, so dass immer klar ist, mit welchen Menschen sie interagieren.

Lässt man sich auf die Google-Welt ein und nutzt auch andere Dienste des Konzerns, fallen noch etliche weitere

ein sehr detailliertes Bild ergeben. Im Google-Dashboard (myactivity.google.com) lässt sich dann haarklein der Tagesablauf nachvollziehen: Von der morgendlichen Google-Abfrage über die Navigation zum Arbeitsplatz, dem Besuch im Supermarkt bis hin zum abendlichen YouTube-Video.

Google sammelt so viele Daten seiner Nutzer, dass es daraus neue Daten ableiten kann. Das zeigt sich bei Google Maps sehr plastisch. Wer Google Maps als Navigationshilfe benutzt, überträgt permanent aktuelle Positionsdaten an die Google-Server. Aus den Bewegungsprofilen der Masse der Maps-Nutzer kann Google so abschätzen, wo sich der Verkehr staut und wo er flüssig läuft - was wieder in die Routenberechnung einfließt.

Erst die Daten, dann das Geschäft

Die kommerzielle Erfolgsgeschichte Googles begann mit einer grundlegenden Entscheidung (siehe S. 16): Statt ihre Technik an Großkunden zu vermarkten, entschieden sich die Google-Gründer, eine öffentliche Suchmaschine für das gesamte Internet zu betreiben. Um ihren Dienst zu finanzieren, starteten sie den Service Adwords (heute Google Ads), der die Reichweite des Angebots besser vermarktet als Werbebanner. Online-Werbung ist bis heute die Haupteinnahmequelle von Google geblieben.

Werbekunden konnten Keywords hinterlegen und ihre Botschaften genau dort platzieren, wo sie vermeintlich die wertvollste Kundschaft fanden: Autoversicherer etwa ließen ihre Werbung ganz oben auf der Suchergebnisseite erscheinen, wenn Nutzer nach Autoversicherungstarifen oder nach neuen Autos suchten. Der Dienst wurde so beliebt, dass Google ein Auktionssystem einführte, bei dem sich etwa Auktionsanbieter im Kampf um die besten Platzierungen überbieten konnten.

Die Werbeausspielung wird aber nicht alleine von Suchworten gesteuert. So wertet der Konzern routinemäßig die genutzte IP-Adresse aus, um den Standort eines Nutzers einzugrenzen und demgemäß regionale Suchergebnisse und auch Werbung auszuspielen. Das lässt sich einfach nachzuvollziehen. Sucht man nach Kino-Filmen, zeigt einem Chrome selbst im Inkognito-Modus das Filmprogramm der Kinos in der Nähe an. Wer im Google-Nutzerkonto eingeloggt ist, macht die Standortbestimmung noch einfacher: Google nimmt einfach die letzte Positionsbestimmung des Handys, um zu ermitteln, wo sich der Nutzer gerade aufhält.

Chrome: Halb Browser, halb Google-Cloud

Das Geschäft hat sich mit dem Erfolg und der Größe Googles gewandelt. Der Konzern hat mittlerweile eine ganze Reihe

Lesen Sie mehr in c’t Daten schützen 2020

ist personalisierte Werbung aktiviert, hat Google in weniger als einer Stunde bereits

Privacy-Checklisten 2020

Neue und verbesserte Handgriffe für mehr Datenschutz

Wer seine digitale Privatsphäre schützen möchte, kommt sich manchmal vor wie Don Quijote: Überall müsste man noch viel mehr unternehmen und die Windmühlen der Konzerne mahlen ohnehin einfach immer weiter. Das Bild trügt aber. Hundertprozentigen Schutz gibt es zwar nicht, aber auch mit wenig Aufwand lässt sich schon viel erreichen. Die aktualisierte Neuauflage unserer Privacy-Checklisten zeigt, wie das geht.

Von Sylvester Tremmel

Der Schutz Ihrer Privatsphäre ist uns sehr wichtig.“ Solche Äußerungen findet man von praktisch jedem Unternehmen – häufig allerdings am Beginn einer länglichen Datenschutzerklärung. Die erläutert dann verklausuliert und schlimmstenfalls im Jargon englischsprachiger Juristen, an welchen vielen Stellen dem Unternehmen doch etwas anderes noch wichtiger ist.

Das kann man resigniert hinnehmen – oder man steuert gegen: Vieles ist nämlich einstellbar oder mit den richtigen Tools und Kniffen vermeidbar. Oft lässt sich schon mit geringem Aufwand und ohne großen Komfortverlust viel erreichen. Unsere Privacy-Checklisten auf den nächsten Seiten helfen dabei.

Datenabfluss allerorten

Es sind immer mehr Geräte, die ins Internet wollen und immer mehr Drittherstel-

meisten Hersteller haben wenig Interesse daran, an der Situation etwas zu ändern. Datensparsam vorzugehen ist oft aufwendiger, als Daten einfach irgendwo zu sam-

kommt es immer häufiger vor, dass Software „beim Kunden reift“. Die Hersteller sparen so Geld, das sie sonst für Tester

Manch ein Hersteller sammelt Daten auch ganz explizit, um sie mit Dritten zu teilen und so Einnahmen zu generieren. „Wenn Du nicht der Kunde bist, bist Du die Ware“, lautet der dazu passende Spruch.

Umso wichtiger, dass man selber Hand anlegt und abwählt und blockiert, was sich abwählen und blockieren lässt. Die jeweiligen – teilweise vom Hersteller gut versteckten – Optionen zeigen unsere Checklisten auf, sortiert nach Anwendungsbereich: Vom Rechner über das Smartphone bis zum vernetzten Zuhause ist alles dabei. Auch Ihren Mail- oder Facebook-Account nutzen Sie mit unseren Checklisten datenschutzfreundlich. Redakteure aus den jeweiligen Fachgebieten haben dabei nicht nur ihr Fachwissen eingebracht. Mit dabei sind auch Beobachtungen aus Kontakten mit Lesern sowie persönliche Erfahrungen und Vorlieben.

Neue Situation – neue Listen

vorgestellt, aber seither hat sich viel getan und wir haben die Listen entsprechend er-

cker blockieren, praktisch jedes Android-Gerät beherrscht mittlerweile differenziertes Berechtigungs-Management und Ende-zu-Ende-verschlüsselte Messenger

durchaus als nützliches Schwert erwiesen: Viele der Abschaltoptionen auf den fol-

den letzten Jahren zuhauf: Apps wurden bei der Weitergabe von Gesundheitsdaten erwischt, Anbieter von Sprachassistenten bei der manuellen Auswertung von Transkripten und Firmen bei der völlig unzureichenden Absicherung von Kundendaten. Deshalb fängt Privatsphärenschutz beim eigenen Verhalten an: Daten, die gar nicht erst in der Welt sind, können weder verschlampt noch verkauft werden. Das geht bei (öffentlich) geteilten Bildern los, die man auch Ende-zu-Ende-verschlüsselt an ausgewählte Empfänger hätte versenden können, und geht weiter über Gratisangebote und Kundenrabatte, für die man lediglich eine E-Mail Adresse angeben muss – ob der Ärger mit dem Newsletter die 10 Prozent wert ist?

Neu ist die Corona-Krise. Im Zuge der schnellstmöglichen Einrichtung des Heimbüros hat der eine oder andere vielleicht nicht sehr genau darauf geachtet, welche Tools er einsetzt – verständlich, schließlich musste alles erst einmal überhaupt funktionieren. Zeit, einen kritischen Blick nachzuholen, eine passende Checkliste haben wir neu erstellt.

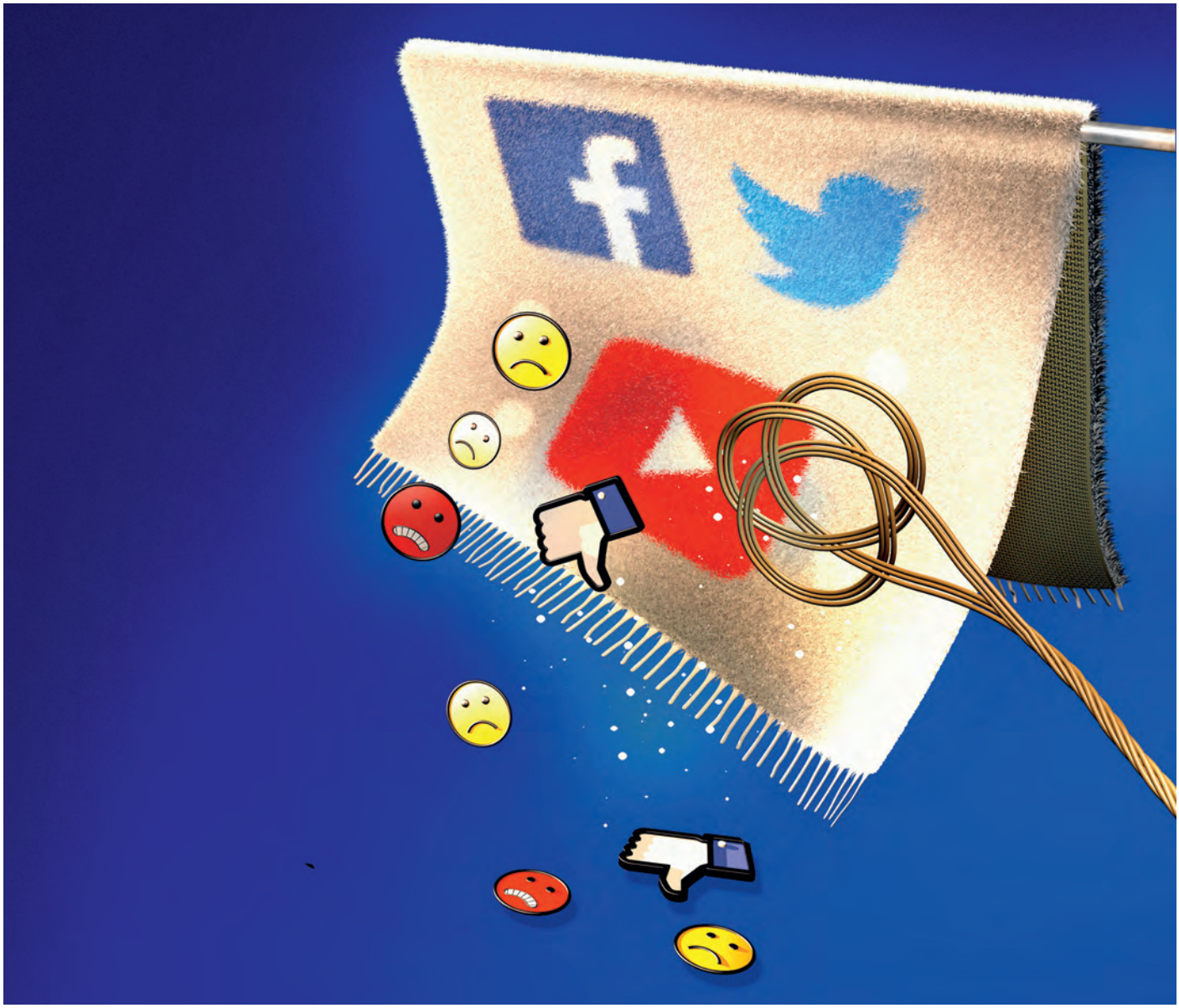
Ebenfalls neu hinzugekommen ist die Liste zu Fitnesstrackern und sie kommt gerade recht: Die „Datenspende“-App des Robert-Koch-Institutes nutzt solche Daten und kam dafür ins Gerede, wie wenig datenschutzfreundlich sie das tut. Eine gute Gelegenheit sich anzusehen, welche Fitnessdaten gesammelt werden und an wen sie weitergegeben werden. Man kann sich ja trotzdem dafür entscheiden, ein so hehres Ziel wie das des RKI zu unterstützten.

Kompromisse statt Radikalkuren

Bei alledem gilt: Natürlich könnte man jede Checkliste endlos fortführen und aufmerksame c’t-Leser können sich sicher an den einen oder anderen Artikel erinnern, der punktuell tiefer geht. Dann nimmt aber sehr schnell der Nutzungskomfort ab und vor allem steigt der Aufwand enorm. Hinzu kommt, dass auch radikalere Maßnahmen keine absolute Privatsphäre ga-

siedler. Die Privacy-Checklisten stellen dagegen einen Kompromiss dar, analog der bekannten 80:20-Regel: Auch

Lesen Sie mehr in c’t Daten schützen 2020



Social-Media-Hygiene

Reinigen Sie Ihre Timelines

Über die Jahre sammelt sich einiger Müll in Social-Media-Konten an, den besser niemand mehr sehen sollte. Zeit also, alte Postings und Likes zu prüfen und gegebenenfalls großflächig zu löschen.

Von Holger Bleich

Ein geplanter Badeurlaub in der Türkei wurde für Osman B. zum Horrortrip. Bei der Einreise am Flughafen Antalya klickten die Handschellen. Der türkischstämmige deutsche Staatsbürger landete in Untersuchungshaft, weil er angeblich zuvor aus Deutschland Terrorpropaganda verbreitet hatte. Der Grund: Jahre zuvor hatte Osman B. bei Facebook Bilder gepostet, auf denen im Hintergrund auch Symbole der prokurdischen HDP, der nordsyrischen YPG und das Konterfei des PKK-Gründers Abdullah Öcalan zu sehen waren.

Erst nach zweieinhalb Monaten Haft kam Osman B. unter Vermittlung des Auswärtigen Amts wieder frei und durfte nach Deutschland zu seiner Familie zurück. Der Fall machte Schlagzeilen, ist aber kein Einzelschicksal. Nicht umsonst warnt das Auswärtige Amt in seinen Reisehinweisen für die Türkei derzeit: „Seien Sie sich bewusst, dass regierungskritische Äußerungen in sozialen Medien, auch wenn sie länger zurückliegen, aber auch das Teilen oder Liken eines fremden Beitrags, Anlass für strafrechtliche Maßnahmen der türkischen Sicherheitsbehörden sein können."

Der Fall zeigt: Öffentliche Postings werden keineswegs nur vom gewollten Adressatenkreis wahrgenommen. Soziale Netzwerke dienen Fremden auch dazu, sich ein Bild von einem unbekannten Menschen zu machen. Das gilt für Grenz-

schutzbeamte genauso wie für Personaler, Vermieter oder Stalker. Selbst wenn Postings nur für den Freundeskreis freigeschaltet sind, droht Denunziation.

Aus dem Sinn

Die vorbeugende Maßnahme ist hinreichend bekannt: Denken Sie stets nach, bevor Sie posten oder liken. Welcher Eindruck entsteht von Ihnen, wenn jemand die Summe Ihrer Aktionen über die Grenzen der Netzwerke hinweg zusammenfasst? Auch an die Metadaten sollten Sie denken. Welche Metadaten sind öffentlich zu lesen? Welchen Facebook-Seiten folgen Sie? Ist Ihre Follower-Liste auf Instagram peinlich? Wer hat Sie auf Fotos markiert?

Aber nur nachzudenken reicht oft nicht mehr. Viele Historien reichen über Jahre zurück. Facebook etwa existiert seit 2004, Twitter ging 2007 an den Start. Wer früh dabei war, ist mit den Netzwerken mitgewachsen und hat vielleicht noch einige Jugendsünden im Keller respektive in versteckten Winkeln der Chroniken, an die er sich gar nicht mehr erinnert.

Der Klassiker: Nach dem Studiumsende folgt die Stellensuche. Dabei vergisst man, welche Fotos von ausschweifenden Saufgelagen auf Erstsemesterpartys noch abrufbar sind – und wundert sich, warum man in Bewerbungsgesprächen ausführlich zu seiner Geselligkeit befragt wird.

Wenn Sie spielerisch eine Idee davon bekommen wollen, welche Datenschätze in Ihren Konten zu bergen sind, installieren Sie die App **Time Hop** auf Ihrem Android-Handy oder iPhone. Einmal mit Ihrem Facebook-, Twitter- oder Instagram-Account verbunden, präsentiert sie hübsch gestaltete Erinnerungsalben aus Texten, Fotos und Videos, die Sie vor einem oder auch vor zehn Jahren veröf-

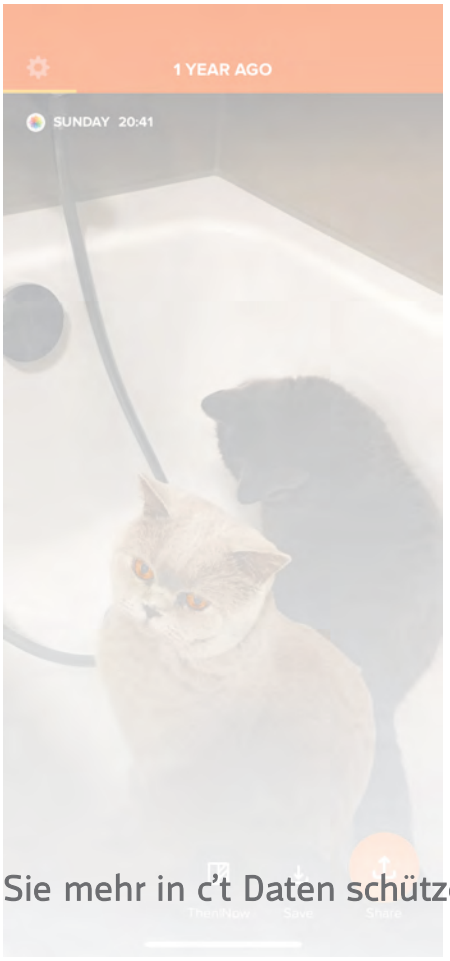
auch unangenehme – Überraschungen, wie wir bei Stichproben mit mehreren Per-

Hilfe beim Großputz

Die sozialen Plattformen animieren dazu, möglichst viel zu interagieren. Nutzer sollen posten und liken, was das Zeug hält: Aktivität und Engagement hilft, viel über die Nutzer zu erfahren und ihnen zielgruppengerecht viel Werbung einzu-

Zum Glück gibt es Tools, die diese Lücke füllen. In den folgenden Artikeln erfahren Sie, wie Sie Ihre Timelines bei Facebook, Instagram und Twitter rückwirkend säubern können. Außerdem erklären wir, wie Sie die Datensammelei und Profilbildung von Google einschränken und Ihre Außendarstellung in den Suchmaschinen verbessern.

Doch nicht nur auf den großen sozialen Plattformen, sondern auch den spezialisierten Netzwerken wie LinkedIn oder Xing und in Blogs und Foren sammelt sich Müll. Im Artikel auf Seite 96 zeigen wir, woran Sie bei Ihrem Frühjahrsputz denken sollten, damit Ihnen nichts durch die Lappen geht. Wohlan: Nehmen Sie Ihre digitalen Feudel in die Hand und wischen Sie großzügig durch die sozialen Accounts. *(hob@ct.de)* c't



Lesen Sie mehr in c't Daten schützen 2020

Bild: Rudolf A. Blaha

Einfach vertraulich

Unkomplizierte Verschlüsselung und Signierung von E-Mails mit S/MIME

Während Messenger wie WhatsApp und Signal sichere Verschlüsselung automatisiert haben, hinkt die gute alte E-Mail immer noch hinterher. Das ist unverständlich, denn mit S/MIME existiert ein bequemes, nahezu automatisiertes Verfahren, das Sie leicht und schnell einrichten.

Von Holger Bleich

Sie ließ nicht nur Bürgerrechtsaktivisten ungläubig zurück: die Verhandlung vor dem jüngsten Urteil des Bundesverfassungsgerichts zum BND-Gesetz. Denn sie legte offen, wie gierig der Bundesnachrichtendienst digitale Kommunikation an den Backbones absaugt, vor allem aber, wie locker der Zugriff darauf gehandhabt wird. Und bald erhält nach dem Willen der GroKo auch noch der Verfassungsschutz leichteren Zugriff, beispielsweise auf die E-Mails der Bürger.

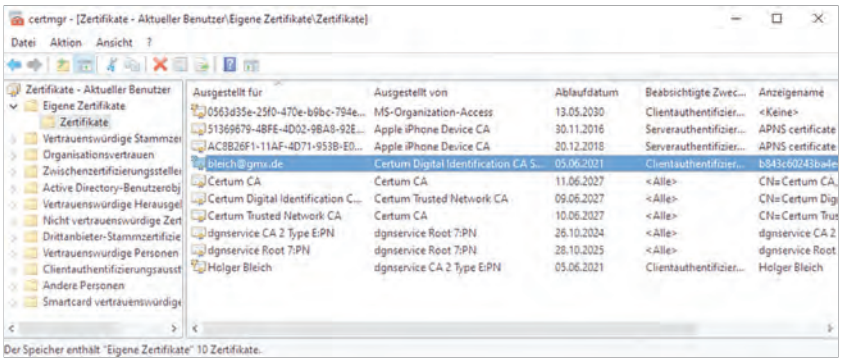
Wer dennoch auf dem „Ich habe ja nichts zu verbergen“-Mantra beharrt, sollte sich klar machen: Vertrauliche, integre Kommunikation ist ein Grundrecht und der einzige Schutz davor, unbemerkt ausgeforscht, vermessen und von Betrügern angegriffen zu werden. Da geht es nicht nur um sensible Gespräche zwischen Geschäftspartnern, sondern auch um private Liebeleien, politische Äußerungen oder schlicht den Versand von Rechnungen, die kein Dritter einsehen sollte.

Während bei Messengern wie WhatsApp oder Signal abhörsichere Ende-zu-Ende-Verschlüsselung deshalb selbstverständlich ist, hat sie sich bei der guten alten E-Mail auch nach fast 50 Jahren nicht flächendeckend durchgesetzt (ja, so lange gibt es E-Mail nun). Pretty Good Privacy (PGP beziehungsweise OpenPGP) gilt zwar technisch als sicher, vielen aber als zu kompliziert (siehe S. 110). Die Methode krankt außerdem an den vielen Insellösungen sowie an Umsetzungsproblemen, beispielsweise der mangelhaften Validierung von an Schlüssel gebundenen E-Mail-Adressen.

Dass mit dem Verschlüsselungsstandard S/MIME seit mehr als 20 Jahren eine funktionierende, sichere Alternative zu OpenPG bereitsteht, hat sich bis heute nur in Unternehmen, kaum aber unter Privatleuten herumgesprochen. Dabei bringt S/MIME einen entscheidenden Vorteil: Das Verfahren ist anders als OpenPG in der Software-Welt etabliert. Die beiden wohl meist verbreiteten Mail-Clients Outlook und Thunderbird unterstützen es (anders als OpenPG) nativ, ebenso wie Apples Mail-Tools in macOS, iPadOS und iOS. Auch für Android gibt es Lösungen.

Die Konzepte von OpenPG und S/MIME ähneln sich sowohl von den Funktionen als auch der Ausführung. Bei beiden handelt es sich um asymmetrische Verschlüsselungsverfahren. Der Nutzer verfügt über zwei Schlüssel, nämlich einen öffentlichen und einen geheimen. Den öffentlichen Schlüssel streut er breit an Kommunikationspartner. Diese verwenden den Schlüssel, um Nachrichten an ihn zu chiffrieren, die er dann nur mit seinem privaten Gegenschlüssel in Klartext umwandeln kann.

Es gibt aber einen entscheidenden Unterschied, der das Handling von S/MIME erleichtert: Das Vertrauen in den Besitzer eines Schlüssels beglaubigt bei OpenPG die diffuse Community innerhalb eines Vertrauensnetzes („Web of Trust“); bei S/MIME dagegen steht eine Schlüssel ausgebende, bekannte Autorität, die Certificate Authority (CA) für die Echtheit des Absenders und dessen Schlüssel ein. Sie zertifiziert die Schlüssel kryptografisch. Die Prüfung übernimmt der E-Mail-Client beziehungsweise das Betriebssystem, ähnlich wie es bei mit SSL-Zertifikaten transportverschlüsselten Webverbindungen der Browser tut, um mit Schlosssymbolen die Sicherheit der Webseite zu signalisieren.



Importierte eigene Zertifikate des Nutzers sollten im Verwaltungsbaum von Windows an dieser Stelle auftauchen.

Erkauftes Vertrauen

S/MIME steht für „Secure Multipurpose Internet Mail Extension“ und ist zuletzt 2019 in einer vierten Version als Standard

möglicht nicht nur, E-Mails samt Dateianhängen vor dem Versand nach dem Stand der Technik sicher zu verschlüsseln (eine Länge des RSA-Schlüssels von mindestens

Mail wirklich von der Absender-Adresse kommt, die im From-Feld steht. Sie zeigt auch, dass die Mail auf dem Weg durchs Netz in keinem Bit verändert wurde.

Als Nutzer benötigt man lediglich einen beglaubigten öffentlichen Schlüssel, das sogenannte Zertifikat. Der Aufbau von S/MIME-Zertifikaten folgt dem ITU-Standard „X.509v3“ – weshalb keine Kompatibilitätsprobleme existieren. Anders als OpenPG-Schlüssel können X.509-Zertifikate nur einmal beglaubigt werden. Wie oben erwähnt sollte eine vertrauenswürdige CA das Zertifikat ausstellen und unterschreiben.

Diese spezialisierten Unternehmen sind mit ihren Stammzertifikaten und vielen Vertrauens-Unterketten zum Abgleich in den Zertifikatspeichern von Betriebssystemen, Browsern und E-Mail-Programmen präsent – aber nur dann, wenn die Softwarehersteller ihnen hundertprozentig vertrauen. Erkennt etwa Microsofts Mailer Outlook die S/MIME-Signatur einer Mail mit der Beglaubigung einer bestimmten CA, sieht es im Zertifikatspeicher von Windows nach, ob Microsoft dieser CA vertraut. Nur dann wird dem Empfänger ein „unbedenklich“ zurückgemeldet.

Daraus ergibt sich, dass man sein Zertifikat von einer CA erwerben sollte, die sich möglichst großes Vertrauen erarbeitet hat, also beispielsweise von Microsoft, Apple, Mozilla und den großen Linux-Distributoren anerkannt ist. In der Tabelle auf Seite 143 haben wir beispielhaft einige solcher CAs zusammengetragen. Bis vor einem Jahr war es bei einigen CAs noch möglich, kostenlose Trial-Zertifikate mit einer Laufzeit von 30 Tagen auszuprobieren. Doch mittlerweile verlangt jede seriöse CA Geld für die Ausstellung eines 12 Monate bis 3 Jahre gültigen S/MIME-Zertifikats. Eine Initiative wie Let’s Encrypt für SSL-Zertifikate ist leider bei S/MIME nicht in Sicht.

Die Kosten richten sich nach der sogenannten Zertifikatsklasse, die sich aus dem Aufwand der Beglaubigung ergibt.

Lesen Sie mehr in c’t Daten schützen 2020

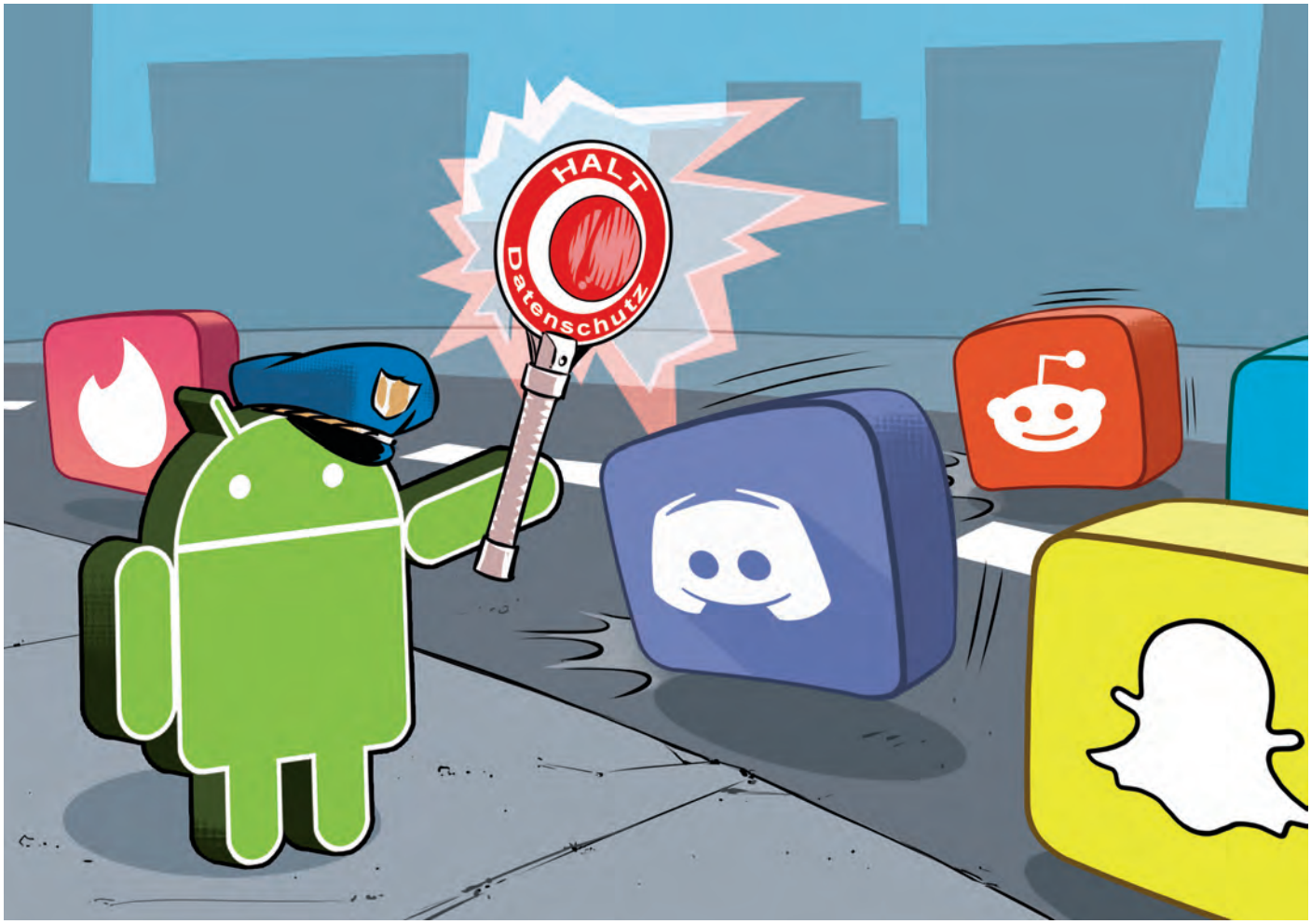


Bild: Albert Hulm

Mobile Verkehrskontrolle

Traffic-Analyse-Apps für Android

Android und die installierten Apps sprechen gern und oft mit dem Internet. Doch welche Daten werden dabei übertragen? Und wohin? Mit den passenden Werkzeugen finden Sie das leicht heraus – ganz ohne Root-Zugriff.

Von Ronald Eikenberg

Android-Apps genießen einen enormen Vertrauensvorschuss: Sie fordern Zugriff auf Kamera, Kontakte, Standort und vieles mehr, ohne jedoch transparent offenzulegen, was davon sie ins Internet schicken und wie diese Übertragung abgesichert ist. Wer wissen möchte, was hinter den Kulissen mit seinen Daten geschieht, muss einen Blick in den Netzwerkverkehr werfen. Mit den passenden Analyse-Apps ist das leichter denn je.

Das etablierte Standardverfahren zur Analyse von Smartphone-Traffic ist der Einsatz eines Analyseproxies wie mitmproxy oder Burp. Diese Vorgehensweise ist jedoch recht umständlich, es funktioniert nur im WLAN und zudem muss ein Rechner in Reichweite sein, auf dem der Proxy läuft. Viel komfortabler ist der Einsatz eines Analyse-Tools direkt auf dem Smartphone. Damit klappt die Traffic-Auswertung überall und jederzeit – sogar im Mobilfunknetz.

Die in diesem Artikel vorgestellten Apps nutzen einen Trick, um sich in den Traffic des Systems einzuklinken: Sie geben sich als VPN-Service aus, wodurch der gesamte Netzwerkverkehr durch sie hindurchgeschleust wird. Diese Schnittstelle nutzen auch VPN-Apps, um die Verbindung zu einem externen VPN-Anbieter herzustellen. Im Fall der Traffic-Analyse-Apps wird der Datenverkehr jedoch lokal ausgewertet und nicht zu einem VPN-Gateway außerhalb gelenkt.

Netzwerkrekorder

Eine der ersten Apps, die den VPN-Trick zur Traffic-Auswertung nutzten, ist tPacketCapture von Taosoftware (siehe ct.de/wqmx). Die Gratis-App beherrscht nur eine Funktion, diese aber mit Bravour: Vergleichbar mit dem unix-Tool tcpdump legt die App Traffic-Mitschnitte im PCAP-Format an, die man am besten am PC auswertet. tPacketCapture läuft unter allen Android-Versionen ab 4.0 und ist denkbar

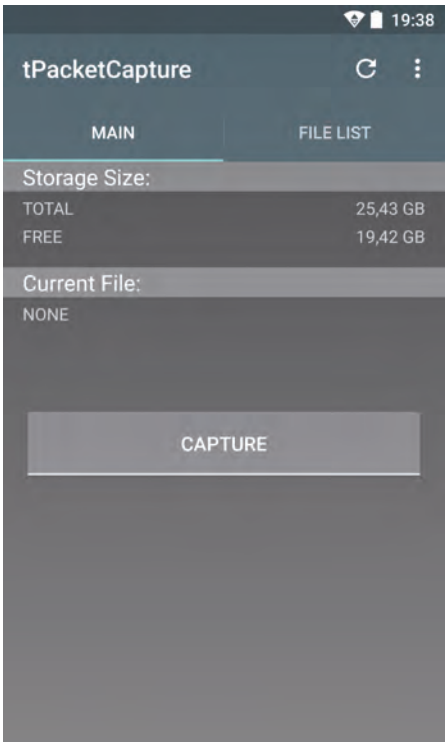
simpel aufgebaut – es gibt nämlich nur einen Knopf namens „Capture“. Betätigen Sie ihn, um die Aufzeichnung zu starten. Danach meldet sich eine Sicherheitsabfrage des Android-Systems und erkundigt sich, ob Sie mit dem Aufbau der VPN-Verbindung durch die Analyse-App einverstanden sind. Diese Abfrage bestätigen Sie mit „OK“. Anschließend finden Sie unter „Current File“ den Dateinamen des laufenden Mitschnitts sowie die Dateigröße. Den Speicherort der Mitschnitte erfährt man auf der Unterseite „File List“. Die Dateien befinden sich im internen Speicher unter /Android/data/jp.co.taosoftware.android.packetcapture/files/. Um die Mitschnitte komfortabel auswerten zu können, übertragen Sie diese auf einen Rechner, zum Beispiel per USB-Kabel oder Mail. Zur Ansicht eignet sich das Analyse-Programm Wireshark (siehe ct.de/wqmx), das unter Windows, Linux und macOS läuft.

Die Auswertungsmöglichkeiten mit Wireshark sind schier grenzenlos. Ein guter Anfang ist die Suche nach Daten, die ungeschützt im Klartext übertragen werden. Tippen Sie hierzu in die Filterzeile von Wireshark („Anzeigefilter anwenden …“) die Zeichenfolge `http` ein und aktivieren Sie den Filter mit Enter. Verschlüsselten Datenverkehr spüren Sie mit dem Filter `tls` auf. Aktivieren Sie unter „Ansicht/Namensauflösung“ die Option „Netzwerkadresse auflösen“, um zu erfahren, welche Server sich hinter den IP-Adressen befinden. Die Funktion „Statistiken/Verbindungen“ fasst zusammen, mit welchen Servern das Smartphone in welchem Umfang kommuniziert hat. Ein Klick auf „Namensauflösung“ zeigt auch hier wieder die zu den IP-Adressen passenden Hostnamen. Wer sich ausschließlich für den Datenverkehr einer bestimmten App interessiert und unnötigen Beifang vermeiden möchte, der kann zu der neun Euro teuren Pro-Version von tPacketCapture greifen. Diese kann bei Bedarf aus-

ter Apps aufzeichnen.

Verschlüsselung aufmachen

tPacketCapture erstellt einen passiven Mitschnitt und greift nicht in den Datenverkehr ein, was den Vorteil hat, dass man einen unverfälschten Eindruck vom Traf-



tPacketCapture ist einfach aufgebaut. Der Capture-Button startet die Aufzeichnung in eine PCAP-Datei.

ein Analysewerkzeug, das aktiv eingreift und den Datenverkehr von Apps und System zunächst entschlüsselt und dann erneut verschlüsselt, ehe die Daten an das eigentliche Ziel weitergereicht werden. Dies ist einfacher, als es klingt. Sie benötigen dazu ein Smartphone oder Tablet, auf dem Android 6.0.x oder älter läuft. Alternativ tut es auch ein Emulator mit einer passenden Android-Version.

Ab Android 7 führen verschärfte Sicherheitsbestimmungen dazu, dass die Analyse von TLS/SSL-Traffic bei vielen Apps nicht mehr ohne Weiteres möglich ist. Betroffen sind alle Apps, die mindestens für den API-Level 24 kompiliert wurden und unter Android 7 ausgeführt werden. In solchen Fällen ist entweder eine Modifikation des Systems (Root-Zugriff) oder der App nötig (siehe ct.de/wqmx). Beides ist recht umständlich – einfacher ist die Anschaffung eines günstigen Android-6-Smartphones zur App-Beobach-

Lesen Sie mehr in c’t Daten schützen 2020

zusehen, können Sie zum Beispiel die kostenlose App NetCapture einsetzen (siehe ct.de/wqmx). Sie agiert ebenfalls als VPN-Service, greift aber – anders als tPacketCapture – aktiv in die Verbindung ein, um den TLS/SSL-Traffic zu entschlüsseln. Beim ersten Start leitet Sie die App durch die Einrichtung. Zunächst müssen Sie der App die Berechtigung einräumen, auf den lokalen Speicher zuzugreifen. Diese benötigt sie zum Speichern der Mitschnitte. Anschließend installiert NetCapture ein SSL-Zertifikat in den Zertifikatsspeicher des Betriebssystems. Dieser Schritt ist notwendig, damit System und Apps dem Analyse-Tool das zum Aufbau der verschlüsselten Verbindungen nötige Vertrauen entgegenbringen. Bestätigen Sie die Installation des Zertifikats. Falls Sie Ihr System noch nicht mit einem Passcode geschützt haben, wird Sie Android nun auffordern, dies nachzuholen. Anschließend öffnet sich der Hauptbildschirm von NetCapture.

Drücken Sie auf den grünen Pfeil oben rechts, um die Aufzeichnung zu starten. Daraufhin erkundigt sich das Tool, ob Sie die „Floating View Function“ aktivieren möchten. Es handelt sich dabei um ein schwebendes Minifenster, über das Sie jederzeit den Traffic-Fluss beobachten können – ganz gleich, welche App sich gerade im Vordergrund befindet. Diese Funktion ist durchaus nützlich, klicken Sie also ruhig auf „Enable“. Im folgenden Dialog schalten Sie für diese Funktion die Berechtigung „Einblenden über anderen Apps zulassen“ scharf. Danach müssen Sie nur noch die Verbindungsabfrage für die lokale VPN-Verbindung zulassen.

Jetzt ist es geschafft: Das Hauptfenster von NetCapture füllt sich nun nach und nach mit den TCP-Verbindungen der installierten Apps und des Systems. Sie erkennen auf den ersten Blick, von welcher App eine Verbindung ausging und welcher Server auf welchem Port kontaktiert wurde. Zudem erfahren Sie den Zeitpunkt der Anfrage, die Größe der übertragenen Pakete, das Protokoll sowie die angefragte URL. Den Inhalt der Pakete sehen Sie, indem Sie auf eine der Verbindungen tippen. In der Detailansicht steht oben in Rot die ausgehende Anfrage, darunter befindet sich in Blau die Antwort des Servers. Wurden Bilder oder Videodateien übertra-