AKTION: Reiner SCT Authenticator mit Leserrabatt (Seite 170)
Schützen Sie Ihren Online-Account effektiv und komfortabel vor Hackern.

c't Daten schützen

So bleiben Ihre persönlichen Daten sicher und privat

Vertraulich kommunizieren

Test: Welche Messenger sind besser als WhatsApp?
Wie Sie E-Mails bestmöglich absichern

Verschlüsselung verstehen

Woran sich Supercomputer die Zähne ausbeißen
Kryptografie für Nicht-Mathematiker

Datenkraken entgehen

Test: Diese Browser schützen vor Tracking
Windows und Office ohne Microsoft-Cloud

Passwörter für alle Systeme

Der Kostenfalle entgehen: KeePassXC statt LastPass
Passwörter kostenfrei und bequem verwalten



facebook.com/ctspecials

So verteidigen Sie Ihre Privatsphäre

Kommunikation verschlüsseln, Überwachung verhindern
Das steckt hinter Sicherheitsversprechen und Datenschutzklauseln

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

4 195957 614908 04

heise Security Pro



Vernetzen, verstehen, umsetzen

Mit heise Security Pro zu mehr IT-Sicherheit.

heise Security Pro liefert Ihnen **Hintergründe, Analysen und vertiefendes Know-how** rund um IT-Sicherheit und **vernetzt IT-Security-Experten.** Werden auch Sie Teil dieser Community und sichern Sie sich jetzt das Profi-Paket für nur 995 € im Jahr*:

- Mindestens 4 Security Webinare
- 1 Ticket für die secIT
- Wöchentlicher Experten-Newsletter
- Jährliche heise Security Konferenz
- heise Security Expertenplattform
- 1 heise+ und 1 Pur-Lizenz

*Weitere Pakete auf Anfrage bei pro-service@heise.de.

JETZT IT-PAKET SICHERN: **heise.de/heisec-pro**

Editorial

Liebe Leserin, lieber Leser,

nicht von ungefähr steht die Datenverschlüsselung seit Jahren unter Beschuss von Gesetzgebern und Geheimdiensten: Sie ist eines der wenigen Bollwerke, mit dem auch Endnutzer ihre Informationen zuverlässig vor übergriffigen Staaten und Konzernen bewahren können. In dieser neuen Auflage des c't-Sonderhefts „Daten schützen“ erfahren Sie deshalb en détail, welche Messenger Ihre Nachrichten wirksam verschlüsseln, wie die Apps mit verräterischen Verbindungsdaten umgehen und inwieweit Sie E-Mails und Telefonate absichern können.



Damit solche Systeme helfen, müssen Sie aber auch die zugehörigen Konten sicher im Griff haben. Dank Passwort-Managern wie Keepass klappt das komfortabel und über Geräte und Plattformen hinweg. Kleine Hardware-Helferlein bieten zusätzlich Unterstützung. Eines davon erhalten Sie nach dem Erwerb dieses Hefts sogar günstiger.

Außerdem erfahren Sie, welche Angriffe Ihre Privatsphäre on- und offline bedrohen – sei es beim Surfen oder beim Verfassen eines Office-Dokuments. Wir zeigen Ihnen auch, mit welchen Tricks Sie sich schützen und welche Werkzeuge dafür besonders gut geeignet sind. Um Ihnen Basis-Know-how an die Hand zu geben, widmen wir uns den Grundlagen von Kryptografie und Datenschutz etwas ausführlicher. Wer sie kennt, dem fällt es leichter, allzu vollmundige Produktversprechen zu durchschauen und bei der Auswahl die Spreu vom Weizen zu trennen.

Wir wünschen Ihnen allzeit gut geschützte Daten!



Holger Bleich und Sylvester Tremmel

Inhalt



VERTRAULICH KOMMUNIZIEREN

Damit Konversation sicher privat bleibt, muss sie Ende-zu-Ende verschlüsselt werden. Außerdem sollten so wenig verräterische Metadaten wie möglich anfallen. Lesen Sie hier, welche Messenger in Frage kommen, wie sie funktionieren und wie Sie Mail-Kommunikation absichern.

6 Verbindungen absichern
10 Sichere Messenger im Test
18 Instant Messages ohne Datenlecks
22 Abhörsicher telefonieren
26 E-Mails bestmöglich absichern
30 Messenger auf Metadaten-Diät
34 Telefonnummern als Messenger-IDs



PASSWÖRTER IM GRIFF

Wirklich sichere Passwörter kann man sich kaum merken. Zum Glück hilft Software wie KeePass, die vielen Zugangsdaten auch über mehrere Geräte hinweg einfach zu verwalten. Wir zeigen, wie das funktioniert und stellen Hardware vor, die zusätzliche Sicherheit schafft.

38 Wie Sie Ihre digitale Identität schützen
46 Passwörter sicher und bequem verwalten
54 So wechseln Sie zu KeePassXC
60 2FA-Generator Reiner SCT Authenticator
64 Universal-Sicherheitsschlüssel TrustKey

ÜBERWACHUNG VERHINDERN

Wer sich im Web bewegt hinterlässt Spuren. Erfahren Sie, welche Browser besonders gut Ihre Privatsphäre schützen und wie man sie dafür optimal konfiguriert. Weitere Tipps helfen Ihnen dabei, auch dem allgegenwärtigen Microsoft das Telefonieren nach Hause abzugewöhnen.

66 Tracking und Cookie-Hinweise loswerden
72 Sieben Browser im Privacy-Check
78 Surfen ohne Cookies, Tracking und Reklame
86 Die Zukunft des Tracking
90 Microsoft Office ohne Cloud
96 Windows ohne Microsoft-Konto nutzen
104 Zeiterfassung per Fingerscan?
107 Spionageschutz mit Access Dots
108 Lauschangriff mit optischem Teleskop



VERSCHLÜSSELN STATT VERTRAUEN

Technischer Datenschutz beruht wesentlich auf starker Verschlüsselung. Wer die Grundlagen dazu kennt, kann besser einschätzen, welche Verfahren sicher und praktikabel sind – insbesondere für vertrauliche Kommunikation.

114 Was Sie über Kryptografie wissen müssen
116 (A-)symmetrische Verschlüsselung
122 Sicher durch Falltürfunktionen
126 Wie kryptografische Hashes funktionieren
132 Sichere Kommunikation

KLEINGEDRUCKTES VERSTEHEN

Im Web und auf dem Smartphone überfluten Anbieter ihre Kunden mit Einwilligungsaufforderungen und Datenschutzerklärungen. Allzu oft nehmen sie sich allzu viele Rechte heraus. Da hilft es, derlei Texte schnell verstehen zu können. Unsere leicht verständliche Einführung in die juristische Sprache unterstützt Sie dabei.

138 Privacy statt Buzzwords
142 Datenschutz-ABC
148 Onlinewerbung und Datenschutz
156 Zwischen Datenschutz und -nutz
164 Datenschutz-Fragezeichen bei Apps

ZUM HEFT

3 Editorial
155 Impressum
170 Aktion: Reiner SCT Authenticator





Verbindungen absichern

Zum Recht auf informationelle Selbstbestimmung gehört auch vertrauliche Kommunikation. Angriffe auf dieses Grundrecht gibt es traditionell nicht nur von Kriminellen, sondern auch von Staaten – einschließlich solchen, die sich gern als freiheitlich-demokratisch einordnen. Jeder Einzelne kann viel tun, um vertraulich zu mailen, zu chatten und zu telefonieren. Oft ganz ohne Komfortverlust.

Von **Jan Mahn**



Bild: Albert Hulm

Vertraulich kommunizieren

Verbindungen absichern	6
Sichere Messenger im Test	10
Instant Messages ohne Datenlecks	18
Abhörsicher telefonieren	22
E-Mails bestmöglich absichern	26
Messenger auf Metadaten-Diät	30
Telefonnummern als Messenger-IDs	34

Deutschland ist ein freies Land – zu dieser Erkenntnis kommen seit Jahren auch die Politikwissenschaftler der unabhängigen Forschungsorganisation Freedom House. Sie machen sich alljährlich die Mühe, die Freiheit aller Staaten der Welt zu erforschen. Für jedes Land schreiben sie einen Bericht und vergeben Punkte in 25 Kategorien (siehe ct.de/wm7p). Darin geht es um Wahlen, Presse- und Demonstrationsfreiheit und auch um die Freiheit im Internet. Mit 94 von 100 möglichen Punkten schneidet Deutschland vergleichsweise gut ab, Österreich kommt auf 93 Punkte, die Schweiz auf 96.

In Kategorie D4 geht es in den Länderberichten um die Freiheit, keine Überwachung fürchten zu müssen. Diese Freiheit ist in Deutschland gesetzlich verankert: Das Grundgesetz kennt das Post- und Fernmeldegeheimnis, die Europäische Menschenrechtskonvention nennt in Artikel 8 das Recht auf Achtung des Privatlebens und den Schutz der Korrespondenz. Es ist also ein Grundrecht, vertraulich mit anderen kommunizieren zu können – auch dann, wenn sich die Gesprächspartner nicht gegenüber sitzen und ein elektronisches Medium die Übertragung übernimmt.

Vertrauliche Kommunikation ist nicht nur für die wenigen Berufsgruppen wichtig, die immer wieder genannt werden, wenn es um verschlüsselte Kommunikation geht: Journalisten, Whistleblower und

Es ist ein Grundrecht, vertraulich mit anderen kommunizieren zu können.

Dissidenten in unfreien Staaten müssen natürlich besonders auf Vertraulichkeit achten, jeder andere sollte von seinem Grundrecht aber ebenfalls großzügig Gebrauch machen.

Denn auch als Normalbürger hat man eine Menge zu verlieren, wenn man sich auf die Vertraulichkeit des Geschriebenen nicht verlassen kann. Wer meint, er habe nichts zu verbergen, sollte am besten von einem Messenger direkt auf Twitter wechseln und die nächste Kneipentour nach der Pandemie mit Freunden in aller Öffentlichkeit planen und im Anschluss auch dort nachbesprechen. Spätestens, wenn man mit Kollegen oder Kunden über dienstliche Inhalte kommuniziert, ist Vertraulichkeit oft entscheidend. Wer mit Kundendaten fahrlässig umgeht, muss die DSGVO fürchten, wer Firmengeheimnisse ungeschützt übermittelt, muss Angst vor Industriespionen haben.

Mühsame Angriffe

Die Gefahr, von staatlichen Stellen abgehört zu werden, wirkt in Europa nicht so groß. Doch auch Deutschland bekommt in dieser Kategorie von den Freedom-House-Forschern Punktabzüge unter anderem für die Quellen-Telekommunikationsüberwachung (TKÜ). Im Visier sind dabei vor allem die Messaging-Dienste. Strafverfolgungsbehörden dürfen auf richterliche Anordnung einen Trojaner auf dem Mobiltelefon einer verdächtigen Person installieren, der zum Beispiel Screenshots der Nachrichten aufzeichnet und diese an die Strafverfolger verschickt. Das Verfahren ist aber mühsam, meist muss ein Ermittler mehrere Minuten Zugriff auf das Telefon des Verdächtigen haben.

Die beschwerliche Quellen-TKÜ ist für die Strafverfolger auch nur eine Notlösung – das Problem für alle, die vertrauliche Kommunikation mitlesen wollen, ist die Ende-zu-Ende-Verschlüsselung. Sie stellt sicher, dass nur die Gesprächspartner einen Schlüssel besitzen, um die Nachrichten lesen zu können. Alle anderen auf dem Weg, also der Betreiber des WLANs, die Internetanbieter, Knotenpunkte, abzapfende Geheimdienste, aber auch zum Beispiel die Betreiber der Messenger selbst, sehen nur verschlüsselten Datensalat. Ende-zu-Ende-Verschlüsselung schützt die Kommunizierenden nicht nur vor individueller Überwachung. Vor allem schützt sie zuverlässig vor der Massenüberwachung ganzer Gesellschaften. Eine solche haben unter anderem die Geheimdienste der USA und Großbritanniens weltweit eingerichtet, indem sie an Internetknotenpunkten große Teile des Internetverkehrs ausleiten und auswerten. Gegen Ende-zu-Ende-verschlüsselte Nachrichten kommen aber auch BND, GCHQ und NSA nicht an.

Das liegt schlicht daran, dass Ende-zu-Ende-Verschlüsselung durch die einzigen Gesetze geschützt wird, die Geheimdienste nicht beugen und Politiker nicht durch Verordnungen aushöhlen können: durch die Gesetze der Mathematik. Die stellen sicher, dass es beim Knacken der Verschlüsselung

aktuell keine Abkürzungen gibt und man auch mit viel teurer Hardware nicht effizient entschlüsseln kann, wenn man den Schlüssel nicht kennt. Wie verschiedene Messenger-Anbieter die Ende-zu-Ende-Verschlüsselung umsetzen und welche Auswirkungen das auf den Komfort hat, lesen Sie ab Seite 18. Einen Einblick in die technischen Details bietet der Artikel auf Seite 132.

Schwere Geschütze

Mit diesem für Überwacher unbefriedigenden Zustand wollen sich auch in Deutschland einige Politiker aber nicht abfinden – allen voran das CSU-geführte Innenministerium. Zusammen mit den europäischen Amtskollegen haben sie eine Resolution auf den Weg gebracht, in der sie Zugriffe für Strafverfolger und zuständige Stellen auf verschlüsselte Kommunikation fordern. Wie die Zugriffe auf die Nachrichten technisch aussehen sollen, ist mehr als unklar. Funktionieren kann das nur, indem man Lücken in die Software einbauen lässt, die Ende-zu-Ende-Verschlüsselung stellenweise deaktiviert, die Kommunikationspartner aber nicht darüber informiert. Ein mathematischer oder informationstechnischer Weg, Verschlüsselung nur ein bisschen zu brechen, existiert nicht. Problematisch sind solche Zugriffe unter anderem rechtlich: In Deutschland muss man keine Strafverfolgung fürchten, wenn man den ungarischen Ministerpräsidenten Viktor Orbán als Diktator und Faschisten bezeichnet, in Ungarn sieht das möglicherweise anders aus. Gäbe es nun eine richterliche Anordnung aus Ungarn an einen Messenger-Betreiber, die Inhalte einer Unterhaltung von zwei Deutschen offenzulegen und die Verschlüsselung zu umgehen – wer sollte entscheiden, welches Recht jetzt schwerer wiegt? Was, wenn die Unterhaltung von einem Deutschen und einem Ungarn geführt wurde?

Davon lassen sich Seehofer und seine Kollegen aber nicht abhalten und sprechen von einem Dialog mit den Anbietern, der nötig sei, um technische Lösungen zu finden. Sollten sie mit ihren Grundrechtseinschnitten im EU-Parlament und später in den nationalen Parlamenten durchkommen, müssten die Messenger-Anbieter dem auch Folge leisten. Tun sie das nicht, droht ihnen der Rauswurf aus den Stores von Apple und Google. Das trifft allerdings vor allem die Mehrheit der Bürger, deren Grundrecht beschnitten wird. Kriminelle würden dann auf andere Kanäle ausweichen. Mit solchen Hintertüren wäre außerdem nicht nur die gezielte Überwachung von Verdächtigen auf richterliche Anordnung möglich. Auch Massenüberwachung, wie sie Europa in den USA immer scharf kritisiert hat, wäre dann technisch kein Problem mehr. Die Geschichte der Hintertüren und Zweitschlüssel zeigt leider: Noch nie ist ein solches Instrument langfristig nur einem kleinen Kreis zugänglich geblieben. Zu den größten Fehlgriffen zählten die Hintertüren, die Netzwerkausrüster Juniper in seine Geräte auf Veranlassung der NSA einbauen musste. Genutzt wurden sie schnell auch vom chinesischen Geheimdienst.

Ende-zu-Ende-Verschlüsselung verhindert zuverlässig die Massenüberwachung ganzer Gesellschaften.

Im Freedom-House-Index dürften solche gesetzlich vorgeschriebenen Hintertüren zu massivem Punktabzug führen, Deutschland und die EU, einst Vorreiter bei der Freiheit, würden ins Mittelfeld abrutschen. Gleichzeitig schwächt man damit auch Argumente für die eigene Weltsicht: Unternehmen werden von der DSGVO aktuell dazu gebracht, personenbezogene Daten nur in Europa zu verarbeiten und nicht in den USA – dort erlaubt es der Cloud Act den Geheimdiensten, auf die Daten in den Rechenzentren zuzugreifen. An diesem Streitpunkt scheiterte zuletzt das Datenschutzabkommen Privacy Shield und Europa konnte immer aus der Position moralischer Überlegenheit argumentieren. Mit eigenen Hintertürgesetzen wäre damit Schluss.

Andere Wege

Möchte man auch dann noch abhörsicher kommunizieren, wenn die Innen- und Sicherheitspolitiker mit ihrer Grundrechtseinschränkung erfolgreich waren, kann man auf dezentrale Kommunikationssysteme umsteigen. Bei der populärsten dezentralen Kommunikationslösung gibt es keinen Anbieter, den man per Gesetz zu Hintertüren zwingen kann: Die gute alte E-Mail wird seit Jahrzehnten aber meist unverschlüsselt verschickt. Das liegt daran, dass Ende-zu-

Ende-Verschlüsselung nicht Teil der Protokolle ist, nicht jeder Mailclient mitspielt und die Einrichtung durchaus mit Komfortverlusten verbunden ist. Auf Seite 26 erfahren Sie, was trotzdem möglich ist und wie Sie vertrauliche E-Mails versenden.

Vertraulichkeit ist nicht nur beim geschriebenen Wort oft wünschenswert. Telefonate sind schon seit vielen Jahrzehnten im Fokus von Mithörern. Was Sie tun können, um möglichst große Teile der Verbindung zwischen Ihrem Telefonhörer und dem Hörer Ihres Gesprächspartners zu verschlüsseln, und ob es wahre Ende-zu-Ende-Verschlüsselung bei Telefonaten überhaupt gibt, erfahren Sie ab Seite 22.

Länderberichte von Freedom House:

ct.de/wm7p

Datenbeiwerk

Nicht nur die Inhalte der Nachrichten sind für alle Arten von Mithörern interessant. Strafverfolger, Geheimdienste, aber auch die Werbewirtschaft interessieren sich brennend dafür, wer mit wem zu welcher Uhrzeit und von welchem Gerät kommuniziert. Mit solchen Metadaten kann man, sofern man genug davon hat, eine Menge über Personen, Netzwerke und Beziehungen erfahren. Scrollen Sie einfach mal durch Ihre letzten Chatverläufe, achten nur auf die Uhrzeiten und überlegen Sie, welche Schlüsse man allein daraus über Sie und Ihre Gesprächspartner ziehen könnte, wenn man diese Informationen systematisch auswertet. Wenn man dann noch einbezieht, wer mit wem in welcher Gruppe ist, wird das Bild komplett.

In den folgenden Artikeln geht es daher nicht nur um die reine Verschlüsselung der Inhalte, sondern auch um den Schutz und die Vermeidung von Metadaten. Die Artikel auf Seite 30 und Seite 34 widmen sich dem Thema explizit. Das Recht auf private Korrespondenz beschränkt sich schließlich nicht nur auf die reinen Gesprächsinhalte. (jam) ct

Kommunikation absichern, modernisieren, konsolidieren und cloudifizieren?

Prozesse digitalisieren und automatisieren?

Ohne Server, Gateways und Hubs?

DIE COMMUNICATIONS PLATFORM!

retarus.de

VIELE WICHTIGE FRAGEN. EINE GUTE ANTWORT.

retarus



Bild: Andreas Martini

Sichere Messenger im Test

WhatsApps Status als De-facto-Standard bröckelt: Immer mehr Menschen mögen ihre Daten nicht dem Facebook-Konzern überlassen. Glücklicherweise gibt es Alternativen, die nicht nur sicherer, sondern auch mindestens so komfortabel sind. Fünf haben wir getestet.

Von **Jan-Keno Janssen, Sylvester Tremmel und Sebastian Trepesch**

Was ein kleines Info-Fenster anrichten kann: Als der populäre Messenger WhatsApp Anfang 2021 darum bat, neuen Nutzungsbedingungen zuzustimmen, hat er damit eine wahre Wechsel-Welle ausgelöst. Laut der App-Analysefirma Sensor Tower wurde beispielsweise Signal zwischen dem 6. und 10. Januar 7,5 Millionen Mal installiert – über 40 Mal mehr als in der Vorwoche. Telegram meldete 25 Millionen neue User in drei Tagen.

Der Mutterkonzern Facebook setzte der WhatsApp-Kundschaft die Pistole auf die Brust: Wer den Änderungen der Nutzungsbedingungen nicht zustimmte, sollte keine Nachrichten mehr lesen und schreiben können. Als Frist galt zuerst der 8. Februar, dann – vermutlich als Reaktion auf die Messenger-Wechsel-Welle – der 15. Mai, und dann wurde erklärt, dass sich WhatsApp doch weiter benutzen lassen wird, ohne die Änderungen zu akzeptieren.

Aber was ändern die neuen Nutzungsbedingungen nun eigentlich? Bei Nachrichten zwischen Privatnutzern laut Facebook nichts, die sind und bleiben für den Konzern nicht lesbar. Betroffen sind vielmehr Chats zwischen Privatnutzern und Unternehmen. Letztere sollen künftig Dienstleister beauftragen dürfen, die Chats in ihrem Namen abzuwickeln. Auch Facebook selbst will diese Dienstleistung seinen Firmenkunden anbieten, hätte in bestimmten Fällen also ebenfalls Zugriff auf die WhatsApp-Chats und könnte sie im Auftrag des Kunden auch für dessen Werbezwecke auswerten. Facebook erhofft sich davon offenbar einen Schub für die Nutzung der Business-Funktionen von WhatsApp. Wie das künftig aussehen könnte, sieht man in China, dort kann man nämlich mit der WeChat-App zum Beispiel eine Pizza oder ein Taxi bestellen und direkt bezahlen.

Insgesamt betreffen die Änderungen bei WhatsApp vor allem die Kundschaft außerhalb der EU, hierzulande schützt die DSGVO davor, dass Facebook zu viele Daten für Werbung auswerten darf. Klar ist auf alle Fälle: Facebook will WhatsApp endlich das Geldverdienen beibringen – ob man das in Einklang mit einer sicheren und datensparsamen Kommunikationsumgebung bringen kann, scheint mindestens fraglich.

Doch wo kann man denn überhaupt sicher kommunizieren und muss dennoch nicht auf den von WhatsApp gewohnten Komfort verzichten? Für diesen Test haben wir fünf WhatsApp-Alternativen ausgewählt: Element, Signal, Telegram, Threema und Wire. Die Auswahl fiel uns nicht leicht, denn eigentlich wäre unser Mindeststandard an Sicherheit der gleiche gewesen, den auch WhatsApp bietet, nämlich voreingestellte Ende-zu-Ende-Verschlüsselung (end-to-end encryption, E2EE). Sprich: Die Nachrichten werden nicht nur zum und vom Server verschlüsselt (Transportverschlüsselung), sondern permanent verschlüsselt gehalten und erst beim Empfänger entschlüsselt. Das macht WhatsApp seit 2016, und zwar mit dem in der Cryptoszene geachteten Double-Ratchet-Verfahren.

Dieses – von Signal erfundene – System ist gut für die asynchrone Kommunikation von Messengern geeignet und bietet wichtige Eigenschaften wie Forward Secrecy (siehe S. 132). Aufgrund solcher Vorteile wird das Verfahren auch von diversen anderen Messengern eingesetzt, im Testfeld neben Signal und WhatsApp auch von Element und Wire.

Den sehr populären Facebook Messenger haben wir nicht mit aufgenommen – er nutzt standardmäßig keine E2EE, und vor allem: Wer von WhatsApp wegen der neuen Facebook-Nutzungsbedingungen weg will, wechselt nicht zu Facebooks Messenger. Wegen unvollständiger E2EE haben wir Skype und Snapchat ebenfalls nicht getestet. Das ansonsten ordentliche iMessage fiel raus, weil es ausschließlich auf Apple-Geräten läuft.

Eine Ausnahme haben wir bei Telegram gemacht, die App umgibt kurioserweise eine Aura der Sicherheit. Der Messenger verschlüsselt standardmäßig nicht Ende-zu-Ende, es lassen sich lediglich manuell „geheime Chats“ starten, die etliche Nachteile haben. So funktionieren sie nur als Einzelchat, nicht in Gruppen. Außerdem sind die verschlüsselten Chats nur auf dem Haupt-Mobilgerät sichtbar, nicht auf dem Desktop-Client. Trotz allem wird Telegram immer



Bei Signal kann man jede einzelne Nachricht mit einem Emoji kommentieren.



Element

Element ist laut Play-Store-Downloadzahlen der bislang unpopulärste Messenger dieses Tests – dafür aber auch der mit dem größten Nerd-Faktor. Die Software hieß früher „Riot.im“ und setzt den offenen Standard Matrix um. Das ist ein Application-Layer-Kommunikationsprotokoll mit föderierenden Servern, ähnlich dem E-Mail-Standard SMTP. Chatpartner müssen also nicht beim selben Server registriert sein oder denselben Client nutzen, um miteinander zu reden.

Matrix schickt sich zumindest an, erfolgreicher zu werden als bisherige offene Instant-Messaging-Protokolle wie XMPP und IRCv3; unter anderem will die französische Regierung langfristig alle Ministerien auf Matrix-Kommunikation umstellen. Das deutsche Verteidigungsministerium testet seit Ende 2019 den „BwMessenger“ auf dienstlichen und privaten Geräten, der ebenfalls auf Matrix basiert.

Element kann als einziger Testkandidat die Kommunikation über einen selbst gehosteten Server laufen lassen. Ansonsten ist die Software eher rudimentär: Es gibt keine GIF-Bibliothek, keine Standort-Übermittlung und keine Sprachnachrichten, obwohl die für viele lebenswichtig sind.

- **gute Verschlüsselung**
- **föderierende, offene Server**
- **erfordert Technikaffinität**
- **keine Sprachnachrichten**



Signal

Das wohl anschaulichste Argument für Signal lieferte der im Exil lebende US-Whistleblower Edward Snowden Anfang des Jahres auf Twitter: „Ich benutze es jeden Tag und bin trotzdem noch nicht tot.“ Der Messenger hat sich seit seinen frickeligen Anfängen als „TextSecure“ in den letzten zehn Jahren erstaunlich entwickelt. Inzwischen kann man die App auch Technik-Laien empfehlen; wer mit WhatsApp klarkommt, bedient auch Signal.

Dem Konkurrenten hat Signal sogar einiges voraus: So funktioniert der Desktop-Client schon lange auch dann, wenn das Handy ausgeschaltet ist – WhatsApp arbeitete an dieser Funktion zu Redaktionsschluss noch. Außerdem kann man bei Signal einzelne Nachrichten mit Emojis versehen, was die Kommunikation effizienter macht. Die Zuverlässigkeit der App hat sich stark verbessert – hakte es Anfang des Jahres noch mit zu spät übertragenen Nachrichten, klappt inzwischen alles zuverlässig.

In Sachen Sicherheit ist Signal quasi der Goldstandard. Die Entwickler der App haben das Double-Ratchet-Verfahren erfunden und vermeiden mehr Metadaten als die Konkurrenz. Einziges Manko: Zur Registrierung und als Nutzer-ID ist die Telefonnummer verpflichtend, eine anonyme Nutzung ist nicht möglich.

- **beste Verschlüsselung**
- **einfache Handhabung**
- **Non-Profit-Entwickler**
- **Telefonnummern-Zwang**



Telegram

Das hat Pavel Durov clever eingefädelt: Durch sein Leben als Exilant – er kehrte Russland 2014 den Rücken – lud er seinen Messenger Telegram mit viel Freiheitskämpfer-Image auf. In letzter Zeit fiel Telegram allerdings vor allem dadurch auf, dass etliche Quer- und Wirrköpfe hier ihre Verschwörungsmythen publizieren – oft nachdem YouTube und Co. ihnen deswegen den Zugang gesperrt hatten. Dabei arbeitet Telegram durchaus mit Regierungen zusammen und wird beispielsweise vom europäischen Polizeiamt gelobt für das „Fördern enger Partnerschaften mit Organisationen wie Europol“.

Telegrams Ende-zu-Ende-Verschlüsselung ist der Double-Ratchet-Konkurrenz technisch unterlegen. Viel schlimmer ist aber, dass Telegram standardmäßig gar keine Ende-zu-Ende-Veschlüsselung nutzt. Der Messenger ist damit klar unsicherer als die anderen Testkandidaten. Außerdem werden die Inhalte normaler Chats auf den Servern des Anbieters gespeichert, wobei unklar ist, wer darauf Zugriff nehmen könnte. In Sachen Komfort und Geschwindigkeit ist Telegram dagegen ganz weit vorne. Außerdem bemerkenswert: Die fantastische Exportfunktion, die liebevollen Stickerpacks und die praktischen Bots.

- **stabil, schnell, viele Funktionen**
- **Cloud praktisch, aber unsicher**
- **nicht vollständig E2E-verschlüsselt**
- **Geschäftsmodell unklar**



Threema

Weil der Name „End-to-End-Encrypting Messaging Application“ (EEEMA) nicht ganz so geschmeidig über die Lippen geht, hat der Schweizer Entwickler Manuel Kasper kurzerhand „Threema“ daraus gemacht. Das war vor neun Jahren – und der Messenger behauptet sich immer noch gegen die Konkurrenz aus dem Silicon Valley. Ende 2020 haben die Macher sich getraut, den Quellcode der Client-Software offenzulegen – den Servercode allerdings nicht.

In Sachen Funktionen ähnelt Threema stark WhatsApp, bietet aber auch Eigenständiges, zum Beispiel das Erstellen von Umfragen. Threema kostet als einzige getestete Software auch für Privatpersonen Geld, je nach Store knapp vier Euro. Für Unternehmen gibt es „Threema Work“, das Mobile Device Management (MDM) unterstützt. Unter anderem wird die Software von der Schweizer Regierung und Daimler verwendet.

Die Verschlüsselung hält nicht mit dem Double-Ratchet-Verfahren mit. Sehr schön ist dagegen, dass der Betreiber seine Software schon mehrfach von Dritten auditieren ließ und sehr offen mit den Ergebnissen umgeht. Ebenfalls ein Plus: Threemas IDs sind anonym und werden nur auf Wunsch mit Telefonnummern oder Mailadressen verknüpft.

- **Server in Europa**
- **anonymer Betrieb möglich**
- **keine Sticker und GIFs**
- **keine kostenlose Version**



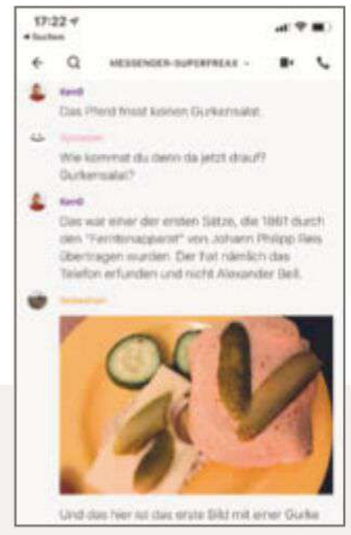
WhatsApp

WhatsApp war lange Zeit das Tempo-Taschentuch der Messenger: Seit Jahren kommt fast keine Junggesellinnen-Vorbereitung oder Kindergeburtstags-Organisation ohne die grüne App aus, zumindest hierzulande. Außer in deutschsprachigen Ländern ist WhatsApp in ganz Europa, Nordamerika, Russland und Indien populär – lediglich in Ostasien nutzen Menschen häufig andere Messenger. Laut Statista verwenden zwei Milliarden Menschen regelmäßig WhatsApp, es ist damit der meistgenutzte Messenger der Welt.

Doch spätestens seit den neuen Nutzungsbedingungen denken immer mehr Leute darüber nach, ob WhatsApp wirklich die beste Wahl ist. Zwar verschlüsselt der Messenger brav Ende zu Ende, aber was ist mit den Metadaten (siehe Artikel auf S. 30), fließen die womöglich doch in Facebooks Datensammlung?

Auch fernab von Sicherheitsbedenken spricht vieles gegen WhatsApp. Schon lange nervt zum Beispiel, dass der Desktop-Client nur läuft, wenn das Mobilgerät mit dem Netz verbunden ist. (Immerhin: Zu Redaktionsschluss testete WhatsApp eine neue Version ohne diesen Mangel.) Außerdem ist ein Datenexport, um ohne WhatsApp-Client auf seine Chats zuzugreifen, sehr umständlich [1].

- **gute Verschlüsselung**
- **einfach zu bedienen**
- **kaum Schutz von Metadaten**
- **Telefonnummern-Zwang**



Wire

Wire wird häufig vergessen, wenn es um sichere Messenger geht – dabei hat die Software durchaus ihre Fans. Die Wire Swiss GmbH sitzt in der Schweiz, entwickelt wird die Software in Berlin, die Server befinden sich in der EU.

Die Wire-Clients wirken nicht ganz so stromlinienförmig wie die Konkurrenz, funktionieren generell aber ordentlich. Etwas nervig ist, dass der App-Start nach dem Tipp auf eine Benachrichtigung häufig mehrere Sekunden dauert. An einigen Stellen versucht Wire, Dinge anders zu machen, zum Beispiel mit einer netten Kritzeln-Funktion.

Zur Verschlüsselung setzt Wire auf eine Variante des Double-Ratchet-Verfahrens. Wer einen Chat als sicher markieren will, muss allerdings alle Geräte seines Gegenübers einzeln verifizieren. Nur dann bekommt man auch angezeigt, wenn sich neue Geräte in einen Chat einklinken. In unverifizierte Chats könnte der Betreiber theoretisch eigene Geräte einschleusen und mitlesen, weil der Wire-Server das dafür nötige Passwort kennt. In Zukunft will Wire diese Lücke durch den Umstieg auf Messaging Layer Security (MLS) schließen, einen Standard für sichere Chatsysteme, an dessen Entwicklung sich Wire beteiligt.

- **Server in EU**
- **gute Verschlüsselung**
- **App manchmal schwerfällig**
- **E2EE-Lücke in unverifizierten Chats**

Sichere Messenger

Name	Element	Signal	Telegram	Threema	WhatsApp	Wire
URL	https://element.io	https://signal.org	https://telegram.org	https://www.threema.ch	https://www.whatsapp.com	https://www.wire.com
Hersteller	New Vector Ltd., künftig Element	Signal Foundation	Telegram Messenger LLP	Threema GmbH	Facebook Inc.	Wire Swiss GmbH
Mobil-Clients für	Android ab 5.0, iOS ab 11.0	Android ab 4.4, iOS ab 11.0	Android ab 4.1, iOS ab 9.0	Android ab 4.4, iOS ab 10.0	Android ab 4.03, iOS ab 9.0 (nur iPhone, nicht iPad)	Android ab 7.0, iOS ab 10.0
Desktop-Clients für	Browser, Windows, macOS, Linux	Windows, macOS, Linux	Browser (konventionell, Chrome-App und React), Windows, macOS, Linux	Browser	Browser, Windows, macOS	Browser, Windows, macOS, Linux
Desktop-Clients ohne aktives Mobilgerät nutzbar	✓	✓	✓	–	–	✓
mehrere Mobilgeräte je Konto	✓	✓[1]	✓	–	–	✓
mehrere Konten je Gerät	–	–	✓	–	–	✓
Deutsche Version verfügbar	✓	✓	✓	✓	✓	✓
Kontakte						
Anmeldung	Matrix-ID, Mailadresse, Telefonnummer, Google-, Apple-, GitLab-, GitHub-, Facebook-, SSO-Account	Telefonnummer	Telefonnummer	Threema-ID	Telefonnummer	Telefonummer oder Mailadresse
Adressbuchabgleich	–	✓	✓ (optional)	✓ (optional)	✓	–
neue Kontakte hinzufügen	Matrix-ID, QR-Code, optional über Identity-Server(Mailadresse, Telefonnummer)	Telefonnummer, Einladung	Telefonnummer, „Kontakte in der Nähe“, optionaler Username	Threema-ID, QR-Code	Telefonnummer, QR-Code	Mailadresse, Telefonnummer, Username
Gruppenchat (maximale Größe)	✓ (unbegrenzt, evtl. Server-limitiert)	✓ (1000)	✓ (200.000, „Broadcast“-Gruppen unlimitiert)	✓ (256)	✓ (256)	✓ (500)
Online-Status (abschaltbar)	– (eigentlich möglich, zurzeit auf matrix.org deaktiviert)	–	✓ (✓)	–	✓ (✓)	–
Inhalte						
fernlöschbare / selbstlöschende Nachrichten	✓ / –	✓ / ✓	✓ (ohne Hinweis) / ✓	– / –	✓ / ✓	✓ (ohne Hinweis) / ✓
Text nachträglich editierbar	✓	–	✓	–	–	✓
Textnachrichten zitieren / weiterleiten	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓ (ohne Hinweis)
Nachrichten liken	✓ (beliebige Emojis)	✓ (beliebige Emojis)	–	✓[2]	–	✓
SMS verwalten	–	✓	–	–	–	–
Emojis / Sticker / GIF-Suche	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / – / –	✓ / ✓ / ✓	✓ / – / ✓
Bilder / Videos / Dateien verschicken	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
Sprachnachrichten	–	✓	✓	✓	✓	✓
Telefonie / Videocalls	✓ / ✓	✓ / ✓	✓ / ✓	✓[2] / ✓[2]	✓ / ✓	✓ / ✓
Standort: fix / Live	– / –	✓ / –	✓ / ✓	✓ / –	✓ / ✓	✓ / –
Umfrage erstellen	–	–	✓	✓	–	–
Info zugest. / gelesen (abschaltbar)	✓ / ✓ (–)	✓ / ✓ (✓)	✓ / ✓ (–)	✓ / ✓ (✓)	✓ / ✓ (✓)	✓ / ✓ (✓)
Suchfunktion Global / Einzelchat	✓ / ✓ (im Test unzuverlässig)	✓ / ✓	✓ / ✓	✓ (nur Android) / ✓	✓ / ✓	– / ✓
Besonderheiten	föderiert, dezentral, offener Standard (Matrix), öffentliche Gruppen, über Bridges Inter-operabilität mit über 20 anderen Messengern	Gesichter blurren in Fotos, Vermeidung von Metadaten	Video-„Sprachnachrichten als Kreisvideo, „In der Nähe-Funktion, öffentliche Gruppen, praktische Bots, WhatsApp-Import	Vertrauensstufen für Kontakte	Mitteilungs-Feed („Status“) für Kontakte, Nachricht-an-alle-Kontakte-Funktion („Broadcast)	Ping, Zeichne-Funktion, Soundeffekte bei Sprachnachrichten

[1]Nur ein Smartphone [2]Nur in 1:1-Chats [3]Für EU-Nutzer [4]Vom Anbieter nicht beworben [5]Optional in 1:1-Chats möglich [6]Double-Ratchet-Variante [7]In Chats, Erläuterungen auf S. 132
[8]Nur in Transportverschlüsselung [9]Über Desktop-App
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ✓ vorhanden – nicht vorhanden

Sichere Messenger

Name	Element	Signal	Telegram	Threema	WhatsApp	Wire
Sicherheit & Privatsphäre						
Geschäftsmodell Anbieter	Optionale Abomodelle, Lizenzierung / Support	Non-profit (spendenfinanziert)	privatfinanziert, geplant: Werbe- und Premium-Features (keine Werbung in Privatchat)	Bezahlapp, Business-Modell	Werbung (geplant)	Optionale Abomodelle
Firmenstandort	UK / Frankreich	USA	VAE	Schweiz	Irland[3]	Schweiz
Serverstandort	Europa	USA	verteilt	Schweiz	verteilt	EU
Open-Source (Client / Server)	✓ / ✓	✓ / ✓	✓ / –	✓ / –	– / –	✓ / ✓
Reproducible Builds möglich	✓ (nur Android)[4]	✓ (nur Android)	✓	✓ (nur Android)	–	–
Chats Ende-zu-Ende-verschlüsselt	✓	✓	–[5]	✓	✓	✓
Chat-Verschlüsselungsprotokoll	Olm[6]/Megolm	Signal[6]	MTProto v2	NaCl crypto_box	Signal[6]	Proteus[6]
Forward Secrecy / Future Secrecy / Deniability[7]	✓[2] / ✓[2] / ✓	✓ / ✓ / ✓	✓ / – / ✓	–[8] / – / ✓	✓ / ✓[2] / ✓	✓ / ✓ / ✓
Server speichert Chat-Verläufe	✓	–	✓	–	–	–
Backup	E2E-verschlüsselt, auf Anbieter-Server	E2E-verschlüsselt, lokal	nicht E2E-verschlüsselt, auf Anbieter-Server (ohne E2EE-Chats)	E2E-verschlüsselt, lokal (Android); Systembackup (iOS)	nicht E2E-verschlüsselt, auf Google- bzw. Apple-Servern	E2E-verschlüsselt, lokal
Export von Chat-Verläufen	–	–	✓[9]	✓	✓	–
Kontakt-Verifizierung	QR, Emoji-Codes	manuell, QR-Code	manuell, visueller Vergleich	QR-Code	manuell, QR-Code	manuell
Profilinformat. E2E-verschlüsselt	–	✓	–	✓	–	–
Kontakt blockieren	✓	✓	✓	✓	✓	✓
App mit PIN- oder Biometrie-Sperre	✓	✓	✓	✓	✓	✓
Bewertung						
Verbreitung	⊖	○	⊕	○	⊕⊕	○
Funktionsumfang	○	⊕	⊕⊕	○	⊕	○
Bedienung	⊖	⊕	⊕⊕	⊕	⊕	⊖
Sicherheit und Privacy	○	⊕	⊖	⊕	○	⊕
Preis	kostenlos	kostenlos	kostenlos	3,99 € (Apple App Store, Google PlayStore), ~3,60 € (Android-APK über shop.threema.ch)	kostenlos	kostenlos

[1]Nur ein Smartphone [2]Nur in 1:1-Chats [3]Für EU-Nutzer [4]Vom Anbieter nicht beworben [5]Optional in 1:1-Chats möglich [6]Double-Ratchet-Variante [7]In Chats, Erläuterungen auf S. 132
[8]Nur in Transportverschlüsselung [9]Über Desktop-App
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ✓ vorhanden – nicht vorhanden



wieder als sicherere WhatsApp-Alternative gehandelt, weshalb wir es in den Test aufgenommen haben.

Unabhängig von der Verschlüsselung der Inhalte fallen beim Versand von Nachrichten Metadaten an. Diese Problematik – mit der Messenger unterschiedlich umgehen – beleuchten wir in einem separaten Artikel auf Seite 30.

Geschäftsmodelle

Interessant sind die völlig unterschiedlichen Geschäftsmodelle der sechs Testkandidaten. Während sich bei WhatsApp erst diffus abzeichnet, wie Facebook mit dem Messenger Geld verdienen will (Werbung und Messaging mit Firmen), sind die Geschäftsmodelle von Threema und Wire deutlich greifbarer: Threema verkauft die Privatkunden-Version der App für rund vier Euro und lizensiert die Geschäftskunden-Variante Threema Work an Unternehmen. Letzteres bietet auch Wire mit Wire Pro und Enterprise an; die Privatkundenvariante ist kostenlos.

Signal muss gar keinen Profit erwirtschaften, wsondern wird von einer US-amerikanischen Non-Profit-Stiftung finanziert. Das Anschubkapital von 50 Millionen US-Dollar kam von WhatsApp-Mitgründer Brian Acton. Außerdem wirbt Signal um Spenden. Bei Element handelt es sich um die Referenzimplementierung des freien Protokolls Matrix, Geld soll mit Support und Beratung sowie mit der Lizenzierung von Apps an Firmen und Behörden verdient werden. Unter anderem setzen die Bundeswehr und die französische Regierung Matrix-Messenger ein.

Und dann ist da noch Telegram: Die Entwicklung wird vor allem vom Milliardär Pavel Durov finanziert, der Russlands populärstes soziales Netzwerk vk.com aufgebaut und 2014 für viel Geld verkauft hat. Laut der Telegram-FAQ soll in diesem Jahr mit der Monetarisierung gestartet werden, um Infrastruktur und Gehälter zu finanzieren. Durov habe eine Strategie entwickelt, um Telegram „langfristig zu sichern“. Das soll so unauffällig passieren, dass „die meisten Nutzer fast keine Veränderung“ feststellen.

Neben einem nachvollziehbaren Geschäftsmodell sorgt ein offener Quellcode für Vertrauen – schließlich kann man im Zweifel nachschauen, was App und Server so machen. Von unseren Testkandidaten sind Element, Signal und Wire komplett quelloffen, also sowohl die Clients als auch die Server-Software. Bei Telegram und Threema kann man sich nur den Client-Code anschauen. Was auf den Servern passiert, bleibt Betriebsgeheimnis. WhatsApp ist vollständig closed-source.

Fazit

Ginge es ausschließlich um Komfort und Funktionsvielfalt, würde Telegram diesen Test mit Pauken und Trompeten gewinnen: Dank Cloud-Speicherung muss man bei Telegram nie nervige Backups machen, außerdem bietet die App etliche Features, die die Konkurrenz nicht hat, zum Beispiel das Hinzufügen von Kontakten nur über den Standort („Leute in der Nähe“) und sogar mehrere superschnelle Browser-Clients. Betrachtet man jedoch die Sicherheit, fällt Telegram durch: Die Cloud-Speicherung ist hochproblematisch, schließlich weiß niemand, wer wie, wann und wo Zugriff auf die Daten hat. Außerdem muss man die Ende-zu-Ende-Verschlüsselung umständlich manuell einschalten und sie hat auch noch etliche Nachteile, zum Beispiel dass man die „geheimen Chats“ nur auf dem Haupt-Mobilgerät abrufen kann. Die anderen Messenger beherrschen saubere Ende-zu-Ende-Verschlüsselung auf mehreren Geräten gleichzeitig.

Ausnahme ist dabei Threema, das keine Kopplung mehrerer Geräte unterstützt. Die Entwickler arbeiten aber dran. Auch bei der Ende-zu-Ende-Verschlüsselung geht Threema eigene Wege und bietet Eigenschaften wie Forward- und Future-Secrecy nicht. Element, Signal, WhatsApp und Wire nutzen dagegen das Double-Ratchet-Verfahren. Unterschiede zeigen sie unter anderem in Gruppenchats – wo manche Kandidaten etwa Forward-Secrecy fallen lassen – und beim „Wartungsaufwand“. Im Test machte besonders Element Probleme; manche Räume mussten wir neu anlegen, damit alle Teilnehmer mitlesen konnten. Bei Wire hakelte die Einbindung zusätzlicher Clients, Logout und Re-Login halfen aber. WhatsApp stahl sich hier bisher aus der Verantwortung: Der Desktop-Client funktionierte nur in Kombination mit dem Handy. Eine neue Version, mit der WhatsApp zur Konkurrenz aufschließt, befindet sich zu Redaktionsschluss im Betatest.

Das größte WhatsApp-Ablöse-Potenzial hat Signal: Es ist einfach zu bedienen, kostet nichts und bietet fast die gleiche Funktionsvielfalt wie die grüne App vom Facebook-Konzern. Allerdings befinden sich die Signal-Server nicht in Europa, weshalb der DSGVO-Status unklar bleibt. Zweifelsfrei nachweisen, ob ein Messenger DSGVO-konform ist, könnte man ohnehin nur mit einer Zertifizierung – die es zurzeit auf dem Markt noch nicht gibt. Am weitesten lehnt sich zu diesem Thema Threema aus dem Fenster, das Unternehmen schreibt auf seiner Website klipp und klar: „Threema ist DSGVO-konform“. (syt) c't

Literatur

[1] Stefan Porteck, **Nichts zurücklassen**, WhatsApp-Chats archivieren, c't 08/2021, S. 20

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.**



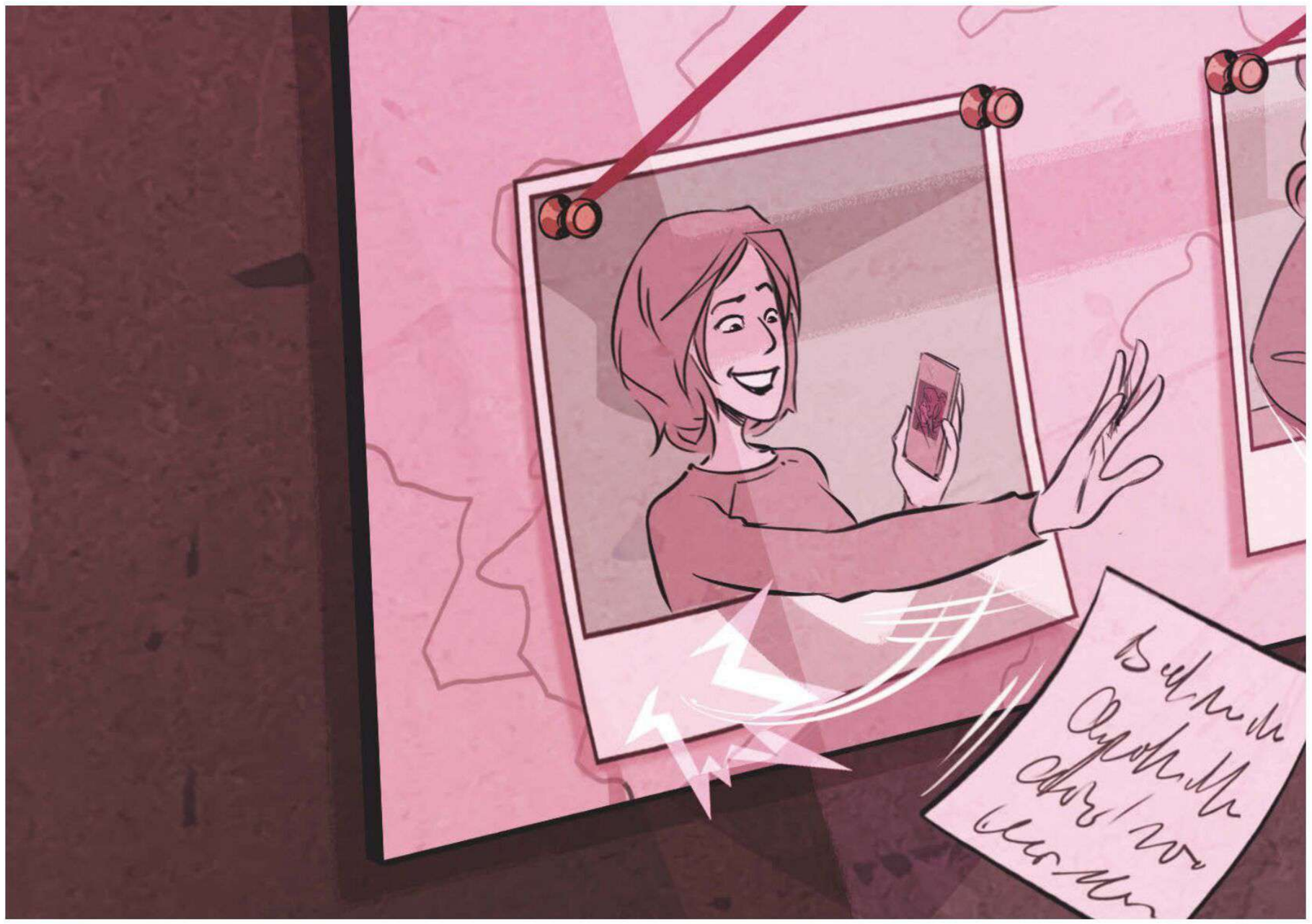


Bild: Albert Hulm

Instant Messages ohne Datenlecks

Über Chats können Sie bequem mit fast jedem Partner plauschen. Aber dass Sie das tun, und was Sie sich da erzählen, bleibt nicht immer privat. Entscheidend dafür ist die Wahl des Werkzeugs.

Von **Hans-Peter Schüler**

Mit WhatsApp erreichen Absprachen zur geplanten Fahrradtour und spontane Fotos der Protestdemo vor dem Rathaus auf Anhieb fast jeden gewünschten Adressaten. Das ist höchst bequem, und die Ende-zu-Ende-Verschlüsselung bei diesem Messenger könnte man als Garantie für den perfekten Datenschutz ansehen – doch das ist zu kurz gedacht.

Beim Gedankenaustausch über Instant Messages sind nämlich dreierlei Risiken zu beachten. Nur eines davon, dass jemand heimlich mitliest, lässt sich mit der Ende-zu-Ende-Verschlüsselung eindämmen.

Schutz von Inhalten

Was Sie Ihren Partnern mitteilen, ist nur dann zuverlässig geschützt, wenn es noch vor der Übergabe ins Internet auf Ihrem Gerät verschlüsselt und erst nach dem Verlassen des Internets auf den Geräten Ihrer Partner entschlüsselt wird. Beim viel gerühmten Dienst Telegram etwa gilt dieses Prinzip nur für wählbare Geheimchats mit eingeschränkten Möglichkeiten. Bei Microsoft Teams, das alle Nachrichten auf dem Server entschlüsselt und erst zur Zustellung wieder verschlüsselt, ist der Datenschutz immer eine Mogelpackung.

Bei WhatsApp und insbesondere den quelloffenen Konkurrenten Signal und Threema sind die Inhalte als sicher zu betrachten. Selbst ein durchgesickerter Kryptoschlüssel ermöglicht nicht unbedingt die Entschlüsselung früherer Nachrichten. Wie das technisch funktioniert erläutert der Beitrag auf Seite 132.

Offenes Buch: Metadaten

Der zweite Gesichtspunkt sind Informationen darüber, wann wer mit wem gechattet hat. Das mag Ihnen bei der Fahrradtour egal sein. Dagegen taugen am Ort und Zeitpunkt der Rathaus-Demo geteilte Fotos durchaus als Anhaltspunkt, um deren Empfänger zu recht oder zu unrecht als Sympathisant einer politischen Gruppierung abzustempeln. Sie sollten deshalb auch darauf achten, wie gut Ihre Kontaktdaten und die Ihrer Gesprächspartner geschützt sind.

WhatsApp möchte schon zur Installation Lesezugriff auf Ihr komplettes Adressbuch, und wenn Sie den nicht ausdrücklich verweigern, landen die Daten postwendend beim Anbieter Facebook. Vorgeblich dient das dazu, die WhatsApp-Nutzer unter Ihren Bekannten für Sie ausfindig zu machen, aber Facebook hat ein profundes Interesse am Besitz dieser Informationen: Sein ganzes Geschäftsmodell beruht darauf, das weltweite soziale Netz mit allen erdenklichen Informationen als perfekte Werbeplattform zu vermarkten und Sie als Adressaten für gezielte Werbung zu charakterisieren.

Man kann WhatsApp zwar auch verwenden, ohne das Adressbuch freizugeben, aber dann kann man nur mit Kunstgriffen Partner anchatten, von denen man noch nie eine WhatsApp-Message erhalten hat [1]. Für dieses Setup lässt man sich zum Beispiel von einem Radtour-Partner eine Nachricht schicken und sich in die Radtour-Absprachegruppe eintragen. Danach kann man sich ohne weltweites Outing an diesen Absprachen beteiligen.

Datenschutz bei Messengerdiensten

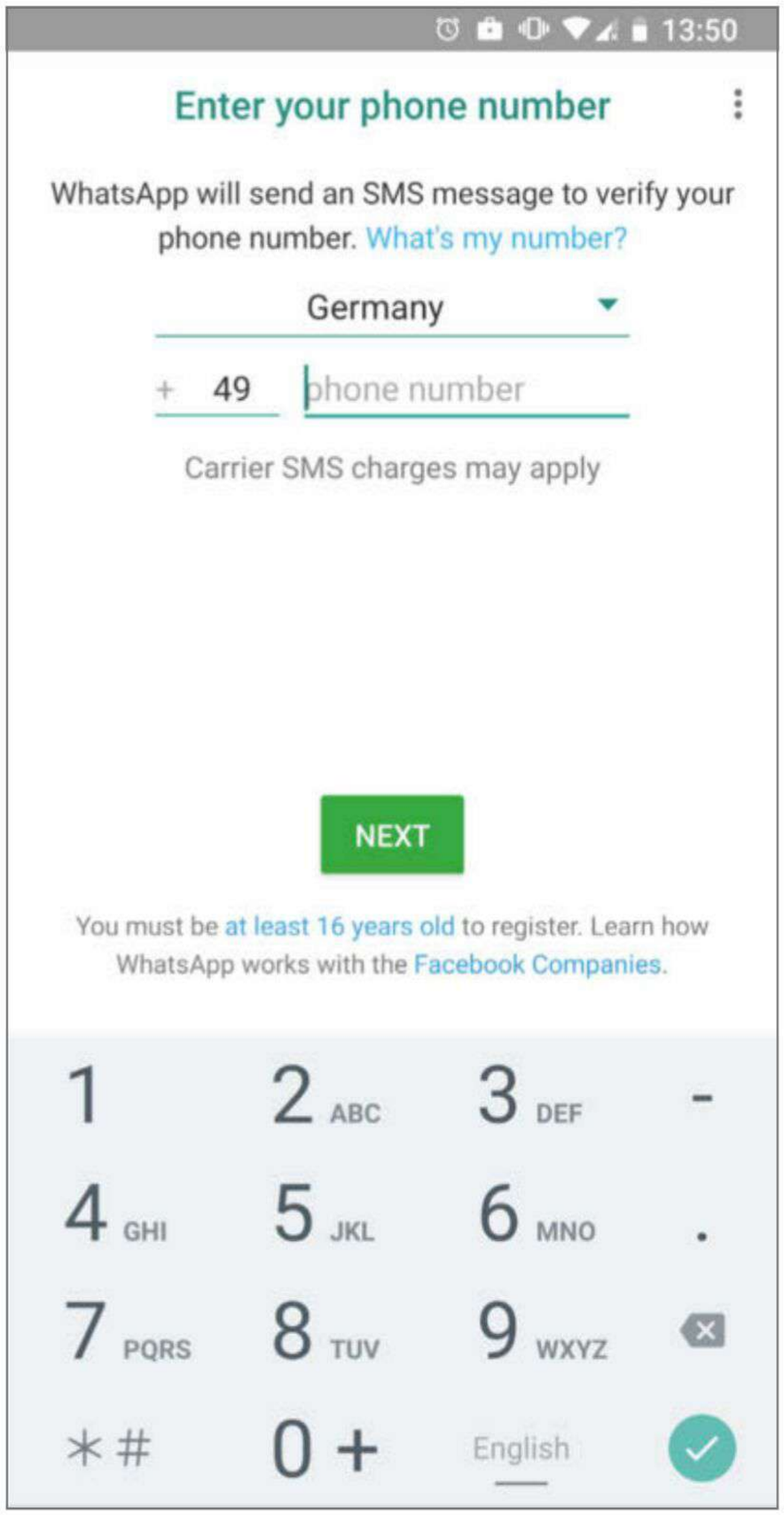
Messenger	Signal	Telegram	Threema	WhatsApp	Slack	Stackfield	Teams
Anbieter	Signal Foundation	Telegram LLC	Threema GmbH	Facebook	Salesforce	Stackfield	Microsoft
Serverstandort	USA	veränderlich	CH	USA	USA	D	USA, EU
Plattformen	Android, iOS, Windows, macOS, Linux	Android, iOS	Android, iOS, Browser	Android, iOS, Windows	Windows, macOS, Linux (Beta), Android, iOS	Windows, macOS, Android, iOS	Windows, macOS, Linux, Browser, Androd, iOS
auf mehreren Geräten nutzbar	✓[1]	✓	–[2]	✓[3]	✓	✓	✓
Client / Server quelloffen	✓ / ✓	✓ / –	✓ / –	– / –	– /–	– / –	– / –
Nutzung							
Funktionen[4]	Zensieren von Gesichtern in Bildern	Add-ons, Bots, Bezahldienst	Umfragen in Chatgruppen	Bezahldienst	Bildschirmfreigabe, programmierbare Abläufe, cloudgestützte Filterfunktionen, API für externe Dienste	Aufgabenverwaltung	Bildschirmfreigabe, Add-ons
E2E-Verschlüsselung	✓	nur in Sonderfällen	✓	✓	✓[5]	✓	–
Kontaktdaten in der Cloud	Nutzer-IDs + Telefonnummern, weitgehend verschlüsselt	Nutzer-IDs + Telefonnummern, unverschlüsselt	nur anonyme Threema-IDs	komplette Nutzer-Adressbücher inkl. Telefonnummern, unverschlüsselt	Nutzer-IDs, unverschlüsselt[6]	Nutzer-IDs, unverschlüsselt[7]	Nutzer-IDs, unverschlüsselt[7]
Schutzfunktionen	PIN oder QR-Code	optischer Code	2FA	2FA	2FA	2FA	MFA über Active Directory

[1] 1 Mobil- + max. 5 Desktop-Clients [2] angekündigt [3] max. 4 Clients (Beta) + Fernsteuerung unter Windows und macOS [4] alle Dienste bieten Einzel- und Gruppenchats, Audio- und Videoanrufe und -konferenzen sowie Dateiaustausch [5] nur über EKM (externe Schlüsselverwaltung) [6] vertraglich regelbar ✓ ja – nein

Trau, schau, wem

Der dritte Knackpunkt betrifft die Identität Ihrer Gesprächspartner. Ein guter Messenger macht es nicht nur schwer, sich im Chat als jemand anderes auszugeben, sondern gibt Teilnehmern auch die Gelegenheit, die Authentizität eines Gesprächspartners zu prüfen. Dieser Schutz ist wichtiger, als man auf Anhieb erkennt: Eine E-Mail, die Sie nach der PIN Ihrer EC-Karte fragt, wird vermutlich sofort Ihren gesunden Menschenverstand alarmieren. Dagegen ist die Situation beim Messenger-Dienst nicht ganz so offensichtlich. Die Nachricht, in der sich angeblich ein guter Freund nach Ihrem WhatsApp-Verifizierungscode erkundigt, lässt sich nach dem Erhalt kaum auf ihre Herkunft prüfen, und scheinbar dient sie nur einer legitimen Sicherheitskontrolle. Doch wenn sich dadurch ein Gauner unter falschem Namen den gewünschten Code erschleicht, kann er damit Ihr WhatsApp-Konto übernehmen, Sie davon aussperren und fortan unter Ihrem Namen auftreten.

Immerhin bemühen sich alle gängigen Messenger, die Zugänge ihrer Nutzer gegen Missbrauch abzusichern. Bei Signal und Telegram können Sie zum Beispiel im Chat einen grafischen Code vom Partner anfordern und mit einer Referenz vergleichen. Für den Fall, dass Sie Ihr Mobilgerät verlieren, lässt sich Missbrauch vorsorglich ausschließen, indem Sie Logins an eine 2FA oder MFA (Zwei-Faktor- oder Multi-Faktor-Authentifizierung) binden.



Viele Messenger nutzen die bestehende Telefonnummer als Gerätekennung und prüfen bei der Installation, dass man die korrekte Nummer eingibt.

Spreu und Weizen

Dienste aus der Mobilfunkszene wie WhatsApp, Telegram, Signal oder Threema unterscheiden sich nur oberflächlich von anderen wie Teams, Slack oder Stackfield, die zuerst als Desktop-Browseranwendungen bekannt geworden sind. Auch wenn sich die Anmeldeprozesse unterscheiden, verschmelzen beide Kategorien miteinander und sind nach denselben Kriterien zu bewerten.

Für WhatsApp, Telegram & Co. registriert man sich mit seiner Telefonnummer per Smartphone, und aus dessen Gerätekennung wird das Benutzerkonto des Dienstes abgeleitet. Wechseln Sie das Handy, womöglich auch ohne Vertragswechsel beim Handy-Provider, müssen Sie den Messaging-Dienst auf das neue Gerät ummelden. Die Einzelheiten variieren von Plattform zu Plattform und von Messenger zu Messenger. Den Prozess starten Sie zum Beispiel aus der auf dem neuen Gerät installierten App heraus und erhalten daraufhin auf dem alten Gerät einen Bestätigungscode, den Sie am neuen Gerät eingeben müssen. Threema ist eine Ausnahme: Es funktioniert ohne personenbeziehbares Benutzerkonto über eine zufällig generierte ID, ohne dass man jemals Rückschlüsse auf seine Person ermöglichen müsste.

Besitzen Sie kein Smartphone oder möchten Ihr privates Smartphone nicht für einen beruflich genutzten Dienst registrieren, sind Sie mit diesen Messengern (abgesehen von Threema) schlecht bedient. In diesem Fall fahren Sie besser mit Diensten

wie Teams, Stackfield oder Slack, bei denen Sie sich per Webseite und Passwort registrieren und die Anmeldung in Reaktion auf eine SMS oder E-Mail vom Provider bestätigen.

Unabhängig von Geräte-IDs können Sie alle gängigen Mobil-Messenger schon jetzt oder in Kürze parallel auf mehreren Geräten nutzen – Details finden Sie in der Tabelle. Telegram bietet zusätzlich die Option, die App mit bis zu drei Konten vom selben Gerät aus zu verwenden.

Jenseits des Tellerrands

Messenger wie Rocket.Chat nach dem Jabber-Nachfolgestandard XMPP oder das dezentralisierte Kommunikationssystem Matrix ermöglichen noch weiter reichende Sicherheitsmerkmale: Für diese Dienste können Sie mit quelloffener Software einen eigenen Server einrichten und autark betreiben. Der Ansatz geht allerdings zulasten der Reichweite: Auch wenn sie einen Standard wie XMPP umsetzen, enthalten die meisten dieser Dienste individuelle Erweiterungen und kooperieren nur unvollständig miteinander.

Wenn Sie mit Dissidenten unter einem totalitären Regime chatten möchten, können Sie den Datenschutz mit dem Briar Project auf die Spitze treiben. Das baut auf Ende-zu-Ende-verschlüsselte Verbindungen über das Tor-Netzwerk auf oder funktioniert sogar ganz ohne durchgehende Internetverbindung, etwa über Zwischenschritte mit geschmuggelten USB-Sticks. Dadurch fehlen aber auch viele Komfort-Funktionen und die Partner müssen sich über einen anderen Kanal auf einen Gesprächstermin einigen, weil nichts gespeichert wird. Dafür stellen sie einen Angreifer aber selbst dann vor Probleme, wenn er auch nur die Gesprächsteilnehmer ausmachen will.

(hps) c't

Literatur

[1] WhatsApp-Kontakt per Telefonnumer: heise.de/s/kZpQ

Für Deine Privatsphäre.



TOCA
WWW.TOCA.SITE

- Anrufe sowie das Senden und Empfangen von Daten wird unterbunden.
- Erster faltbarer Faraday-Käfig für Handys; hergestellt aus deutschem Abschirmstoff.
- Kompakt, wasserdicht und fair produziert.

GPS Daten WLAN Bluetooth NFC/RFID

GET YOURS!
Jetzt QR-Code scannen und Versandkosten sparen.
CTMAGFREESHIP

Für Geschäftsanfragen: sales@toca.site



Bild: Albert Hulm

Abhörsicher telefonieren

Der Ausbruch von Corona war der Durchbruch für viele Kommunikations-Apps: Sie sind als Ersatz für persönliche Treffen mit Familie, Freunden und Kollegen eingesprungen. Doch Anrufe und Videotelefonate lassen sich in vielen Fällen leicht abhören. Mit der richtigen App haben Lauscher jedoch keine Chance.

Von **Ronald Eikenberg**

Wenn man Familie, Freunde und Kollegen nicht persönlich treffen kann, dann bleibt man zumindest per Ton und Bild in Kontakt – der modernen Technik sei Dank. Doch diese Kommunikationswege bergen Tücken, denn anders als beim Vieraugengespräch vor Ort ist die Vertraulichkeit oft nicht gegeben. Schlimmstenfalls kann jeder die Gespräche belauschen, der den Datenverkehr abzwacken kann.

Doch auch modernere Kommunikationsmittel wie Microsoft Teams oder Telegram sind nicht automatisch sicher. Dabei kommt zwar eine Transport-

verschlüsselung zum Einsatz, diese sorgt aber nur dafür, dass die Gespräche jeweils zwischen Gesprächsteilnehmer und Anbieter verschlüsselt sind. Wenn der Anbieter wollte – oder im Falle einer behördlichen Anordnung muss – kann er die Telefonate und Videogespräche seiner Nutzer also problemlos aufzeichnen.

Die gute Nachricht ist, dass Sie sich leicht schützen können, indem Sie vorhandene Verschlüsselungsfunktionen aktivieren oder einen anderen Dienst nutzen. Denn bei vielen Anbieter ist eine gute, nachvollziehbare Verschlüsselung längst Standard. Im Idealfall kommt eine Ende-zu-Ende-Verschlüsselung (E2E) zum Einsatz, die gewährleistet, dass nur die Gesprächsteilnehmer den Anruf entschlüsseln können. Damit kommunizieren Sie annähernd so sicher, als würden sie sich im gleichen Raum wie Ihr Gesprächspartner befinden.

Eine der meistverbreiteten Apps ist ohne Zweifel **WhatsApp** (siehe S. 18). Es ist also naheliegend, die Chat-App auch für Telefonate und Videochats zu verwenden. In puncto Verschlüsselung spricht auch nichts dagegen: WhatsApp nutzt das Secure Real-Time Transport Protocol (SRTP) für die Audio- und Videokommunikation. Die Gespräche sind E2E-verschlüsselt und lassen sich nach derzeitigem Stand nicht belauschen. Im einfachsten Fall rufen Sie besser über WhatsApp an als vollkommen unverschlüsselt über Festnetz oder Handy-Telefonat. Das funktioniert sogar in Gruppen mit bis zu 8 Teilnehmern. Mit den Desktop-Apps für Windows und macOS kann man auch am Rechner videotelefonieren, WhatsApp Web unterstützt dies aktuell nicht.

Doch die Sache hat auch einen Haken: und der heißt Facebook. Der Megakonzern hat sich WhatsApp vor einiger Zeit einverleibt und verdient sein Geld bekanntlich mit den Daten seiner Nutzer. Die Versuchung, sich zumindest an den Metadaten der Nutzer zu bedienen und zum Beispiel das Telefonbuch auszuwerten, ist groß. Und falls eines Tages eine Krypto-Backdoor angeordnet werden sollte, dann wäre WhatsApp vermutlich der erste Dienst, der sie umsetzen muss.

Sicheres Signal

Wer Wert auf Datenschutz legt, greift daher zu **Signal**. Die App funktioniert wie WhatsApp und nutzt die gleiche Verschlüsselung, versucht aber möglichst wenig Metadaten anfallen zu lassen und ist Open Source. Wer möchte, kann also eigenhändig im Quellcode nach Backdoors suchen. Auch über Signal kann man



Zoom bietet auch Gratis-Nutzern eine Ende-zu-Ende-Verschlüsselung für Videomeetings.

in Ton und Bild telefonieren, das klappt auch am Rechner. Vor Kurzem wurden die Videocalls für Gruppen mit bis zu fünf Teilnehmern freigeschaltet.

Viele weitere Chat-Apps eignen sich inzwischen ebenfalls für verschlüsselte Anrufe, darunter etwa **Threema** und **Wire**. Während man bei Threema aktuell nur mit einer Person gleichzeitig sprechen kann, unterstützt Wire bereits Gruppenanrufe mit bis zu 25 Teilnehmern. Bei Videocalls liegt das Limit bei 12 Teilnehmern. Grundsätzlich gilt: Wählen Sie am besten den Messenger, den die meisten Ihrer Kontakte bereits einsetzen. Apple-Nutzer können über **FaceTime** durchgängig Ende-zu-Ende-verschlüsselt kommunizieren, erreichen darüber allerdings ausschließlich andere Apple-Nutzer. Das Limit liegt hier bei 32 Teilnehmern.

Googles Pendant heißt **Google Duo** und setzt ebenfalls auf E2E, das Limit liegt ebenfalls bei 32 Personen. Passende Apps gibt es für Android und iOS, am Rechner kann man auf die Web-App per Browser zurückgreifen. Google macht auf seiner Website kein Geheimnis daraus, dass Metadaten wie Telefonnummern und Geräte-IDs der Gesprächsteilnehmer „ungefähr einen Monat lang sicher auf Google-Servern“ gespeichert werden, „um Fehler zu beheben und Funktionen zu verbessern“.

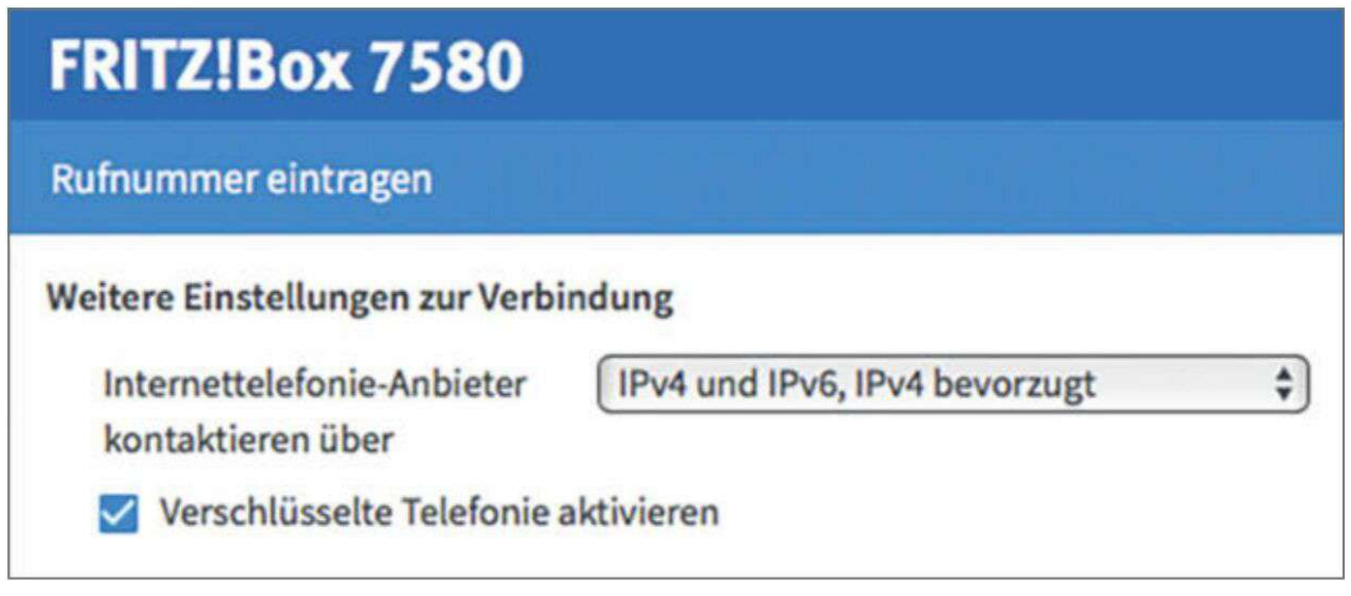
Berufsgeheimnis

Im beruflichen Umfeld muss eine Videochat-Lösung für virtuelle Meetings gruppentauglich und am Rechner nutzbar sein. **Microsoft Teams** ist zwar komfortabel und dockt nahtlos an andere Microsoft-Produkte an. Doch dieser Komfort hat einen hohen Preis: Teams beherrscht aktuell keine E2E-Verschlüsselung. Vertrauliche Gespräche, die vormals in Konferenzräumen von Angesicht zu Angesicht geführt wurden, lassen sich somit prinzipiell belauschen, wenn man Zugriff auf die Microsoft-Server erlangt. **Skype**-Anrufe sind nur dann E2E-verschlüsselt, wenn man explizit einen „privaten Anruf“ startet. Das klappt allerdings noch nicht mit der Web-Version des Tools.

Die Videokonferenz-Plattform **Zoom** ist schon einen großen Schritt weiter und beherrscht E2E-verschlüsselte Videokonferenzen mit bis zu 200 Teilnehmern (siehe Whitepaper unter ct.de/wygq). Die Verschlüsselung kann von jedem Gastgeber aktiviert werden. Klicken Sie hierzu auf der Zoom-Website nach dem Einloggen auf „Mein Account/Einstellungen“ und schalten Sie die Option „End-to-End-Verschlüsselung nutzen“ ein. Zudem sollten Sie darunter die „Vorgegebene Verschlüsselungsart“ auf „End-to-End-Verschlüsselung“ stellen, damit Ihre Meetings bestmöglich geschützt sind. Verwechseln Sie die Funktion jedoch nicht mit der „Erweiterten Verschlüsselung“: Diese ist weniger sicher, da hier auch Zoom die Schlüssel für die E2E-Verschlüsselung kennt.

Innerhalb eines Meetings erkennen Sie die E2E, indem Sie auf den grünen Schutzschild oben links klicken. Steht dort „Verschlüsselung: Durchgehend“, dann haben Sie alles richtig gemacht. Darunter können Sie mit „Verifizieren“ einen Sicherheitscode anzeigen, dieser muss bei allen Gesprächsteilnehmern identisch sein. Eine E2E-Verschlüsselung gibt es auch für andere professionelle Videokonferenz-Programme wie **Cisco WebEx**. Erkundigen Sie sich am besten direkt beim Anbieter nach dem aktuellen Stand der Dinge.

Im Idealfall nutzen Sie für vertrauliche Kommunikation keine fremde Infrastruktur, sondern betreiben den Server im eigenen Haus. Das hat den Vorteil,



Fritzboxen können Festnetzgespräche (VoIP) verschlüsselt übertragen. Sie müssen die Option nur noch einschalten.

dass sie alles unter Ihrer Kontrolle haben, einschließlich der Metadaten. Die Gespräche verlassen das Firmennetz bestenfalls erst gar nicht und die Mitarbeiter im Homeoffice werden verschlüsselt über VPN angebunden. Gute Fortschritte macht die quelloffene Videokonferenz-Lösung **Jitsi**. Sie können den Server selbst betreiben, passende Clients gibt es für iOS und Android und als Web-Version. Das Entwicklerteam ist gerade dabei, eine E2E-Verschlüsselung zu implementieren. Sie können die Funktion schon jetzt ausprobieren. Wer eine Nextcloud betreibt, der kann mit **Nextcloud Talk** ebenfalls Ende-zu-Ende-verschlüsselt in Echtzeit kommunizieren.

Festnetz verschlüsselt

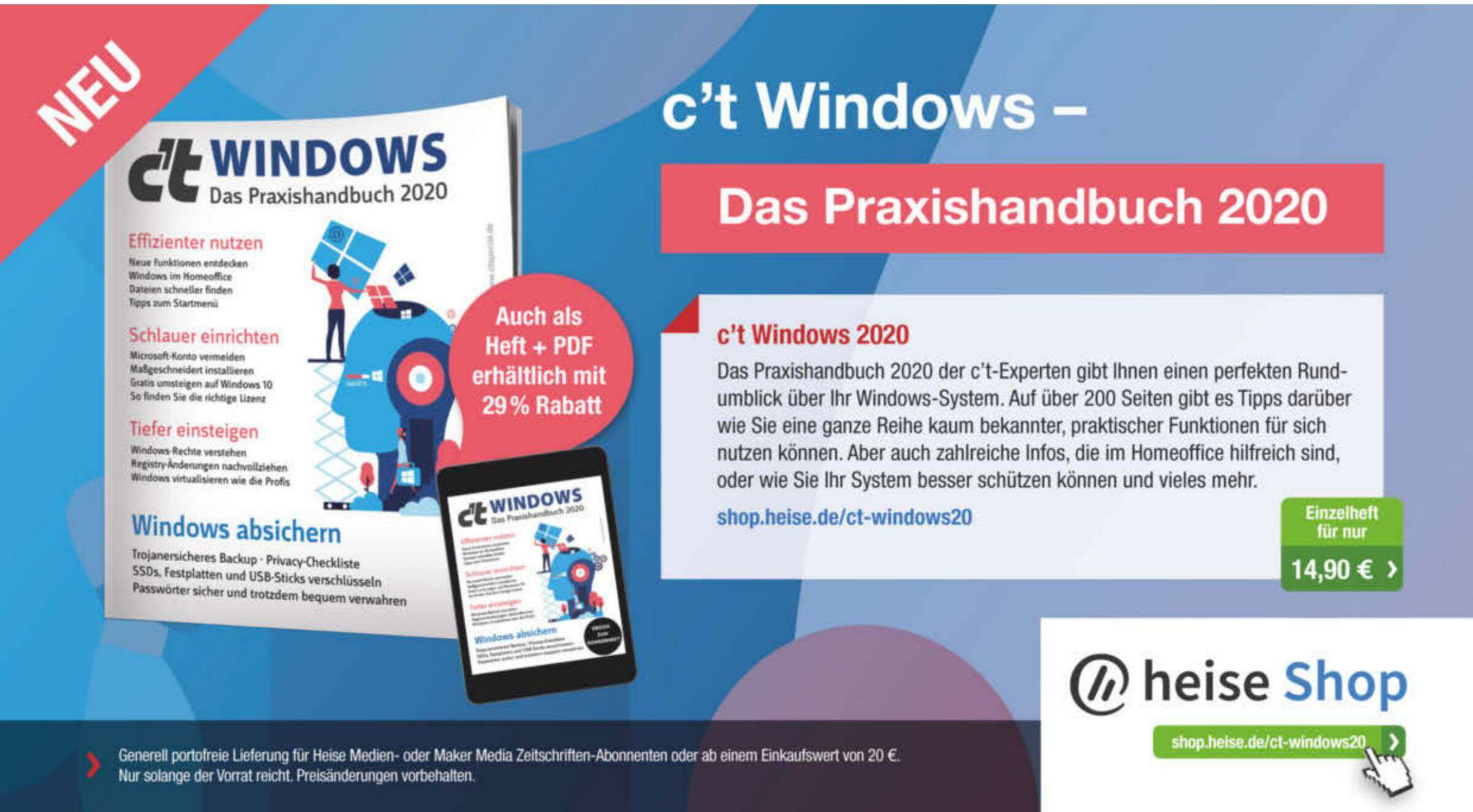
Wie eingangs erwähnt, ist auch die Festnetztelefonie problematisch: Die meist per VoIP übertragenen Gespräche sind vollkommen unverschlüsselt. Wer die Daten auf dem Transportweg zum Ziel abgreift, kann die Gespräche problemlos mithören und manipulieren. Eine E2E-Verschlüsselung ist zwar nicht ohne Weiteres umsetzbar, jedoch ist zumindest eine Transportverschlüsselung zum VoIP-Anbieter drin: Bei den **AVM-Fritzboxen** können Sie seit FritzOS-Version 7.20 die verschlüsselte Telefonie aktivieren. Spielt Ihr VoIP-Anbieter mit, dann werden die Gespräche verschlüsselt zu ihm übertragen – und im Idealfall auch von dort aus weiter verschlüsselt zum Gesprächspartner. Hierbei kommt SIP-over-TLS (SDES-sRTP) zum Einsatz.

Apps & Hintergrundinfos

ct.de/wygq

Fazit

Ganz gleich, ob es um die Alltagskommunikation mit Familie und Freunden oder virtuelle Meetings im Homeoffice geht: Mit der Wahl des richtigen Kanals können Sie schon jetzt in allen Fällen komfortabel und verschlüsselt kommunizieren. Es gibt keinen Grund, es nicht zu tun und auch das Argument „Ich habe doch nichts zu verbergen“ zählt schon lange nicht mehr. Gerade in Zeiten, in denen Apps das persönliche Treffen ersetzen, sollten Sie so viel verschlüsseln, wie Sie können. (rei) c't



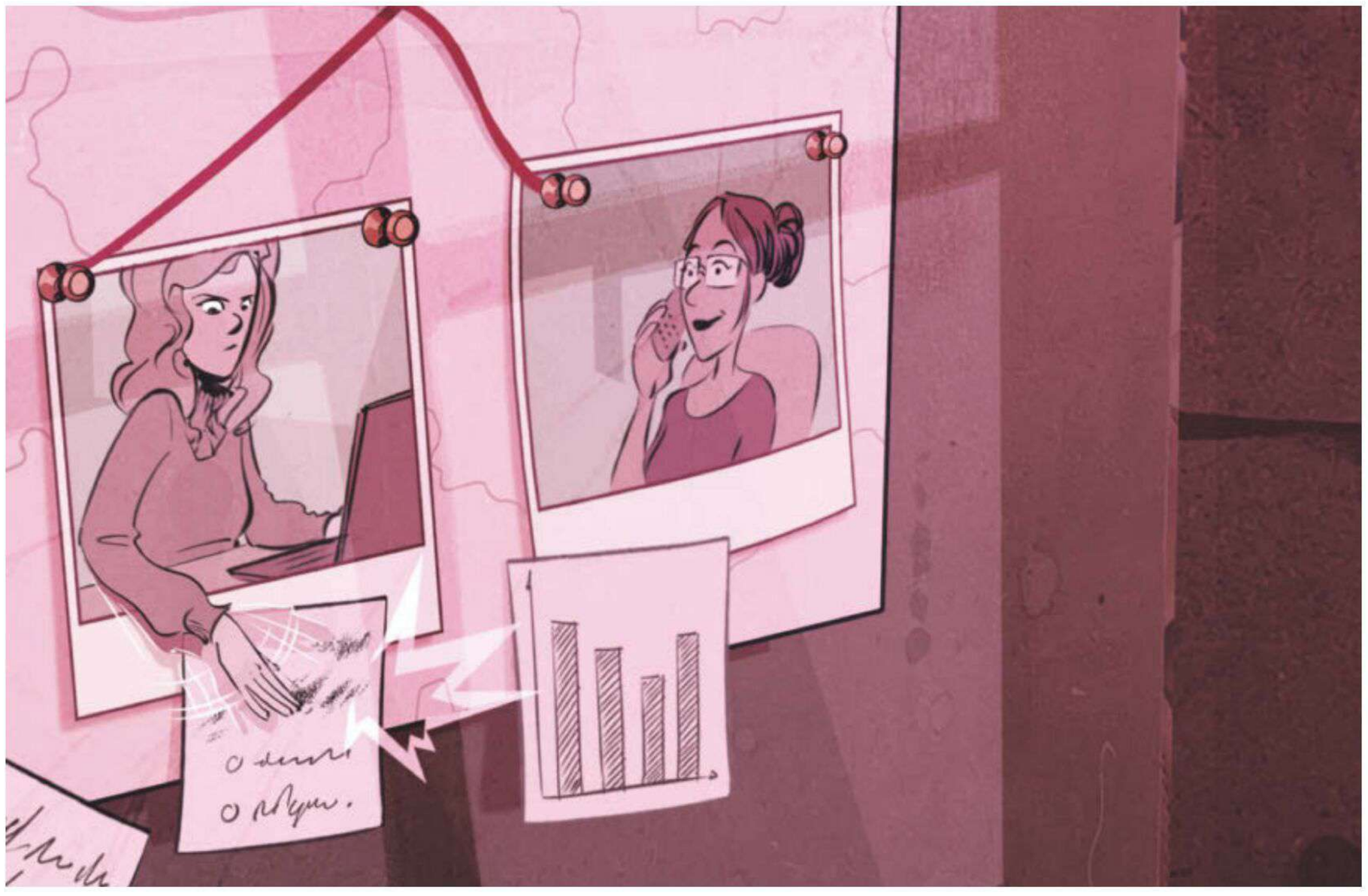


Bild: Albert Hulm

E-Mails bestmöglich absichern

„E-Mails sind nicht sicher“, hat vermutlich jeder schon mal gehört. Benutzt werden sie trotzdem und ganz so schlimm ist die Situation auch nicht: Die wichtigsten Sicherungen lassen sich nachrüsten.

Von **Sylvester Tremmel**

Als E-Mails aufkamen, galt es, Computernetzwerke gegen atomare Erstschläge zu sichern. Seither hat sich einiges geändert – die Gefahren sind eher Malware und Industriespionage, womit das Medium leider kaum Schritt hielt: Mails sind standardmäßig weder verschlüsselt noch authentifiziert – von fortschrittlicheren kryptografischen Eigenschaften ganz zu schweigen.

Unterwegs verschlüsselt

Relativ weit gekommen sind E-Mails bei der Transportverschlüsselung. Heutzutage ist es üblich, seine Mails nur transportverschlüsselt abzuholen, egal ob per IMAP oder POP3. Das geschieht, indem der Mail-Client eine verschlüsselte Verbindung aufbaut (TLS) oder eine normal aufgebaute Verbindung nachträglich

verschlüsselt (STARTTLS). Beides beherrschen praktisch alle Clients und Mailserver, Sie müssen nur sicherstellen, dass Ihr Mailprogramm in den Servereinstellungen TLS oder STARTTLS nutzt. Auf diese Weise verhindern Sie zumindest, dass WLAN-Betreiber oder andere Gäste im öffentlichen Hotspot mitlesen.

Schwieriger wird es schon beim Versand von E-Mails. Hier sind zwar ebenfalls TLS und STARTTLS verbreitet, aber die so initiierte Transportverschlüsselung reicht naturgemäß nur bis zum eigenen Mailprovider. Von dort muss die E-Mail weiter zum Provider des Adressaten und diese Übertragung geschieht unter Umständen unverschlüsselt, je nachdem ob die beteiligten Mailserver angeben, Verschlüsselung zu unterstützen. Zwischengeschaltete Angreifer (man in the middle, MITM) können diese Angaben sogar manipulieren und so eine unverschlüsselte Verbindung erzwingen, auch wenn eigentlich TLS verfügbar wäre.

Als Endnutzer können Sie dagegen nicht viel ausrichten. Es gibt Ansätze, solche Attacken zu verhindern (zum Beispiel via DANE oder den Standard MTA-STS), aber sie werden noch nicht universell unterstützt. Letztlich hängt es von den beteiligten Mail-Providern ab, ob Transportverschlüsselung zum Einsatz kommt. Initiativen wie „E-Mail made in Germany“ garantieren Verschlüsselung zumindest bei Übertragungen zwischen ihren Mitgliedern. Es gibt auch Mailserver, etwa die des Landes Niedersachsen, die Mails nur annehmen, wenn sie transportverschlüsselt eingehen. Manche Mail-Provider – zum Beispiel mailbox.org oder posteo.de – bieten auch die Option, E-Mails gar nicht erst zu versenden, wenn sie keine Transportverschlüsselung aufbauen können. Die Option finden Sie – falls Ihr Provider sie anbietet – in dessen Webmail- oder Account-Verwaltung.

Aber auch mit durchgehender Transportverschlüsselung werden E-Mails nicht zum absolut sicheren Medium. Zum einen können immer noch alle beteiligten Mail-Provider mitlesen. Die Verschlüsslung besteht nur zwischen ihnen, um Lauschern auf der Leitung einen Strich durch die Rechnung zu machen. Die Provider-Systeme sehen die E-Mails im Klartext. Wenn es um unternehmensinterne Mails geht und der firmeneigene Mailserver der einzige beteiligte „Provider“ ist, dann mag dieser Zustand akzeptabel sein. Erstrebenswert ist er jedenfalls nicht. Vielleicht verlassen die Mails ja doch irgendwann den Firmenserver – zum Beispiel wenn das Unternehmen sich für ein Cloud-Backup entscheidet.

Zum anderen gibt es auch bei transportverschlüsselten Mails keinerlei Authentifizierung: Eine Mail von chef@example.com muss keineswegs wirklich vom Account „chef“ und den Servern in der Domain example.com stammen – ein Grund, warum E-Mail-Spam so alltäglich ist. Mit SPF, DKIM und DMARC gibt es wieder verschiedene Ansätze, die die Situation verbessern. Sie setzen sich aber (wie DANE und MTA-STS) nur langsam durch und sind nichts, was Sie als Endnutzer in der Hand haben [1].

Immer verschlüsselt

Sie können die Probleme allerdings angehen, indem Sie Ende-zu-Ende-Verschlüsselung nutzen (End-to-end encryption, E2EE). Dann kann niemand auf dem Weg mehr mitlesen, auch nicht die Mail-Provider. Gängige E2EE-Methoden erlauben außerdem, Nachrichten zu authentifizieren, indem der Versender sie digital signiert. Zwei Varianten von E2EE sind im E-Mail-Universum verbreitet: S/MIME und OpenPGP. „Verbreitet“ ist allerdings relativ zu verstehen – die allermeisten E-Mails nutzen keine Ende-zu-Ende-Verschlüsselung.

Wie E-Mail selbst sind auch S/MIME und (Open-) PGP recht betagt und haben mit Alterserscheinungen zu kämpfen. Manche Designentscheidung würde man heutzutage anders treffen und fortschrittlichere Eigenschaften wie perfect forward secrecy oder post-compromise security (siehe S. 132) lassen sich damit kaum realisieren. Das sollte Sie aber nicht davon abhalten, S/MIME oder OpenPGP zu nutzen. Besser als Mails ohne E2EE sind die Systeme allemal.

S/MIME ist vor allem im Firmenumfeld verbreitet. Um es zu nutzen braucht man ein kostenpflichtiges Zertifikat. Dafür unterstützen die meisten E-Mail-Clients S/MIME out-of-the-box. Wie Sie S/MIME einrichten und wo es Zertifikate zu annehmbaren Preisen gibt, haben wir im Sonderheft c’t Daten schützen 2020 beschrieben [2]. Kostenlos und gerade im privaten Umfeld verbreiteter ist OpenPGP. Auch das haben einige Clients eingebaut, für diverse andere (inklusive Outlook) gibt es Plug-ins. Mit Mailvelope existiert sogar ein Browser-Add-on, das OpenPGP für Webmailer nachrüstet und von verbreiteten Mailprovidern wie GMX oder Web.de unterstützt wird.

Einfach ist was anderes

OpenPGP wird – leider aus guten Gründen – nachgesagt, dass es kompliziert und lästig in der Handhabung sei. Die verschiedenen Implementierungen versuchen auf unterschiedliche Weise, diese Komplexität zu verbergen oder zugänglich zu machen.

Vergleichsweise einfach ist es beim Mail-Client Thunderbird, der seit Version 78 OpenPGP eingebaut hat. Langjährige Nutzer des zuvor verfügbaren Plugins Enigmail üben an der Neuimplementierung durchaus Kritik, aber gerade für PGP-Neulinge bietet sich der Mailer an: Man bekommt alles Nötige aus einer Hand, kann nicht allzu viel falsch machen und im Fall von Problemen ist die Community groß. Eine Einführung in Thunderbirds PGP-Funktionen, finden Sie in c't 19/2020 und c't 7/2021 [3, 4].

Man muss auch nicht vollständig auf Thunderbird umsatteln, nur weil man gelegentlich Mails verschlüsseln will (und mit der PGP-Unterstüzung des eigenen Clients nicht zurande kommt). E-Mail basiert auf offenen Standards und nichts spricht dagegen, zwei oder mehr Clients parallel zu nutzen – zumindest für IMAP-Nutzer. Auch proprietäre Systeme wie Microsofts Exchange bieten IMAP- und SMTP-Schnittstellen, über die Thunderbird parallel genutzt werden kann.

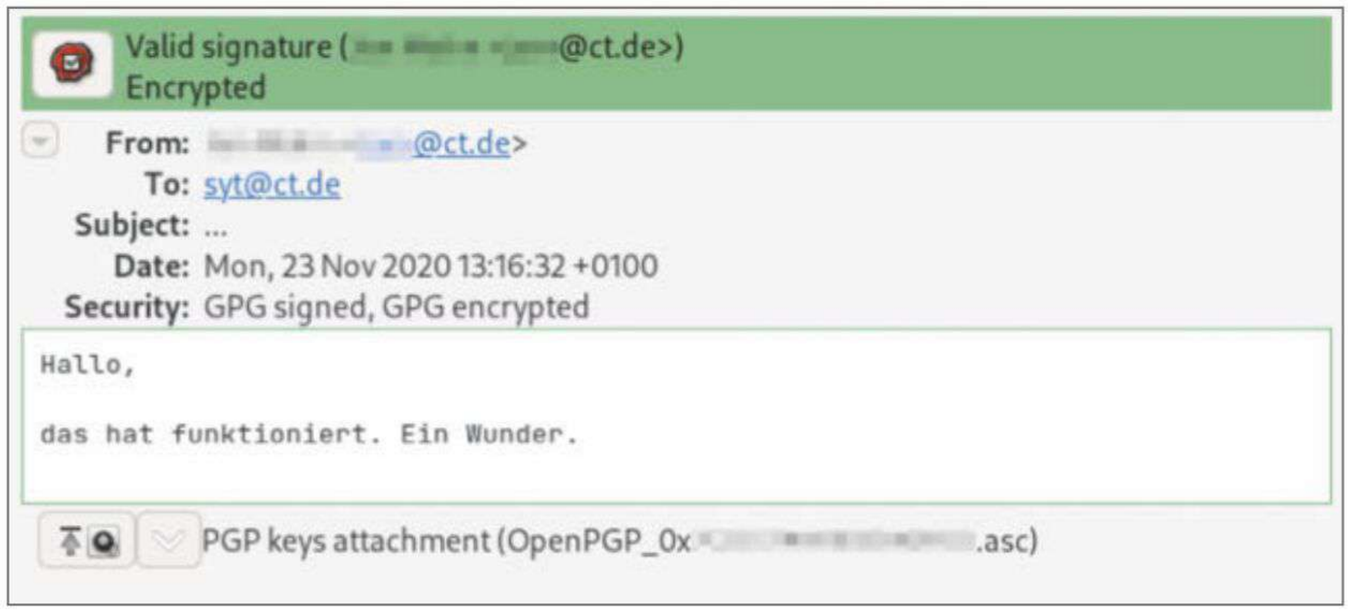
Schlüsselverwaltung

Einige Probleme von OpenPGP kann aber kein Client übertünchen, etwa das der Schlüsselverwaltung. Ihren privaten PGP-Schlüssel müssen Sie hüten wie Ihren Augapfel: Gerät er in die falschen Hände, kann jeder in Ihrem Namen E-Mails signieren und aktuelle sowie in der Vergangenheit aufgezeichnete Kommunikation entschlüsseln. Schützen Sie den Schlüssel daher mit einem Passwort (Thunderbird macht das über das Master-Passwort) und lassen Sie nicht jedermann an Ihren Mail-Client.

Auch vor Verlust müssen Sie den privaten Schlüssel schützen, um alte Nachrichten für immer lesen zu können. Wichtig ist das auch bei Nachrichten, die archiviert werden sollen. Am besten exportieren Sie den privaten Schlüssel in ein sicheres Backup.

Ihren öffentlichen PGP-Schlüssel müssen Sie dagegen publizieren, damit Gesprächspartner mit Ihnen verschlüsselt Kontakt aufnehmen können. Idealerweise kann auch niemand gefälschte Schlüssel in Ihrem Namen publizieren und so Korrespondenten in die Irre führen. Das von OpenPGP dafür vorgesehene Konzept namens Web of Trust hat aber eklatante Mängel. Eine verbreitete Notlösung ist der Server keys.openpgp.org. Für dort publizierte Schlüssel wird allerdings nur sichergestellt, dass die E-Mail-Adresse stimmt. Manche Clients – inklusive Thunderbird – können direkt bei keys.openpgp.org suchen, wenn kein passender Schlüssel lokal vorhanden ist.

Es gibt Projekte wie Pretty Easy Privacy (pEp), Autocrypt oder Web Key Directories (WKD), die OpenPGP-Verschlüsselung und insbesondere die problematische Schlüsselverwaltung weiter vereinfachen wollen. Zumindest aktuell ist ihre Unterstützung bei Clients aber so eingeschränkt, dass sie sich nicht allgemein nutzen lassen. Thunderbird unterstützt immerhin WKD und Teile der Autocrypt-Spezifikation.



Verschlüsselt und signiert, alles grün. Leider beherrscht das abgebildete Evolution keine Betreffverschlüsselung und zeigt nur drei Punkte an.

Metadaten

Ein weiteres Problem von E-Mails können auch die E2EE-Lösungen nicht beheben: Es fallen massenweise Metadaten an. Absurderweise ist sogar der Betreff einer E-Mail technisch gesehen ein Metadatum und wird deswegen üblicherweise nicht verschlüsselt. Das zumindest ändert sich langsam, Mailer wie Thunderbird verschlüsseln auch den Betreff. Dadurch zeigen allerdings Clients, die zwar OpenPGP kennen, aber nicht diese Betreffverschlüsselung, immer „…“ als Betreff an.

Echte Metadaten wie Adressaten und Sende- oder Empfangszeitpunkte lassen sich bei E-Mails grundsätzlich nicht verschlüsseln, sie werden zur Zustellung benötigt beziehungsweise fallen dabei an. Um das zu ändern, müsste man ein neues Protokoll einführen, mit dem normale E-Mail-Clients und -Server nicht kompatibel wären. Wer wann mit wem redet, wissen also auch mit E2EE alle beteiligten Mailserver (bei durchgängiger Transportverschlüsselung immerhin nur die). Nicht alles lässt sich nachträglich in ein 50 Jahre altes Protokoll einbauen. Wer mehr will – oder sich einfach nur möglichst wenig mit Verschlüsselung beschäftigen möchte – sollte seine Kommunikation auf Messenger umstellen (siehe S. 10). (syt) c't

Literatur

[1] Leo Dessani und Jan Mahn, **DKIM-Fail**, Fehler bei Hostern gefährden die Sicherheit von DKIM, c't 01/2021, S. 126

[2] Holger Bleich, **Einfach vertraulich**, Unkomplizierte Verschlüsselung und Signierung von E-Mails mit S/MIME, c't Daten schützen 2020, S. 106

[3] Sylvester Tremmel, **Eingebaute Verschlüsselung**, OpenPGP-Unterstützung in Thunderbird 78, c't 19/2020, S. 154

[4] Sylvester Tremmel, **FAQ: PGP-Verschlüsselung mit Thunderbird**, https://heise.de/-5074725

enterJS

Die Konferenz für Enterprise-JavaScript

29. – 30. September 2021 – Online

www.enterjs.de

Jetzt Tickets zum Frühbucher-Rabatt sichern!

Veranstalter

iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

heise Developer

dpunkt.verlag

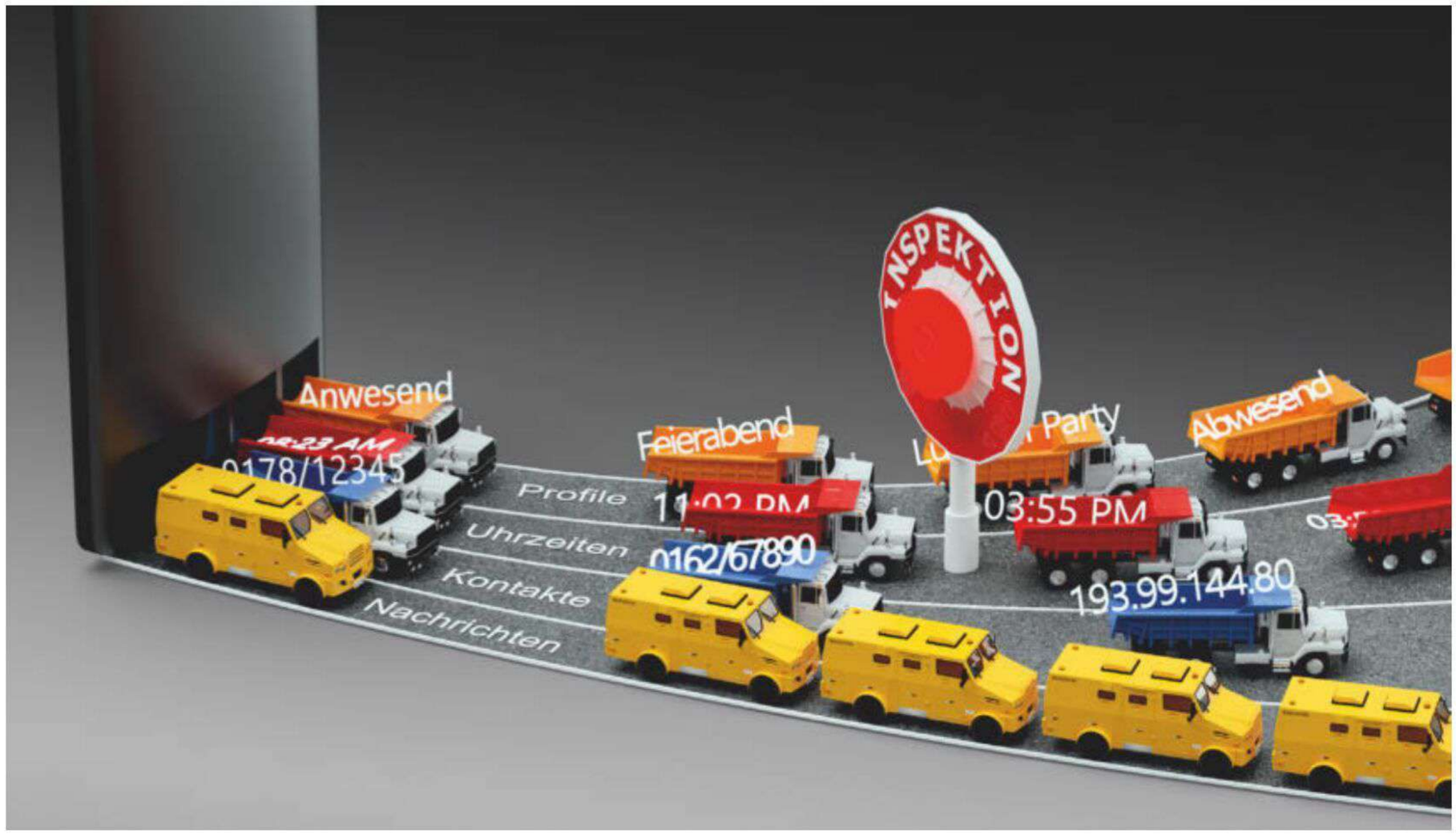


Bild: Andreas Martini

Messenger auf Metadaten-Diät

Seit immer mehr Messenger Ende-zu-Ende-verschlüsseln, rücken die sogenannten Metadaten in den Fokus. Aus ihnen lassen sich viele Schlüsse ziehen – kein Wunder, dass WhatsApp mit Metadaten eher indiskret umgeht. Andere Messenger machen das besser.

Von **Sylvester Tremmel**

Metadaten sind Daten über Daten. Im Kontext von Messengern gehören dazu zum Beispiel die Accounts von an einem Chat beteiligten Personen, Informationen über die Mitglieder einer Gruppe, Versand- und Empfangszeitpunkte und so weiter – Informationen, die zwar zur Kommunikation gehören, aber nicht selbst Inhalt der Kommunikation sind. Ende-zu-Ende-Verschlüsselung schützt Metadaten nicht, weshalb Chat-Betreiber und teilweise auch Dritte diese trotzdem auswerten können.

Aus solchen Auswertungen lassen sich vielfältige Schlüsse ziehen. Neben den Freundes- und Bekanntenkreisen – die viel verraten – kann man zum Beispiel auch Tagesabläufe rekonstruieren: Die erste Reaktion auf eine Nachricht vom Vorabend schränkt den Zeitpunkt des Aufstehens ein. Eine Messenger-App, die sich werktäglich unter der IP-Adresse eines Unternehmens meldet, lässt auf den eigenen Arbeitgeber schließen. Ulmer Forscher konnten allein aus dem Anwesenheitsstatus bei WhatsApp zum Beispiel

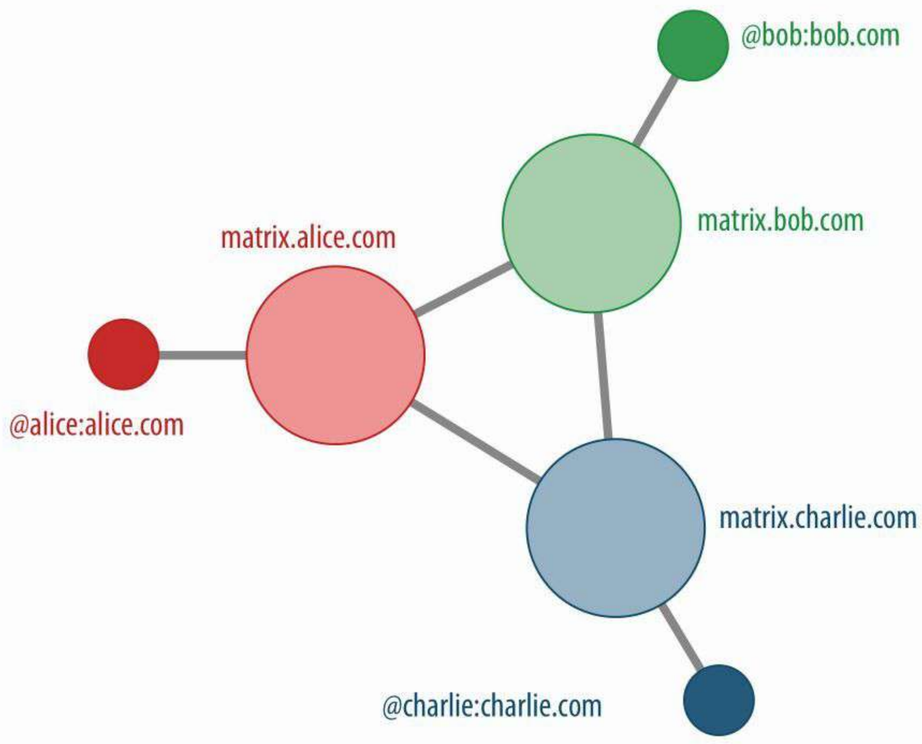
Tagesabläufe und Abweichungen davon rekonstruieren sowie herausfinden, wer mit wem sprach [1].

Aber wie verhindert man solche Rückschlüsse? Nachrichten haben nun mal notwendigerweise einen Absender, eine Reihe von Empfängern und werden zu bestimmten Zeitpunkten versendet und empfangen. Metadaten gänzlich zu vermeiden ist tatsächlich nicht möglich. Aber man kann sie reduzieren, Zugriffe auf sie beschränken und vermeiden, dass Metadaten miteinander oder mit anderen Daten korreliert werden.

Es lässt sich zum Beispiel nicht verhindern, dass Sende- und Empfangszeitpunkte existieren. Man kann sich zwar einen Messagingdienst suchen, der angibt, solche Daten nicht zu speichern, aber kontrollieren kann man das nicht. Wer dem Versprechen nicht traut, muss eigene Server betreiben: Der Messenger Element nutzt zum Beispiel Matrix, ein offenes Chatprotokoll. Wer will, kann selbst einen Matrix-Server aufsetzen und darüber zum Beispiel mit der eigenen Familie chatten. Um Metadaten muss man sich dann keine Sorgen machen. Neben Matrix ist auch das offene Chatprotokoll XMPP verbreitet. Beide Protokolle „föderieren“, man kann also auch mit Leuten chatten, die sich bei anderen Servern angemeldet haben – dann muss man sich aber wieder um Metadaten sorgen und den Betreibern dieser Server vertrauen.

Föderationen

Matrix-Server „föderieren“, sodass es viele Server (große Kreise) geben kann und trotzdem alle Nutzer (kleine Kreise) miteinander chatten können. Wer einen eigenen Server aufsetzt und keine Unterhaltung über Servergrenzen hinweg führt, muss sich um Metadaten kaum Sorgen machen.



Schutz durch Pseudonyme

Der Messenger Threema geht das Problem anders an. Er versucht zu verhindern, dass entstehende Metadaten aufschlussreich sind: Threema kann zwar sehen, dass Account X Nachrichten mit Account Y austauscht, aber Accounts werden bei Threema über bedeutungslose Kennungen identifiziert. Mit der Information, dass „UVB8A8CN“ mit „63IMJ3F7“ chattet, lässt sich – egal ob mit oder ohne Uhrzeit – wenig anfangen. Ähnliches lässt sich bei Messengern wie Element oder Wire erreichen. Sie erlauben, Benutzernamen frei zu wählen – wer sich eine sinnlose Zeichenkette als Name ausdenkt, chattet unerkannt.

Bei Messengern, die stattdessen E-Mail-Adressen oder Telefonnummern als IDs nutzen, können die Accounts deutlich leichter Personen zugeordnet werden. Schlimmstenfalls ist die Telefonnummer öffentlich verzeichnet und die E-Mail-Adresse enthält den vollen Namen. Trotzdem gehen auch datenschutzfreundliche Messenger diesen Weg, weil dadurch Gesprächspartner einander viel leichter finden – wer kennt schon die Threema-ID jedes Arbeitskollegen. Ab Seite 34 haben wir ausführlich erklärt, wie Messenger versuchen, mit dieser Problematik umzugehen.

Damit pseudonyme Adressen wirklich schützen, dürfen Nutzer sie natürlich nicht mit anderen identifizierenden Daten verknüpfen. Wenn „UVB8A8CN“ als E-Mail-Adresse „max-mustermann@firma.de“ im Account hinterlegt hat, ist zumindest für den Dienstbetreiber klar, mit wem „63IMJ3F7“ chattet. Aber auch ohne solche Fehler können pseudonyme Adressen nicht verhindern, dass Netzwerke entstehen. A redet mit B und C, C antwortet B nur selten, chattet aber viel mit D und so weiter. Solche Netzwerke lassen sich – zumindest theoretisch – mit anderen bekannten sozialen Graphen vergleichen, um herauszufinden, wer A, B, C und D sind. Und bekannte soziale Graphen stehen von Google über Facebook zu Twitter vielfach zur Verfügung.

Von der Post lernen

Um solche Vergleiche unmöglich zu machen, wissen Messenger-Anbieter idealerweise gar nichts über

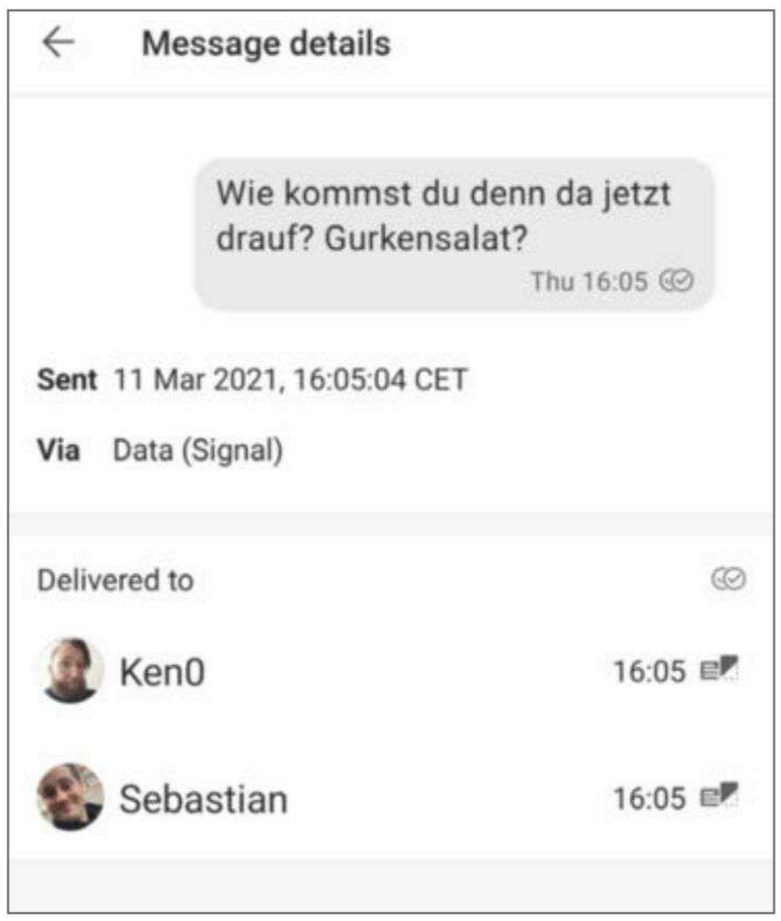
die Bekanntschaftsnetzwerke. Aber wie soll Alice Bob eine Nachricht schicken, ohne dem Dienstbetreiber zu offenbaren, dass Alice und Bob sich kennen? Dass das möglich ist, zeigt ein analoges Beispiel: Die Post stellt einen Brief von Alice an Bob auch dann zu, wenn Alice nicht als Absender auf dem Brief vermerkt ist.

Damit das praktisch funktioniert – und auch wirklich die Kommunikation zwischen Alice und Bob verschleiert – müssen aber zwei Voraussetzungen erfüllt sein. Erstens muss es eine Art Briefkasten geben, der anonym Briefe annimmt. Wenn Alice mit ihrem Brief zum Postamt geht, ist es unerheblich, ob sie einen Absender notiert; die Post sieht ja, wer den Brief aufgibt. Zweitens muss man solche Briefkästen irgendwie vor Spam schützen. Wenn jeder und jede unerkannt Briefe einwerfen darf, wäre unerwünschte Post sonst kaum zu vermeiden. Bei der realen Post schützen die Kosten für eine Briefmarke – bedingt – vor Spam.

Der einzige Messenger im Test auf Seite 10, der so ein System tatsächlich umsetzt, ist Signal. Die App nennt das Feature „Sealed Sender“ (siehe ct.de/wtqw). Es ist für Nachrichten von bekannten Kontakten immer aktiv und funktioniert im Prinzip wie das Beispiel mit der Post: Statt sich am Server anzumelden und eine Nachricht samt Adressat abzugeben, kontaktiert die App den Server anonym und übergibt die Nachricht. Der Server stellt sie dann zu, ohne zu wissen, von wem sie stammt.

Damit man Nachrichten nicht unter falschem Namen versenden kann, ist eine Sealed-Sender-Mitteilung zweifach verschlüsselt. Der Empfänger B entfernt die erste Verschlüsselung und findet darin die eigentliche Nachricht und eine Art Unterschrift des Absenders. So überprüft er, dass die Nachricht von A kommt, was der Server ja nicht weiß. Wenn die Nachricht authentisch ist, entfernt B auch die innere Verschlüsselung und liest die Nachricht.

Das Spam-Problem umgeht Signal, indem es Sealed-Sender-Nachrichten nur von Kontakten erlaubt, die der Empfänger bereits kennt. Wer solchen Missbrauch nicht fürchtet, kann die Beschränkung in den Einstellungen der App aufheben.



Auf Wunsch zeigt Signal den Sealed-Sender-Status an (kleine Icons rechts unten): Die Nachricht wurde an beide Gesprächspartner übermittelt, ohne dass der Server wusste, von wem sie stammt.

Verkehrsüberwachung

Sealed-Sender verhindern auf der Ebene des Messenger-Protokolls, dass bekannt wird, wer mit wem redet. Hundertprozentigen Schutz bieten sie aber nicht. Zum Beispiel lassen sich Sender und Empfänger von Nachrichten auch auf Ebene der IP-Adressen korrelieren. Wenn IP X 3412 Bytes an einen Messenger-Server schickt und der gleich darauf 3412 Bytes an IP Y, dann liegt der Schluss nahe, dass X mit Y chattet.

Solche Traffic-Analysen kann nicht nur der Messagingdienst selbst anstellen, sondern auch ein Lauscher auf der Leitung oder der Server- beziehungsweise Rechenzentrums-Dienstleister. Traffic-Analysen sind aber, zumindest bei einigermaßen rege genutzten Messengern sehr aufwendig. Systeme wie Sealed Sender bieten daher durchaus einen echten Nutzen – ganz besonders für Dienste wie Signal, die Telefonnummern als Adressen verwenden. Wem das nicht reicht, der muss zu extremeren Maßnahmen wie dem dezentralen Messenger Briar greifen: Der nutzt das Tor-Netzwerk, um Nachrichten auszutauschen und dabei die beteiligten IP-Adressen zu verschleiern. Aber auch Tor garantiert keine absolute Sicherheit, und Briars kompromissloser Fokus auf Datenschutz schränkt die Benutzerfreundlichkeit durchaus ein. Zum Beispiel müssen Kommunikationspartner gleichzeitig online sein, um chatten zu können.

IP-Adressen sind nicht nur problematisch, weil sie eventuell verraten, wer mit wem redet. Sie lassen sich oft auch einem geografischen Gebiet zuordnen und verraten damit den ungefähren Aufenthaltsort. Messenger tun das einerseits gegenüber dem Chat-Anbieter und eventuellen Dienstleistern – ungut, aber ein ganz allgemeines Problem: Jeder Webseitenaufruf verrät dem Webseitenbetreiber dieselbe Information (und noch viel mehr).

Problematisch wird die Geolokalisierung von IP-Adressen auch an anderer Stelle, nämlich wenn Chatpartner Sprach- oder Videoanrufe tätigen. In gängigen Implementierungen tauschen die beteiligten Apps dabei direkt Daten aus und leiten sie nicht über Server des Anbieters. Das verrät den Gesprächsparteien die IP-Adressen ihrer Gegenüber. Wer das ist, wissen sie meist ohnehin, aber die IPs erlauben eben auch eine Einschränkung des Standorts, was eventuell nicht gewünscht ist. Manche Messenger erlauben daher, auch Sprach- und Videodaten über den Anbieterserver zu leiten. Je nach Standort und Auslastung des Servers kann das aber die Performance beeinträchtigen.

Members only

Neben dem eigentlichen Nachrichtenaustausch können Messagingdienste auch noch durch eine andere verbreitete Funktion erfahren, wer wen kennt – durch Gruppen. Auf den ersten Blick mag das überraschen: Gruppenmitglieder kennen einander natürlich, aber wieso muss der Dienstanbieter wissen, wer in welcher Gruppe ist? Tatsächlich muss er das an sich nicht. Damit Alice, Bob und Charlie eine Gruppe bilden, reicht es im Prinzip, wenn die drei sich darauf einigen. Nachrichten an so eine „Gruppe“ sind ganz normale Nachrichten, nur sendet jeder eben immer zwei Stück gleichzeitig. Alice sendet an Bob und Charlie, Bob an Alice und Charlie und Charlie an Alice und Bob. Für den Anbieterserver ist nichts besonderes zu erkennen, er weiß nicht mal, dass eine Gruppe existiert.

Tatsächlich hat Signal seine Gruppen früher so organisiert, aber dieser naive Ansatz hat erhebliche Probleme. In modernen Messengern sind Gruppen nämlich nicht nur eine Ansammlung von Nutzern. Sie haben einen Namen und eventuell ein Bild oder eine Beschreibung – alles schützenswerte Metadaten. Außerdem sollen gelegentlich neue Mitglieder aufgenommen oder alte entfernt werden. All das muss man bei diesem Ansatz über Nachrichten zwischen den Gruppenmitgliedern lösen, der Anbieter weiß schließlich nicht mal, dass eine Gruppe existiert.

Solche Verwaltungsnachrichten, die Gruppeninformationen ändern und Mitglieder bearbeiten, können sich aber überschneiden, wenn mehrere Gruppenmitglieder sie parallel versenden. Diese Race-Conditions treten bei Messengern leicht auf: Gruppenmitglieder sind oft nicht gleichzeitig online und es dauert dadurch lange, bis Nachrichten alle Mitglieder erreicht haben.

Vollends an seine Grenzen stößt der Ansatz, wenn Gruppenmitglieder unterschiedliche Rechte haben sollen. Welche Instanz kontrolliert, wer was darf? Was, wenn sich eine Nachricht zum Entzug eines Rechts mit einer anderen Nachricht, die dieses Recht ausübt, überschneidet? Letztlich ist auch Signal wegen solcher Beschränkungen von dem System abgerückt und speichert Gruppeninformationen mittlerweile auf dem Server. Andere Messenger machen das seit jeher so; deren Betreiber wissen also, wer in welchen Gruppen ist, wie Gruppen heißen et cetera.

Um diesen Preis nicht zu zahlen, verschlüsselt Signal die Gruppeninformationen so, dass der Server sie nicht lesen kann. Das ist alles andere als trivial, schließlich soll der Server das Rechtesystem durchsetzen. Er muss also entscheiden, ob ein Nutzer die Informationen ändern darf, ohne zu erfahren, wer dieser Nutzer ist. Die Signal-Entwickler haben sich dafür mit Kryptografie-Forschern von Microsoft zusammengetan und ein mathematisch ausgefeiltes System von „anonymous credentials“ – anonymen Legitimationen – erarbeitet (siehe ct.de/wtqw).

Fazit

Ganz ohne Metadatenspuren kann man nicht chatten. Manche Informationen lassen sich kaum vermeiden und manche Einschränkungen führen zu weit. Man kann es aber zumindest besser machen als WhatsApp. Dieser Messenger nutzt nämlich (anders als Threema) keine pseudonymen IDs, erlaubt (im Gegensatz zu Element) keine eigenen Server und versucht nicht (wie Signal) Kontakte und Gruppenmitgliedschaften zu verschleiern. Rigorose Versprechen, Metadaten nicht zu speichern oder weiterzugeben, findet man bei WhatsApp ebenso wenig. Alle genannten Alternativen bieten also Vorteile gegenüber WhatsApp, am weitesten treibt Signal die Metadatenvermeidung. Die ideale Schnittmenge – verschleierte Absender und Gruppen, eigene Server und pseudonyme IDs – bietet aktuell allerdings keiner der Messenger. (syt) c't

Literatur

[1] Andreas Buchenscheit et al, Privacy Implications of Presence Sharing in Mobile Messaging Applications: https://dl.acm.org/doi/10.1145/2677972.2677980

Informationen zu Sealed Sender und anonymen Gruppen

ct.de/wtqw



Bild: Albert Hulm

Telefonnummern als Messenger-IDs

WhatsApp und Signal funktionieren ohne Angabe der Telefonnummer gar nicht, Telegram will sie zumindest bei der Accounteröffnung kontrollieren und auch Threema bietet an, das Adressbuch auszulesen. Warum machen die Messenger das, wenn doch XMPP oder Matrix beweisen, dass es auch ohne geht?

Von **Sylvester Tremmel**

Software zur sozialen Vernetzung steht vor einem doppelten Problem: Ein neuer Dienst funktioniert nur dann gut, wenn, erstens, viele Menschen ihn nutzen und diese, zweitens, sich auch gegenseitig finden können. Letzteres wird häufig mit dem englischen Begriff „Contact Discovery“ bezeichnet und ist schwierig zu lösen. Selbst wenn man weiß, dass Max Mustermann den Dienst nutzt, woher weiß man, dass sein Account „themaxman0815“ heißt? Einen Vorteil bieten hier Produkte wie der Facebook Messenger, die an ein etabliertes soziales Netzwerk angeschlossen sind. Wer Leute

auf Facebook kennt, kann sie auch per Messenger erreichen. Sich an Konzerne wie Facebook zu binden, ist aus Datenschutzsicht aber sehr bedenklich und kommt gerade für Freunde sicherer Messenger eher nicht in Frage. Aber welche anderen Netzwerke könnte man nutzen?

Soziales Netzwerk frei Haus

Ein soziales Netzwerk im allgemeinen Sinne, nämlich Familie, Freunde und Bekannte, hat jeder – und in der Regel ist dieses Netzwerk auch dokumentiert: in Form eines Adressbuches, das Telefonnummern und E-Mail-Adressen enthält. Ein Dienst, der darauf zugreifen darf, bekommt die Vernetzung seiner Benutzer praktisch frei Haus. Er muss lediglich deren Adressbücher vergleichen und kann sofort markieren, wer über den Dienst bereits erreichbar ist.

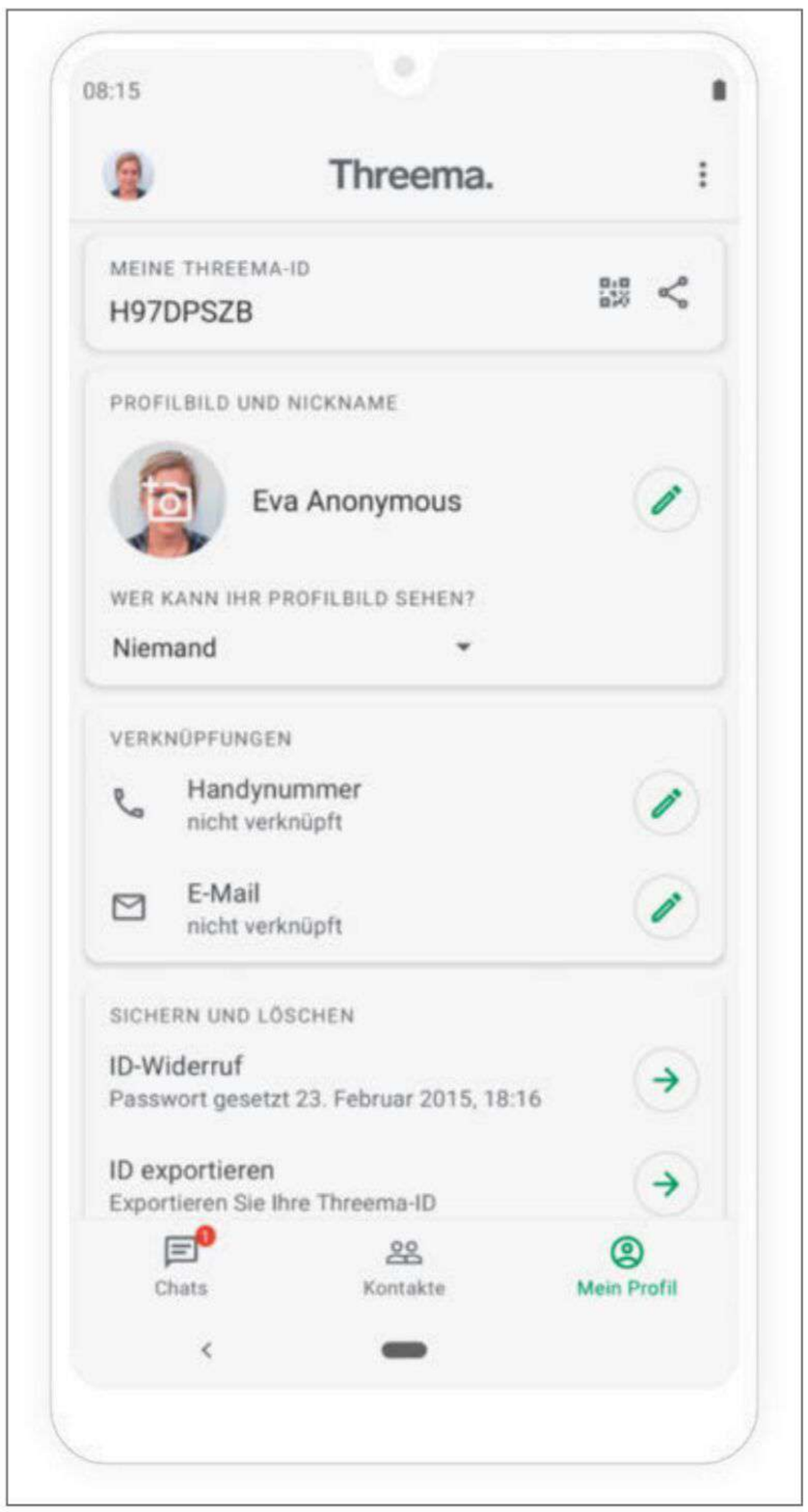
Das ist praktisch für Anbieter und Nutzer und führt zu rasanter Verbreitung, wie zum Beispiel Clubhouse hierzulande im Frühjahr 2021 bewies. So vorzugehen wirft aber auch erhebliche Datenschutzprobleme auf. Der Dienstleister erfährt dadurch nicht nur, welche Nutzer des Dienstes einander kennen, sondern sieht auch alle anderen Kontakte seiner Anwender inklusive Telefonnummern und Mailadressen – Merkmale, die sich gut verknüpfen, für Werbezwecke ausschlachten und anderweitig missbrauchen lassen. Zumindest im Geltungsbereich der DSGVO ist das auch rechtlich problematisch: Telefonnummern sind personenbeziehbar und deshalb zu schützen. Die Kontakte wissen in der Regel aber nicht einmal, dass jemand ihre Nummern zu solch einem Dienst übertragen hat – eingewilligt haben sie erst recht nicht.

Dennoch gehen viele Messenger diesen Weg. Bekanntestes Beispiel ist WhatsApp – was kaum überrascht, schließlich verdient der Mutterkonzern Facebook sein Geld mit Werbung. Aber auch Konkurrenten, die sich als Alternativen mit besserem Datenschutz positionieren, wie Signal oder Telegram, verlangen von ihren Nutzern die Telefonnummer. Wer als Anbieter darauf verzichtet und stattdessen eigene Benutzernamen vergibt, dessen Nutzer können sich nur schwer finden und benötigen einen alternativen Kommunikationsweg, um einander ihre Benutzernamen mitzuteilen – kein guter Start für einen Kommunikationsdienst.

Sogar Dienstleister wie Threema – ein Messenger, der ohne Telefonnummer funktioniert – können sich diesem Wachstumsdruck schlecht entziehen und erlauben ebenfalls, das Adressbuch abzugleichen, um die eigenen Bekannten zu finden. Nach Angaben des Betreibers entscheiden sich etwa 70 Prozent aller Threema-Nutzer dafür.

Unter anderem auf Basis von Protokollen wie XMPP oder Matrix gibt es darüber hinaus noch diverse Dienste, die in den sauren Apfel beißen und auf Telefonnummern oder Mailadressen verzichten. Es ist aber kein Zufall, dass sie weit weniger verbreitet sind als die Konkurrenten, die auf die Analyse bestehender sozialer Netze zurückgreifen.

Bild: Threema GmbH



Keine Handynummer, keine E-Mail-Adresse, nur eine Threema-ID – anonymer gehts kaum, aber woher wissen Evas Freunde, dass sie unter H97DPSZB zu erreichen ist?

Schützen trotz verknüpfen

Doch auch beim Nummernabgleich gibt es gravierende Unterschiede zwischen den Anbietern. Wichtig

ist zu wissen, dass die Contact Discovery per Telefonnummer keine dauerhafte Speicherung des Nutzeradressbuches erfordert. Es reicht, wenn der Service den Adressbuchinhalt mit bekannten Nutzern abgleicht, die Schnittmenge zurückliefert und dann den Adressbuchinhalt löscht. Services wie Threema und Signal versprechen, so vorzugehen, was das Feature datenschutzkonformer macht – falls sie ihr Versprechen halten. Besser wäre, wenn der Server den Adressbuchinhalt gar nicht lesbar zu Gesicht bekäme. Dann müsste man sich auch nicht um den Fall sorgen, dass ein Angreifer den Server übernimmt.

So eine „Private Contact Discovery“ ist leider sehr schwierig. Es bietet sich an, die Nummern (oder Mailadressen) nicht im Klartext zu übertragen, sondern daraus eindeutige kryptografische Hashwerte zu berechnen und diese an den Server zu schicken. Theoretisch kann der Server aus den Hashwerten keine Originaldaten errechnen. Somit spielt es keine Rolle, ob er die Hashes speichert oder nicht.

Praktisch ist die Zahl möglicher Telefonnummern aber sehr überschaubar. Ein böswilliger Anbieter – oder ein Angreifer, der Serverzugriff erlangt hat – könnte einfach alle möglichen Nummern hashen und so nachsehen, welcher Hashwert welcher Nummer entspricht. Solche Tabellen mit Hashwerten zu allen möglichen Eingaben können auch für E-Mail-Adressen erstellt werden.

Zum Schutz von Passwörtern wird gewöhnlicherweise ein zufälliger Wert, ein sogenannter Salt, mit in den Hash einbezogen. Das „Salz“ ist dem Anbieter zwar bekannt, unterscheidet sich aber von Passwort zu Passwort. Dadurch müsste ein Angreifer für jedes Passwort eine eigens berechnete Tabelle erstellen, was den Aufwand enorm in die Höhe treibt. Das Salt-Verfahren lässt sich aber auf Hashes zur Contact-Discovery nicht gut anwenden: Wenn zwei Nutzer dieselbe Nummer hashen, muss derselbe Hash entstehen – eben damit der Kontakt gefunden werden kann. Zufällige Salts würden zu unterschiedlichen Hashes führen, auch wenn die Nummer übereinstimmt.

Trotz dieser Probleme nutzen Messenger wie Threema, Signal oder WhatsApp ungesalzene Hashes von Telefonnummern zur Contact Discovery – schlicht aus Mangel an Alternativen, wie die Signal-Entwickler in ihrem Blog erläutern: Kryptografisch sichere Verfahren bieten entweder wenig Privatsphärenschutz unter realistischen Rahmenbedingungen oder stellen Anforderungen an Rechenkapazitäten, die insbesondere mobile Geräte nicht erfüllen können. Allerdings gibt es hier durchaus Fortschritte in der Forschung (alle Links unter ct.de/wjve).

Einstweilen versucht zumindest Signal, das Maximum aus dem Stand der (Ingenieurs-)Technik herauszuholen und nutzt SGX-Enklaven auf den Servern, um den Hashabgleich durchzuführen. Solche Enklaven sind speziell geschützte Speicherbereiche, auf die andere Programme und sogar das Betriebssystem selbst keinen Zugriff haben. Prinzipiell garantiert das den Chat-Clients, dass der Server tatsächlich nur die Hashes abgleicht und sie danach löscht. Allerdings ist die Implementierung kompliziert und auch die Enklaven selbst wiesen bereits Sicherheitslücken auf [1].

Privat oder anonym?

Ein anderes Problem können auch perfekte Contact-Discovery-Methoden nicht lösen: Telefonnummern und E-Mail-Adressen identifizieren Personen; in vielen Ländern muss man sich sogar ausweisen, um eine Telefonnummer zu erhalten. Selbst wenn ein Messenger diese Informationen anderen Kontakten nicht anzeigt, identifizieren sich Nutzer dadurch gegenüber dem Betreiber des Dienstes. Eine wirklich anonyme Nutzung ist so nicht möglich. Nichtssagende IDs, wie sie zum Beispiel Threema seinen Nutzern zuordnet, sind hier von Vorteil. Zur automatischen Contact Discovery greift Threema wie erwähnt auf Telefonnummern oder Mailadressen zu, aber das ist optional. Wer anonym bleiben will, gibt sein Adressbuch eben nicht heraus – und muss potenziellen Kontakten irgendwie seine Threema-ID zukommen lassen, bevor er den Messenger nutzen kann.

Im Signal-Umfeld wurde das Problem lange als nicht sehr relevant angesehen: Signal sei ein privater, aber eben kein anonymer Messenger, heißt es in den Foren. Der Service veröffentliche schließlich nichts: Nur wer eine Nummer schon kennt, kann nach ihr suchen und erfährt dann, ob ein Signal-Account zu dieser Nummer gehört. Aber wer die Nummer schon kennt, kann ohnehin Kontakt aufnehmen, etwa per Telefon oder SMS.

Das stimmt zwar, aber Anonymität kann dennoch wünschenswert sein. Zum einen sind Services prinzipiell für Crawling-Angriffe anfällig, wenn sie Nutzer über Werte wie Telefonnummern identifizieren, die man durchprobieren kann: Im Rahmen einer Studie vom September 2020 konnten Forscher bei Signal zumindest ausspionieren, welche Telefonnummern den Dienst nutzen und bei Whats-

App und Telegram noch weitergehende Informationen abgreifen (siehe ct.de/wjve). Crawling lässt sich zwar serverseitig einschränken, aber nicht komplett unterbinden.

Zum anderen kann schon die Information, dass eine Telefonnummer einen Dienst nutzt, heikel sein: zum Beispiel, wenn die App im Land der Nummernregistrierung verboten ist. Allmählich scheint man bei Signal umzudenken: Die Entwickler arbeiten offenbar seit einiger Zeit an „Adressierung, die nicht nur auf Telefonnummern basiert“, wie sie es in ihrem Blog nennen. Dabei wird es sich vermutlich um Benutzernamen oder um nichtssagende IDs wie bei Threema handeln, sodass man seine Nummer nicht mehr preisgeben muss, um mit jemandem zu kommunizieren.

Erhebliche Vorarbeiten dazu haben die Entwickler bereits abgeschlossen. Das war nötig, weil Telefonnummern noch einen Vorteil gegenüber IDs oder dienstspezifischen Benutzernamen haben: Sie sind beim Nutzer gespeichert, und zwar nicht nur in der Messenger-App. Das Kontaktnetz ist in den Telefonbüchern diverser Geräte, oft sogar in physischen Adressbüchern dokumentiert und lässt sich rekonstruieren, selbst wenn das Handy kaputt oder verloren geht und man kein Backup der Messenger-App hat. Schlimmstenfalls verliert man also „nur“ die Gesprächsinhalte und nicht auch die Möglichkeit, seine Kontakte mit einem neuen Gerät anzusprechen.

Kryptische IDs oder Benutzernamen einzelner Dienste finden sich aber in der Regel nicht in den Telefonbüchern. Um auch solche Kontaktdaten vor Verlust zu schützen, will Signal sie auf den Servern des Dienstes speichern. Geschähe dies in lesbarer Form, würde das Datenschutzproblem aber größer als je zuvor. Signal hat darum PINs eingeführt, die unter anderem als Schlüssel für Nutzerdaten auf dem Server dienen. Der Anbieter kann Kontakte so chiffriert – und für ihn selbst unlesbar – speichern und Nutzer können sie auch mit einem neuen Gerät rekonstruieren – sofern sie sich an die PIN erinnern.

Fazit

Telefonnummern zur Nutzeridentifikation schienen lange ein notwendiges Übel für erfolgreiche Messenger. Wer sie nutzt, kann deutlich schneller wachsen und die anonyme Konkurrenz hinter sich lassen. Messenger wie Threema beweisen aber, dass die Contact Discovery per Telefonnummer zumindest nicht verpflichtend sein muss. Signal zeigt dagegen, wie gut man die Nummern absichern kann.

Auf das Beste aus beiden Welten muss man aktuell leider noch verzichten. Jedenfalls gibt es keinen technischen Grund dafür, Kontaktdaten grundsätzlich und kaum geschützt hochzuladen, wie es zum Beispiel WhatsApp und neuerdings Clubhouse machen. Aus Anwendersicht ist das unverständlich und legt den Verdacht nahe, dass die Anbieter die Daten sammeln wollen. (syt) c't

Achtung beim Nummernwechsel

Telefonnummern sind ein zweifelhaftes Identifikationsmerkmal. Zum einen kann man sie durch technische Maßnahmen oder Täuschung kapern. Vor allem aber vergeben die Netzbetreiber alte Nummern neu. Das wird zum Problem, wenn der Vorbesitzer die Nummer einem oder mehreren Messengern zugeordnet und seine Accounts nicht um- oder abgemeldet hat: Bekannte des neuen Nummernbesitzers nehmen dann eventuell irrtümlich an, dass er einen WhatsApp- oder Signal-Account hat, weil sie die Accounts des Vorbesitzers sehen. Schlimmstenfalls nutzt der Vorbesitzer den Account sogar noch und erhält darüber Nachrichten, die für den neuen Besitzer der Nummer bestimmt sind.

Besitzer einer neuen Nummer tun daher gut daran, sie zumindest bei den verbreiteteren Messengern selbst zu registrieren und alte Accounts dadurch auszusperren. Wer den Dienst nicht selbst nutzen will, kann den Account anschließend löschen.

Aus dem gleichen Grund sollte man Accounts nach einem Nummernwechsel umziehen und nicht unter der alten Nummer weiter betreiben – auch wenn das unpraktisch sein kann. Andernfalls riskiert man, vom neuen Besitzer einer Nummer unvermittelt und unwiderruflich ausgesperrt zu werden.

Literatur

[1] Christof Windeck, **Datenstrom**, Sicherheitslücke „Platypus“ nutzt Leistungsmessfunktion von Intel-Prozessoren, c't 25/2020, S. 34

Private Contact Discovery

ct.de/wjve

Wie Sie Ihre digitale Identität schützen

Schützen Sie Ihre digitale Identität – sie ist ein wertvolles Gut! Mit einigen gezielten Maßnahmen und Strategien können Sie das Risiko, Opfer von Identitätsmissbrauch zu werden, deutlich reduzieren und dafür sorgen, dass sich der Schaden im Fall der Fälle in Grenzen hält.

Von **Ronald Eikenberg**

Passwörter im Griff

So schützen Sie Ihre digitale Identität	38
Passwörter sicher und bequem verwalten	46
So wechseln Sie zu KeePassXC	54
2FA-Generator Reiner SCT Authenticator	60
Universal-Sicherheitsschlüssel TrustKey	64

Es gibt zwei Arten von Menschen: Die einen wurden Opfer von Identitätsdiebstahl, die anderen werden es noch. Die gute Nachricht ist, dass Sie wenig zu befürchten haben, wenn Sie einige grundlegende Tipps befolgen. Damit mit der Sicherheit des Hundefutter-Shops oder des Gaming-Forums nicht auch die Sicherheit Ihrer gesamten digitalen Identität steht und fällt, sollten Sie dort so wenig Daten hinterlassen, wie nur irgendwie möglich. Im Idealfall verzichten Sie auf eine Registrierung; in vielen Shops kann man schließlich auch als Gast bestellen.

Wenn eine Anmeldung verlangt wird, geben Sie ein Passwort an, das nur dort zum Einsatz kommt. Ein solches ist für einen Angreifer nämlich nahezu wertlos, nachdem er es erbeutet hat. Denn er kann damit nur etwas anfangen, wenn es auch bei anderen Diensten passt. Am besten nutzen Sie einen Passwort-Manager wie KeePass (siehe S. 46) oder Bitwarden. Damit können Sie für jede Gelegenheit ein neues Passwort wie LXeGqzhiTg generieren. Zugegeben, das kann man sich schwer merken – das nimmt Ihnen jedoch der Passwort-Manager ab. Wenn Sie das konsequent durchziehen und für jeden Dienst ein anderes Passwort einsetzen, dann können Sie sich bei dem nächsten Passwort-Leak entspannt zurücklehnen.



Mit einem Passwort-Manager wie KeePass müssen Sie sich nie wieder Passwörter ausdenken und merken.

Wenn Sie Ihre Passwörter nicht einem digitalen Manager anvertrauen möchten, dann können Sie ganz altmodisch Zettel und Stift verwenden. Verwahren Sie den Zettel an einem sicheren Ort, etwa in Ihrem Portemonnaie, und legen Sie eine Kopie zu Ihren wichtigsten Unterlagen – am besten in einen feuerfesten Tresor. Wenn Sie auf Nummer sicher gehen wollen, können Sie sich ein Grundpasswort wie JRaJ6wUGTo überlegen, das Sie zum Bestandteil aller Passwörter machen – jedoch nicht mit auf den Zettel schreiben. Das ist quasi das Master-Passwort für Ihren Passwort-Manager auf Papier.

Eine beliebte Methode des Passwort-Managements kommt ganz ohne Software und Papier aus: Denken Sie sich eine Methode aus, um im Kopf aus einem Grundpasswort und dem Namen der Seite, bei der Sie sich anmelden möchten, ein Passwort zu generieren. Sie können zum Beispiel den ersten und letzten Buchstaben des Dienstes vorne und die Anzahl der Buchstaben seines Namens hinten an das Grundpasswort anhängen. Aus dem Grundpasswort JRaJ6wUGTo wird im Fall von eBay: eyJRaJ6wUGTo4. Je individueller Ihre persönliche Methode ist, desto besser.

Passwort vergessen

Hat es ein Angreifer gezielt auf Sie abgesehen, wird er nicht lange probieren, das Passwort zu erraten. Damit kommt er bei Online-Diensten viel zu langsam voran. Zudem hat er wahrscheinlich nur eine begrenzte Anzahl an Fehlversuchen. Stattdessen sucht der Eindringling in spe nach anderen Wegen, in Ihren Account einzusteigen. Ein beliebter Weg sind Passwort-Recovery-Mechanismen. Oft ist diese Hintertür nur mit Informationen gesichert, die sich der Angreifer leicht aus sozialen Netzen ziehen kann – etwa dem Mädchennamen Ihrer Mutter.

Bei Passwort-Fragen gilt daher: Lügen Sie, bis sich die Balken biegen! Die einzige Einschränkung ist, dass Sie sich hinterher noch an die Lügen erinnern müssen, damit Sie im Fall der Fälle das Passwort zurücksetzen können. Machen Sie sich also am besten Notizen. Eine weitere Variante wäre, auch hier wieder einen individuellen Teil in die Antworten einfließen zu lassen: Statt in „Hannover“ wurden Sie also etwa in „eyHannover4“ geboren, wenn Sie eBay danach fragt.

Von HPI Identity Leak Checker <sec-checker-admin@hpi.de>
Betreff Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker
An [redacted]

Antworten | Allen antworten | Weiterleiten | Archivieren | Junk | Löschen | Mehr

24.01.2019, 22:04

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse [redacted] taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf.
Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnum
Unknown (Collection #1-5)	Jan. 2019		2.191.498.885	Betroffen	–	–	–	–
	Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannt							
badoo.com	Mär. 2016		122.495.418	Betroffen	Betroffen	Betroffen	–	–
Unknown (Zoosk.com)	Mär. 2013		54.103.990	Betroffen	–	–	–	–
dropbox.com	Sep. 2012	✓	68.658.165	Betroffen	–	–	–	–

Der Identity Leak Checker verrät Ihnen, welche Ihrer persönlichen Daten bereits im Darknet kursieren.

Und wenn Sie schon mal in den Einstellungen Ihrer Accounts sind, sollten Sie dafür sorgen, dass überall valide Notfall-Kontaktinformationen hinterlegt sind. Falls ein Angreifer in Ihren Account eingestiegen ist, können Sie darüber mit etwas Glück die Kontrolle über Ihren Zugang zurückgewinnen.

Faktor zwei

Eine weitere wichtige Schutzbarriere für Ihre Online-Accounts ist die Zwei-Faktor-Authentifizierung (2FA). Ist sie eingeschaltet, benötigen Sie beim ersten Login auf einem Gerät neben Nutzername und Passwort noch einen einmalig gültigen Code. Diesen schickt Ihnen der jeweilige Dienst etwa per SMS aufs Handy. Noch sicherer sind die 2FA-Verfahren TOTP und HOTP, bei denen der Code lokal generiert wird, zum Beispiel von der Smartphone-App Google Authentificator oder einem Hardware-Token wie dem YubiKey.

2FA sorgt dafür, dass Ihr Account auch dann noch geschützt ist, wenn Ihre Zugangsdaten einem Online-Angreifer in die Hände fallen: Versucht sich ein solcher mit Ihren Daten einzuloggen, scheitert er daran, dass er den Einmalcode nicht empfangen kann. Da SMS ein unsicherer Übertragungskanal ist, sollten Sie möglichst ein anderes 2FA-Verfahren wählen. Wenn Sie keine andere Wahl haben, ist die SMS-Übertragung aber immer noch besser, als ganz auf einen zweiten Faktor zu verzichten.

Die Zwei-Faktor-Authentifizierung kann Ihnen aber auch zum Verhängnis werden: wenn sich etwa Ihre Handynummer ändert oder Sie Ihr Smartphone verlieren, auf dem sich die Authentificator-App befindet. Wenn Sie keine Vorsorgemaßnahmen treffen, sind Sie dann von Ihren Accounts ausgesperrt. Falls Sie 2FA per SMS oder Anruf nutzen, müssen Sie die in den Accounts hinterlegten Rufnummern rechtzeitig ändern. Es ist eine gute Idee, mehrere 2FA-Methoden einzurichten, sofern der jeweilige Dienst dies zulässt. Dann können Sie im Fall der Fälle noch auf die zweite Methode zurückgreifen, falls die erste versagt.

Besonders große Sorgfalt sollten Sie bei der Absicherung Ihres Mail-Kontos an den Tag legen. Es ist quasi der Generalschlüssel zu Ihrer digitalen Identität. Wer darauf zugreifen kann, der kann sich auch zu allen anderen Diensten weiterhangeln, die Sie mit Ihrer Mail-Adresse nutzen – ganz einfach über die Passwort-vergessen-Funktion.

Zwei-Faktor-Authentifizierung ist für den Mail-Account daher Pflicht. Wenn möglich, sollten Sie zudem von Zeit zu Zeit einen Blick auf die letzten Kontozugriffe und aktive Sitzungen werfen. Bei Google

finden Sie über ct.de/ww9h eine Übersicht. So können Sie stille Mitleser überführen, die zum Beispiel eine Browser-Sitzung auf einem anderen Rechner nutzen, die Sie nicht explizit beendet haben.

Passwörter prüfen

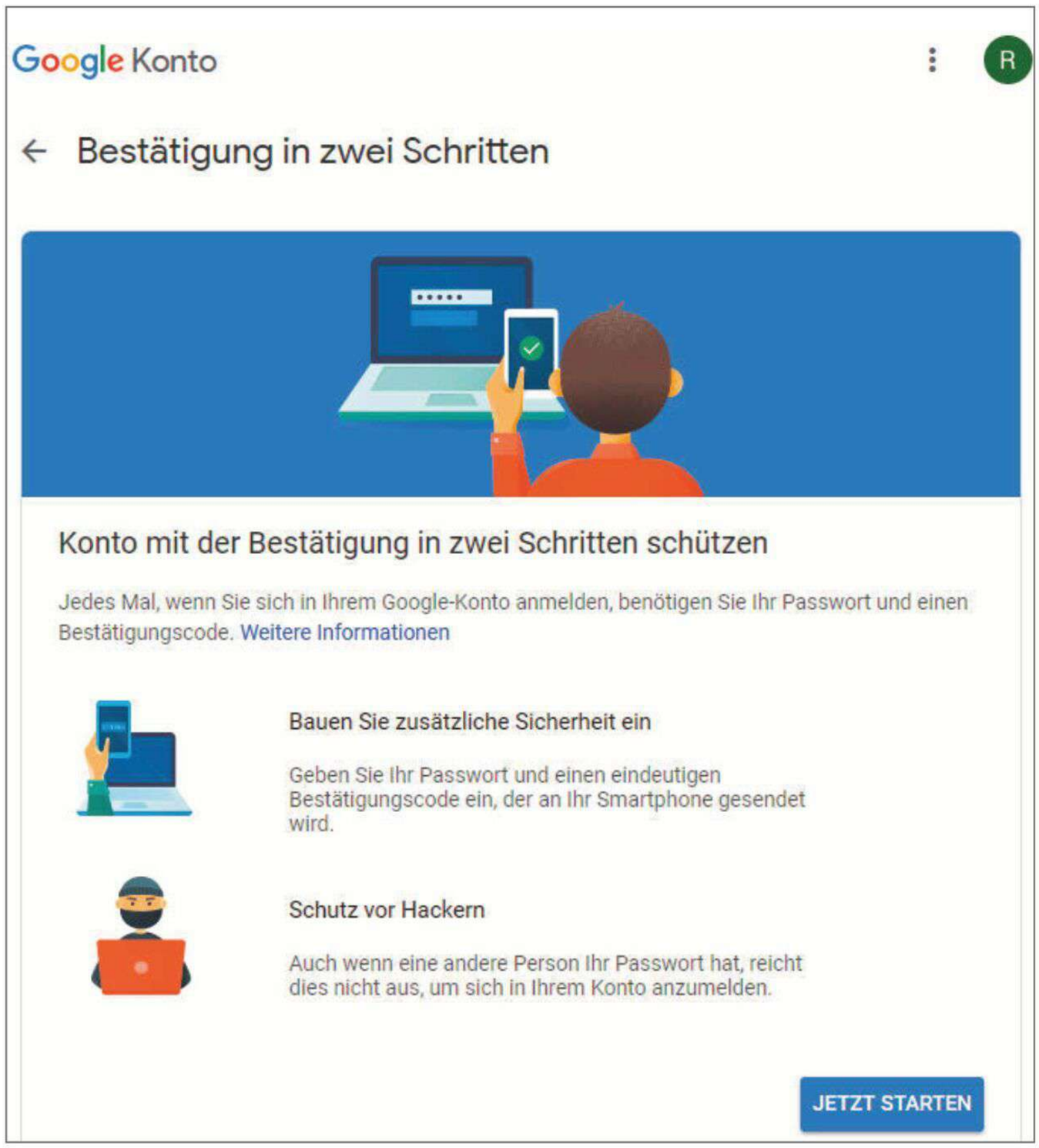
Um herauszufinden, ob Ihre Daten bereits im Darknet gehandelt werden, können Sie die Dienste Have I Been Pwned (HIBP) des Sicherheitsexperten Troy Hunt und den Identity Leak Checker des Hasso-Plattner-Instituts nutzen (siehe ct.de/ww9h). Beide Dienste greifen auf Datenbanken zu, in denen Milliarden gehackte Accounts gelistet sind. Wenn Sie dort eine Mail-Adresse eingeben, erfahren Sie, ob und meist auch bei welcher Gelegenheit Ihre Daten von Cyber-Ganoven abgegriffen wurden. Zudem informieren Sie die Dienste in vielen Fällen darüber, welche Art von Daten betroffen sind – also etwa, ob neben der Mail-Adresse auch ein Passwort oder gar Zahlungsdaten kopiert wurden.

HIBP zeigt Ihnen das Suchergebnis direkt im Browser an, der Identity Leak Checker verschickt seine ausführliche Auswertung per Mail. Die Dienste können zwar bestätigen, dass ein Account betroffen ist. Werden sie nicht fündig, bedeutet das jedoch nicht zwangsläufig, dass Ihre Accounts bisher von Hackern verschont wurden – die Datenbanken kennen zwar sehr viele, jedoch bei Weitem nicht alle Daten-Leaks. Bei HIBP können Sie unter „Notify me“ Ihre Mail-Adresse hinterlassen, um eine Alarm-Mail zu erhalten, wenn Sie von einem neuen Leak betroffen sind.

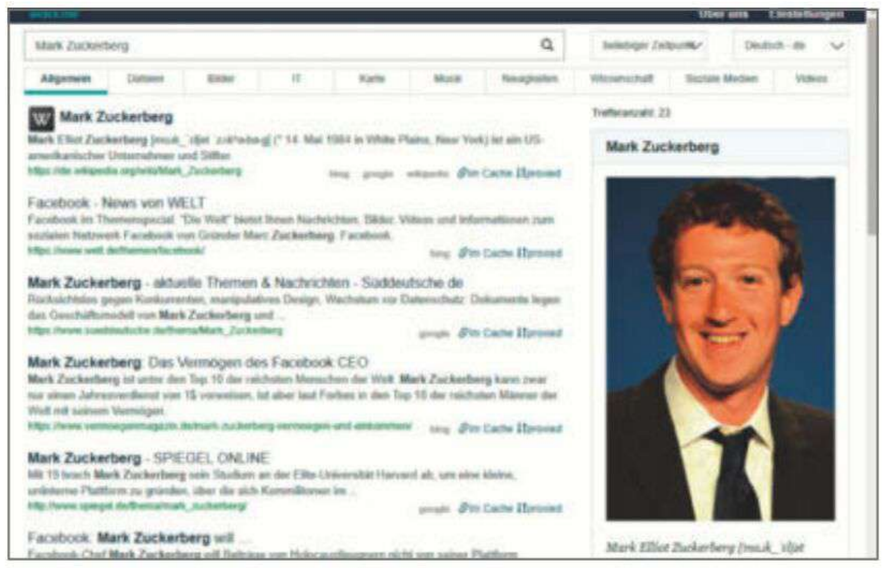
Ebenfalls von Troy Hunt wird Pwned Passwords (siehe ct.de/ww9h) betrieben. Die Seite kennt über 550 Millionen Passwörter, die im Darknet gehandelt werden. Wenn Sie dort Ihr Passwort eingeben, erfahren Sie, ob es bereits in einschlägigen Kreisen kursiert. In diesem Fall sind Sie gut damit beraten, es zu ändern. Grundsätzlich sollten Sie Ihre Kennwörter niemals auf irgendwelchen Webseiten eingeben, die nicht zu dem Dienst gehören, zu dem das Passwort passt. Pwned Passwords ist eine seltene Ausnahme, da die Site zum einen von einem renommierten Sicherheitsexperten betrieben wird und er zum anderen nachvollziehbar dokumentiert, dass die eingetippten Passwörter niemals an seine Server übertragen werden.

Hunt hat einen Verschleierungsmechanismus entwickelt, der verhindert, dass Ihr Passwort übertragen wird: Die Website hasht das Passwort lokal im Browser mit SHA-1 und schickt lediglich die ersten fünf der 40 Stellen des Hashes an den Server. Dieser liefert daraufhin die Hashes aller kursierenden Passwörter zurück, die mit diesen fünf Stellen beginnen. Schließlich überprüft ein JavaScript lokal im Browser, ob sich der Hash des eingegebenen Passworts auf der vom Server gelieferten Liste befindet. Wenn Ihnen das nicht geheuer ist, können Sie die mehrere GByte große Liste der Passwort-Hashes herunterladen und selbst durchsuchen. Wir haben zu diesem Zweck ein kleines Python-Skript entwickelt, das Sie in c't 5/2019 [1] finden.

Inzwischen befragen auch einige Passwort-Manager wie 1Password auf Wunsch die riesige Datenbank von Troy Hunt. So können Sie leicht herausfinden,



Geringer Aufwand, viel Sicherheit: Die Zwei-Faktor-Authentifizierung macht es Angreifern schwer, Ihre Accounts zu kapern.



Stalken Sie sich selbst, bevor es jemand anderes tut: Mit Meta-Suchmaschinen wie searx.me können Sie unerwartete Datenspuren ans Tageslicht fördern.

ob die von Ihnen genutzten Passwörter von einem Leak betroffen sind. Unter ct.de/ww9h finden Sie zudem eine Anleitung, wie Sie die von KeePass verwalteten Kennwörter in einem Rutsch abfragen können. Viele Browser wie Chrome, Edge und Firefox warnen Sie mittlerweile auch selbstständig, wenn ein im Browser gespeichertes Passwort kompromittiert wurde.

Stalke Dich selbst

Begeben Sie sich in die Position eines Fremden, der so viel wie möglich über Sie herausfinden will. Durchforsten Sie das Netz nach Ihrem Namen mit bekannten und weniger bekannten Suchmaschinen wie Google, Bing, Qwant und DuckDuckGo. Nützlich sind auch Meta-Suchdienste wie Searx.me, welche die Suchergebnisse mehrerer Lieferanten zusammenführen. Deaktivieren Sie einen etwaigen Jugendschutzfilter und experimentieren Sie mit Suchregion und -sprache. Ändern Sie die Region etwa in USA, um potenziell weitere Suchtreffer zu landen.

Auch Spezial-Suchmaschinen wie die Personensuche von DasTelefonbuch und Yasni können vergessen geglaubte Informationen über Ihre Person ans Tageslicht fördern (siehe ct.de/ww9h). Überprüfen Sie zudem, ob in sozialen Netzwerken wie Facebook und Business-Netzen wie LinkedIn oder Xing Profile auf Ihren Namen existieren. Haben Sie dort in der Vergangenheit Accounts angelegt, die Sie nicht mehr nutzen, sollten Sie diese löschen. Entdecken Sie Fake-Profile, die andere in Ihrem Namen angelegt haben, melden Sie diese dem Betreiber.

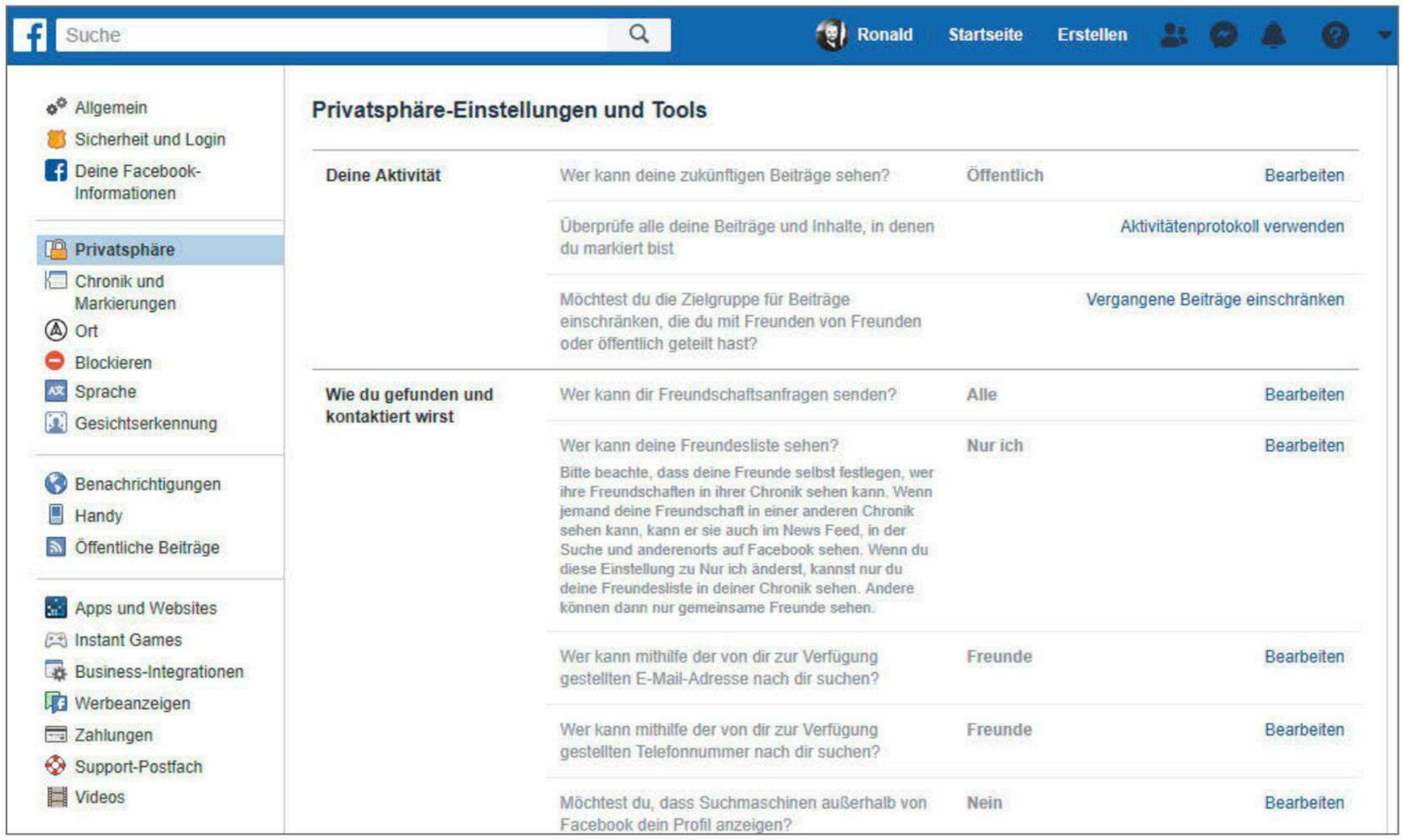
Wer auf dem Laufenden bleiben möchte oder muss – etwa, weil er in der Öffentlichkeit steht –, kann dazu die Google Alerts nutzen (siehe ct.de/ww9h): Wenn Sie einen Alert anlegen, bekommen Sie von Google eine Mail, sobald neue Suchergebnisse zu einem bestimmten Begriff vorliegen.

Sozial abgesichert

Wenn Sie in sozialen Netzwerken wie Facebook unterwegs sind, dann sollten Sie überprüfen, welche Ihrer Daten für Freunde oder gar öffentlich einsehbar sind. Über ct.de/ww9h finden Sie die Privatsphäre-Einstellungen, mit denen Sie unter anderem festlegen, wer zukünftige Beiträge sehen darf. Sehr wichtig sind auch die Optionen im Abschnitt „Wie du gefunden und kontaktiert wirst“. Setzen Sie die Einstellung „Wer kann deine Freundesliste sehen?“ am besten auf „Nur ich“, damit niemand Einblick in Ihr Facebook-Adressbuch erhält. Diese Informatio-



Über ein Online-Formular können Sie Google anweisen, Suchtreffer zu entfernen, die sich auf Ihre Person beziehen.



Facebook ist eine wertvolle Datenquelle für Online-Schurken. Überprüfen Sie genau, wer welche Daten sehen darf.

nen können einem Angreifer helfen, Sie und Ihre Facebook-Freunde anzugreifen.

Über die beiden Einstellmöglichkeiten darunter legen Sie fest, ob Sie über Ihre Mail-Adresse respektive Ihre Telefonnummer bei Facebook aufgespürt werden können. Stellen Sie entweder „Freunde“ oder „Freunde von Freunden“ ein, da ansonsten jeder, der Ihre Mail-Adresse oder Telefonnummer kennt, herausfinden kann, wem sie gehört. Außerdem sollten Sie noch „Möchtest du, dass Suchmaschinen außerhalb von Facebook dein Profil anzeigen?“ auf „Nein“ stellen, damit Ihr Profil nicht von Google & Co. indexiert wird. Facebook bietet Diensten die Möglichkeit, weitreichend auf Ihren Account zuzugreifen. Kontrollieren Sie in den Einstellungen unter „Apps und Websites“, welchen Diensten Sie Zugriff auf Ihr Konto gewährt haben und sortieren Sie gründlich aus.

Ausgesperrt

Zugunsten des Komforts bleibt man bei den meisten Diensten für einen sehr langen Zeitraum eingeloggt. Oder wann haben Sie zuletzt das Login-Formular von Facebook oder Google gesehen? Viele Anbieter lassen die Sitzungen fast beliebig lange offen. Durch Session-Cookies ist man somit immer eingeloggt. Was im Alltag praktisch ist, kann jedoch in einigen Situationen auch unangenehme Konsequenzen haben: Wenn Sie „nur mal eben schnell“ bei einem Kumpel Ihre Mails checken wollen, kann dieser anschließend beliebig lange auf Ihren Posteingang zugreifen und an Ihrem digitalen Leben teilhaben. Noch unangenehmer ist die Vorstellung, dass völlig fremde Personen Zugriff erhalten, nachdem Sie sich etwa in einer Bibliothek oder am Arbeitsplatz eingeloggt haben.

Insbesondere wenn Sie fremde Rechner nutzen, sollten Sie daher immer darauf achten, sich vor dem Gehen bei den Diensten auszuloggen, wodurch Ihre Sitzung beendet wird. Darüber hinaus ist es empfehlenswert, in solchen Situationen den Inkognito-Modus des Browsers zu nutzen, um keine allzu offensichtlichen Datenspuren – etwa im Browserverlauf – zu hinterlassen. Hundertprozentige Sicherheit verschaffen Ihnen diese Maßnahmen jedoch nicht, da Sie einem fremden Rechner nie vertrauen können. Es wäre zum Beispiel denkbar, dass ein Keylogger



Der Sperrbildschirm ist ein effektives Mittel, um neugierige Mitmenschen fernzuhalten. Sorgen Sie dafür, dass der Rechner automatisch gesperrt wird, wenn Sie unterwegs sind.



Über den Ratgeber Internetkriminalität informiert die Polizei Niedersachsen über aktuelle Cyber-Bedrohungen.

installiert ist, der sämtliche Tastatureingaben einschließlich Ihrer Passwörter aufzeichnet. Das eigene Smartphone sollten Sie im Zweifel immer einem fremden PC vorziehen.

Hinter Identitätsdiebstahl muss nicht zwangsläufig ein Online-Krimineller stecken – auch Personen aus Ihrem persönlichen Umfeld können mit Ihren Daten viel Unheil anrichten. Sorgen Sie dafür, dass niemand ohne Weiteres auf Ihre Geräte zugreifen kann. Schützen Sie Rechner, Smartphones und Tablets mit einem Sperrbildschirm, der mindestens eine sechsstelligen PIN, besser noch ein Passwort, einen Fingerabdruck oder einen Gesichtsscan einfordert. Sperren Sie Ihren Rechner, wenn Sie ihn verlassen – auch, wenn Sie sich im Büro nur einen Kaffee holen. Die Windows-Tastenkombination zum Sperren Windows+L geht schnell in Fleisch und Blut über. Sorgen Sie dafür, dass der Sperrbildschirm bei Inaktivität automatisch aktiv wird. Unter Windows können Sie dies in den Bildschirmschoner-Einstellungen festlegen („Anmeldeseite bei Reaktivierung“ einschalten).

Kenne die Tricks

Informieren Sie sich über aktuelle Betrugsmaschen, damit Sie Ihre Daten nicht versehentlich Online-Gaunern in die Hände spielen. Wertvolle Anlaufstellen sind die zentralen Ansprechstellen Cybercrime der Polizeien sowie heise Security (siehe ct.de/ww9h). Bleiben Sie skeptisch, wenn Sie jemand aus heiterem Himmel nach Ihren persönlichen Daten oder gar einem Scan Ihres Personalausweises fragt – auch wenn diese Anfrage vermeintlich von einem Ihrer Facebook-Kontakte stammt.

Um es Angreifern nicht leichter als nötig zu machen, sollten Sie auch die Security-Basics befolgen: Halten Sie Betriebssystem und Programme auf dem aktuellen Stand, erstellen Sie regelmäßig Backups Ihrer wichtigen Dateien und stellen Sie sicher, dass ein Virenschutz mit aktuellen Signaturen läuft. Seit Windows 8 reicht der Defender aus. Weitere Hinweise zur Absicherung liefern Ihnen unsere Sicherheits-Checklisten, die Sie unter **ct.de/check2021** abrufen können. (rei)

Literatur

[1] Pina Merkert, Passwortsuche mit Turbo, c't 5/2019, S. 42

Tools und Links

ct.de/ww9h



Exklusiver Frühbucher-Rabatt!

heise Academy

Sie wollen Ihre IT absichern? Dann vertrauen Sie unserem Angebot aus Workshops und Konferenzen.

Unser Angebot

heise Security Tour

9. September

KONFERENZ

Cybersicherheit
Aktuelle Angriffstechniken und ihre Abwehr

9. – 10. September

WORKSHOP

Linux Server härten

14. – 17. September

WORKSHOP

secIT Special –
Cybersicherheit für KMU

16. September

KONFERENZ

Transportverschlüsselung
mit dem Postfix-Mailserver

20. September

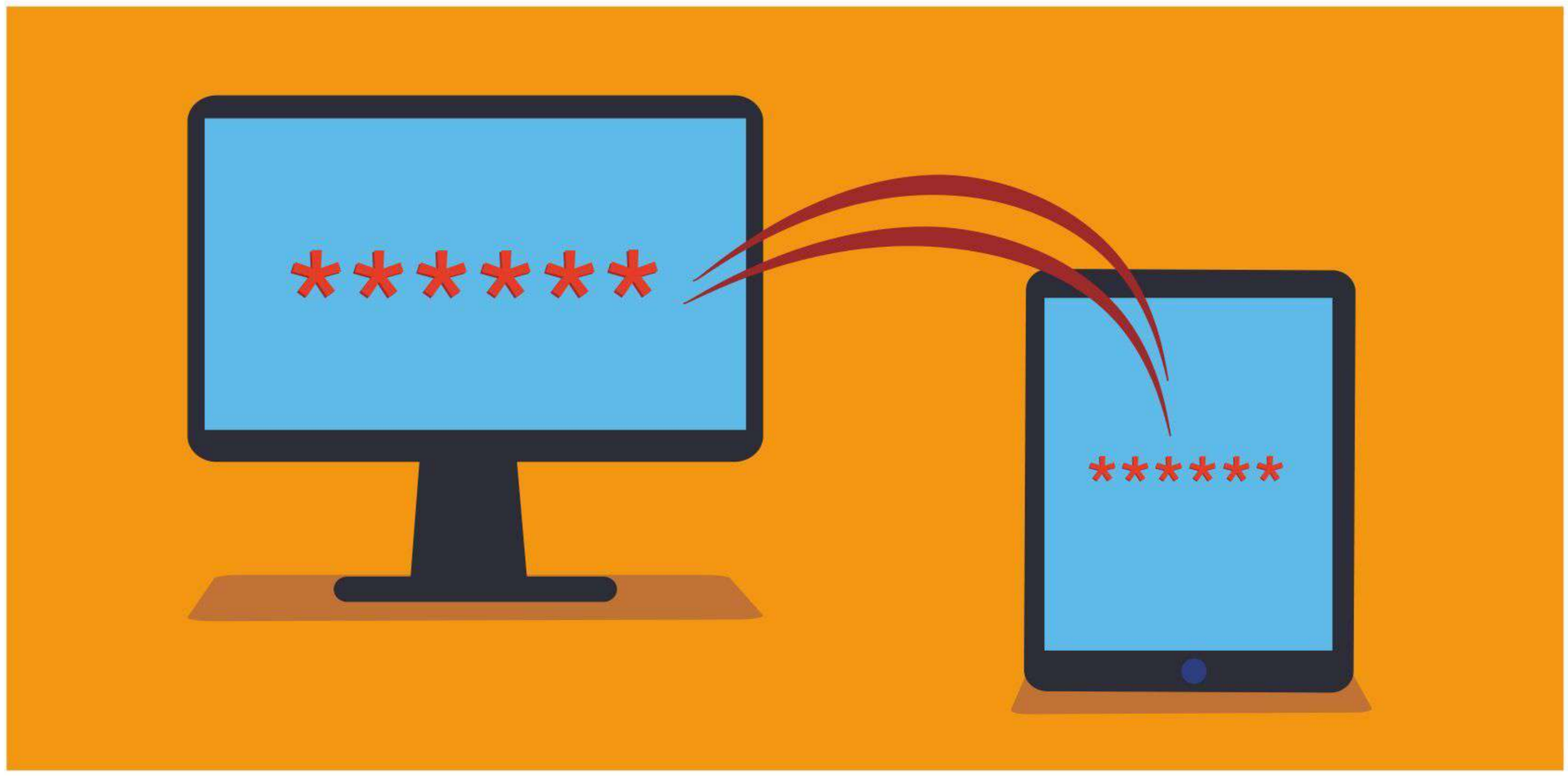
WORKSHOP

KRITIS:
Zusätzliche Prüfverfahrenskompetenz für § 8a BSIG

20. – 21. September

WORKSHOP

Mehr Informationen: heise-academy.de/security



Passwörter sicher und bequem verwalten

Der kostenlose Passwortmanager Keepass verwaltet Zugangsdaten systemübergreifend für Desktop-Rechner, Tablets und Smartphones. Das Setup der Open-Source-Software für Windows, macOS, Linux, Android und iOS erlaubt in Verbindung mit einem Cloud-Dienstleister wie Dropbox den bequemen und sicheren Umgang, sodass sie sich künftig nur noch an ein einziges Passwort erinnern müssen.

Von **Marvin Strathmann**

Niemand kann sich all die komplexen, individuellen Passwörter für jeden Dienst merken. Passwortmanager helfen: Der Mensch muss nur noch ein Hauptpasswort im Kopf behalten und die Maschine speichert den Rest. Aber die Kennwörter sollen ja nicht nur auf einem einzelnen Rechner zur Verfügung stehen. Man benötigt sie unter Windows, auf einem Desktop-Linux oder mobil auf dem iPhone. Die Daten müssen synchron gehalten werden, damit man bequem auf dem Handy etwas ändern kann und später das Desktop-Programm auf dem aktuellen Stand ist.

Unsere Anleitung hilft beim Einrichten so eines Systems: Wir zeigen Ihnen ein Beispiel-Setup, das auf Keepass basiert, einem zuverlässigen und kostenlosen Open-Source-Tool. Dank zahlreicher Abwandlungen (Forks) können viele Programme mit dem Keepass-Datenbankformat KDBX umgehen, egal ob Sie auf Windows, Linux, macOS, iOS oder Android unterwegs sind. Sämtliche Download-Links haben wir unter ct.de/w37h für Sie zusammengetragen. Die Synchronisierung der Daten übernimmt ein Cloud-Dienst. Es ist nahezu egal, welchen Sie verwenden, in diesem Beispiel zeigen wir die Einrich-

tung mit Dropbox. Das Setup eignet sich dank seiner Einfachheit auch gut für Familien-Admins, die anderen zu mehr Passwortsicherheit verhelfen möchten.

Grundlagen gegen die Zettelwirtschaft

Passwörter lassen sich ganz traditionell auf einem Stück Papier aufbewahren. Eine Tabelle mit drei Spalten reicht schon: Einfach Benutzername und Passwort für jeden Dienst aufschreiben. Lagern muss man dieses wichtige Papier trotzdem irgendwo. Nicht jeder hat einen Tresor im Arbeitszimmer, um den Zettel dort sicher aufzubewahren.

Ein Zettel ist zudem sehr unpraktisch. Haben Kriminelle das Passwort erbeutet und taucht es etwa in einer Leak-Datenbank auf, muss man es ändern. Mit der Zettelwirtschaft bedeutet das: Durchstreichen und sich ein neues ausdenken. Zudem können sehr schnell neue Passwörter hinzukommen: das neue WLAN-Passwort, die PIN vom gestern gekauften Handy oder die Benutzerdaten für eine gerade heruntergeladene App. Wer alle wichtigen Daten gemeinsam auf einen Zettel behalten will, kann schnell die Übersicht verlieren.

Passwortmanager nehmen einem die Arbeit ab. In einer sicheren Datenbank speichern Sie alle wichtigen Informationen und Kontodaten. So können Sie die beiden wichtigsten Passwortregeln beherzigen: Für jeden Dienst ein individuelles Passwort verwenden, das ausreichend komplex ist. „123456“ zählt also nicht, genauso wenig wie „Martins-Facebook1“. Denn Kriminelle könnten solche einfachen Kombinationen erraten. Sie sollten für jeden Dienst ein eigenes Passwort verwenden, um den Schaden zu begrenzen: Wird dieser Account gehackt, etwa weil das Unternehmen schlampig mit den Daten umgeht, ist nur dieser eine Dienst betroffen. Die anderen nicht. So müssen Sie nur ein Passwort ändern und können dann wie gewohnt weitermachen.

Zudem bieten Passwortmanager viele Komfortfunktionen: Mit einem Manager können Sie etwa Login-Felder im Browser automatisch ausfüllen, Passwörter zufällig nach bestimmten Vorgaben erstellen lassen oder in Leak-Datenbanken nach kompromittierten Daten von Ihnen suchen.

Grundsätzlich gilt: Jeder Passwortmanager ist besser als keiner. Für dieses Beispielsetup verwenden wir Keepass: Die Software ist bewährt, kostenlos, Open Source und bietet viele Erweiterungen. Allerdings ist Keepass nicht sehr einsteigerfreundlich. Die Optik erinnert mit den vielen grauen Schaltflächen eher an die 1990er-Jahre. Und der Nutzer muss sich eine eigene Cloudlösung suchen, wenn die Passwörter nicht nur auf einem Rechner liegen sollen.

Vertrauensfrage

Als Cloud nutzen wir in diesem Beispiel Dropbox. Der Dienst ist für Laien gut verständlich und in zahlreiche Apps und Programme integriert. In der kostenlosen Variante von Dropbox lassen sich drei Geräte miteinander verknüpfen. Wer mehr Geräte hat, kann sein Dropbox-Konto für zehn Euro im Monat erweitern.

Auch andere Cloud-Dienste, etwa Microsoft Onedrive oder Google Drive, synchronisieren die Passwortdateien zuverlässig. Wichtig ist, dass sich der Nutzer mit dem Dienst wohlfühlt und der Client für alle verwendeten Geräte komfortabel zur Verfügung steht. Sehen Sie daher $Dropbox eher als Variable und ersetzen Sie es durch den Dienst Ihrer Wahl. (Wie Sie Passwortdateien ganz ohne Clouddienst synchronisieren können, erklärt der Artikel auf Seite 54.)

Sie müssen auch Vertrauen mitbringen. Denn einen externen Clouddienst zu nutzen bedeutet, dass Sie etwa Dropbox die KDBX-Datei anvertrauen, in der Keepass alle Passwörter verschlüsselt speichert. Damit geben Sie ein wenig die Kontrolle über die Datei ab, da Sie einen kommerziellen Dienst dazu verwenden, diese wichtige Datei zu speichern und über alle Geräte synchron zu halten. Es klingt etwas paradox, aber dafür müssen Sie am Ende Keepass mehr vertrauen als Dropbox.

Denn Keepass verschlüsselt die Datenbankdatei standardmäßig mit dem Advanced Encryption Standard (AES) und einer Schlüsselgröße von 256 Bit. AES-256 ist quasi der aktuelle Goldstandard der Verschlüsselung. Wenn das Hauptpasswort lang genug ist, würde ein Angreifer Tausende Jahre brauchen, um das Kennwort durch Ausprobieren zu erraten.

Diese Sicherheit ist aber nur gegeben, wenn Keepass alles richtig macht. Implementiert der Manager die Verschlüsselung falsch, sind Ihre Daten in Gefahr. Dabei spielt es keine Rolle, in welcher Cloud sie liegen. Dieses Sicherheitsrisiko sollten Sie im Kopf behalten.

Sie können Ihre Datenbank auch zusätzlich absichern, indem Sie eine Schlüsseldatei erstellen. Nur wer das Hauptpasswort kennt und die Schlüsseldatei besitzt, kann dann auf die Daten zugreifen. Die Schlüsseldatei speichern Sie einmalig auf jedem

verwendeten Gerät lokal. Sie muss nicht synchron gehalten werden und daher auch nicht in einem Cloud-Ordner liegen.

Hier kommt es auf die persönliche Gefahreneinschätzung an, ob Sie die Schlüsseldatei wirklich brauchen – und auf die Willigkeit des Nutzers, bei jedem Login nicht nur das Hauptpasswort einzugeben, sondern zusätzlich die Schlüsseldatei auszuwählen.

Windows

Die Dropbox-Software für Windows finden Sie unter www.dropbox.com. Legen Sie zudem auf der Homepage des Dienstes ein Dropbox-Konto an.

Das Programm lädt den Dienst herunter und installiert Dropbox. Das kann mehrere Minuten dauern. Anschließend finden Sie den Dropbox-Ordner unter C:\Users\<Benutzername>. Dort speichern Sie alle Dateien ab, die Sie über Dropbox mit den anderen Geräten teilen möchten. Ziel ist es, darüber die Datenbankdatei von Keepass synchron zu halten. Für etwas mehr Ordnung können Sie etwa einen Unterordner im Dropbox-Ordner erstellen und später dort die Passwortdatenbank abspeichern.

In diesem Beispiel nutzen wir Windows als Startpunkt für die Passwortverwaltung. Hier sollen Sie die Datenbank erstellen und Ihre Daten zu Beginn eintragen. Daher beschreiben wir diese Schritte genauer. Anschließend machen Sie die Datenbankdatei über Dropbox für alle anderen Systeme verfügbar.

Keepass einrichten

Auf der Webseite des Keepass-Projekts können Sie den Manager für Windows herunterladen. Oben links finden Sie die aktuelle 2.x-Version der Software, die wir für diese Anleitung verwenden, konkret Version 2.48.1.

Nach der Installation sollten Sie die Sprache ändern, denn standardmäßig ist Keepass auf Englisch. Auf der Projektseite des Programms finden Sie viele verschiedene Sprachdateien als Download. Um etwa die deutsche Sprachdatei zu installieren, laden Sie die deutsche ZIP-Datei für Version 2.x herunter und entpacken die Datei German.lngx in den Languages-Ordner im Keepass-Verzeichnis. Den Ordner finden Sie etwa unter C:\Program Files\Keepass Password Safe 2\Languages. Zurück in Keepass klicken Sie auf „View“, dann auf „Change Language...“ und wählen unter „Installed Languages“ den Eintrag „German (Deutsch)“ aus. Anschließend starten Sie Keepass neu.

Nun legen Sie eine Passwortdatenbank an. Das geht bei Keepass über „Datei“ und dann „Neu...“. Bestätigen Sie den Hinweis und wählen Sie anschließend einen Speicherort und einen Namen für Ihre Datenbank. Der Speicherort sollte in diesem Beispiel der neu angelegte Ordner in der Dropbox sein. Für andere Cloud-Dienste passen Sie ihn entsprechend an.

Anschließend sollen Sie ein Hauptpasswort festlegen. Es sollte sehr sicher und gleichsam gut merkbar sein.

Phrase ausdenken

Eine Passphrase ist dafür Ideal: Sie besteht aus einem Satz oder aus mehreren zufälligen Wörtern hintereinander. Wenn Sie einen Satz verwenden, sollte es kein bekannter Satz sein. „Sesam öffne dich“ ist etwa eine schlechte Passphrase, denn Angreifer könnten ihn durch Ausprobieren erraten. Denken Sie sich besser einen individuellen Satz aus.

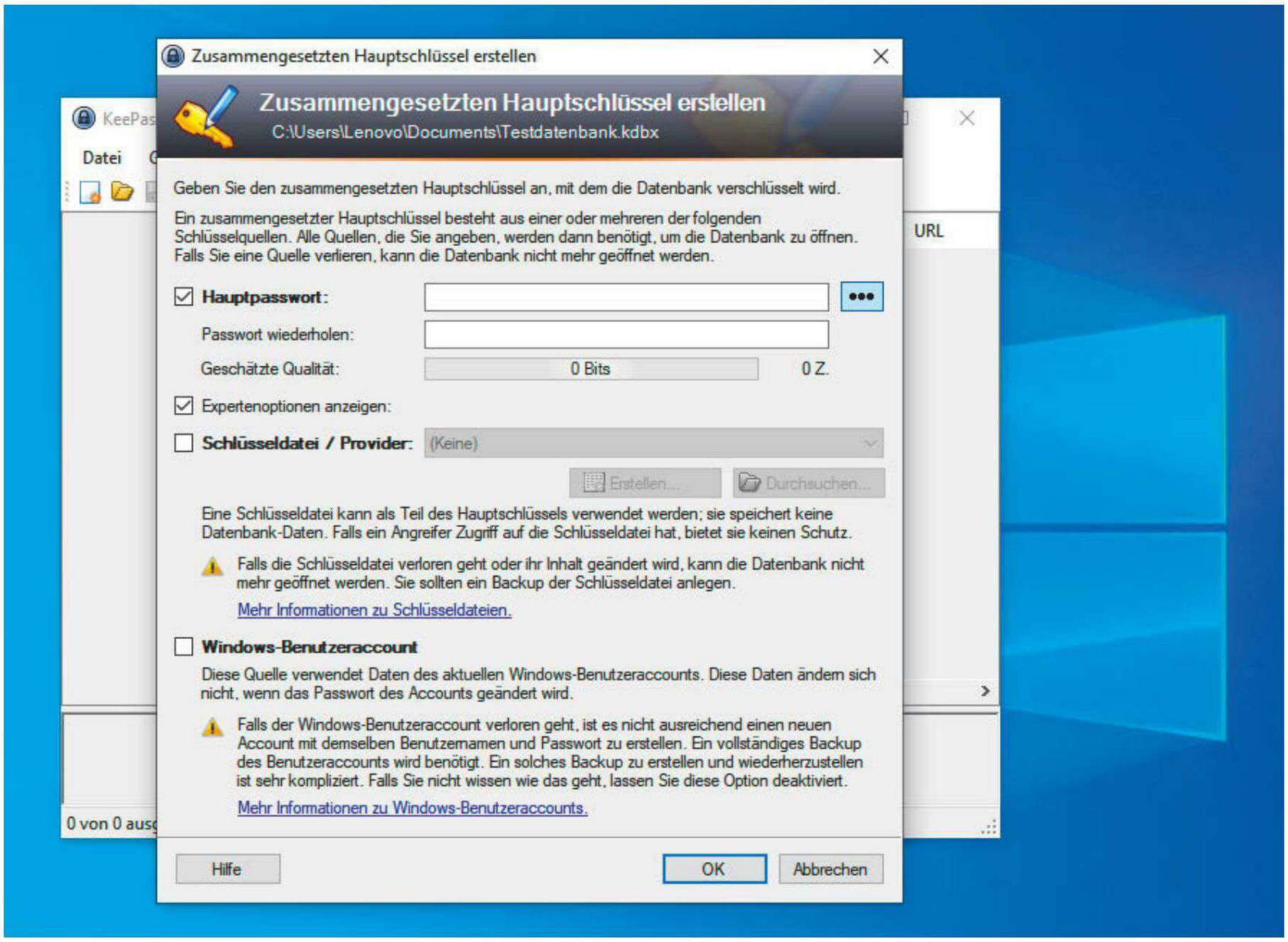
Zufällige Wörter erhalten Sie etwa aus einem Buch, in dem sie mit dem Finger zufällig herumtippen oder aus Diceware-Listen im Netz (siehe ct.de/w37h). Bei der Diceware-Methode würfeln Sie pro Wort fünfmal mit einem sechsseitigen Würfel und schreiben das daraus resultierende Wort aus der Liste auf. Je länger die Passphrase wird, desto besser. Achten Sie darauf, dass Sie sich die Phrase merken können.

Ihre Passphrase tragen Sie bei Keepass im Feld „Hauptpasswort“ ein. Wenn Sie den Haken bei „Expertenoptionen anzeigen“ setzen, können Sie zudem eine Schlüsseldatei als zweiten Faktor festlegen. Nutzen Sie diese Option, falls Sie noch stärker auf Sicherheit setzen möchten und vor allem dann, wenn Sie Keepass oder Dropbox nicht vertrauen. Die Schlüsseldatei speichern Sie in einem Ordner, der nicht mit Dropbox synchronisiert wird.

Nach einem Klick auf „OK“ geben Sie der Datenbank einen internen Namen. Der Einfachheit halber können Sie die Datenbank so nennen wie die Datenbankdatei. Die restlichen Einstellungen belassen Sie so, wie sie sind. Die voreingestellte Verschlüsselung ist AES-256.

Zuletzt bittet Keepass Sie, ein Notfallblatt auszudrucken, wo etwa der Speicherort der Datenbankdatei zu finden ist und Sie den Hauptschlüssel eintragen können. Verwahren Sie dieses Blatt sicher. Wer das Hauptpasswort kennt, kann schließlich auf all Ihre Passwörter zugreifen.

Das Hauptpasswort sollte möglichst lang und gut merkbar sein. Wenn Sie noch mehr Sicherheit benötigen, sollten Sie eine Schlüsseldatei hinzufügen.



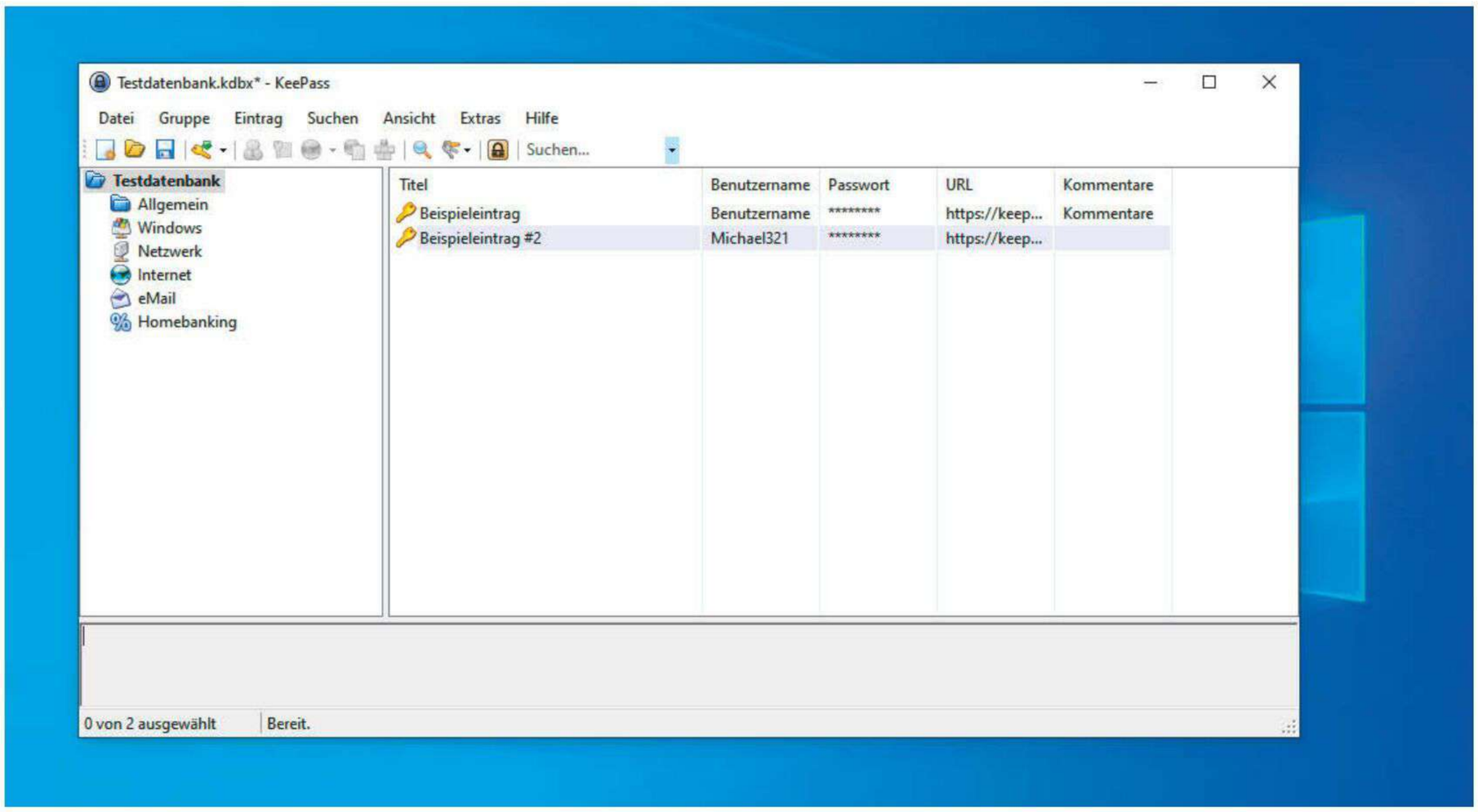
Passwort-Einträge hinzufügen

Das Hauptfenster von Keepass ist in drei Teile gegliedert. In der Ordnerstruktur links organisieren Sie Ihre Passwort-Einträge. Keepass hat bereits einige Ordner erstellt, etwa „Netzwerk“, „eMail“, „Homebanking“ und „Allgemein“. Wenn Sie auf einen Ordner klicken, zeigt Keepass rechts die Einträge im Ordner an.

Nun tragen Sie Ihre Kontodaten samt Passwörter in die Datenbank ein. Das geht über das Schlüsselsymbol mit dem grünen Pfeil in der Symbolleiste. Im Feld „Titel“ legen Sie einen eindeutigen Namen für einen Eintrag fest, etwa „Telekom-Kundencenter“, „heise online“ oder „Handy PIN“. Die Felder „Benutzername“, „Passwort“ und „Passwort-Wdh.“ sind selbsterklärend – hier tragen Sie Ihren Benutzernamen und das Passwort für den jeweiligen Dienst ein. Der Button mit den drei Punkten rechts zeigt das Passwort im Klartext an oder versteckt es. Die Leiste neben „Qualität“ zeigt anhand von Entropie-Bits, wie sicher Ihr gewähltes Passwort ist; neben „URL“ tragen Sie die Login-URL ein, etwa https://www.heise.de/sso/login/ für heise online – das Feld ist wichtig, damit Keepass Anmeldefelder automatisch ausfüllen kann. Das Kommentar-Feld lässt zudem Platz für Anmerkungen.

Für jedes Konto erstellen Sie einen eigenen Eintrag. Auch WLAN-Passwörter oder Backup-Codes können Sie so speichern. Wenn Sie von null beginnen, werden Sie recht viel zu tun haben. Es kann Tage dauern, alle Benutzerkonten zu finden, sich einzuloggen und das Passwort sowie den Benutzernamen in Keepass einzutragen.

Durchforsten Sie etwa die Passwort-Speicher ihrer Browser nach Einträgen oder schauen Sie in Ihrem E-Mail-Postfach, welche Konten damit verknüpft sind. Bei neuen Accounts sollten Sie sich in Zukunft angewöhnen, die Anmeldedaten direkt in Keepass zu speichern. Falls Sie Passwörter bereits digital gespeichert haben, kann die CSV-Import-Funktion von KeePass hilfreich sein.



Das Hauptfenster von Keepass wirkt etwas karg. Oder, um es etwas positiver zu formulieren, „Es wirkt sehr aufgeräumt“.

Browser-Verknüpfung

Auf der Plug-in-Seite von Keepass finden Sie unter anderem das Plug-in Kee, das Keepass mit Webbrowsern verbindet und Formulare automatisch ausfüllt. Dafür laden Sie erst das Plug-in KeepassRPC von GitHub herunter und verschieben die PLGX-Datei in den Plugins-Ordner des Keepass-Verzeichnisses. Ein Neustart von Keepass aktiviert das Plug-in. Anschließend installieren Sie das Addon Kee für Firefox oder Chrome.

Linux

Auch unter einem Desktop-Linux sollen alle Passwörter zur Verfügung stehen. Für dieses Beispiel-Setup verwenden wir Ubuntu 20.04.1 LTS und KeepassXC 2.6.6. KeepassXC ist ein Fork des originalen Keepass-Programms, der ohne das .NET- oder Mono-Framework funktioniert. KeePassXC bringt außerdem von Haus aus die Browser-Integration mit – eine Funktion, die man beim Originalprogramm unter Windows erst nachinstallieren muss – und einen etwas komfortableren CSV-Import-Assistenten (siehe S. 54).

In den Ubuntu-Paketquellen findet man einen Dropbox-Client für den Dateimanager Nautilus. Er lässt sich mit einem simplen Befehl installieren:

```
sudo apt install nautilus-dropbox
```

Dropbox selbst bietet auf seiner Website noch DEB- und RPM-Dateien in je 32- und 64-Bit an.

Anschließend kann man Dropbox über das Anwendungsmenü starten. Das Programm installiert den Dienst und leitet den Nutzer zur Dropbox-Website weiter. Dort loggt man sich mit seinen Anmeldedaten ein und verknüpft so den Account. Nun erscheint im persönlichen Ordner ein neuer Dropbox-Ordner, in dem alle Dateien synchronisiert werden.

KeepassXC installieren

Distributionsübergreifend installieren Sie KeepassXC als Snap mit diesem Befehl:

```
snap install keepassxc
```

Um es per apt für Ubuntu zu installieren, führen Sie stattdessen diesen Befehl aus:

```
sudo apt install keepassxc
```

Weitere Befehle, etwa für Fedora oder Arch Linux, finden Sie auf der Homepage von KeepassXC. Dort können Sie zudem das App Image und Snap Package herunterladen.

KeepassXC läuft normalerweise in der Sprache des Systems. Falls es auf Englisch startet und Sie es manuell auf Deutsch umstellen wollen, klicken Sie auf das Menü „Tools“, anschließend auf „Settings“ und scrollen runter bis zum Eintrag „General“. Dort können Sie neben „Language“ den Eintrag „German“ aus der Dropdown-Liste wählen. Nach einem Neustart erscheint KeepassXC in der gewählten Sprache.

Wenn Sie bereits eine KDBX-Datei erstellt haben, etwa mit Keepass auf Windows, dann wählen Sie im Startmenü „Existierende Datenbank öffnen“.

Browser verbinden

Im Menü „Werkzeuge“ aktivieren Sie unter „Einstellungen“ und „Browser-Integration“ die KeepassXC-Browser-Integration. Voraussetzung ist außerdem das KeepassXC-Browser-Addon für Ihren bevorzugten Browser – die Links finden Sie in den Einstellungen. In unserem Beispiel ist das der Firefox 89.0.1 für Ubuntu.

Nach einem Klick auf „Firefox“ öffnet sich der Mozilla-Browser und zeigt das KeepassXC-Browser-Addon. Fügen Sie es zu Firefox hinzu und bestätigen Sie die aufploppenden Dialoge. Oben rechts in der Menüleiste von Firefox finden Sie das Icon des KeepassXC-Browser-Addons. Klicken Sie darauf und anschließend auf den Button „Verbinden“. KeepassXC meldet sich nun mit einer Verbindungsanfrage und möchte, dass Sie einen beliebigen Namen in das Feld eintippen, etwa „Browserverbindung“. Bestätigen Sie Ihre Wahl per Klick auf „Speichern und Zugriff erlauben“.

Wenn Sie nun eine URL aufrufen, die Sie in den jeweiligen Einträgen angegeben haben, dann erscheint ein Dialogfenster: KeepassXC fragt, ob es die gespeicherten Daten verwenden darf. Bestätigen Sie das und klicken Sie auf „Entscheidung merken“, wenn Sie nicht jedes Mal gefragt werden wollen. Wird etwas nicht automatisch ausgefüllt, können Sie per Rechtsklick auf ein Login-Feld klicken, die Option „KeepassXC-Browser“ auswählen und die passenden Daten einfügen.

macOS

Um die Passwörter auf den Mac zu bekommen, nutzen wir in diesem Setup wie schon unter Ubuntu KeepassXC. Falls ein Nutzer Linux und macOS verwendet, muss er sich so kaum umgewöhnen und arbeitet mit einer ähnlichen Oberfläche.

Laden Sie den DMG-Installer für Dropbox von www.dropbox.com herunter. Nach der Installation melden Sie sich mit Ihren Daten an und verknüpfen so das Programm mit Ihrem Profil. Anschließend wählen Sie den Speicherort für Ihre Dateien und können den Dropbox-Ordner nun im Finder ansteuern.

Auf der Website von KeepassXC finden Sie zwei DMG-Installer, einen für Macs mit Intel-Prozessoren und einen für Macs mit Apple Silicon. Generell kann man sagen: Ist Ihr Mac vor Ende 2020 auf den Markt gekommen, sind Sie wohl mit einem Intel-Prozessor unterwegs. Um genau herauszufinden, welchen Prozessor Ihr Mac verwendet, klicken Sie oben links auf das Apple-Menü und wählen „Über diesen Mac“. Im aufploppenden Fenster steht neben „Prozessor“, welches Modell in Ihrem Mac drinsteckt. Als Beispiel nutzen wir ein Macbook Air von 2018 mit macOS Catalina in der Version 10.15.7 – also ein Mac mit Intel-Prozessor.

Neben den DMG-Installern können Sie das Programm auch mit dem Paketmanager Homebrew installieren. Dafür geben Sie `brew install --cask keepassxc` in die Konsole ein.

Nach dem Start von KeepassXC wählen Sie „Existierende Datenbank öffnen“ und navigieren im Dropbox-Ordner zu Ihrer Datenbankdatei. Nachdem Sie Ihr Hauptpasswort eingegeben haben, stehen Ihnen auch auf dem Mac alle Kennwörter zur Verfügung.

Wie schon unter Ubuntu aktivieren Sie in den Einstellungen die Browser-Integration. Dazu klicken Sie auf das Zahnrad oben rechts und wählen links in der Leiste „Browser-Integration“ aus. Zwar werden Firefox, Chrome und Edge unterstützt, der Apple-Browser Safari fehlt allerdings derzeit noch.

Safari-Nutzer müssen folglich den umständlichen Weg über die Zwischenablage gehen, um Anmeldedaten hin und her zu kopieren. Wenn Sie in der Hauptübersicht einen Eintrag auswählen, finden Sie oben in der Leiste Buttons, um das Passwort oder den Benutzernamen in die Zwischenablage zu verfrachten: das schwarze Benutzersymbol mit Pfeil beziehungsweise das schwarze Schlüsselsymbol mit Pfeil.

iOS

Auch auf einem iPad oder iPhone dürfen die Passwörter nicht fehlen. Im Appstore findet man mehrere Programme, die mit der Keepass-Datenbank kompatibel sind, etwa Keepass Touch, Kypass oder Keepassium – letzteres wählten wir aufgrund seiner zahlreichen Funktionen aus.

Den Clouddienst Dropbox finden Sie im Appstore und laden ihn dort herunter. Nach der Installation müssen Sie sich nur mit Ihren Daten einloggen und

können anschließend auf die gespeicherten Dateien zugreifen.

Die iOS-App laden Sie wie gewohnt aus dem Appstore von Apple herunter. Anschließend starten sie die App und wählen „Vorhandene Datenbank hinzufügen“ aus. Über die „Speicherorte“ in der linken Leiste haben Sie Zugriff auf Ihren Dropbox-Ordner. Wählen Sie die Datenbank aus und entsperren Sie sie wie gewohnt mit Ihrem Hauptpasswort.

Die App zeigt die Einträge und Ordner in einem Listenformat an. Wenn Sie einen Eintrag auswählen und anschließend auf den Benutzernamen oder das Passwort tippen, landet dieses Datum direkt in der Zwischenablage und Sie können es in das Feld Ihrer Wahl kopieren.

Damit Keepassium die Autofill-Funktion nutzt, müssen Sie in die Einstellungen ihres iOS-Gerätes gehen. Unter „Passwörter“ beziehungsweise „Passwörter & Accounts“ finden Sie die Option „Automatisch ausfüllen“. Dort können Sie Keepassium als Standard setzen. In den Einstellungen von Keepassium finden Sie die Option über das Zahnrad-Menü am unteren Rand und anschließend im Eintrag „Passwörter automatisch eintragen“.

Um das Entsperren per Fingerabdruck zu aktivieren, tippen Sie auf das Zahnradsymbol am unteren Rand und wählen anschließend „Zugangsschutz“. Dort können Sie auf „Touch ID verwenden“ tippen und einen Fingerabdruck zum Entsperren hinterlegen. Auch die Einstellungen für Face ID finden Sie an dieser Stelle, wenn Ihr Gerät die Funktion anbietet.

Android

Es gibt mehrere Apps, die KDBX-Dateien unter Android verwalten. Zu den bekannteren gehören Keepass2Android, Keepassdroid, KeepassDX und KeepShare. Da sich das kostenlose Keepass2Android für Einsteiger eignet und umfangreiche Einstellungen mitbringt, beschreiben wir die Einrichtung für das Beispiel-Setup genauer.

Um die KDBX-Datei mit Keepass2Android zu laden, benötigen Sie natürlich erst Dropbox. Sie müssen ja auf die synchronisierte Datei zugreifen können. Die App dazu finden Sie im Play Store.

Mach der Installation öffnen Sie die App und loggen sich mit Ihren Dropbox-Daten ein. In der App sehen Sie Ihre Dropbox-Ordnerstruktur und damit auch den Keepass-Ordner mit Ihrer KDBX-Datei.

Keepass2Android installieren Sie wie jede gewöhnliche App über den Play Store von Google. Sie können die App auch manuell installieren, indem Sie die APK-Datei von Github herunterladen. Die App nutzt standardmäßig die Sprache, in der auch das System gehalten ist. Sie müssen also nicht extra eine Sprachdatei nachladen.

Nach dem ersten Start können Sie das Changelog einsehen und bestätigen. Anschließend wählen Sie „Datei öffnen...“. Nun können Sie aus mehreren Cloud-Diensten und Speicherorten wählen, praktischerweise ist auch Dropbox dabei. Tippen Sie darauf und melden Sie sich anschließend mit Ihren Dropbox-Daten an.

Gewähren Sie Keepass2Android Zugriff auf Ihre Dropbox und wählen Sie die Datenbankdatei aus. Danach melden Sie sich mit Ihrem Hauptpasswort für Ihre Datenbank an. Mit einem Tipp auf „Autofill aktivieren“ erlauben Sie, dass keepass2Android Passwortfelder automatisch ausfüllt, etwa im Browser. Das funktioniert allerdings nicht immer. Sie können stattdessen auch die Daten aus den Einträgen mit einem Tipp kopieren und im Feld wieder einfügen. Keepass2Android bietet Ihnen die Option bei geöffnetem Eintrag dann etwa in der Benachrichtigungsleiste oben an oder Sie nutzen das Dreipunkt-Menü neben jedem Datum.

In den Einstellungen, erreichbar über das Dreipunkt-Menü oben rechts, können Sie einige nützliche Optionen aktivieren: So finden Sie im Bereich „Datenbank“ den Punkt „Biometrisches Entsperren“. Dort können Sie etwa ein Entsperren mit dem Fingerabdruck aktivieren und sparen sich das umständliche Eintippen des Masterpassworts.

Ebenfalls sehr nützlich ist „Quickunlock“, das Sie über den Einstellungspunkt „Anwendung“ finden. Nachdem Sie Ihre Datenbank einmal entsperrt haben, müssen Sie mit aktiviertem Quickunlock beim nächsten Mal nur noch die letzten drei Zeichen Ihres Hauptpassworts eingeben, um an die Passwörter zu kommen. Wenn Sie die Datenbank endgültig schließen und nicht nur sperren, wird Quickunlock zurückgesetzt und Sie müssen beim nächsten Start wieder das vollständige Hauptpasswort eingeben.

Fazit

Ein kleines bisschen lästig sind wirklich gute Passwörter immer, aber das macht die gewonnene Sicherheit allemal wett. Durch die beschriebene Kombination aus Keepass und einem Clouddienst wie Dropbox geht kaum Komfort verloren und Sie können praktisch jede Art von Gerät mit einbeziehen. Wer sich so ein Setup einmal eingerichtet hat, möchte es bald nicht mehr missen. (syt) c't

Sämtliche Downloadlinks

ct.de/w37h

Ein Hoch auf Brotkasten und Co.!

NEU



Auch als PDF zum Download

Retro Gamer Spezial Heimcomputer

VC-20, Acorn BBC Micro, Sinclair ZX 81, Commodore 64, Sinclair Spectrum, Apple II, Atari 800 XL, Schneider CPC, Atari ST und Commodore Amiga - die zum Teil vergessenen Stars dieses brandneuen Sonderheftes!

Über 150 Spiele-Klassiker auf den wichtigsten Maschinen der 1980er beleuchtet das neue Retro Gamer-Sonderheft auf fast 200 Seiten: Bard's Tale, Zak McKracken, Defender of the Crown, Another World und viele viele mehr.

shop.heise.de/rg-homecomputer

16,95 € ›

› 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

shop.heise.de/rg-homecomputer ›



Bild: Thorsten Hübner

So wechseln Sie zu KeePassXC

LastPass hat die Gratisnutzung eingeschränkt. Jetzt bietet sich ein Wechsel zu KeePassXC an, das nicht nur Open Source ist, sondern mithilfe von Syncthing auch ohne Cloud synchronisiert.

Von **Jan Schüßler**

Im Frühjahr 2021 hat LastPass die Schrauben bei der Gratisversion seines Passwortmanagers angezogen: Sie lässt sich seitdem nur noch entweder auf mobilen Geräten oder auf Desktops nutzen. Wer weiterhin zwischen beiden Gerätekategorien synchronisieren will, braucht mindestens die Premiumversion für 35 Euro im Jahr. Doch neben den Kosten gibt es einen weiteren Grund für einen Umstieg: Wie unsere Tests gezeigt haben, tracken nicht nur LastPass, sondern auch diverse andere Anbieter von Passwortmanagern ihre Kunden recht schamlos.

Einen hervorragenden Schutz vor Tracking – und vor der Abhängigkeit von einem Hersteller – bieten quelloffene Passwortmanager aus dem KeePass-Universum. In unserer Anleitung konzentrieren wir uns auf Windows und Android, geben aber auch iOS-Nutzern ein paar Tipps. Auf dem Windows-Desktop haben wir uns für KeePassXC entschieden. Eine Anleitung für das reguläre KeePass finden Sie auf Seite 46. Auf Android kommt KeePassDX zum Einsatz. Eine Kernfunktion von LastPass ist die komfortable Synchronisierung des Passworttresors zwischen mehreren Geräten. Für diese Aufgabe verwenden wir die quell-

offene Sync-Software Syncthing. Sie kommt ohne Cloudspeicher aus und funktioniert trotzdem auch unterwegs, über NAT-Grenzen hinaus.

Export aus LastPass

Um den Umstieg so elegant wie möglich hinzubekommen, exportieren Sie zunächst die in LastPass eingetragenen Passwörter als CSV-Datei, die alle gespeicherten Login-Daten im Klartext enthält. Aus der Weboberfläche heraus ist der Export seit geraumer Zeit kaputt und zeigt die Passwörter nur als Text im Browser an, statt sie herunterzuladen. Der Weg des Erfolgs führt deshalb über die LastPass-Browsererweiterung. Klicken Sie im Menü der Erweiterung auf „Kontooptionen / Erweitert / Exportieren / Lastpass-CSV-Datei“.

Am besten speichern Sie die CSV-Datei auf einem verschlüsselten Laufwerk ab. Falls Ihr Systemlaufwerk nicht verschlüsselt ist, können Sie auch einen verschlüsselten USB-Stick dafür benutzen, wie wir ihn in [1] beschrieben haben. So stellen Sie sicher, dass nach dem späteren Löschen der Datei keine zum Beispiel für einen Dieb des PCs verwertbaren Rückstände auf der Systemfestplatte beziehungsweise -SSD zurückbleiben – immerhin enthält sie Ihre Passwörter im Klartext.

KeePassXC: Ersteinrichtung

Laden Sie nun KeePassXC herunter (siehe ct.de/wka6) und installieren und starten Sie es. Klicken Sie auf „Aus CSV importieren“ und wählen Sie die zuvor gesicherte Datei lastpass_export.csv aus. Als Nächstes können Sie einen Namen für die Passwortdatenbank vergeben oder die Vorgaben einfach bestätigen. Gleiches gilt für die Verschlüsselungseinstellungen.

Dann vergeben Sie ein starkes Masterpasswort nach den bekannten Regeln: nicht zu kurz und nicht einfach zu erraten. Um die Sicherheit zu erhöhen, ohne das Masterpasswort endlos lang und kompliziert machen zu müssen, empfiehlt es sich, eine Schlüsseldatei als zweiten Faktor hinzuzunehmen. In diesem Fall fragt KeePassXC beim Öffnen eines Passworttresors nicht nur nach dem Masterpasswort, sondern verlangt auch nach der Schlüsseldatei. Auch wenn jemand Ihre Passwortdatenbank (eine Datei mit der Endung .kdbx) klaut und Ihr Masterpasswort ausspäht, fehlt immer noch die Schlüsseldatei. Auf die Datei sollten Sie gut aufpassen und sie keinesfalls an einem öffentlich zugänglichen Ort speichern. Kopieren Sie sie am besten auf direktem Wege, also etwa per USB-Stick oder -Kabel, auf die Geräte, mit denen Sie auf den Passworttresor zugreifen möchten. Sie können KeePassXC eine Schlüsseldatei erzeugen lassen, aber Sie können auch eine beliebige, schon vorhandene Datei nehmen. Ideal ist irgendein Handyfoto, das Sie nirgendwo veröffentlicht haben – es ist unauffällig und quasi garantiert einmalig. Um die Sicherheit noch weiter zu erhöhen, legen Sie Ihre Schlüsseldatei nicht direkt auf dem PC ab, sondern auf einem verschlüsselten USB-Stick, den Sie immer dabei haben [1].

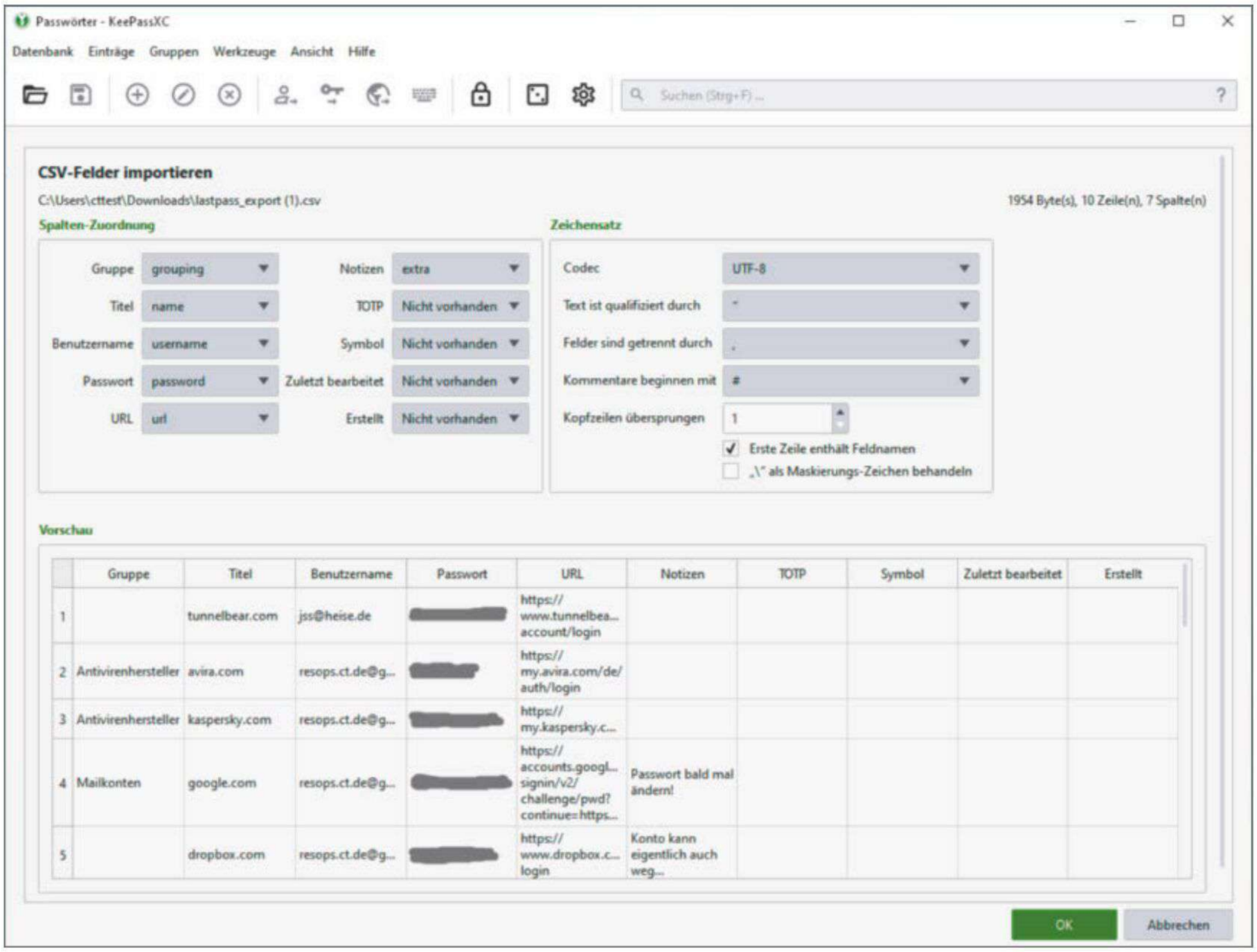
Um Chaos bei der späteren Synchronisierung zu vermeiden, empfehlen wir im nächsten Schritt, die Datei nicht einfach im Dokumentenordner, sondern in einem eigenen Unterordner zu speichern. Den legen Sie per Rechtsklick in den freien Bereich des Fensters und „Neu / Ordner“ an. Nennen Sie ihn zum Beispiel „Passwortordner“, öffnen Sie ihn und bestätigen Sie mit „Speichern“.

Jetzt folgt der eigentliche Import Ihrer Passwörter. Weil KeePassXC nicht wissen kann, wie die Einträge der CSV-Datei sortiert sind, müssen Sie ihm mitteilen, was was ist. Setzen Sie im Bereich „Zeichensatz“ ein Häkchen vor „Erste Zeile enthält Feldnamen“. Sortieren Sie dann die Spalten unter „Spalten-Zuordnung“: Gruppe=grouping, Titel=name, Benutzername=username, Passwort=password, URL=url, Notizen=extra. Die restlichen vier Felder setzen Sie auf „Nicht vorhanden“.

Falls in der LastPass-Datenbank auch Einträge liegen, die keine Passwörter sind – also etwa Notizen, Kreditkartendaten oder Formulardaten –, werden die ebenfalls übernommen. Der Nutzen hält sich in Grenzen, denn KeePassXC unterstützt solche Datensätze nicht und interpretiert sie einfach als Passworteinträge. Zwar kann man mit einigem Aufwand händisch Einträge mit benutzerdefinierten Feldern für Kartennummern, Anschriften oder Telefonnummern erstellen und befüllen, doch beim CSV-Import stopft KeePassXC Kreditkarten & Co. einfach ins Passwortschema. Wir empfehlen daher, diese Importe zu löschen und solche Einträge bei Bedarf von Hand neu anzulegen.

Komfort im Browser

Sie könnten KeePass XC nun direkt verwenden, doch die Bedienung im Alltag wäre noch ein wenig sperrig, weil Sie Webseiten-Passwörter jedes Mal umständlich aus dem Programm heraus aufrufen



Die Importfunktion von KeePassXC übernimmt Ihre Passwortliste problemlos – die Spalten müssen nur passend sortiert werden.

müssten. Diese Arbeit nimmt Ihnen eine Browsererweiterung ab. Es gibt sie sowohl für Firefox als auch für Chrome (und damit auch für Chromium-Browser wie Brave, Edge, Vivaldi & Co.). Nur Safari geht leer aus.

Die Funktion aktivieren Sie über die „Einstellungen“ im Menü „Werkzeuge“. Wählen Sie links „Browserintegration“, setzen Sie das Häkchen vor „Browserintegration aktivieren“ sowie vor Ihren Browser und laden Sie die passende Erweiterung über den dazugehörigen Link herunter, der sich direkt darüber befindet. Bestätigen Sie die Einstellungen mit OK. Klicken Sie nun im Browser auf die Erweiterung – im Regelfall oben rechts im Fenster – und dann auf „Verbinden“. In der Verbindungsanfrage vergeben Sie einen Namen wie „Desktop-Firefox“.

Beim Aufruf von Webseiten, für die KeePassXC Logindaten kennt, sollte nun automatisch eine Zugriffsanfrage im Browser erscheinen, um Benutzername und Passwort einzutragen. Sofern Sie diese Anfrage nicht bei jedem Aufruf der Seite erneut sehen möchten, setzen Sie ein Häkchen bei „Merken“. So oder so lassen sich die Login-Daten dann per Klick auf das kleine KeePassXC-Icon im Benutzernamenfeld eintragen.

Im Regelfall sollte die Browsererweiterung auch neue Login-Daten erkennen und fragen, ob es sie in der Datenbank speichern soll – wenn Sie neue Einträge lieber direkt in KeePassXC anlegen, schalten Sie die Funktion in den Einstellungen der Browsererweiterung ab (per Klick aufs Erweiterungs-Icon und „Einstellungen“). Dort können Sie noch mehr einstellen, etwa, ob Login-Daten automatisch eingetragen und / oder abgeschickt werden.

Sync ohne Cloud

Wie kommt die Passwortdatenbank nun auf andere Geräte? Die bequemste Lösung wäre es, sie einfach im lokalen Ordner eines Cloudspeichers wie Drop-

box oder OneDrive abzulegen. Das funktioniert gut (siehe S. 46), aber es erfordert ein Konto bei einem Cloudanbieter.

Eine andere Lösung ist Peer-to-Peer-Synchronisierung (P2P), wofür wir das quelloffene Tool Syncthing verwenden. Damit sich Geräte auch über NAT-Grenzen hinweg finden und synchronisieren können, betreibt Syncthing Discovery-Server, die die Verbindung vermitteln. Zudem existieren weltweit ein paar hundert Community-gestützte Relay-Server, die als Proxy arbeiten, falls Daten nicht auf direktem Wege ausgetauscht werden können. Da die Übertragungen Ende-zu-Ende-verschlüsselt sind, ist das kein Sicherheitsproblem.

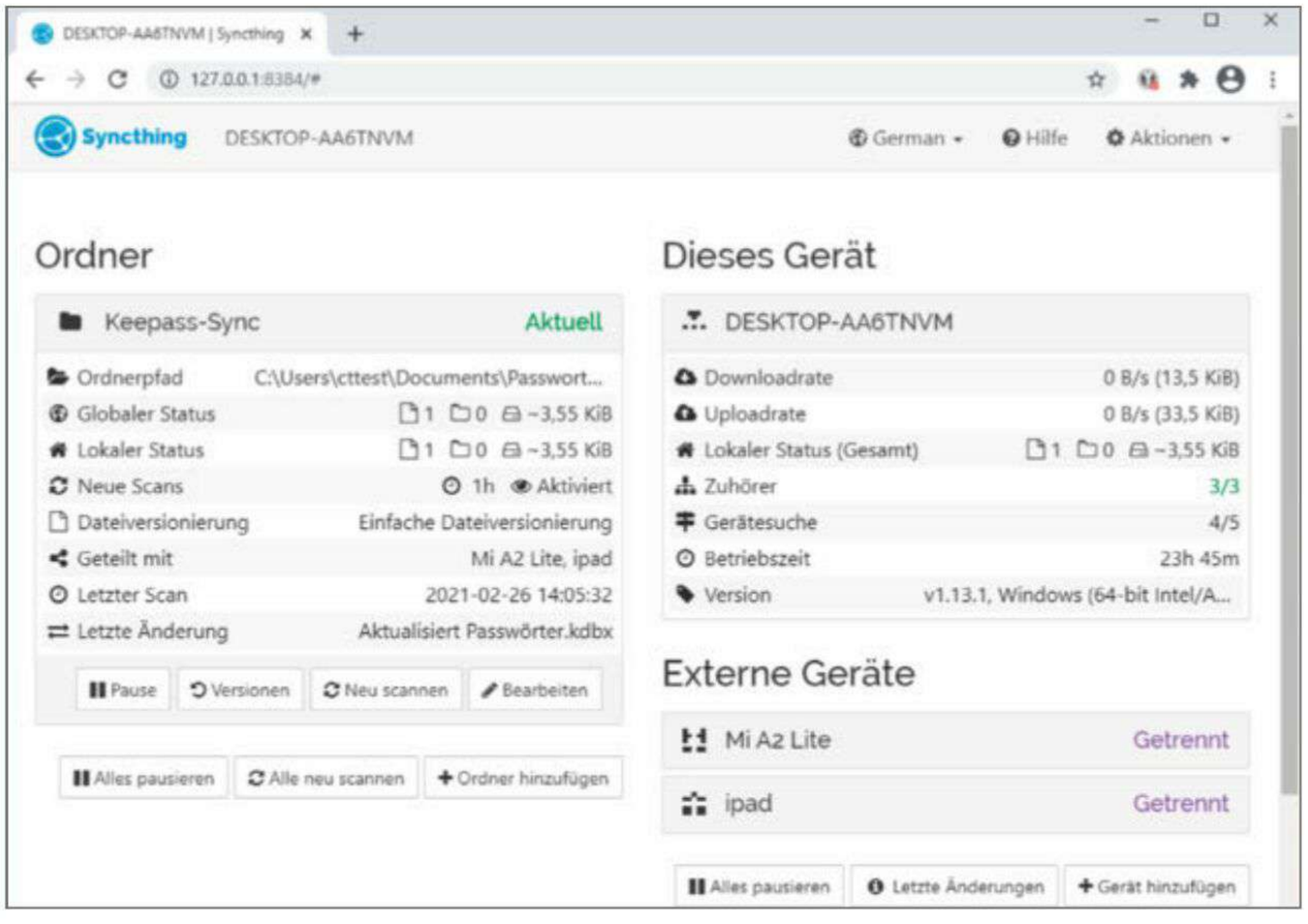
Die Windows-Version von Syncthing hat kein Installationsprogramm, aber das macht nichts, denn die Software lässt sich mit ein paar Handgriffen automatisch starten. Entpacken Sie den Download (siehe ct.de/wka6) und legen Sie ihn irgendwohin, wo er nicht stört, zum Beispiel ins Stammverzeichnis Ihres Benutzerprofils. Dazu öffnen Sie einen Datei-Explorer, tippen in die Adresszeile `%homepath%` ein und bestätigen mit der Eingabetaste. Ziehen Sie das Syncthing-Programmverzeichnis dort hinein.

Nun legen Sie eine Autostart-Verknüpfung an. Dazu drücken Sie Windows+R, tippen `shell:startup` ein und bestätigen mit der Eingabetaste. Klicken Sie mit der rechten Maustaste in den leeren Bereich des Ordners, auf „Neu / Verknüpfung“ und auf „Durchsuchen“. Hangeln Sie sich zum Syncthing-Programmordner durch, markieren Sie die Datei „syncthing.exe“ und bestätigen Sie mit OK. Ergänzen Sie die Pfadzeile noch um ein Leerzeichen gefolgt von `-no-console -no-browser`, und klicken Sie die Dialoge bis zum Ende durch.

Geräte verknüpfen

Um die Synchronisierung einzurichten, rufen Sie das Programm syncthing.exe in seinem Programmordner per Doppelklick auf und bestätigen eine eventuelle Firewall-Abfrage. Die Konfiguration geschieht per Browser und ist jederzeit unter der Adresse `127.0.0.1:8384` erreichbar – am besten erstellen Sie ein Lesezeichen. Zunächst sollten Sie die Oberfläche mit Benutzernamen und Passwort schützen, worum Sie Syncthing beim Aufruf der Seite auch direkt als Erstes bittet.

Dann empfiehlt es sich, Syncthing auf allen weiteren Geräten einzurichten und sie miteinander zu verknüpfen. Für Android ist die App im Google Play Store und in F-Droid verfügbar. Nach der Installation und dem Abnicken einiger Berechtigungen tippen Sie unter „Geräte“ oben rechts aufs Pluszeichen. Tippen Sie unter „Geräte-ID“ den 56-stelligen Code ein, den Sie auf dem PC oben rechts im Menü „Aktionen“ unter „Eigene Kennung“ aufrufen können. Vergeben Sie unter „Name“ noch eine Be-



Einmal eingerichtet, verrichtet Syncthing seinen Dienst unauffällig im Hintergrund.

zeichnung (zum Beispiel „Desktop-PC“) und bestätigen Sie den Dialog per Häkchen oben rechts. Falls Ihnen das Eintippen des Codes zu mühsam ist, können Sie in der Android-App auch auf das kleine QR-Code-Logo in der Zeile „Geräte-ID“ tippen und einfach den Code scannen, den Sie auf dem Desktop ebenfalls sehen.

Auf dem Desktop-Rechner erscheint das Gerät jetzt im besten Fall schon automatisch auf der Hauptseite, wo man es per Klick hinzufügen kann. Wenn nicht: Im Bereich „Externe Geräte“ auf „Gerät hinzufügen“ klicken und unter „Gerätekennung“ den 56-stelligen Gerätecode eingeben, den Sie im Menü der Android-App (die drei Striche oben links) unter „Geräte-ID anzeigen“ aufrufen können.

Falls Ihre Geräte im gleichen Subnetz hängen (etwa zu Hause am DSL-Router), finden sie sich übrigens meist schon von selbst, was Ihnen das Eintippen oder Abscannen der Geräte-ID erspart. Schauen Sie einfach auf dem Desktop nach, ob Syncthing IDs potenzieller Gegenstellen im Hinzufügedialog vorschlägt.

Datenbank synchronisieren

Sind alle Geräte verbunden, klicken Sie in Syncthing auf dem PC im Bereich „Ordner“ auf „Ordner hinzufügen“. Tragen Sie auf der Registerkarte „Allgemein“ im Feld „Ordnerkennung“ einen eindeutigen Namen ein, zum Beispiel „KeePass-Sync“. Unter „Ordnerpfad“ tragen Sie den Ordner ein, in dem Ihre Passwortdatenbank liegt, also etwa „C:\Users\cttest\Documents\Passwortordner“. Syncthing bietet leider keinen Dialog für die Ordnerauswahl – statt den Pfad von Hand einzutippen, können Sie den Ordner mit der Datenbank im Explorer öffnen und dort auf die Adresszeile klicken. So lässt sich der Pfad einfach kopieren und in Syncthing einfügen. Die „Ordnerbezeichnung“ kann leer bleiben.

Auf der Registerkarte „Teilen“ setzen Sie Häkchen vor alle Geräte, zwischen denen die Passwortdatenbank synchronisiert werden soll. Zu guter Letzt können Sie unter „Dateiversionierung“ einstellen, dass ältere Versionen der Datenbankdatei eine Zeit lang aufbewahrt werden. Sinnvoll ist die „Einfache Dateiversionierung“ mit automatischem Löschen nach 14 Tagen und Aufbewahrung von bis zu 100 alten Versionen. Bestätigen Sie nun mit „Speichern“.

Auf einem Android-Gerät sollte Ihnen nun eine Benachrichtigung mitteilen, dass der Desktop-PC einen Ordner mit Ihnen teilen möchte. Tippen Sie sie an. Sie sehen einen fast fertig ausgefüllten Dialog für einen synchronisierten Ordner – fast, weil Syncthing in der Zeile „Verzeichnis“ noch wissen möchte, in welchem lokalen Ordner es die Passwörter synchronisieren soll. Wir empfehlen, in dem von der App vorgeschlagenen Download-Ordner einen Unterordner zu erstellen und auszuwählen – denn andernfalls landen sämtliche Inhalte des Download-Ordners auch auf Ihren anderen Geräten. Stellen Sie auch hier auf Wunsch noch eine Versionierung ein und bestätigen Sie oben rechts per Tipp aufs Häkchen.

Ob der Sync funktioniert, können Sie nun in der Dateimanager-App Ihres Smartphones prüfen. Im synchronisierten Unterordner sollte sich nach kurzer Wartezeit Ihre KDBX-Datei befinden.

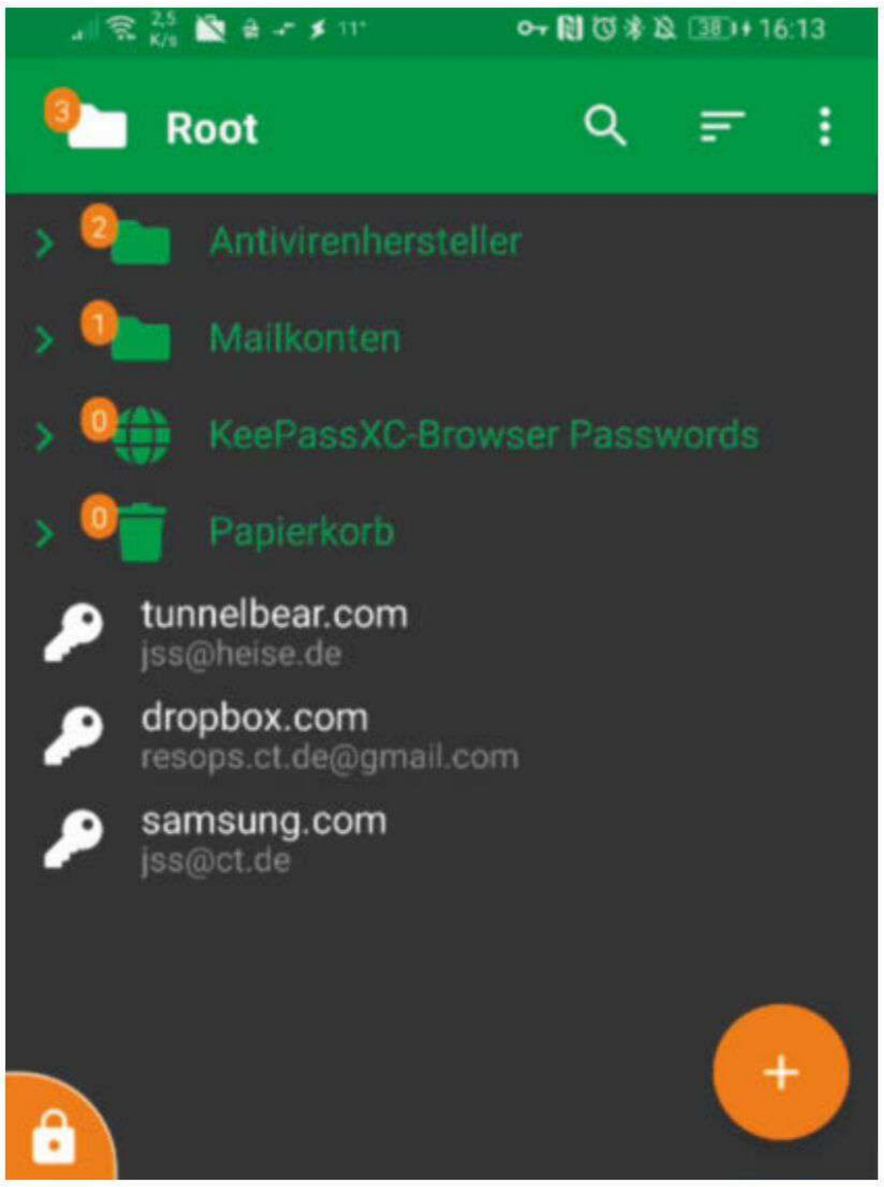
KeePass auf Android

Unter den diversen Apps, die die KeePass-Community entwickelt hat, besteht im Prinzip freie Auswahl, solange sie mit dem KDBX-Format umgehen können. Wir haben uns für KeePassDX entschieden. Es ist sowohl im Play Store als auch in F-Droid zu finden.

Vorab sollten Sie die Schlüsseldatei – sofern Sie eine solche zusätzlich zum Masterpasswort zum Öffnen des Passworttresors verwenden – aufs Smartphone kopieren. Im Idealfall erledigen Sie das per lokaler Verbindung (Datenkabel) und legen sie in einem Ordner ab, der nicht in irgendeiner Weise synchronisiert wird. Beim Öffnen von KeePassDX binden Sie nun den Passworttresor per Tipp auf „vorhandene Datenbank öffnen“ und Auswahl der KDBX-Datei ein. Tippen Sie das Masterpasswort ein und teilen Sie der App gegebenenfalls mit, wo die Schlüsseldatei liegt. Um künftig den Fingerabdrucksensor statt des Masterpassworts zu benutzen, tippen Sie nach Eingabe von Passwort und Schlüsseldatei nicht unten auf „Öffnen“, sondern auf das orangene Fingerabdruck-Logo.

Automatisch ausfüllen

Wie andere mobile Passwortmanager hilft auch KeePassDX beim Ausfüllen von Login-Feldern im Browser und anderen Apps. Dafür stehen zwei Funktionen bereit. Zum einen die KeePassDX-Tastatur, genannt Magikeyboard. Um sie zu verwenden, öffnen Sie in KeePassDX die Einstellungen und unter „Formularausfüllung“ die „Gerätetastatur-Einstellungen“. Schalten Sie „Magikeyboard“ ein und bestätigen Sie die Abfragen.



Es gibt so einige KeePass-Apps für Android – KeePassDX ist komfortabel und übersichtlich.

Zum Ausfüllen tippen Sie in ein Login-Feld und schalten die Tastatur auf „Magikeyboard“ um – wie das geht, kann von Gerät zu Gerät verschieden sein; oft gibt es dafür ein kleines Tastatursymbol unten rechts auf der Navigationsleiste. Tippen Sie dann auf das Schlüsselsymbol, woraufhin sich KeePassDX öffnet. Tippen Sie die Datenbank an, entsperren Sie sie und wählen Sie den passenden Passworteintrag aus. Die App führt Sie zurück zum Browser, wo Sie Benutzername und Passwort einfach nacheinander per Tipp auf das Personen-Icon sowie auf das „****“-Icon einfügen können.

Neben dem Magikeyboard gibts noch einen Autofill-Dienst. Er bedient sich komfortabler, funktioniert möglicherweise aber nicht auf allen Smartphones. Ihn aktivieren Sie in den Einstellungen unter „Formularausfüllung“ mit einem Tipp auf „Standarddienst für automatisches Ausfüllen festlegen“ und Auswahl von „KeePassDX“. In Login-Feldern von Browsern und anderen Apps erscheint im Regelfall schon beim Tipp auf ein Feld der Vorschlag, KeePassDX zu benutzen – wenn nicht, holen Sie die Funktion mit einem langen Tipp ins Eingabefeld und dann auf „Autofill“ hervor.

iOS-Lösungen

Von Syncthing selbst gibt es keine App für iOS, aber es gibt Möbius Sync. Das ist zwar nicht komplett Open Source, integriert aber die quelloffene Syncthing-Engine. Die Bedienung etwa auf einem iPad gleicht der auf dem Desktop nahezu vollständig. Möbius Sync ist zunächst kostenlos, doch wer einen Datenbestand größer als 20 MByte synchronisieren will, muss das für rund 5 Euro freischalten – einmalig, nicht per Abo. Geht es nur um eine Passwortdatenbank, dürfte die Gratisversion meist ausreichen.

Als Passwortmanager für iOS empfehlen sich etwa KeePassium oder Strongbox, die zwar quelloffen sind, aber für den vollen Funktionsumfang per Abo oder Einmalzahlung freigeschaltet werden wollen. Die Einschränkungen im Gratisbetrieb erweisen sich bei Strongbox als etwas lästiger, weil es biometrische Authentifizierung dann zwar zum Öffnen der App, nicht aber zum Öffnen von Passworttresoren erlaubt und jedes Mal das Masterpasswort fällig wird. Die Preise für Monatsabo, Jahresabo und Dauerlizenz liegen für Strongbox bei 3 Euro, 15 Euro und 50 Euro und für KeePassium bei 2 Euro, 15 Euro und 50 Euro.

Anders machen

Diese Anleitung eignet sich nicht nur zum Umstieg von LastPass. Sie können Sie in ähnlicher Weise auf jeden anderen Passwortmanager münzen, von dem Sie loskommen möchten – sehr wahrscheinlich wird es beim CSV-Import hier und dort Unterschiede in der Spaltensortierung geben.

Auch spricht nichts gegen die Verwendung anderer Apps, wenn Sie etwas finden, das Ihnen besser gefällt: Auf dem Smartphone zum Beispiel KeePass2Android, auf dem Desktop die reguläre KeePass-Software. Sie ist zwar bei Weitem nicht so schick wie KeePassXC, lässt sich aber durch Plug-ins fast beliebig im Funktionsumfang erweitern. Entscheidend ist in erster Linie, dass die Software das quelloffene KDBX-Format für Passwortdatenbanken unterstützt. Und auch bei der Synchronisierung sind Sie flexibel. Wer etwa schon gute Erfahrungen mit Resilio Sync gemacht hat, kann auch das nehmen – einen Überblick über verschiedene Sync-Programme finden Sie in [2]. (jss) c't

Literatur

[1] Jan Schüßler, **Taschentresor**, USB-Medien sicher verschlüsseln, c’t 14/2018, S. 116

[2] Jan Mahn, **Synchrone Satelliten**, Vier Programme für Peer-to-Peer-Synchronisation im Test, c’t 23/2018, S. 78

Alle Downloads

ct.de/wka6



2FA-Generator Reiner SCT Authenticator

Der Reiner SCT Authenticator sichert Online-Accounts als zweiter Faktor ab. Das ist komfortabler und leichter verständlich als per Smartphone-App.

Von **Ronald Eikenberg**

Ein zweiter Faktor ist das Beste, was Ihren Online-Accounts passieren kann: Haben Sie die Zwei-Faktor-Authentifizierung (2FA) aktiviert, dann ist Ihr Account auch dann noch geschützt, wenn ein Hacker Ihr Passwort kennt (siehe S. 38). Der zweite Faktor ist zum Beispiel ein Einmalcode, den Ihnen der Dienst per SMS zuschickt oder den eine Authenticator-App generiert. Das Einloggen gelingt mit 2FA nur dann, wenn sowohl das Passwort als auch der aktuell gültige Einmalcode stimmen.

Damit der Schutz wirksam ist, darf der Hacker nicht die Chance bekommen, den Einmalcode abzurufen oder zu generieren.

Würde der Code-Generator einfach nur als Software auf dem Rechner laufen, mit dem Sie sich einloggen, könnte ein Trojaner nicht nur das eingetippte Passwort, sondern auch den Code-Generator mit allen Geheimnissen abgreifen. Daher ist es sinnvoll, den Code mit einer separaten Hardware zu generieren. Das kann im einfachsten Fall das Smartphone mit Authenticator-App sein, aber auch ein USB-Stick wie ein YubiKey oder TrustKey (siehe S. 64).

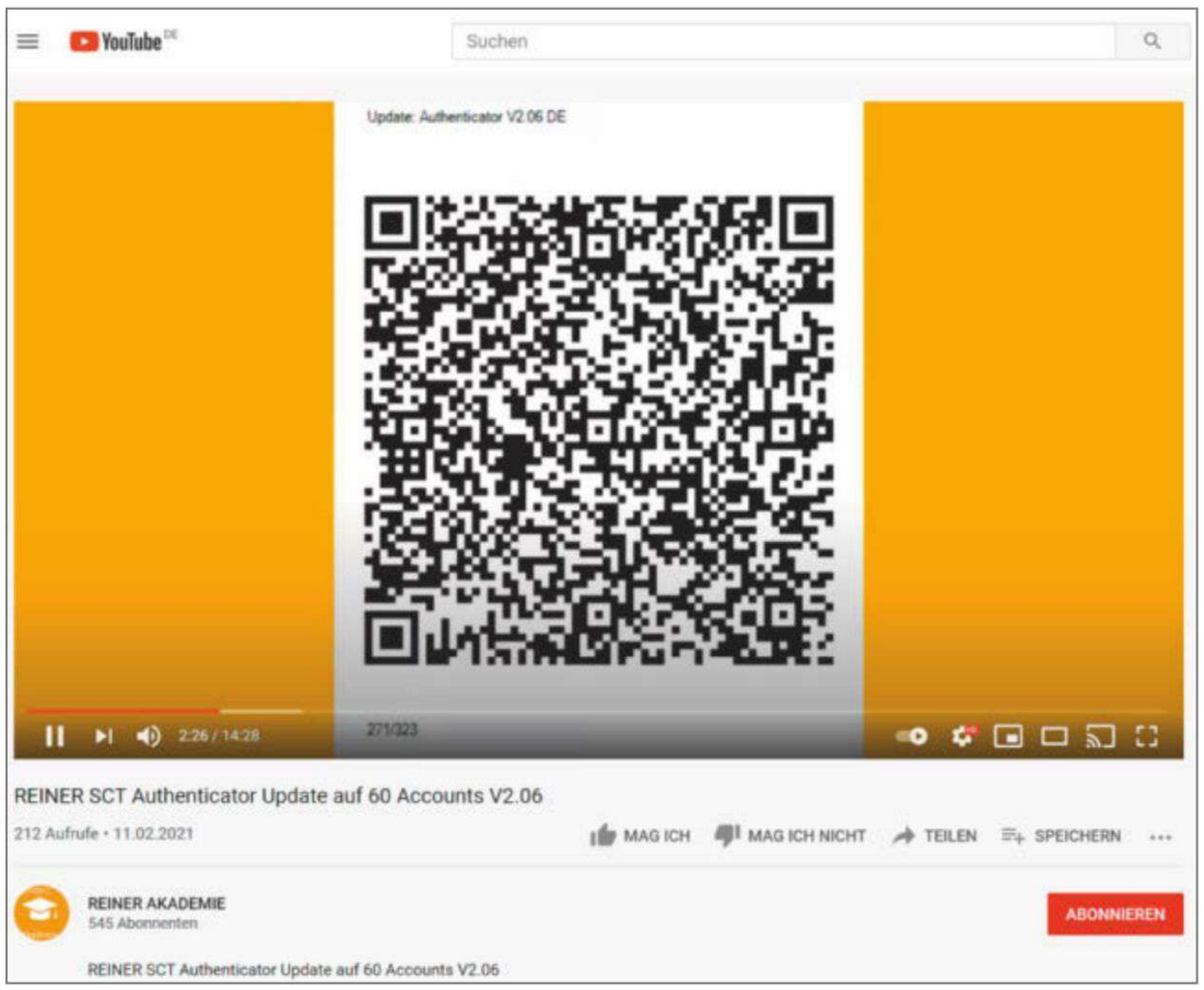
Der deutsche Kartenleser-Hersteller Reiner SCT bietet eine dritte Option an, die bei näherer Betrachtung durchaus sinnvoll ist: Der Reiner SCT Authenticator ist ein autarkes Gerät mit Zifferntastatur und Farbdisplay. Er besitzt keine Schnittstellen zur Außenwelt. Somit ist gewährleistet, dass ein Trojaner, der eventuell auf Ihrem Rechner oder Smartphone lauert, keinen Zugriff darauf hat und keine Einmalcodes generieren kann.

Der Authenticator arbeitet nach dem zeitbasierten TOTP-Verfahren (Time-based One-time Password), das die meisten Online-Dienste unterstützen, die Zwei-Faktor-Authentifizierung anbieten, darunter Google, Facebook und Twitter. Das Gerät ist mit einem Display und einer Zifferntastatur ausgestattet und erinnert äußerlich an einen Taschenrechner. Neue Accounts fügt man jedoch nicht umständlich über die Zifferntasten hinzu, sondern über die kleine Kamera auf der Rückseite: Sie scannt das für TOTP nötige Krypto-Geheimnis einfach als QR-Code vom Webdienst.

PIN-Sperre mit Selbstzerstörung

Nach dem Einschalten drückt man zwei Mal auf den OK-Knopf, um das Gerät in den Scanmodus zu versetzen und den Code zu scannen. Das hat im Test zuverlässig funktioniert, das Scannen dauerte lediglich eine Sekunde. Anschließend generiert der Authenticator einen passenden TOTP-Code, wenn man den gewünschten Account in der Liste auswählt. Der Zugriff lässt sich durch eine bis zu 12-stellige PIN schützen. Ist der PIN-Schutz aktiv, führt das Gerät nach fünf Fehlversuchen einen Reset auf Werkseinstellungen durch.

Damit ist der Funktionsumfang auch schon fast erzählt. Über das zweckmäßige Menü kann man die PIN-Sperre konfigurieren, Account-Einträge umsor-



Ungewöhnlich, aber effektiv: Der Reiner-Authenticator zieht sein Firmware-Update, indem er ein YouTube-Video abfilmt. Die Update-Daten sind in die flimmernden QR-Codes kodiert.



Auf der Rückseite des Authenticators befindet sich eine Kamera, mit der man QR-Codes fotografiert. So kann man Online-Accounts leicht mit dem Gerät verknüpfen.

tieren und löschen sowie Batteriestatus und Seriennummer abfragen. Hier lässt sich zudem eine Komfortansicht aktivieren, die sich jedoch kaum von der Standardansicht unterscheidet. Der Authenticator ist mit einer Uhr ausgestattet, die er benötigt, um die zeitbasierten OTP-Codes zu erzeugen. Sie kann über das Menü oder das Scannen eines QR-Codes gestellt werden. Eine Pufferbatterie sorgt dafür, dass man sich circa eine Minute mit dem Wechseln der vier AAA-Batterien Zeit lassen kann, ohne dass die eingestellte Uhrzeit verloren geht. Laut Hersteller halten die Batterien fünf Jahre, wenn pro Jahr 500 TOTP-Codes generiert werden.

Firmware-Update über YouTube

Ursprünglich konnte sich der Reiner SCT Authenticator lediglich zehn Accounts merken, inzwischen hat der Hersteller jedoch mit der neuen Firmware-Version 2.06 auf 60 aufgestockt. Wer das Gerät mit der alten Firmware gekauft hat, kann das Update nachträglich installieren – das ist ziemlich interessant, weil der Authenticator keine der üblichen Datenschnittstellen wie USB hat. Der Hersteller hat dieses Problem kreativ gelöst: Das Update erfolgt per YouTube-Video. Im Video flimmern einige Minuten QR-Codes über den Bildschirm, in die das Firmware-Update kodiert ist. Versetzt man den Authenticator in den Scan-Modus und filmt den Bildschirm einige Minuten ab, während im Hintergrund berühigende Musik läuft, ist das Gerät anschließend auf dem aktuellen Firmware-Stand. Das klingt seltsam, funktioniert aber. Der Hersteller empfiehlt, das Video mit der 360p-Auflösung abzuspielen, damit das Update reibungslos über die Bühne geht.

Im Alltagstest hat sich der Authenticator erstaunlich gut bewährt. Liegt das quietschgelbe Gerät neben der Tastatur, hat man den geforderten TOTP-Code schnell parat. Das geht schneller von der Hand, als etwa das Smartphone aus der Hosentasche zu ziehen, zu entsperren und den Google Authenticator zu starten. Wer bereits eine Authenticator-App mit allen Accounts eingerichtet hat, kann diese mit etwas Glück schnell auf den Reiner Authenticator übertragen: Mit der Android-App andOTP konnten wir einfach QR-Codes zu den hinterlegten Accounts anzeigen lassen, die sich mit dem Reiner-Gerät einlesen ließen. Der bei andOTP eingestellte „Aussteller“ wurde anschließend auf dem Reiner Authenticator als Dienstname angezeigt. Mit dem Google Authenticator klappte der Export jedoch nicht, das Gerät wusste mit den angezeigten QR-Codes nichts anzufangen. Es ist problemlos möglich, den von einem Webdienst angezeigten QR-Code mit mehreren Authentifikatoren zu scannen und das Reiner-Gerät parallel mit einer App zu nutzen.

Fazit

Die Zwei-Faktor-Authentifizierung ist mit dem Reiner SCT Authenticator zugänglicher als per Smartphone-App oder USB-Stick. Durch seinen reduzierten Funktionsumfang ist das Gerät intuitiv bedienbar, die Nutzung hat Parallelen zu TAN-Verfahren beim Online-Banking. Damit ist es auch für Personen verständlich, die mit der Nutzung einer Authenticator-App überfordert wären. (rei) c't

Reiner SCT Authenticator

OTP-Generator	
Hersteller	Reiner SCT, www.reiner-sct.de
Anschlüsse	–
OTP-Verfahren / Accounts	OATH-TOTP (SHA 1, SHA 256, SHA 512) / 60
Display / Auflösung	1,77"-TFT / 128 × 160 Pixel
Größe / Gewicht	102 mm × 62,5 mm × 19 mm / 80 g
Stromversorgung	4 × AAA-Batterien
Preis	40 €

AKTION:
Für den Reiner SCT Authenticator gibt es einen Leserrabatt auf Seite 170.

Produktseite, Update-Video
ct.de/wtez

betterCode()

JAVA 17

Die Heise-Konferenz zur neuen LTS-Version

Online am 14. September 2021

Jetzt Tickets sichern und Richtung modernes Java gehen

Die betterCode() Java 17 gibt Ihnen Antworten auf wichtige Fragen:

- Was sind die zentralen Neuerungen seit Java 11?
- Was ändert sich mit Java 17?
- Wie können Sie von Records, Pattern Matching und Switch Expressions profitieren?
- Was sind die relevanten API-Änderungen?
- Was macht ein LTS-Release genau aus?
- Warum jetzt wechseln?
- Was gilt es bei der Migration zu beachten?

heise Developer dpunkt.verlag

java.bettercode.eu

Universal-Sicherheitsschlüssel TrustKey

Die TrustKey-Sicherheitsschlüssel beherrschen drei Verfahren zur Absicherung von Online-Accounts und sind damit vielseitig einsetzbar.

Von **Ronald Eikenberg**



Die beiden FIDO2-Sicherheitsschlüssel TrustKey T110 (USB-A) und T120 (USB-C) schützen Online-Accounts zuverlässig vor Zugriffen durch Hacker. Sie arbeiten als zweiter Faktor zusätzlich zum Passwort oder sogar als Passwortersatz. Ist so ein Sicherheitsschlüssel erstmal mit dem Account verknüpft, dann muss er fortan beim Einloggen mit dem Rechner oder Smartphone verbunden sein, ansonsten schlägt der Login fehl. Hat ein Hacker das Passwort erbeutet, kann er sich damit also nicht einloggen, sofern er den USB-Schlüssel nicht ebenfalls geklaut hat.

Neben dem modernen FIDO2-Verfahren, das sogar sichere Logins ohne Passwort vorsieht, unterstützen die beiden TrustKey-Sticks auch das ältere U2F (FIDO1) sowie OTP. Das macht sie vielseitig, denn nach wie vor ist die Anzahl der Online-Dienste überschaubar, bei denen man sich mit FIDO2 authentifizieren kann. Die U2F-Unterstützung ist keine Überraschung, da die meisten FIDO2-Schlüssel dazu abwärtskompatibel sind. OTP (One-Time Password) ist hingegen eine andere Baustelle und hat mit den beiden FIDO-Standards wenig zu tun. In den meisten Fällen wird für OTP vermutlich eine Authenticator-App wie der Google Authenticator genutzt. Dieser generiert kurzzeitig gültige Zahlencodes, die man beim Einloggen nach dem Passwort eintippen muss.

Das können auch die beiden TrustKey-Sticks, wenn man den TrustKey Key Manager von der Herstellerwebsite installiert. Aktuell gibt es ihn für Windows und macOS. Der Windows-Installer des Tools verwirrte uns im Test, da er nur kurz auf dem Bildschirm aufblitzte und uns nicht wie erwartet durch die Installation leitete. Anschließend ließ sich der Key Manager dennoch über das Startmenü ausführen. Der Funktionsumfang des Tools ist aufs Nötigste reduziert.

QR-Code-Scan

Zunächst muss man den Sicherheitsschlüssel mit einer PIN schützen, anschließend kann man Accounts mit ihm verknüpfen. Das geht leicht von der Hand:

TrustKey T110 & T120

FIDO2-Sicherheitsschlüssel		
Modell	T110	T120
USB-Anschluss	USB-A	USB-C
Resident Keys / U2F / OTP	✓ / ✓ / ✓	✓ / ✓ / ✓
Preis	28,56 € zzgl. 5,95 € Versand	30,34 € zzgl. 5,95 € Versand
Bezugsquelle	webshop.pointblank.de	webshop.pointblank.de
Bewertung		
Kompatibilität	⊕⊕	⊕⊕
Bedienung	⊕	⊕
Extras	⊕	⊕
Robustheit	⊕⊕	⊕⊕

⊕⊕ sehr gut ⊕ gut ✓ vorhanden – nicht vorhanden

Das Tool durchsucht den Bildschirm automatisch nach dem QR-Code, den die meisten Onlinedienste bei der Einrichtung von OTP anzeigen. Alternativ kann man auch einen Kryptoschlüssel in den Einrichtungsdialog des Key Managers kopieren. Den Kryptoschlüssel erhält man vom jeweiligen Onlinedienst während der Einrichtung. Anschließend erscheint ein Eintrag für den hinzugefügten Dienst im Hauptfenster des Key Managers. Ein Klick darauf erzeugt einen passenden Einmalcode und zeigt ihn an.

Gegenüber einer einfachen OTP-Generator-App ist der Hauptvorteil auch hier wieder die feste Bindung an den Sicherheitsschlüssel: Nur wer den TrustKey-Stick physisch besitzt, kann OTP-Codes damit generieren. Er ist nicht kopierbar. Die Sicherheitsschlüssel unterstützen die beiden gängigen Verfahren TOTP und HOTP.

Die Authentifizierung mittels FIDO2 und U2F funktionierte im Test ebenfalls reibungslos. Auch das Einloggen ohne Passwort, etwa bei Microsoft, klappte auf Anhieb. Die beiden Sicherheitsschlüssel verhielten sich identisch, sie unterscheiden sich lediglich durch USB-Anschluss: Der T110 ist mit dem weit verbreiteten USB-A-Anschluss ausgestattet, der T120 nimmt über das moderne USB-C Kontakt auf.

Fazit

Beide Modelle sind gut verarbeitet und wirken robust. Zur Bestätigung einer FIDO-Authentifizierung muss man die goldfarbene Kontaktfläche lediglich leicht berühren, wodurch der USB-Anschluss nicht mechanisch belastet wird. Zur Nutzung von OTP muss auf dem Sicherheitsschlüssel eine aktuelle Firmware laufen, die auf den derzeit vom deutschen Shop ausgelieferten Exemplaren bereits vorinstalliert ist. Nachträglich aktualisieren lässt sich die Firmware derzeit nicht. (rei) c't



Tracking und Cookie-Hinweise loswerden

Inhalte geraten im World Wide Web zur Nebensache, stattdessen dominieren meterlange Cookie-Dialoge, aufdringliche Reklame und ausuferndes Tracking. Wer das Internet ohne solche Nervereien nutzen will, muss zunächst verstehen, wie und wo seine Daten abfließen.

Von **Jo Bager**



Bild: Sven Hauth

Überwachung verhindern

Cookies und anderes Generve	66
Sieben Browser im Privacy-Check	72
Surfen ohne Cookies, Tracking und Reklame	78
Die Zukunft des Tracking	86
Microsoft Office ohne Cloud	90
Windows ohne Microsoft-Konto nutzen	96
Zeiterfassung per Fingerscan?	104
Spionageschutz mit Access Dots	107
Lauschangriff mit optischem Teleskop	108

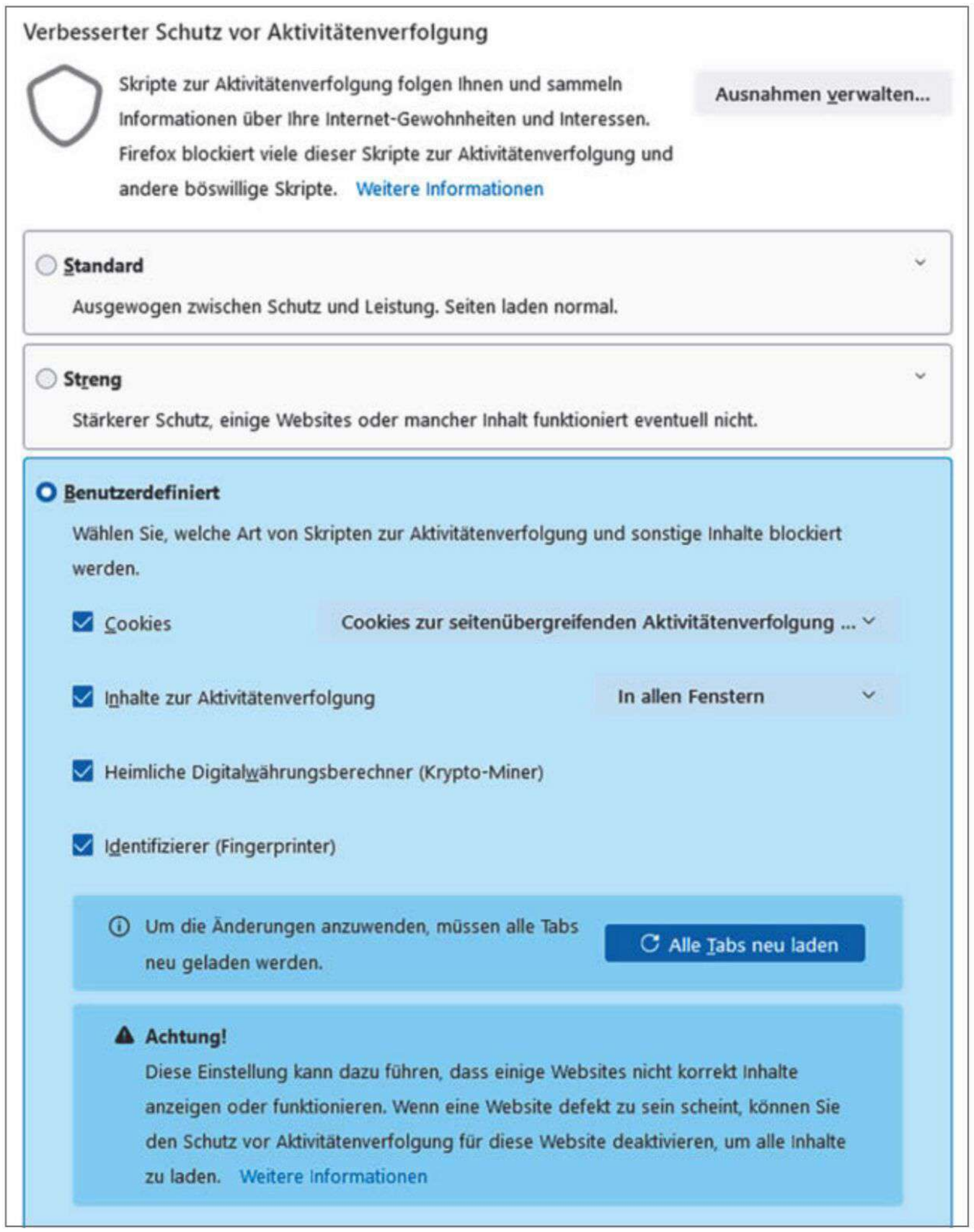
Consent-Banner, auch Cookie-Banner genannt, sind die Geißel des modernen Webs. Kaum eine Webseite kann man noch „einfach so“ abrufen. Stattdessen drängelt sich ein Dialogfenster in den Vordergrund, eine Art digitaler Türsteher. Und der lässt einen nur rein, wenn man sein Einverständnis gibt.

Wehe dem, der nicht auf den Button „Alles akzeptieren“ klickt. Wer stattdessen genau erfahren möchte, wofür er eigentlich sein Einverständnis geben soll und die entsprechenden Einstellungen einzeln vornehmen will, der sollte Zeit mitbringen. Denn dann gilt es, ellenlange Erklärtexte durchzulesen und Dutzende oder Hunderte Einzeleinstellungen vorzunehmen.

Dabei erfüllen Consent-Banner eigentlich einen guten Zweck: Kein Website-Betreiber soll gemäß der Datenschutzgrundverordnung mit den Daten seiner Besucher einfach machen dürfen, was er will. Stattdessen soll jeder Surfer eine informierte Entscheidung darüber treffen können, was mit seinen Daten geschieht. Und dafür muss er erklärt bekommen, was der Website-Betreiber mit seinen Daten zu tun beabsichtigt und dazu sein Einverständnis geben.

In der Praxis klicken Anwender die Consent-Banner aber meistens schnell weg und die Banner verfehlen ihr Ziel. Dabei versuchen viele dieser Consent-Banner, dem Besucher durch Tricksereien auf der Bedienoberfläche am Ende doch noch die für ihn ungünstigeren Einstellungen unterzujubeln. Die Datenschutzorganisation noyb jedenfalls sieht massenhaft Verstöße bei Cookie-Bannern, weshalb sie begonnen hat, bei Websites per Software-Roboter bessere Cookie-Dialoge anzumahnen.

Dieser Artikel erklärt die technischen Grundlagen der Cookies sowie anderer Techniken, mit den Sie getrackt werden, und welche Rolle Online-Werbung dabei spielt.



Browser, wie hier Firefox, blockieren zunehmend auch Tracking-Skripte.

Bittere Kekse

Consent-Banner sind der Auswuchs eines schon länger währenden Kampfes gegen die Umtriebe der modernen Internet-Werbeindustrie. Um zu verstehen, worum es eigentlich geht und was dabei schiefläuft, muss man in der Vergangenheit und bei den Basics anfangen: den Cookies.

Cookies sind in den 90er-Jahren erfunden worden, um eine Schwäche des HTTP(S)-Protokolls wettzumachen, mit dem Browser Webseiten vom Server aufrufen. HTTP ist ein zustandsloses Protokoll. Das heißt, der Web-Server bearbeitet jede HTTP-Abfrage unabhängig von den vorhergehenden. So kann sich aber zum Beispiel ein Webshop nicht merken, welcher Kunde welche Artikel in den Warenkorb legt.

Cookies ergänzen diese Möglichkeit. Mit einem bestimmten HTTP-Header veranlasst der Webserver den Browser, einen Identifier zu speichern, der mit der Website assoziiert ist: das Cookie. Ruft der Browser eine weitere Seite von einem Server ab, der ein

Cookie gesetzt hat, dann liefert der Browser das Cookie mit. Damit kann der Server den Benutzer – genauer gesagt seinen Browser – wiedererkennen und den Seitenabruf mit früheren in Verbindung bringen.

Es gibt neben dem Warenkorb viele weitere nützliche Anwendungsfälle für Cookies. So können sich Webdienste damit merken, dass sich ein bestimmter Nutzer eingeloggt hat oder welche Einstellungen er bevorzugt. Stammt das Cookie von der Website, die man gerade besucht, spricht man von First-Party-Cookies. Problematisch sind erst die sogenannten Third-Party-Cookies, die man sich durch eingebettete Inhalte von Drittanbietern einhandelt.

Viele Webseiten enthalten zum Beispiel eingebettete YouTube-Videos oder Tweets. Betreiber großer Websites lagern Bilder und andere Mediendateien oft in sogenannten Content-Delivery-Netzwerken von Drittanbietern aus, die sich auf die schnelle Auslieferung solcher Inhalte spezialisiert haben. Viele Sites betten zudem Werbung von externen Anbietern in ihre Seiten ein. Auch Unternehmen, die Inhalte in Webseiten einbetten, können dort Cookies setzen.

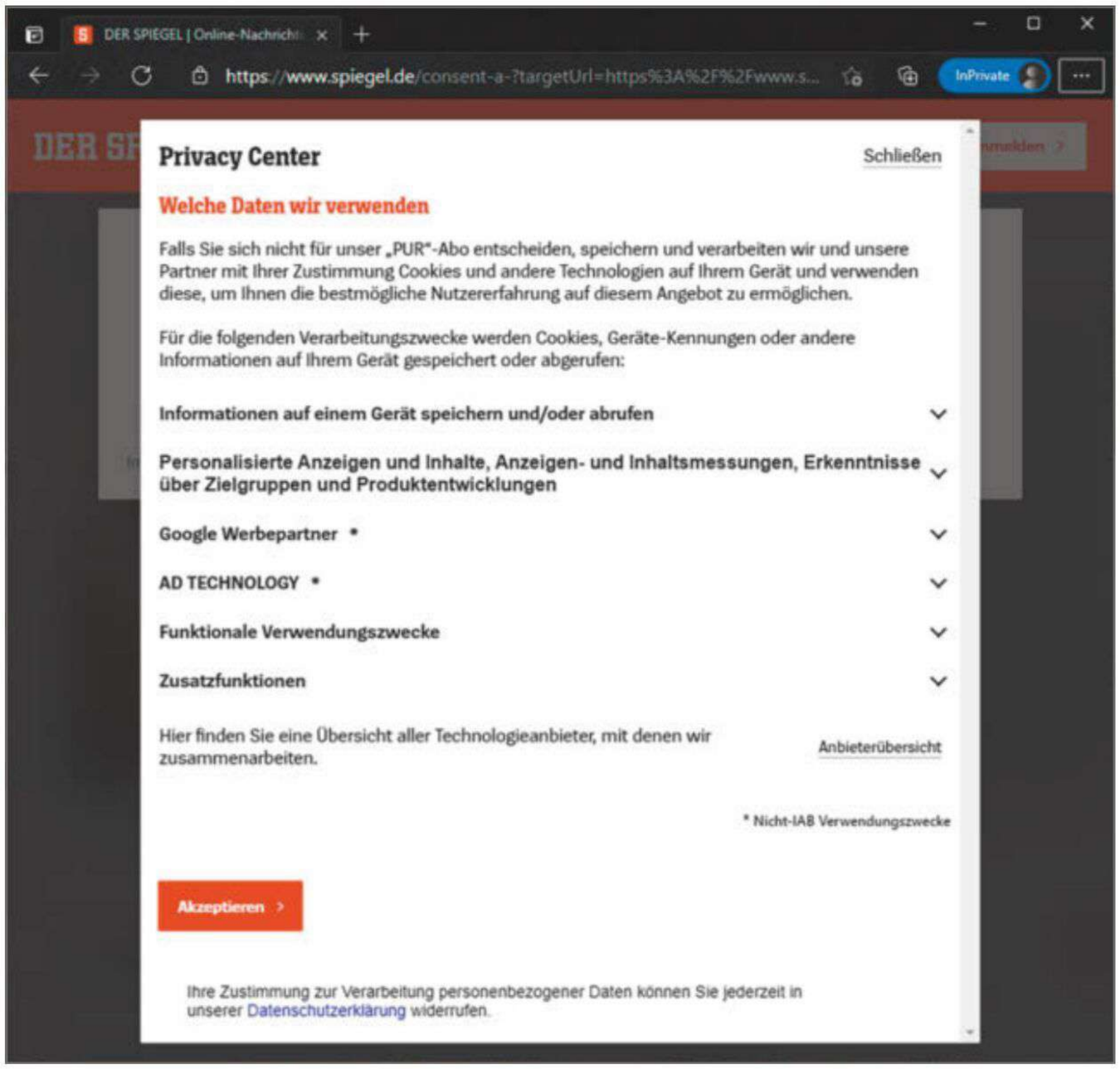
Für solche Third-Party-Cookies gibt es ebenso viele legitime Anwendungen. So können Content-Delivery-Netzwerke mithilfe von Cookies ihr Load Balancing besser austarieren, was letztlich zu schneller ladenden Sites für den Surfer führt. Und mit einem Analytics-Dienst wie Google Analytics kann der Website-Betreiber die Datenströme auf seiner Site untersuchen und sie damit für jeden Besucher besser gestalten. Allerdings erfährt Google Analytics zu diesem Zweck jeden einzelnen Seitenabruf, was wiederum zulasten der Privatsphäre geht.

Ganz zuungunsten der Benutzer hat sich die Nutzung von Cookies auf dem Werbemarkt entwickelt, der ja eigentlich auch ein legitimes Mittel bietet, um Websites zu refinanzieren. Doch die Online-Werbebranche giert nach immer mehr Daten der Surfer.

Das hat damit zu tun, dass ein immer größerer Teil der Online-Werbung über Echtzeitmarktplätze des sogenannten Programmatic Advertising ausgeliefert wird. Dabei sollen Nutzer mit einem passenden Werbeprofil angesprochen werden und so nur Reklame zu Gesicht bekommen, die sie wahrscheinlich interessiert. Werbetreibende werten dazu mithilfe von Cookies aus, auf welchen Webseiten sich Nutzer welche Inhalte ansehen.

Dabei kommt großen Werbediensten zugute, dass sie regelrechte Netzwerke betreiben, die auf vielen Websites Werbung ausliefern. Mit ihren Cookies können sie Surfer daher Klick für Klick von Site zu Site verfolgen. Website-Betreiber blenden nicht selten Werbung mehrerer Werbenetze ein, liefern also die Daten ihrer Besucher gleich an mehrere Weiterverarbeiter.

Mit der Verarbeitung der so gewonnenen Informationen verdient eine riesige Marketing- und Adtech-Industrie ihr Geld. An der Weiterverarbeitung der Daten, die beim Abruf einer einzelnen Webseite anfallen, sind oft Dutzende Unternehmen beteiligt. Adtech-Anbieter versuchen aus den Daten Rückschlüsse über Alter, Geschlecht, Einkommenssituation, Hobbies und vieles mehr zu ziehen, um im Rahmen des „Predictive Behavioral Advertising“ jedem Surfer maßgeschneiderte Werbung präsentieren zu können [1].



Eigentlich verfolgen Consent Banner ein hehres Ziel, in der Praxis nerven sie meist aber nur.

Gar nicht super, Cookie!

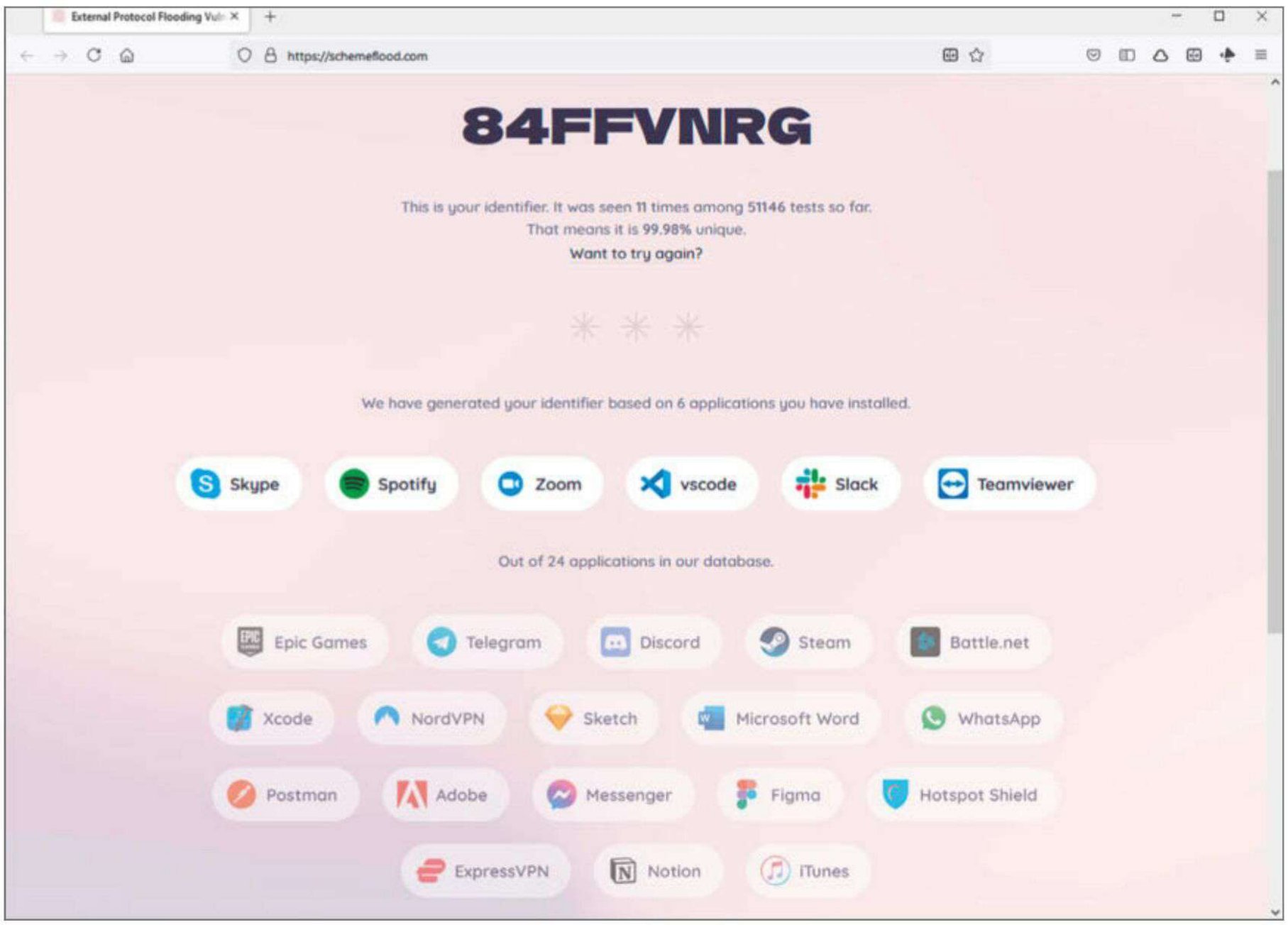
Nicht nur HTTP-Cookies lassen sich dazu benutzen, um Benutzer bei ihren Streifzügen im Web zu tracken. So gut wie jede Technik, mit der Websites im Browser Inhalte speichern, hat das Potenzial dazu, Surfer wiedererkennbar zu machen. Man spricht dann auch von Supercookies. Mozilla zählt in seinem Blog ein knappes Dutzend Cache-Speicher auf, die dafür infrage kommen, zum Beispiel den Bilder- oder den Font-Cache.

In einer Anfang 2021 veröffentlichten Studie haben Forscher demonstriert, wie man sogar Favicons nutzen kann, um Browser zu identifizieren – die kleinen Logos der Websites, die in der Tab-Leiste und im Bookmark Manager angezeigt werden (siehe ct.de/w37j). Das funktionierte selbst bei aktivierten Anti-Tracking-Maßnahmen, Inkognito-Modus und dem gezielten Löschen des Surf-Verlaufs.

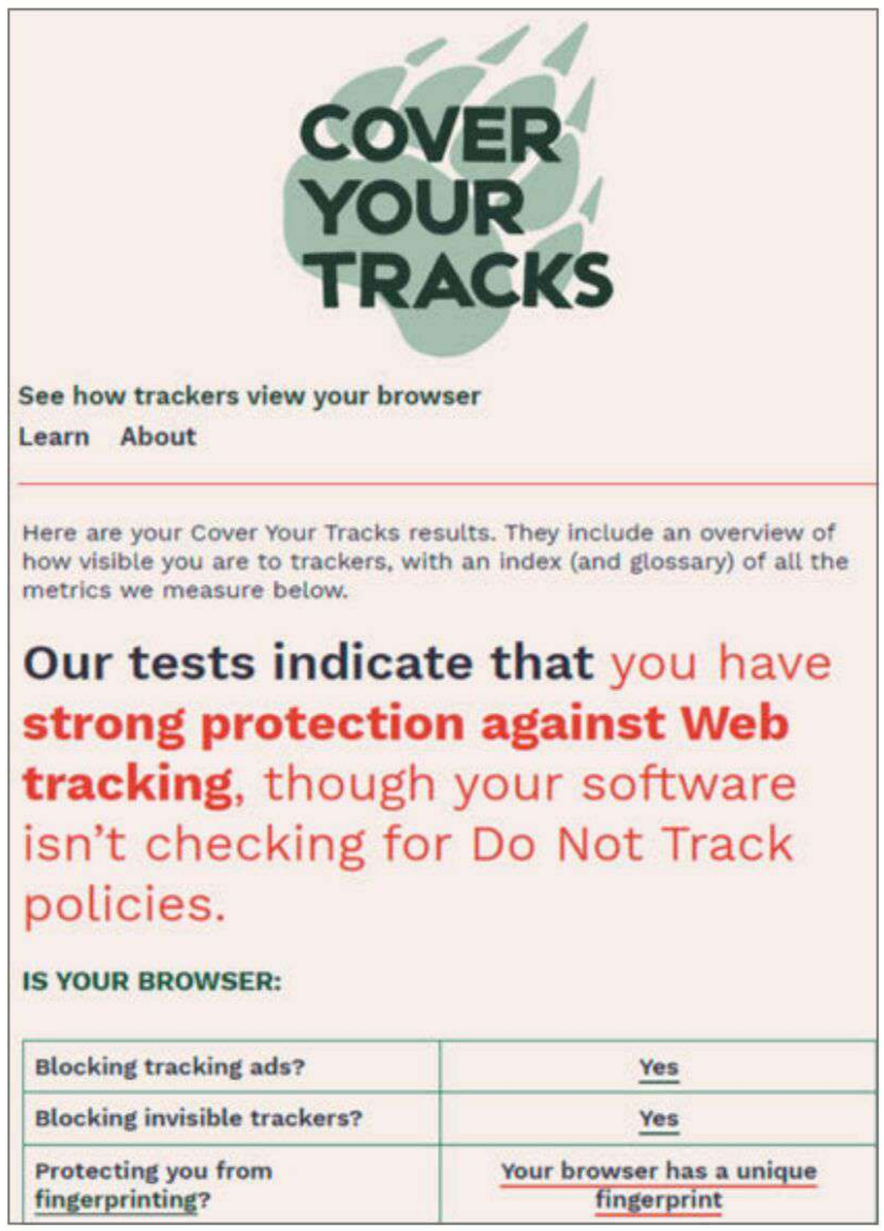
Im Zweifelsfall muss man davon ausgehen, dass solche Methoden nicht lange theoretische Szenarien bleiben, sondern dass findige Werbeunternehmen sie ausnutzen, wenn die Browser ihnen die Möglichkeit dazu bieten. Der Hacker Samy Kamkar hat gezeigt, wie sich aus verschiedenen Speichertechniken auch ein sehr schwer zu löschendes Cookie bauen lässt: Sein „Evercookie“ nutzt mehrere Speichertechniken des Browsers. Löscht der Benutzer einzelne Elemente des Evercookies, stellt es diese aus den anderen wieder her (siehe ct.de/w37j).

Verräterische Fingerabdrücke

Kaum zwei PCs, kaum zwei Browser sind identisch konfiguriert. Werber machen sich das zunutze, um Surfer wiederzuerkennen, ohne einen Identifier speichern zu müssen. Der eindeutige virtuelle Finger-



schemeflood.com versucht einen Fingerabdruck anhand der installierten Anwendungen zu ermitteln.



Wie eindeutig ist Ihr Browser wiedererkennbar? Bei Online-Tests wie hier „Cover your Tracks“ können Sie das ausprobieren.

abdruck des Browsers genügt. Diese Technik nennt sich daher auch Browser Fingerprinting.

Schon beim Seitenabruf übermittelt jeder Browser Informationen, beispielsweise die eigene Versionsnummer, die Bildschirmauflösung, das Betriebssystem, installierte Plug-ins und Schriften. Daraus ergibt sich bereits ein Bild des Systems, auf dem der Browser läuft. Mit eingebettetem JavaScript lässt sich das beliebig verfeinern.

Besonders effektiv ist das sogenannte Canvas Fingerprinting. Unsichtbar für den Anwender lässt ein Skript den Browser Bilder oder Texte rendern. Diese sind so gestaltet, dass sich von Browser zu Browser kleine, messbare und eindeutig zuzuordnende Unterschiede im Layout ergeben.

Mittlerweile hat die Industrie Dutzende Techniken und Programmierschnittstellen gefunden, mit denen sich eindeutige Rückschlüsse auf den Browser ziehen lassen. Nach den Angaben des Anbieters FingerprintJS.com, der das Fingerprinting als Dienstleistung anbietet, eignet sich zum Beispiel das Web Audio API hervorragend dafür.

FingerprintJS.com sagt über sich selbst, dass es einzelne Browser mit einer Trefferquote von 99,5 Prozent wiedererkennen kann. Wenn Sie selbst herausfinden möchten, wie eindeutig der Fingerabdruck Ihres Browsers ist, finden Sie dazu unter amiunique.org und coveryourtracks.eff.org zwei Tests.

In einer Untersuchung der weltweit meistbesuchten 100 000 Sites aus dem Jahr 2020 haben Forscher zwar nur auf jeder zehnten Website Fingerprinting-Skripte gefunden. Die Technik ist laut der Studie aber umso verbreiteter, je beliebter eine Website ist. Unter den Top 1000 der Websites betrug der Anteil der Fingerprinter mehr als 30 Prozent.

Virtuelle Paravente

Auch wenn sich die Trackingfirmen immer neue Tricks einfallen lassen, sollten Sie nicht vor der Datengier der Konzerne kapitulieren: Browser haben verschiedene Schalthebel, mit denen Sie der Datensammelei einen Riegel vorschieben können. Für das Management von Cookies zum Beispiel gibt es schon seit langem Einstellungsmöglichkeiten. Sie können zum Beispiel Third-Party-Cookies pauschal blockieren lassen.

Aber das Ende der Third-Party-Cookies ist ohnehin besiegelt. Google hat angekündigt, aus dem Geschäft auszusteigen. Das Unternehmen will auch keine anderen Identifikationslösungen nutzen, die dazu genutzt werden können, einzelne Nutzer zu tracken. Wenn also selbst der Werbekonzern Google das Tracking mit Cookies einstellt, kann man davon ausgehen, dass diese demnächst allenfalls eine untergeordnete Rolle spielen werden.

Viel Ungemach können Sie zudem blockieren, wenn Sie JavaScript deaktivieren: Sowohl zum Setzen und Auslesen von Browserspeicher als auch für das Fingerprinting müssen Skripte laufen. Deaktiviert man JavaScript allerdings pauschal, funktionieren viele Sites nicht mehr richtig.

Gezielter lassen sich Skripte mit Werbe- und Inhalteblockern wie den Browsererweiterungen uBlock Origin und uMatrix aushebeln, die zum Beispiel Inhalte nur von bekannten Tracking-Domains ausfiltern. Browser übernehmen solche Funktionen zunehmend auch selbst.

Erst seit relativ kurzer Zeit setzen Browser zudem Containerisierung ein, um Tracking zu erschweren:

Literatur

[1] Torsten Kleinz, **Gezerre um die Zukunft der Online-Werbung**, Googles Cookie-Ausstieg: Streit um „Tracking Light“, c’t 8/2021, S. 28

Weiterführende Informationen

ct.de/w37j

Inhalte werden jeweils nur noch im Kontext der zugehörigen Domain gespeichert, und zwar auch die Inhalte von Partnern, etwa Werbetreibenden. Die können so zwar immer noch ihre Cookies setzen oder andere Dateien speichern. Die Sites können aber nicht mehr aus dem Kontext einer anderen Website darauf zugreifen und die Surfer also nicht mehr auf ihren Streifzügen verfolgen. Um es Werbetreibenden zu erschweren, eindeutige Fingerabdrücke zu erzeugen, setzen Browser zudem auf Verschleierung (obfuscation). Dabei geben sie nicht mehr von sich aus so viele Informationen über sich preis.

Doch wie gut schützt welcher Browser Ihre Privatsphäre? Im Beitrag ab Seite 72 klopfen wir Brave, Chrome, Edge, Firefox Opera, Safari und Vivaldi auf ihre Datenschutzfunktionen hin ab. Der Artikel ab Seite 78 erklärt, wie Sie Firefox so aufrüsten, dass er Ihre Privatsphäre bestmöglich schützt und gleichzeitig Nervereien wie Cookie-Banner unterdrückt.

Das Ende der Third-Party-Cookies – die sogenannte Cookiecalypse – und Browser, die immer besser die Privatsphäre schützen, werden aber nicht verhindern, dass die Werbebranche Surfer auch in Zukunft trackt. Das Geschäftsmodell viel zu vieler Unternehmen hat mit der Aufbereitung von Nutzerdaten zu tun. Derzeit herrscht ein heftiges Gezerre darum, welche Standards an Stelle der Cookies treten. Im Artikel ab Seite 86 geben wir einen Überblick.

Überwachung und Tracking sind aber nicht nur im Browser ein Problem, sondern betreffen auch viele andere Anwendungen. Wehren kann man sich fast überall: Die Artikel auf den Seiten 90 und 96 zeigen, wie man Microsofts Office heikle Datenübertragungen abgewöhnt und Windows gegen alle Widerstände ohne Online-Account nutzt. Auf Seite 107 erfahren Sie, wie Sie Ihr Smartphone auf unerwünschte Lauscher kontrollieren; auf Seite 104 dagegen, wann Überwachung zum Zwecke der Arbeitszeiterfassung zu weit geht. Einen Einblick in Überwachung auf Geheimdienstniveau und den Stand der Forschung gibt der Artikel auf Seite 108. (jo) c't

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



Jetzt Mini-Abo testen:
3 Hefte + Bluetooth-Tastatur nur 16,50 €

www.iX.de/testen

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

iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

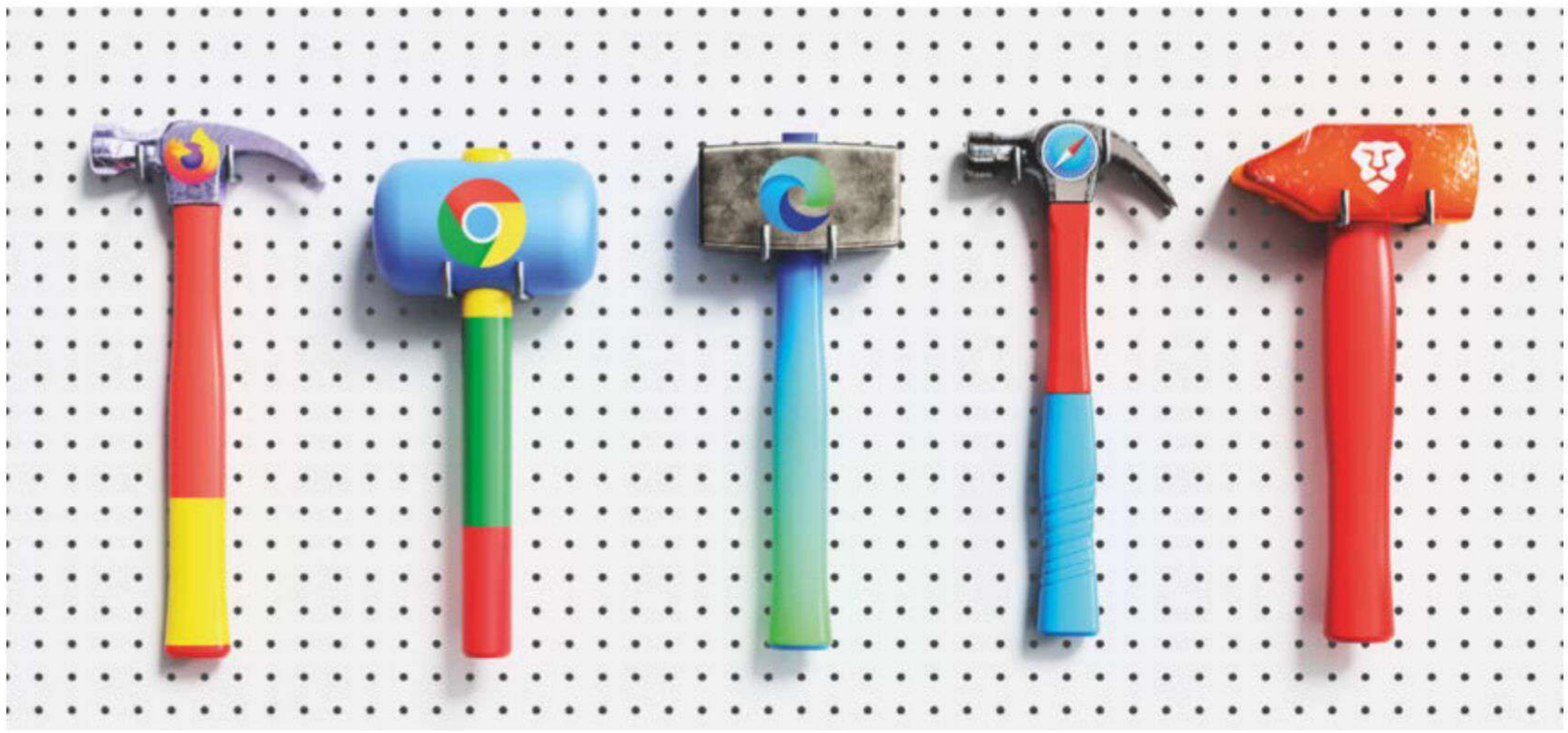


Bild: Andreas Martini

Sieben Browser im Privacy-Check

Kümmert sich Ihr Browser um den Schutz Ihrer Daten oder funkt er sie gleich selbst in die weite Welt hinaus? Unser Privacy-Check liefert die Antworten.

Von **Ronald Eikenberg**

Die Wahl des Browsers ist eine Vertrauensfrage, denn kaum eine andere Software kommt mit so vielen sensiblen Daten in Kontakt: Surfverhalten, Passwörter, Banking, Kommunikation und vieles mehr. Im besten Fall nimmt der Browser den Schutz Ihrer Daten ernst, im schlechtesten Fall ist er selbst eine Datenpetze. Wir haben die Desktop-Browser Brave, Chrome, Edge, Firefox, Opera, Safari und Vivaldi einem Privacy-Check unterzogen, um die Spreu vom Weizen zu trennen. Auch wenn die Browser auf den ersten Blick alle das Gleiche tun, könnten die Ergebnisse kaum unterschiedlicher sein.

Uns hat sowohl interessiert, welche Trackingschutzfunktionen die Browser mitbringen und wie effektiv diese arbeiten, als auch, welche Daten die Browser eigenmächtig in die Welt hinaussenden. Denn der beste Trackingschutz ist wertlos, wenn schon der Browser selbst das Datenschutzproblem ist. In unserem Testparcours zeigte sich etwa, ob ein Browser unsichtbare Tracker und Werbung abwehrt, die den Nutzer verfolgt. Auch die Identifizierbarkeit des Browsers mittels Fingerprinting haben wir überprüft.

Wir ließen die Browser unter anderem auf die Onlinetests „Cover your tracks“ der Electronic Frontier Foundation (EFF), Browserleaks und FingerprintJS los, das Browser-Installationen mit einer Zuverlässigkeit von 99,5 Prozent wiedererkennen soll – ganz ohne Cookies. Die Browser mussten unseren Testparcours sowohl im Auslieferungszustand als auch mit maximal hochgedrehten Schutzfunktionen absolvieren.

Zudem überprüften wir, ob die Browser bestimmte Datenschutzfunktionen wie DNS-over-HTTPS (DoH) anbieten, durch das IP-Adressen zu Domains transportverschlüsselt bei einem DoH-Server abfragt werden. Weniger effektiv ist der „Do Not Track“-Header, durch den der Browser einer Website signalisieren kann, dass sein Nutzer nicht getrackt werden möchte. Die Website kann darauf Rücksicht nehmen, muss sie aber nicht. Man sollte ihn dennoch aktivieren können. Darüber hinaus wollten wir wissen, welche Filterlisten die Tracking- und Werbeblocker der Browser nutzen, beliebt sind zum Beispiel die Listen EasyPrivacy und EasyList.

Um herauszufinden, was die Browser aus eigenem Antrieb ins Internet übertragen, haben wir ihren Traffic durch den SSL-Proxy mit mproxy geleitet. So konnten wir live mitverfolgen, welche Daten wohin verschickt wurden. Während manche Browser auf leisen Sohlen unterwegs waren, meldeten andere schon das Tippen in der Adresszeile Zeichen für Zeichen an den Server eines Internetriesen, um Suchvorschläge abzurufen. Manche Browser hinterließen selbst im Inkognito-Modus gut lesbare Datenspuren im Netz.

Es handelt sich bei unserem Privacy-Check um eine Momentaufnahme: Die Browser-Welt dreht sich schnell und auch beim Tracking ist gerade einiges in Bewegung. Sie werden jedoch einen fundierten Eindruck davon bekommen, welche Browser das Thema Datenschutz ernst nehmen.

Google Chrome

Chrome kommt nach wie vor minimalistisch und ohne Fremdwerbung daher. Der Browser kommunizierte während unserer Analyse hauptsächlich mit Google und lud nach der Installation eine Handvoll Erweiterungen nach, vor allem zur Integration der Google-Dienste. Zudem zog er sich auf unser Windows-System einen On-Demand- Virenscanner, den Google von Eset entwickeln ließ. Er ist in den Einstellungen über „Zurücksetzen und bereinigen / Computer bereinigen“ aufrufbar.

Bei der Adresseingabe übertrug Chrome erwartungsgemäß jedes Zeichen an Google, um die Suchvorschläge abzurufen. Die angesteuerten URLs funkte der Browser hingegen nur an sein Mutterschiff, wenn wir das optionale „Erweiterte Safe Browsing“ eingeschaltet hatten. Chrome meldet gelegentlich an https://beacons.gcp.gvt2.com/domainreliability/upload, wenn Google-Domains nicht erreicht werden konnten, offenbar um Google dabei zu helfen, die Verlässlichkeit der Dienste im Blick zu behalten

Der Google-Browser erkundigt sich dann und wann nach Updates und Inhalten für die „Neuer Tab“-Seite. Es gibt auch einen Mechanismus, um darauf Promotion-Aktionen anzuzeigen, der Google-Server hatte jedoch während unserer Analyse keine in petto. Alles in allem sind die Kontaktversuche nach außen selbst mit aktivierter Diagnose-Option überschaubar und nachvollziehbar. Auffällig war, dass Chrome eine Reihe zufällig generierter URLs zu kontaktieren versuchte. Der Browser versuchte so zu erkennen, ob der Internetprovider ungültige URLs abfängt, um etwa Werbung anzuzeigen (DNS-Antwort NXDOMAIN).

Einen Tracking- oder Adblocker sucht man vergeblich. Einzig die Chromium-Basics wie das Blockieren von Drittanbieter-Cookies, den „Do No Track“-Header und verschlüsseltes DNS über HTTPS kann man konfigurieren, um die Privatsphäre zu verbessern.



Komfort versus Datenschutz: Sind Suchvorschläge für die Adressleiste aktiv, melden viele Browser jedes eingetippte Zeichen an einen Server.

Mozilla Firefox

Mozilla schärft den in Firefox integrierten Trackingschutz immer weiter nach (siehe S. 78). Einen Werbeblocker gibt es zwar nicht, der Trackingblocker filtert auf maximaler Stufe jedoch vieles weg. Die Daten für den Trackingschutz wurden im Vorfeld direkt von Mozilla geladen. Anfragen an detectportal.firefox.com/success.txt stellten sicher, dass eine ungestörte Verbindung zum Internet besteht.

Firefox öffnete zudem eine WebSocket-Verbindung zu Mozillas Push-Service, um Benachrichtigungen von Websites empfangen zu können. Bei openh264.org holte sich Firefox den H.264-Videocodec ab, bei Google eine Bibliothek für das Video-DRM Widevine

sowie eine Datei mit Informationen über gefährliche Websites (Safe Browsing). Die Website-Überprüfung beim Surfen fand anschließend offline statt. Eingeschaltet waren jedoch die Suchvorschläge, wodurch Eingaben in die Adresszeile an Google übertragen wurden. Im privaten Modus war aber Ruhe.

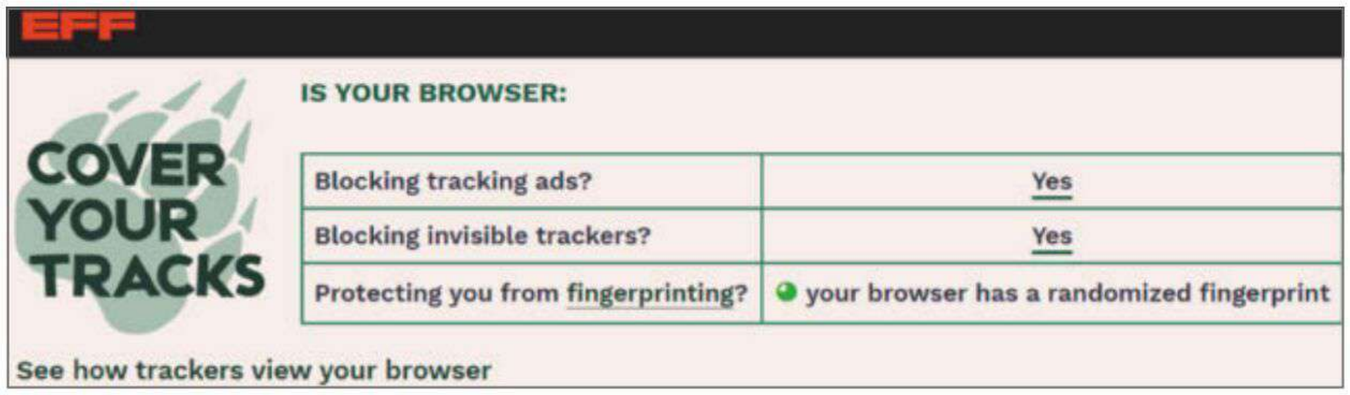
Standardmäßig war auch die Übertragung von Diagnosedaten aktiv, was wir auch im Firefox-Traffic nachvollziehen konnten. Der Umfang der an incoming.telemetry.mozilla.org übermittelten Daten war überschaubar: Bei uns interessierte sich Mozilla etwa dafür, ob bestimmte Funktionen wie die Bild-in-Bild-Funktion für Videos aktiv sind. Firefox hat die Übertragung der Diagnosedaten nachvollziehbar beendet, nachdem wir die „Datenerhebung durch Firefox“ in den Einstellungen deaktiviert hatten.

Mozilla nutzt die „Neuer Tab“-Seite auch für moderate Werbeeinblendungen. Während unseres Tests waren etwa gesponserte Links zu Amazon und eBay sichtbar, die sich jedoch über den jeweiligen Menüknopf leicht entfernen ließen. Darunter empfiehlt Firefox aktuelle Nachrichten, die direkt von dem zu Mozilla gehörenden Dienst Pocket geladen wurden.

Microsoft Edge

Microsoft verteilt seinen von Grund auf überarbeiteten Edge-Browser seit gut einem Jahr per Systemupdate an die Windows-Nutzer. Der auf Chromium aufbauende Browser erinnert optisch an Google Chrome, allerdings hat Microsoft ihn auf seine eigenen Dienste zugeschnitten und Funktionen nachgerüstet. Dazu zählt auch ein Trackingblocker mit drei Stufen, von denen standardmäßig die mittlere eingestellt ist („Ausgewogen“).

Richtig effektiv arbeitete er bei uns erst auf im „strengen“ Modus. Mit dieser Einstellung filtert Edge auch viel Reklame weg. Edge-Nutzer haben den Trackingschutz bitter nötig, denn die ersten Begegnungen mit Third-Party-Trackern machen sie schon beim Browserstart: Edge öffnet in jedem neuen Tab eine überladene Startseite, die jedes Mal von MSN.com nachgeladen wird. Sie nutzt externe Tracker wie Taboola, Zemanta und ScorecardResearch – da wundert es nicht, dass Microsoft sogar ein Cookie-Consent-Banner davorgeschaltet hat. Ironischerweise waren es dann auch Taboola und Zemanta, welche die Liste der am häufigsten blockierten Tracker während unserer Analyse anführten. Wir konnten keinen Weg finden, diese Seite über die Browser-Einstellungen loszuwerden. Abhilfe schaffen unabhängige Erweiterungen wie „Custom New Tab“ oder „Tabliss“.



Im Tracking-Test der EFF konnte nur Brave das Fingerprinting effektiv verhindern.

Statt der Google-Suche setzt Edge auf Bing.com, wodurch Eingaben in die Adressleiste Zeichen für Zeichen dorthin übertragen wurden. Auch die Safe-Browsing-Funktion SmartScreen läuft über Microsoft-Server. Sie schickt die URLs aufgerufener Websites zur Überprüfung an Microsoft. Das passierte während unserer Analyse auch im „InPrivate“ getauften Inkognito-Modus von Edge – anhand der übertragenen Daten bekommt Microsoft also selbst im privaten Browsermodus mit, welche Adressen geöffnet wurden. Die Übertragung von „erforderlichen Diagnosedaten“ konnten wir bei Edge nicht abschalten.

Brave

Der Browser Brave basiert ebenfalls auf Chromium. Die Kommunikation mit Google beschränkt sich auf den Abruf intern genutzter Erweiterungen. Weitere Add-ons zog Brave direkt bei seinem Hersteller, etwa ein Update für den Adblocker. Von dort stammten auch die Daten fürs Safe Browsing.

Regelmäßig kommunizierte der Browser mit p3a.brave.com, um Diagnosedaten abzuliefern. Brave hat das Verfahren öffentlich dokumentiert (siehe ct.de/wxn5). Demnach lassen sich die Daten nicht einzelnen Nutzern zuordnen und enthalten keine Informationen über den Browserverlauf. Nachdem wir die „vollständig privaten Produktanalysen“ deaktiviert hatten, hörte der Spuk auf. Eingaben in die Adressleiste hinterließen keine Datenspuren, da die automatischen Suchvorschläge abgeschaltet sind. Statt Google war die Privacy-freundliche Suchmaschine DuckDuckGo voreingestellt. Beim Surfen blieben die angesteuerte URLs privat, da Brave keine Echtzeitüberprüfung für seine Safe-Browsing-Funktion unternahm.

Der integrierte Adblocker arbeitet bereits mit den Voreinstellungen äußerst effektiv. Brave nutzt neben den Blocklisten EasyList und EasyPrivacy auch die

Liste von uBlock Origin, über den Menüeintrag „Brave Werbeblocker“ lassen sich zudem weitere Listen auswählen und eigene hinzufügen. Wer die blockierte Werbung vermisst, kann mit „Brave Rewards“ zurückhaltende Reklame einschalten, die der Browser als Benachrichtigungen anzeigt. Den aus der Werbung geschöpften Gewinn teilt Brave mit seinen Nutzern und Website-Betreibern durch Kryptogeld, das ins in den Browser integrierte Krypto-Wallet fließt. War die Funktion aktiv, hat Brave gelegentlich einen vierstelligen Hash an seinen Hersteller geschickt, um zu überprüfen, ob eine Site am Rewards-Programm teilnimmt. Weitere Kryptomünzen kann man über die reichlich überladene „Neuer Tab“-Seite verdienen, die von Zeit zu Zeit Werbung als Hintergrundbild anzeigt. Anders als etwa bei Edge konnten wir die Seite jedoch einfach über die Einstellungen deaktivieren.

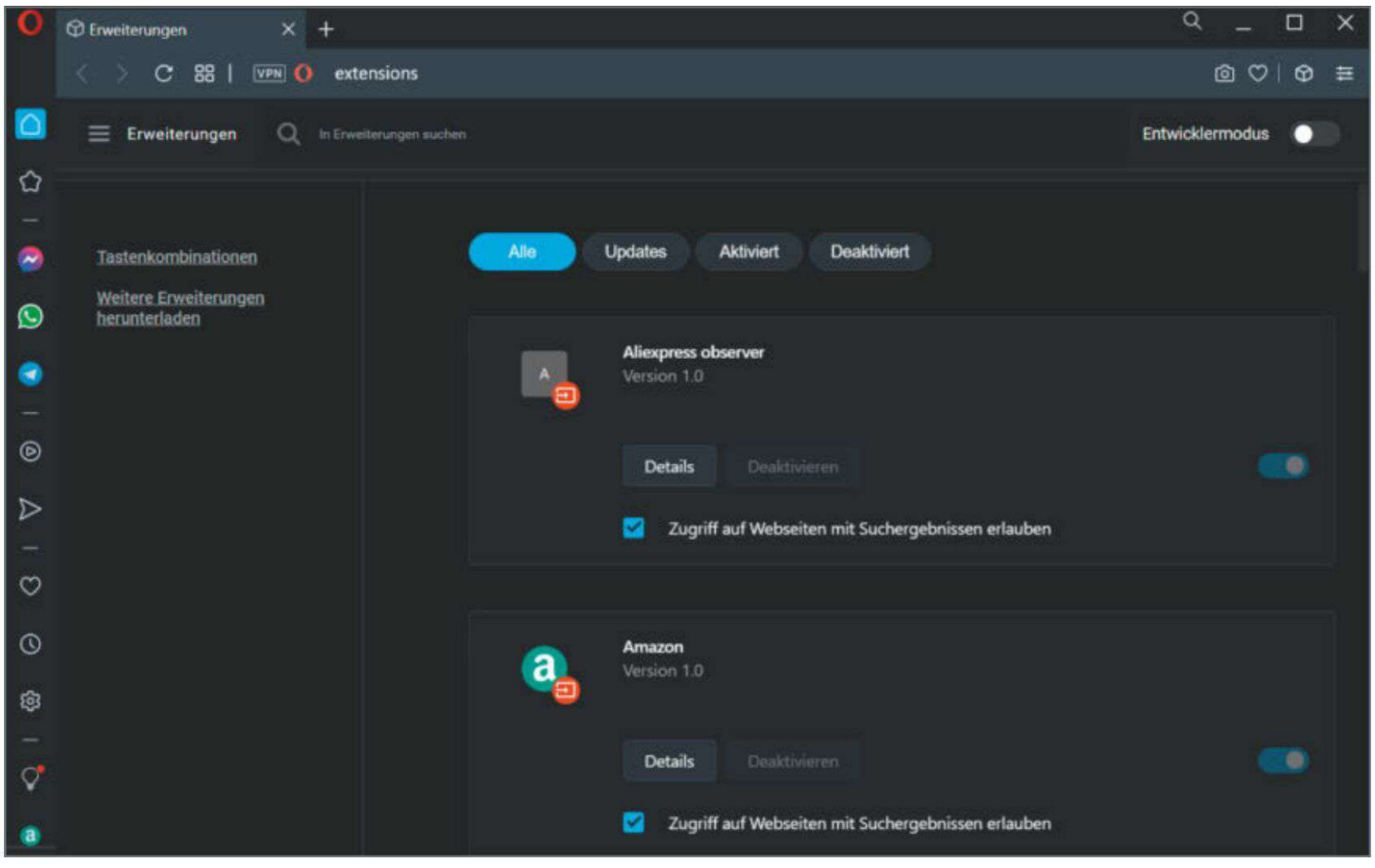
Als einziger Browser im Testfeld hat Brave einen integrierten Tor-Client, der auf Wunsch für private Browserfenster aktiviert wird. Brave ist zudem der einzige Browser, der bei den Trackingtests bereits im Auslieferungszustand sehr gut abschnitt und sogar Canvas-Fingerprinting verhindern konnte. Gegen besonders ausgefeilte Fingerprinting-Methoden wie FingerprintJS (siehe ct.de/wxn5) kommt jedoch auch Brave derzeit nicht an.

Vivaldi

Schon beim ersten Start von Vivaldi entdeckten wir Anfragen an Google-Dienste wie YouTube sowie die Werbenetzwerke DoubleClick und Google Ads. Offenbar standen diese in direktem Zusammenhang mit der Herstellerseite, die der Browser in einem Hintergrund-Tab geöffnet hatte. Die Aktualität der Browser-Add-ons überprüfte Vivaldi bei Google. Nachgeladen wurde ein Add-on zur Einschätzung der Stärke von Passwörtern. Jeder Browserstart führte zudem zu einer Anfrage an update.googleapis.com.

Die Kommunikation mit dem Hersteller war indes überschaubar: Außer der Website zog sich Vivaldi dort etwa eine Liste mit Suchpartnern und mehrere Filterlisten wie EasyList, AdBlock Plus und DuckDuckGo Tracker Radar. Ansonsten verhielt sich Vivaldi mit Ausnahme eines Verbindungstests leise.

Als Standardsuchmaschine war Bing eingestellt. Die Startseite war gespickt mit großen bunten Werbekacheln, die zum Onlineshopping einladen sollen. Diese wird man über den Minus-Button schnell los.



Unerwünschte Dreingaben: Opera bringt mehrere Shopping-Erweiterungen wie den Amazon Assistant mit.

Startseite und „Neue Tab“-Seite konnten wir leicht über die Einstellungen nach unseren Wünschen ändern. Suchvorschläge in der Adressleiste waren standardmäßig inaktiv und die geöffneten URLs wurden nicht an einen Safe-Browsing-Server gemeldet – die Bedrohungsinfos hatte sich der Browser im Vorfeld bei Google abgeholt.

Werbe- und Trackingschutz sind bei Vivaldi standardmäßig ausgeschaltet, lassen sich jedoch während der Ersteinrichtung aktivieren, die sich als Website im ersten Tab öffnet. Der Trackingblocker überzeugte uns anfangs nicht, er schnitt jedoch zu einem späteren Zeitpunkt gut ab – mutmaßlich nach einem Update der Filterliste (DuckDuckGo). Die Privatsphären-Einstellungen sind übersichtlich gegliedert. Dort werden etwa die Filterlisten für Tracking- und Werbeblocker konfiguriert. Zwei Listen gegen Cookie-Banner stehen zur Wahl, sind jedoch nicht besonders effektiv. Zudem lassen sich hier die mitgelieferten Google-Add-ons abschalten.

Uns fiel auf, dass beim Adblocker eine Ausnahmeliste für Werbepartner von Vivaldi ausgewählt war, die wir jedoch problemlos in den Privacy-Einstellungen unter „Tracker- und Werbeblocker / Quellen verwalten“ abwählen konnten. Die Verschlüsselung von DNS-Anfragen (DoH) konnten wir über die Vivaldi-Einstellungen nicht aktivieren, über die Adresse chrome://settings/security erreicht man jedoch die gewohnten Chromium-Einstellungen mit DNS-over-HTTPS-Option („Sicheres DNS“).

Opera

Das Geschäftsmodell von Opera erschließt sich schon beim ersten Start: Die Startseite ist mit Links zu diversen Onlineshops verknüpft. Besonders weitreichend ist die Kooperation mit Amazon: Standardmäßig ist die Erweiterung „Amazon Assistant“ vorinstalliert. Aktiviert man sie, überwacht sie das Surfverhalten, um etwa beim Googeln konkrete Verkaufsangebote einzublenden, die sich auf die Suchbegriffe beziehen.

Das ist nicht der einzige Einkaufshelfer: Bei der Analyse des Datenverkehrs stellten wir fest, dass Opera heimlich eine Erweiterung namens „Rich Hint Agent“ nachgeladen hatte, die offenbar in Verbindung mit dem Cashback-Dienst Dify steht. Die Erweiterung tauchte nicht in der Liste der installierten Add-ons auf und wurde erst sichtbar, nachdem wir den Browser mit dem Parameter `--show-component-extension-options` gestartet hatten. So entdeckten wir dann auch noch den „Aliexpress observer“, der anscheinend beim Einkaufen auf der chinesischen Handelsplattform aktiv wird.

Bei der Adresseingabe übertrug der Browser jedes Zeichen an Google, um die Suchvorschläge abzurufen. Für den Sicherheitscheck (Safe Browsing) meldete Opera zudem jede angesteuerte URL an sitecheck.opera.com. Die Safe-Browsing-Funktion war sogar bei der Nutzung der privaten Fenster aktiv, die ihrem Namen daher nicht gerecht werden.

Auf der Habenseite stehen ein integrierter Werbeblocker und Trackingschutz. Beides muss man allerdings erst einschalten. Der Opera-Werbeblocker vertraut standardmäßig auf die EasyList sowie NoCoin, die JavaScript-Cryptominer umfasst. Beliebige weitere Listen lassen sich ergänzen. Eine Besonderheit von Opera ist der eingebaute VPN-Dienst ohne Traffic-Limit, über den man seine externe IP-Adresse verschleiern kann. Im Test erreichten wir darüber flotte 100 MBit/s und mehr.

Apple Safari

Apple hat den macOS-Systembrowser mit einem Trackingschutz ausgestattet, der standardmäßig eingeschaltet ist. Viel zu konfigurieren gibt es nicht, in den Datenschutz-Einstellungen lässt sich das „websiteübergreifende Tracking“ lediglich aus- und wieder einschalten. Ferner kann man dort die „Datenschutzwahrende Messung der Werbewirksamkeit“ abschalten.

Dabei handelt es sich um einen von Apple erdachten Standard, um Klicks auf Werbeanzeigen datenschutzfreundlich zu erfassen, der jedoch von den Werbenetzen implementiert werden muss. Apple macht auch beim „Do Not Track“-Header sein eigenes Ding und unterstützt ihn nicht mehr. Ein Werbeblocker ist ebenfalls nicht an Bord. Die „Neuer Tab“-Seite ist auch bei Safari mit Werbelinks gespickt. Man kann sie leicht über die Favoriten entfernen.

Bei unserem Trackingtest schnitt Safari nur mittelgut ab, ungefähr vergleichbar mit der mittleren Anti-Tracking-Einstellung anderer Browser. Dieses Ergebnis ist jedoch nur bedingt aussagekräftig, da Safaris Trackingschutz laut Apple-Dokumentation dynamisch arbeitet (siehe ct.de/wxn5), was schwer messbar ist. Demnach werden Tracker lokal durch maschinelles Lernen klassifiziert und zudem zeitabhängig blockiert. Das bedeutet etwa, dass ein Third-Party-Cookie möglicherweise am ersten Tag noch funktioniert, aber am zweiten schon nicht mehr. So soll verhindert werden, dass zum Beispiel Single-Sign-on-Dienste gestört werden.

Browser im Privacy-Check

Name	Brave	Chrome	Edge	Firefox	Opera	Safari	Vivaldi
Version	1.25.68	91.0.4472.77	91.0.864.37	89.0	76.0.4017.154	14.1.1	3.8.2259.42
Engine	Blink	Blink	Blink	Gecko	Blink	WebKit	Blink
Plattform	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux (Beta)	Windows, macOS, Linux	Windows, macOS, Linux	macOS	Windows, macOS, Linux
Datenschutz							
blockt Tracker effektiv (Standard / maximal)	✓ / ✓	– / –	– / ✓	teilweise / ✓	– / ✓	teilweise / teilweise	– / ✓
blockt Fingerprinting effektiv	✓[1]	–	–	–	–	–	–
überträgt URL-Eingaben an (Standard / Inkognito)	– / –	Google / –	Microsoft / –	Google / –	Google / –	Google, Apple / –	– / –
überträgt aufgerufene URLs an (Standard / Inkognito)	– / –	– / –	Microsoft / Microsoft	– / –	Opera / Opera	– / –	– / –
Diagnosedaten aktiv / deaktivierbar	✓ / ✓	✓ / ✓	✓ / –	✓ / ✓	✓ / ✓	– / –	✓ / –
Privacy-Bewertung	⊕⊕	○	⊖	⊕	⊖	⊕	○

[1] außer FingerprintJS ⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht ✓ vorhanden – nicht vorhanden

Bei Safari ist Google als Suchmaschine voreingestellt und bei der Analyse des Datenverkehrs zeigte sich, dass der Browser erwartungsgemäß Eingaben in der Adresszeile dorthin überträgt. Eine Überraschung erwartete uns dennoch: Denn die Eingaben gingen zusätzlich an api-glb-euc1a.smoot.apple.com raus, also direkt an Apple. Apple blendet damit eigene Vorschläge ein, zum Beispiel Wortdefinitionen aus einem Lexikon. Wer möglichst privat surfen möchte, sollte in den Safari-Einstellungen unter „Suchen“ die Optionen „Suchmaschinenvorschläge“ und die „Safari-Vorschläge“ ausschalten. Dann kommuniziert Safari nur sehr sparsam aus eigenem Antrieb.

Fazit

Die Wahl des Browsers hat beträchtliche Auswirkungen auf die Privatsphäre, wie unser Privacy-Check gezeigt hat. Wer möglichst wenig Spuren hinterlassen möchte, sollte zu **Brave** greifen: Der Browser ist gut vorkonfiguriert und verhindert sogar das Canvas-Fingerprinting. Allerdings bringt er auch einige Funktionen wie ein Krypto-Wallet mit, die nicht jeder braucht. Direkt darauf folgt **Mozilla Firefox**, der einerseits mit einem guten Trackingschutz daherkommt und andererseits selbst nicht allzu viel in die Welt hinausposaunt.

Wer macOS nutzt, macht mit **Safari** wenig falsch, auch wenn der Trackingblocker mehr Einflussnahme erlauben könnte. Die doppelt gemoppelten Suchvorschläge sollte man jedoch besser deaktivieren. **Google Chrome** gibt sich recht neutral und hat Trackern wenig entgegenzusetzen, kommuniziert dafür aber auch nur in überschaubarem Umfang mit seinem Mutterschiff.

Vivaldi fiel vor allem durch unnötige Übertragungen an Google und Werbung auf. Ignoriert man die Einrichtungs-Website beim ersten Start, ist der Trackingschutz erst mal inaktiv, ansonsten arbeitet er aber mittlerweile zuverlässig. **Opera** ist mit Werbe-Addons gespickt und zu redselig: Durch die Kombination von Opera- und Google-Diensten bekommen gleich zwei Unternehmen das Surfverhalten mit. Der Microsoft-Browser **Edge** hat zwar einen guten Trackingschutz, liefert seine Nutzer jedoch über die nicht deaktivierbare „Neuer Tab“-Seite gleich selbst ans Messer. Zudem erfährt Microsoft viel über das Surfverhalten, selbst im Inkognito-Modus.

Gegen die ausgefeilten Tracking-Methoden von FingerprintJS waren übrigens alle Browser machtlos, was zeigt, dass es keinen absoluten Schutz vor Tracking gibt – solange man nicht an anderer Stelle Kompromisse eingeht.

Mehr aus Firefox herausholen

Dieser Artikel klärt nur die Datenschutzfrage, in der Titelstory von c’t 2/2021 [1] finden Sie einen ausführlichen Test der wichtigsten Browser, der auch Geschwindigkeit und Funktionsumfang berücksichtigt. Auf den folgenden Seiten zeigen wir Ihnen, wie Sie Firefox so einrichten, dass Sie einerseits wenig Datenspuren hinterlassen, aber andererseits noch sehr komfortabel surfen. (rei) c't

Literatur

[1] Jo Bager, **Der Über-Browser und die anderen**, Googles (un)heimliche Browser-Vorherrschaft, c’t 02/2021, S. 60

Testseiten, Hintergrundinfos

ct.de/wxn5



Bild: Andreas Martini

Surfen ohne Cookies, Tracking und Reklame

Man nehme Firefox, eine Handvoll Einstellungen und eine Prise Erweiterungen: Heraus kommt ein datenschutzfreundlicher Browser, der Ihre Nerven schont. Mit unserem Browser-Rezept surfen Sie deutlich entspannter – ganz ohne Cookie-Banner, Tracking und aufdringliche Reklame.

Von **Ronald Eikenberg**

Unerwünschte Dreingaben wie Tracking-Cookies und Werbung sind tägliche Begleiter, wenn man nur mal die News lesen oder online shoppen möchte. Doch das müssen Sie nicht hinnehmen: Mit unseren Empfehlungen konfigurieren Sie den Firefox-Browser so, dass er alle lästigen Elemente entfernt. Das schont Ihre Nerven und schützt Ihre Daten, denn hinter den Kulissen arbeitet ein effektiver Trackingschutz. Und die Zeiten, in denen Sie ein Cookie-Banner weggeklickt haben, sind auch vorbei.

Wir haben den von Haus aus datenschutzfreundlichen Firefox-Browser so eingerichtet, dass die Inhalte im Vordergrund stehen und unser Setup über

mehrere Monate im Alltag getestet. Das Experiment verlief erfolgreich und der Unterschied ist deutlich sichtbar: Wo beim Aufrufen einer Website bislang nur ein schmaler Schlitz vom eigentlichen Inhalt zu sehen war – den Rest hatten Cookie-Banner und Werbung unter sich aufgeteilt – wurde nach den Änderungen die gesamte Bildschirmfläche für die eigentlichen Inhalte genutzt. Außerdem hinterließen wir beim Surfen deutlich weniger Datenspuren.

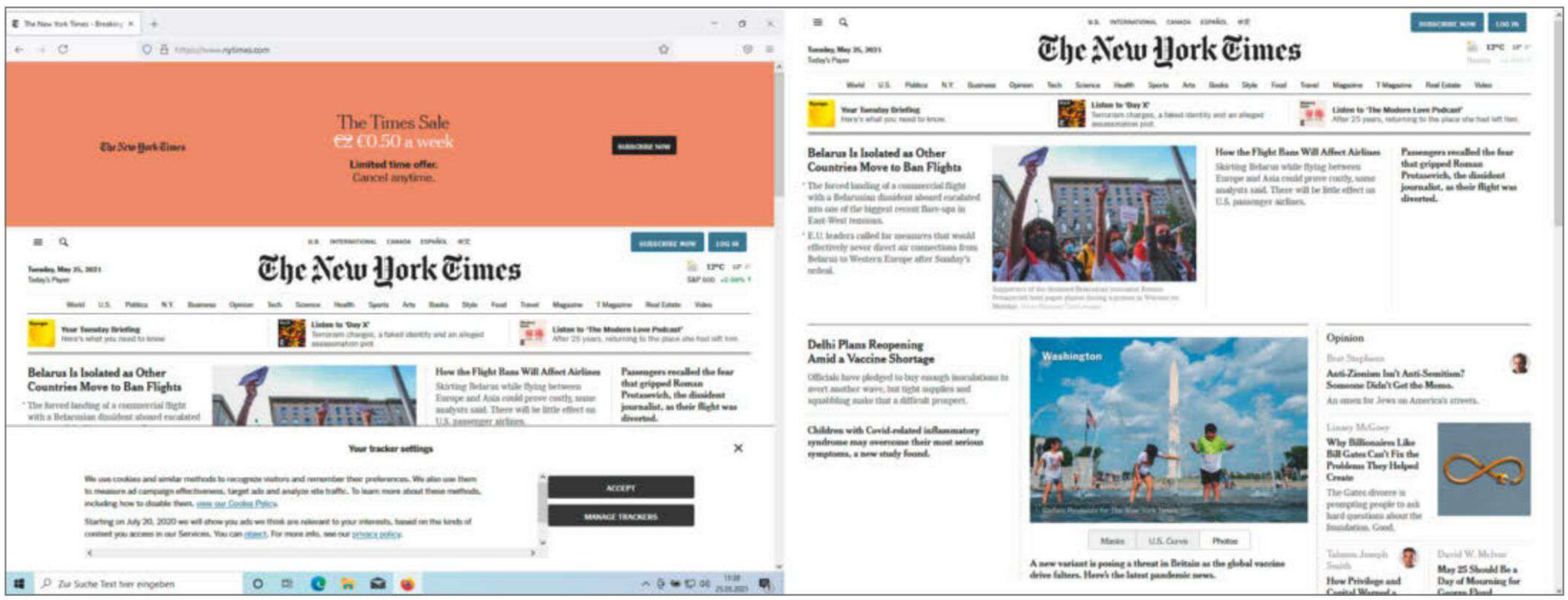
Unsere Beispielkonfiguration für PCs und Macs ist bestmöglich auf Komfort und Datenschutz ausgerichtet, was durchaus einen Kompromiss bedeutet: Denn viel Komfort bedeutet oft wenig Datenschutz und umgekehrt. Uns war wichtig, dass der Browser komfortabel bedienbar bleibt und Websites weitgehend wie gewohnt funktionieren, ohne dass ein Nachjustieren der Privacy-Schutzfunktionen nötig ist. Dennoch sollte ein effektiver Schutz vor dem Website-übergreifenden Tracking greifen.

Starten Sie am besten mit einer frischen Installation der aktuellen Firefox-Version. Wenn Sie den Mozilla-Browser bereits eingerichtet haben und unsere Empfehlungen erstmal risikolos testen möchten, können Sie hierfür einfach ein neues Profil anlegen: Öffnen Sie mit Firefox die interne Adresse `about:profiles` und klicken Sie auf „Neues Profil anlegen“. Geben Sie dem Profil einen beliebigen Namen, etwa „Ungestört surfen“ und klicken Sie danach, zurück in der Profilverwaltung, auf „Profil zusätzlich ausführen“, um eine neue Browserinstanz mit dem leeren Profil zu öffnen. Das neue Profil wird automatisch zum Standard und fortan mit Firefox gestartet. Um das rückgängig zu machen, klicken Sie in der Profilverwaltung beim alten Profil (etwa „default-release“) auf „Als Standardprofil festlegen“.

Strenger Tracking-Schutz

Zunächst gilt es, die Bordmittel von Firefox optimal einzurichten. Öffnen Sie die Einstellungen über den Menüknopf oben rechts (drei Linien) und wechseln Sie auf „Datenschutz & Sicherheit“. Stellen Sie den Trackingschutz unter „Verbesserter Schutz vor Aktivitätsverfolgung auf „Streng“ für die bestmögliche Privatsphäre. Seit Firefox 86 schalten Sie damit die „Total Cookie Protection“ ein, die quasi dafür sorgt, dass jede Website Ihre eigene Keksdose bekommt.

Angenommen, Facebook liefert Ihnen beim Besuch von Website A ein Cookie, weil dort ein Like-Button oder ein Facebook-Post eingebettet wurde. Anschließend surfen Sie auf Website B, die ebenfalls mit eingebetteten Facebook-Inhalten arbeitet. Normalerweise würde Ihre Browser jetzt das Cookie von Website A an Facebook senden, weil es zur gleichen externen Domain passt und Facebook könnte nachvollziehen, dass Sie zunächst auf Website A und dann auf



Vorher und nachher: Wenn Sie alle Empfehlungen befolgen, zeigt Ihnen Firefox schon beim ersten Besuch einer Website deutlich mehr vom eigentlichen Inhalt.

Website B waren. Die neue Schutzfunktion verhindert dies effektiv, weil sich Firefox merkt, dass das Cookie beim Besuch von Website A ausgeliefert wurde. Beim Besuch von Website B steht es nicht zur Verfügung.

So wird verhindert, dass Sie beim Surfen auf Schritt und Tritt durch Third-Party-Cookies verfolgt werden können. Firefox warnt davor, dass „einige Websites nicht korrekt Inhalte anzeigen oder funktionieren“, wenn Sie den Trackingschutz voll aufdrehen. Im Alltag konnten wir jedoch nur geringe Komforteinbußen feststellen. So wurden von extern eingebettete Social-Media-Inhalte auf Websites nicht mehr automatisch geladen. Stattdessen fanden wir jedoch stets einen Link vor, über den wir den jeweiligen Beitrag direkt aufrufen konnten.

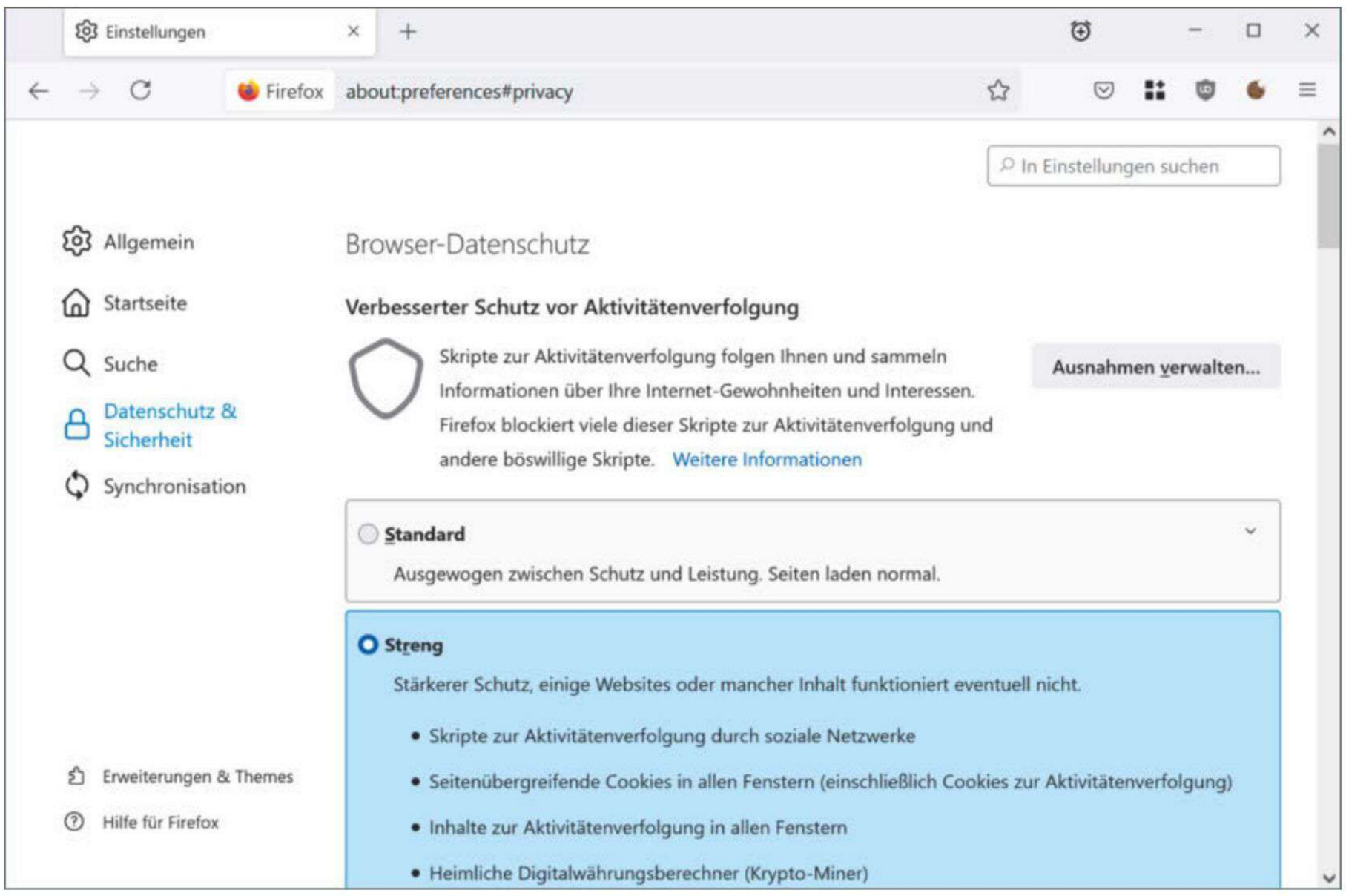
Mozilla nennt diesen Schutz auch „Dynamic Partitioning“ (siehe ct.de/wpts), er betrifft neben den Cookies etwa auch das localStorage-API. Hinter den Kulissen speichert Firefox den Ursprung der Cookies in seiner Cookie-Datenbank (cookies.sqlite) durch einen sogenannten Partition-Key, zum Beispiel `partitionKey=(https,heise.de)`.

Falls Ihnen der erweiterte Trackingschutz einmal in die Quere kommt, klicken Sie einfach auf das Schutzschild-Symbol links in der Adressleiste und deaktivieren Sie den Schalter „Verbesserter Schutz vor Aktivitätsverfolgung ist für diese Website AKTIVIERT“, um die problematische Website auf die Ausnahmeliste zu setzen. Dort erfahren Sie auch, was Firefox auf der aktuellen Website blockiert hat.

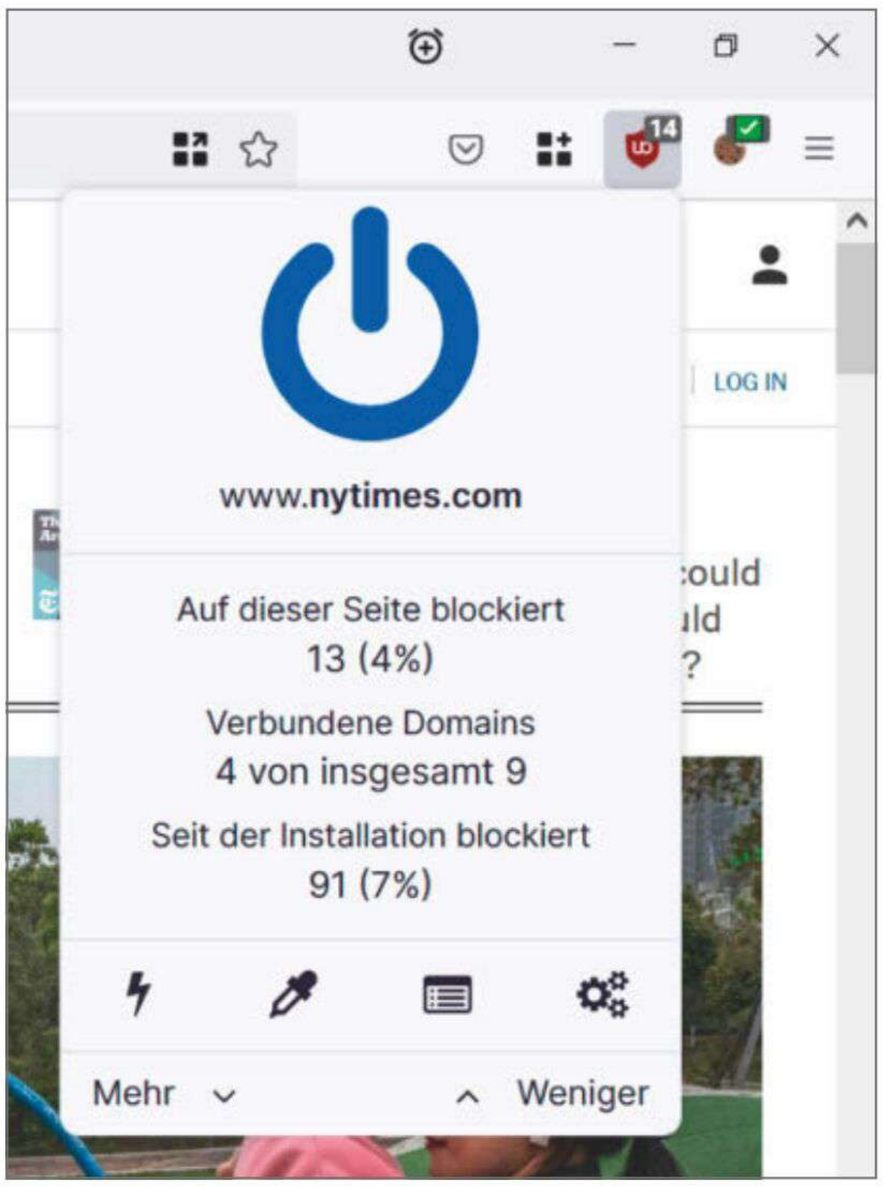
Alternativ können Sie den Tracking-Blocker auch im Standardmodus betreiben – das ist immer noch deutlich besser als nichts, denn Firefox blockiert auch in diesem Modus bekannte Tracking-Cookies und -Skripte. Zudem ist in beiden Betriebsmodi das sogenannte „Network Partitioning“ aktiv, welches Supercookies eliminieren soll, die Browserfunktionen als Tracking-Helfer zweckentfremden. Aktivieren Sie unterhalb der Tracking-Blocker-Einstellung noch die „Do No Track“-Header, um Websites mitzuteilen, dass Sie nicht getrackt werden möchten.

Diagnose und Sicherheit

Wenn Sie mögen, können Sie unter „Datenerhebung durch Firefox und deren Verwendung“ alle Häkchen entfernen, damit Firefox keine Diagnosedaten über Ihre Installation an Mozilla sendet. Sie sollten auch



Viel hilft viel: Auf der Stufe „Streng“ fängt der Trackingschutz von Firefox jede Menge weg.



Wer ungestört surfen will, sollte einen unabhängigen Content-Blocker wie uBlock Origin nachrüsten.

in Erwägung ziehen, unter „Suche“ die Suchvorschläge in der Adressleiste zu deaktivieren. Diese Funktion sorgt dafür, dass Firefox beim Tippen in der Adresszeile jedes Zeichen an Google sendet, um passende Suchvorschläge abzurufen. Wenn Ihnen Google ohnehin suspekt ist, sollten Sie hier auch gleich eine andere Standardsuchmaschine einstellen, zum Beispiel die Privacy-freundliche Alternative DuckDuckGo.

Noch kurz ein Wort zum Thema Sicherheit: Der wichtigste Schutz heißt Aktualität! Halten Sie Ihren Browser stets auf dem aktuellen Versionsstand, da mit fast jedem Update auch Sicherheitslücken geschlossen werden. Stellen Sie sicher, dass in den Einstellungen unter „Allgemein / Firefox-Updates“ die Option „Firefox erlauben … Updates automatisch zu installieren (empfohlen)“ ausgewählt ist. Unter „Datenschutz & Sicherheit / Sicherheit“ sollte zudem der „Schutz vor betrügerischen Inhalten und gefährlicher Software“ aktiv sein sowie darunter die automatische Überprüfung von Zertifikaten mittels OCSP.

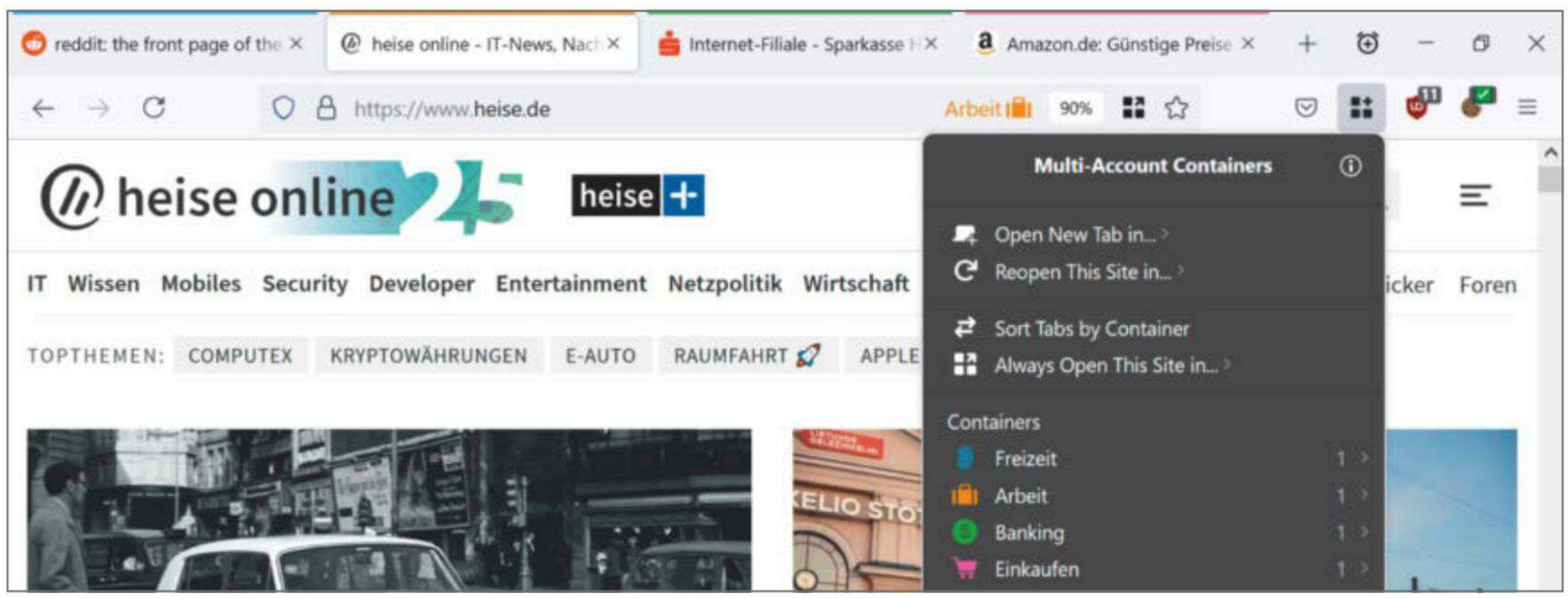
Um zu verhindern, dass Firefox Daten im Klartext in die weite Welt schickt, können Sie darunter den „Nur-HTTPS-Modus in allen Fenstern aktivieren“. Dann zeigt Firefox eine Warnung an, bevor eine unverschlüsselt übertragene HTTP-Website geöffnet wird. Davon gibt es noch ein paar, Sie werden den Warnhinweis also dann und wann zu Gesicht bekommen. In diesem Fall wissen Sie Bescheid, dass Sie auf der folgenden Website keine sensiblen Daten eintippen sollten. Sinnvoll ist auch, unter „Allgemein / Verbindungs-Einstellungen“ ein Häkchen bei „DNS über HTTPS aktivieren“ zu setzen, damit Firefox Ihre DNS-Anfragen verschlüsselt durchführt. Sie haben die Wahl zwischen Cloudflare und NextDNS, die beide an Mozillas Trusted-Recursive-Resolver-Programm teilnehmen. Damit verpflichten sie sich unter anderem, anfallende Daten über die Nutzung nach spätestens 24 Stunden zu löschen. Alternativ können Sie einen beliebigen anderen Anbieter einstellen, dem Sie vertrauen.

Bitte keine Werbung einwerfen

Damit haben Sie die wichtigsten Browsereinstellungen erledigt. Nach so viel Fleißarbeit hinter den Kulissen soll es jetzt um den Komfort gehen. Mit geringem Aufwand können Sie Ihren Surfalltag sicht- und spürbar verbessern, indem Sie all die nervigen Dinge auf Websites eliminieren.

Zunächst einmal sollten Sie Ihren Browser mit einem unabhängigen Content-Blocker ausstatten, der Websites auch – aber nicht nur – von Werbung befreit. Bewährt hat sich uBlock Origin von Raymond Hill, das Sie über das Add-on-Verzeichnis (siehe ct.de/wpts) mit zwei Klicks an den Start bringen. Den Content-Blocker gibt es übrigens nicht nur für Firefox, sondern für alle wichtigen Desktop-Browser. Er ist stimmig vorkonfiguriert, sodass Sie normalerweise nichts weiter einstellen müssen. Da sich auf den voreingestellten Filterlisten auch etliche bösartige URLs befinden, sorgt uBlock nicht nur für Komfort, sondern auch für Sicherheit.

Über den roten Schutzschild in der Symbolleiste erfahren Sie, wie viele Elemente uBlock auf der aktuellen Website blockiert hat. Klicken Sie ihn an und zweimal auf „Mehr“, erfahren Sie auch, um welche Elemente es geht. Von den rot markierten Domains hat die Erweiterung sämtliche Elemente blockiert, von den orange markierten nur manche. Wenn eine Website nicht wie gewohnt funktioniert, klicken Sie einfach auf den großen blauen Ausschalter im uBlock-Menü und auf den Aktualisieren-Knopf, der rechts daneben erscheint. Der Content-Blocker ist dann für diese Website deaktiviert. Dies ist insbesondere dann nötig, wenn eine Website den Blocker erkennt und die Auslieferung der Inhalte verweigert.



Container schotten Websites voneinander ab und schützen so effektiv vor Tracking.

Falls Ihnen die vordefinierten Filter mal nicht weit genug gehen, klicken Sie im uBlock-Menü auf das Blitzsymbol, um den Element-Entfernungsmodus zu starten. Klicken Sie anschließend auf das störende Element der Website, um es sofort zu entfernen. Mit der Pipette neben dem Blitz können Sie den neuen Filter nach der Auswahl des Elements zunächst ausprobieren und feinjustieren, ehe Sie ihn dauerhaft übernehmen. Ihre neuen Filter, die genutzten Filterlisten und viele weitere Einstellungen finden Sie in den uBlock-Optionen, die Sie über das Zahnrad-Symbol erreichen.

Keksdiät

Sie surfen jetzt zumeist werbefrei, ein weiterer Störfaktor ist jedoch noch übrig: Auf fast allen Websites werden Sie von Cookie-Consent-Bannern begrüßt, um die sich uBlock Origin erstmal nicht kümmert. Es gibt zwar kompatible Filterlisten dagegen, jedoch haben diese in unserem Praxistest nur mäßig funktioniert, da es häufig nicht ausreicht, das Banner zu blockieren – es muss bestätigt werden. Greifen Sie daher am besten gleich zu der Browser-Erweiterung „I don't care about cookies“, die es für alle relevanten Desktop-Browser gibt (siehe ct.de/wpts).

Die Erweiterung tut, was nötig ist, um das Cookie-Banner loszuwerden. In Härtefällen klickt sie auf den „Akzeptieren“-Knopf, was Sie daran erkennen, dass das Banner zunächst angezeigt wird und im nächsten Augenblick wieder verschwindet, ohne dass Sie aktiv werden müssen. Behalten Sie bei der Konfiguration Ihres Browsers im Hinterkopf, dass Sie „I don't care about cookies“ zwar vor den lästigen Cookie-Dialogen bewahrt, nicht aber vor den Cookies selbst. Sie sollten also zusätzlich den Trackingschutz wie oben beschrieben scharf schalten.

Es ist sinnvoll, uBlock Origin und „I don't care about cookies“ auch für den privaten Browsermodus zu freizugeben, denn standardmäßig sind Add-ons dort nicht aktiv. Öffnen Sie hierzu die Add-ons-Verwaltung über das Firefox-Menü oder `about:addons`. Klicken Sie bei der jeweiligen Erweiterung rechts auf den Knopf mit den drei Punkten und „Verwalten“. Unter „Details / In privaten Fenstern ausführen“ wählen Sie anschließend „Erlauben“ aus. Bei den nun im Artikel folgenden Erweiterungen ist dies hingegen nicht nötig.

Datenschutz-Container

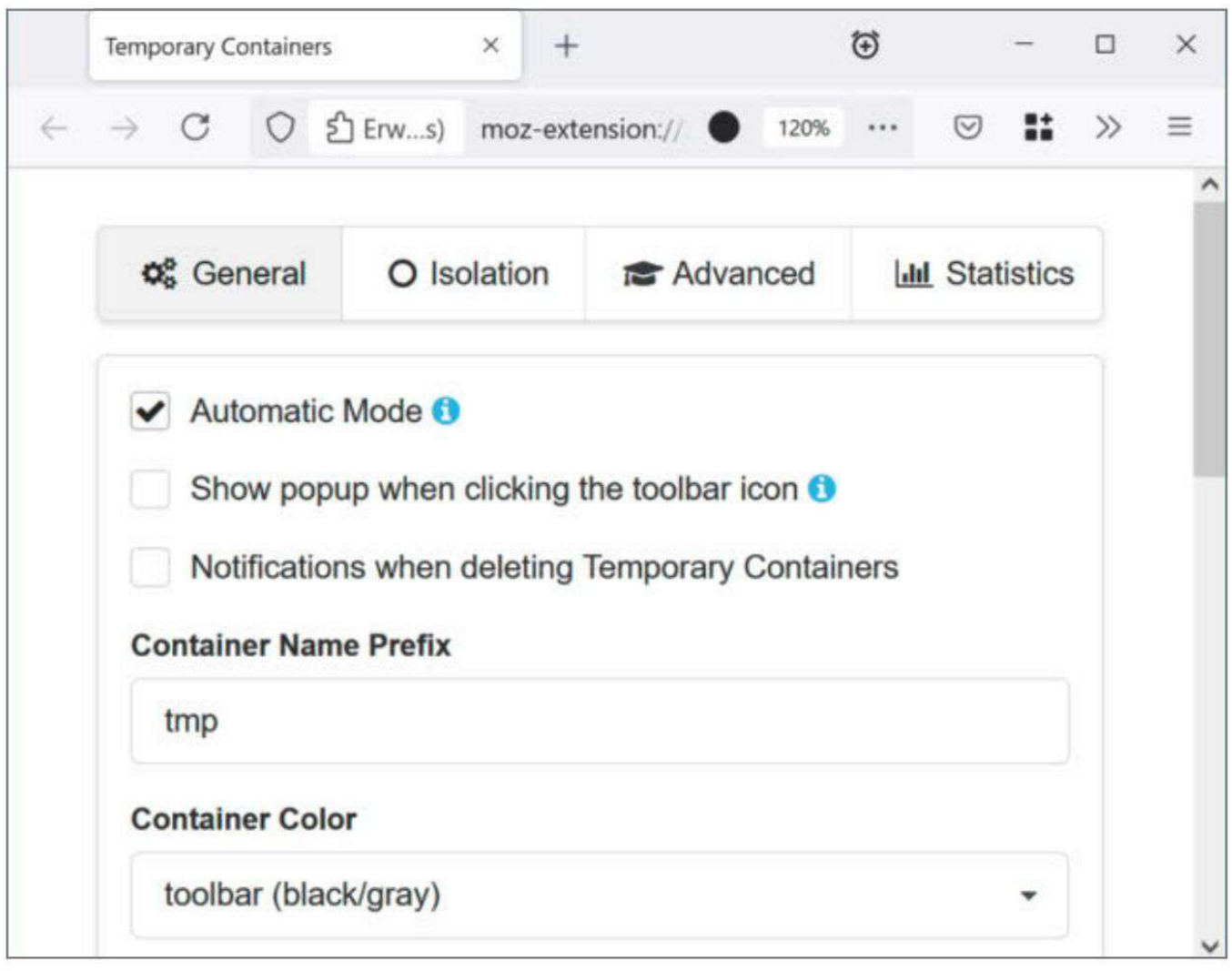
Mit Cookies ist es kompliziert: Es geht nicht mit, aber auch nicht ohne. Die oben vorgestellte Total Cookie Protection von Firefox versucht bereits, das Problem für Sie zu lösen, indem sie praktisch für jede Website einen eigenen Cookie-Speicher anlegt. Das funktioniert gut, allerdings haben Sie keine Kontrolle darüber. Mit Containern könnten Sie das Konzept weiter ausbauen.

Das Prinzip ist schnell erklärt: Sie öffnen Websites in Containern, die von voneinander abgeschottet sind. Die Websites in Container A können nicht auf die Ressourcen von Container B zugreifen. Das ist fast so, als würden Sie mehrere Browser parallel nutzen – nur viel komfortabler, da die Container als farblich markierte Tabs im gleichen Browserfenster laufen. So verhindern Sie nicht nur Website-übergreifendes Tracking, Sie können zum Beispiel auch Berufliches

und Privates sauber voneinander trennen oder sich auf einer Website mit zwei Accounts gleichzeitig einloggen, indem Sie die Site in zwei Containern öffnen.

Wir haben das Konzept über Monate im Alltag ausprobiert und zu schätzen gelernt. Wenn Sie Ihre wichtigsten Websites einmalig mit passenden Containern verknüpfen, etwa Arbeit, Freizeit, Banking und Shopping, haben Sie damit anschließend keine Arbeit mehr: Die Websites werden fortan automatisch in den gewünschten Containern geöffnet. Wenn Sie den erweiterten Trackingschutz aktiviert haben, arbeitet dieser parallel dazu weiter. Gehen Sie am besten noch einen Schritt weiter und lassen Sie alle anderen Websites in temporären Tabs öffnen, um zu verhindern, dass selten oder einmalig angesteuerte Sites Cookies auf Ihrem Rechner hinterlassen – auch das ganz automatisch.

Die wichtigste Container-Erweiterung heißt „Firefox Multi-Account Containers“ und stammt direkt von Mozilla (siehe ct.de/wpts). Nach der Installation finden Sie einen neuen Knopf mit drei Kästchen und einem Pluszeichen oben rechts in der Symbolleiste des Browsers. Nach der Begrüßung können Sie darüber (oder über Strg+Punkt) die Container-Einstellungen öffnen. Es sind bereits vier Container für Freizeit, Arbeit, Banking und Einkaufen eingerichtet, die Sie direkt benutzen können. Beliebige weitere legen Sie über „Manage Containers“ an.



Die Firefox-Erweiterung „Temporary Containers“ öffnet Websites auf Wunsch in Wegwerf-Containern. So können Sie sorglos alle Cookies akzeptieren, denn nach dem Schließen des Tabs werden sie ohnehin gelöscht.

Klicken Sie im Menü der Erweiterung auf einen Container, öffnet sie einen neuen Browser-Tab. Sie erkennen den aktuell genutzten Container an der farbigen Linie am oberen Rand des Tab-Titels und dem Containernamen in der Adresszeile. Richtig komfortabel wird das Leben mit den Containern erst, wenn Sie die Erweiterung anweisen, bestimmte Websites automatisch im passenden Container zu öffnen. Steuern Sie hierzu eine Website an und klicken Sie anschließend auf den Knopf der Erweiterung und „Always Open This Site in…“. Danach wählen Sie den Container aus, in dem die Site künftig geöffnet werden soll. Beim nächsten Aufruf der Website werden Sie noch gefragt, ob sie wirklich im zugeordneten Container geöffnet werden soll. Damit diese Rückfrage in Zukunft ausbleibt, klicken Sie auf „Remember my decision for this site“ und „Open in [Name] Container“. Fahren Sie so mit allen Websites fort, die Sie regelmäßig ansteuern.

Wenn Sie in einem Container-Tab einen Link anklicken oder eine beliebige Adresse eintippen, wird auch die folgende Website in dem Container geöffnet. Das ist nicht immer erwünscht: Wenn Sie etwa den Container „Arbeit“ ausschließlich mit Intranet-Websites verknüpft haben, möchten Sie wahrscheinlich nicht, dass auch Links auf externe Websites darin laufen. Das verhindern Sie, indem Sie unter „Manage Containers“ auf einen Container klicken und dort die Option „Limit to Designated Sites“ aktivieren. Wenn es keinen passenden Container gibt, werden externe Sites dann wie gewohnt containerlos geöffnet. Wichtig ist, dass Sie den Browserverlauf aktiviert haben, da die Erweiterung ansonsten nicht funktioniert.

Cookies im Wegwerf-Container

Grundsätzlich sollten Sie sich die Frage stellen, ob Websites, denen Sie keine Container zugeordnet haben, überhaupt dauerhaft Cookies speichern sollen – denn dort profitiert man nur selten davon. Während unseres Experiments haben wir Gefallen an einer weiteren Container-Erweiterung gefunden, nämlich „Temporary Containers“ von stoically (siehe ct.de/wpts).

Sie öffnet auf Wunsch sämtliche Websites, die nicht mit einem Container verknüpft sind, in kurz-

lebigen Wegwerf-Tabs. Schließt man einen solchen Tab, killt die Erweiterung den dazugehörigen Container samt Cookies nach fünfzehn Minuten. Das ist fast so, als würden Sie die ganze Zeit im privaten Modus surfen, mit Ausnahme der Sites, die Sie mit Containern verknüpft haben. Nach der Installation öffnet Temporary Containers seine Einstellungen. Hier sollten Sie ganz oben den „Automatic Mode“ aktivieren, damit Sie sich um nichts kümmern müssen. Alternativ können Sie über das Wecker-Symbol jederzeit selbst Tabs in temporären Containern öffnen. Die kurzlebigen Container erkennen Sie am Namen, der stets mit „tmp“ beginnt.

Mehr Schutz

Die Liste möglicher Privacy-Gefährdungen ist fast beliebig lang. Wer sich gegen alle Eventualitäten absichern will, erreicht schnell einen Punkt, an dem das Surfen sehr mühsam ist, weil Websites nicht mehr wie gewohnt funktionieren und die Schutzfunktionen häufig nachjustiert werden müssen. Zu den sinnvolleren Maßnahmen gehört ein Schutz gegen das Canvas-Fingerprinting (siehe Seite 66). Bei dieser Trackingart werden Zeichenfunktionen des Browsers zur Identifizierung missbraucht.

Abhilfe verschafft die Firefox-Erweiterung Canvas-Blocker, welche die Identifizierung durch zufällige Daten erschwert. Im Alltag stand Sie uns jedoch häufig im Weg, weil wichtige Elemente auf Websites fehlten und Browsertabs unvermittelt abstürzten. Recht beliebt sind Skript-Blocker wie NoScript oder uMatrix: Damit kann man unter anderem feingranuliert festlegen, welche Skripte auf welchen Websites ausgeführt werden dürfen. Das funktioniert gut, macht aber auch Arbeit: Die Filterregeln müssen nicht selten nachjustiert werden, ehe eine Website funktioniert. Diese und weitere zusätzliche Schutzmaßnahmen haben wir in unserem Firefox-Sicherheitskompendium zusammengestellt (siehe ct.de/wpts).

Nach so viel Datenschutz soll es noch mal um den Komfort gehen: Wenn Sie mit einem Notebook oder einem kleineren Monitor arbeiten, dann zählt jedes Pixel. Für unseren Versuch nutzten wir oft ein kompaktes Notebook mit gerade einmal 13,5-Zoll Bildschirmdiagonale. Um Komfort und Effizienz unserer Firefox-Installation abzurunden, haben wir hier noch die Erweiterung „Auto Fullscreen“ von tazeat (siehe ct.de/wpts) nachgerüstet. Der Name ist Programm: Nach der Installation läuft Firefox dauerhaft im Vollbildmodus, wodurch die Websites die gesamte Bildschirmfläche einnehmen. Die Bedienelemente des Browsers erscheinen sofort, wenn man mit dem Mauszeiger den oberen Bildschirmrand berührt und verschwinden wieder, wenn sie nicht länger gebraucht werden.

Zweigleisig surfen

Mit unserer beispielhaften Firefox-Konfiguration surfen Sie nicht nur ungestört ohne Cookie-Banner und Werbung, sondern auch weitgehend ohne Tracking. Passen Sie unseren Vorschlag gern nach Ihren eigenen Vorstellungen an. Falls Sie ihn erstmal in Ruhe ausprobieren möchten, installieren Sie Firefox und die Erweiterungen einfach parallel zu Ihrem bisherigen Browser und schauen Sie, ob unsere Empfehlungen für Sie passen. Ein zweiter Browser ist auch für Fälle nützlich, in denen eine Webseite aufgrund der angezogenen Trackingbremsen nicht wie gewohnt funktioniert.

Falls Sie bereits hauptsächlich Firefox nutzen, dann werden Sie sich schnell zurecht finden. In diesem Fall probieren Sie unsere Vorschläge am besten mit einem zweiten Profil aus, das Sie wie eingangs beschrieben anlegen können. Möchten Sie das neue Profil nur dann und wann nutzen, legen Sie einfach eine weitere Verknüpfung zur firefox.exe an, die den Browser automatisch mit dem gewünschten Profil öffnet. Das Verknüpfungsziel kann unter Windows wie folgt lauten: `"C:\Program Files\Mozilla Firefox\firefox.exe" -p "Profilname"`. Starten Sie Firefox wie gewohnt, um das eingestellte Standardprofil zu nutzen. Wenn Sie die neue Verknüpfung doppelklicken, öffnet sich der Browser hingegen direkt mit dem neuen Profil. So können Sie von Fall zu Fall entscheiden, welche Konfiguration Sie nutzen möchten.

Abschließend noch ein Hinweis, auch in eigener Sache: Insbesondere der Einsatz eines Content-Blockers wie uBlock Origin ist ein zweischneidiges Schwert. Sie entfernen damit nicht nur invasive Werbung, die Ihnen häufig auf Grundlage Ihrer persönlichen Interessen ausgeliefert wird. Sie schneiden den Websites auch eine wichtige Einnahmequelle ab. Statten Sie Ihren Lieblingssites also ruhig mal ohne Content-Blocker einen Besuch ab und setzen Sie eine Site auf die Ausnahmeliste, wenn Sie die Werbung nicht stört. Viele Website-Betreiber können Sie zudem für eine Handvoll Euro im Jahr durch ein Abo oder Spenden unterstützen. Manche Websites bieten auch ein Pur-Abo an, mit dem Sie Tracking und Werbung für einen kleinen Betrag weitgehend loswerden. (rei) c't

Firefox-Erweiterungen

ct.de/wpts

c't iX Mac&i heise Developer heise Security



ALLES AUF ANFANG

Neustart der IT-Weiterbildung

Kennst du schon die neue interaktive Lernplattform für IT-Professionals?

Bei uns findest du das Wissen zu den angesagten IT-Themen – von Experten für Professionals.

Jetzt testen! Hier geht's zu den ersten Gratis-Videos:

heise Academy

heise-Academy.de | @heise_Academy | #heiseAcademy



Bild: Andreas Martini

Die Zukunft des Tracking

Browserhersteller, Datenschutzadvokaten, Online-Werbeunternehmen und viele weitere Interessengruppen der Web-Welt diskutieren derzeit, wie Third-Party-Cookies ersetzt werden können. Dabei stehen auch wesentlich invasivere Verfahren zur Diskussion, als es Third-Party-Cookies jemals waren.

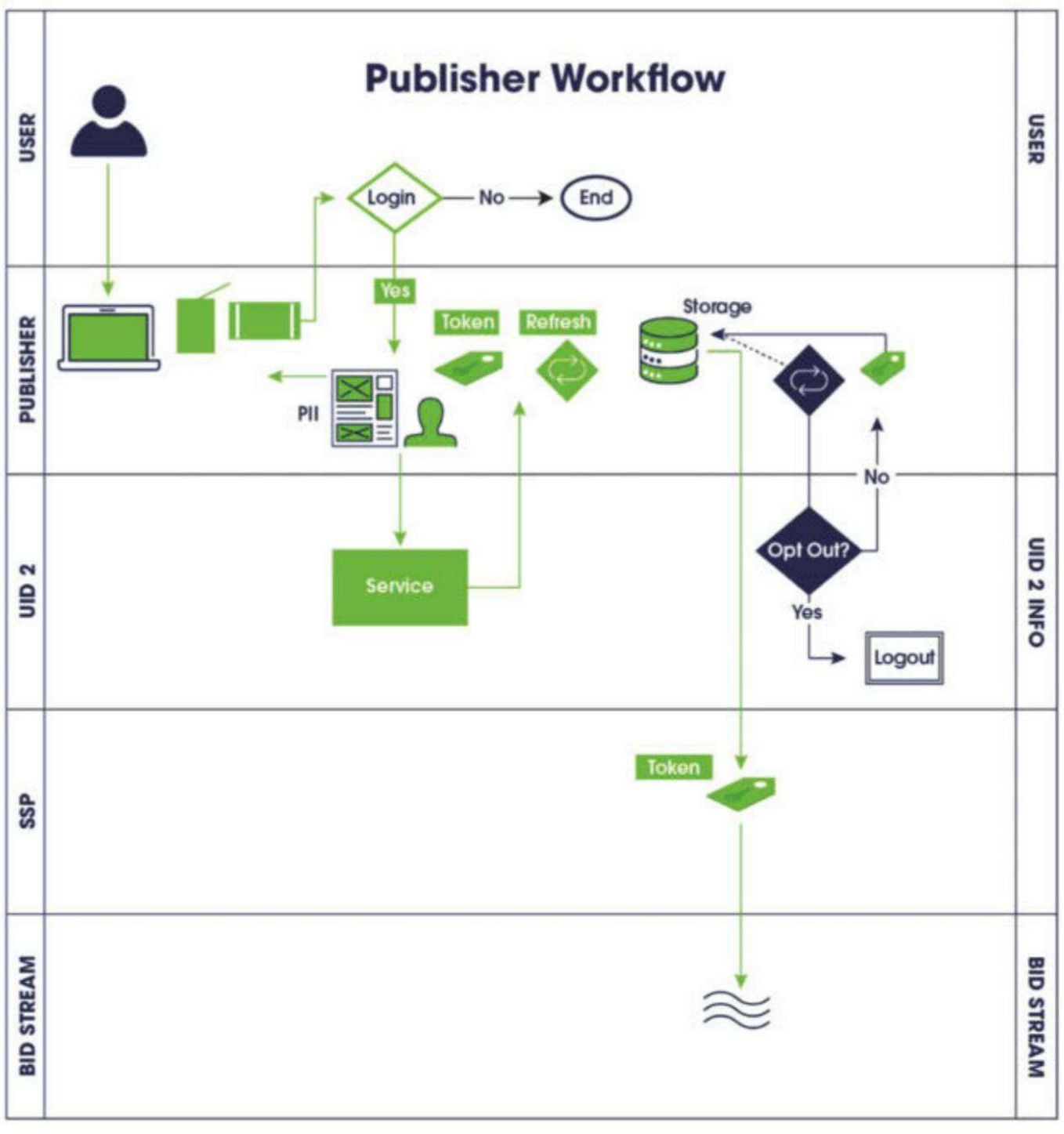
Von **Jo Bager**

Safari schmeißt Third-Party-Cookies nach 24 Stunden weg; Firefox sperrt Cookies in Website-spezifische Container ein; Google wird sich vom Tracking mit Third-Party-Cookies verabschieden – das bevorstehende Ende der Cookies erschüttert die Online-Werbebranche, weil sie die Axt an eine wichtige Erlösquelle anlegt: Ein immer größerer Anteil der Online-Werbung wird als sogenanntes Programmatic Advertising vermarktet, das dem Surfer zielgenau auf ihn abgestimmte Werbung präsentiert. Dies setzt aber möglichst akkurate Nutzerprofile voraus. Um Profile anlegen zu können, müssen die Werbetreibenden den Surfer bei seinen Streifzügen im Netz wiedererkennen, wofür sie Third-Party-Cookies nutzen.

Ein für alle Seiten akzeptabler Nachfolger für Third-Party-Cookies ist noch nicht gefunden. So gut wie jede Interessengruppe hat unterschiedliche Vorstellungen, wie Tracking in Zukunft funktionieren soll, seien es Browserhersteller, Adtech-Unternehmen, Standardisierungsgremien, Werbevermarkter, Datenschützer oder die Politik: eine sehr unüberschaubare Melange sich widersprechender Interessen.

Wie über Kreuz die Vorstellungen der verschiedenen Gruppen liegen, lässt sich gut am prominentesten Vorschlag festmachen: Googles FLoC (Federated Learning of Cohorts). Dabei wertet der Browser aus, welche Sites der Nutzer besucht, und weist ihn daraufhin einer Werbe-Kohorte von mehreren Tausend Nutzern zu.

Bild: github.com/UnifiedID2/uid2docs



Unified ID verwendet Token, die auf personenbeziehbare Informationen (PII) aufsetzen, zum Beispiel E-Mail-Adressen oder Telefonnummern.

Das soll keine Rückschlüsse auf den einzelnen Nutzer zulassen, aber dennoch zielgruppengenaue Werbung ermöglichen – grundsätzlich eine deutliche Verbesserung beim Datenschutz im Vergleich zu Cookies. Google testet das neue Verfahren bereits bei einem kleinen Nutzerkreis, allerdings nicht im Geltungsbereich der DSGVO.

Facebook hat sich kürzlich in einem Hintergrundgespräch positiv zu FLoC geäußert und will den Vorschlag offenbar unterstützen. Viele andere Unternehmen und Interessenvertreter lehnen FLoC dagegen ab. Die Browserhersteller Mozilla, Microsoft, Apple, Vivaldi und Brave wollen FLoC in ihren Browsern nicht umsetzen, ihnen geht der Datenschutz nicht weit genug. Das sagt auch die Bürgerrechtsorganisation Electronic Frontier Foundation. Sie befürchtet, dass sich auch bei FLoC einzelne Nutzer identifizieren lassen.

Kein vollwertiger Ersatz

In der Online-Marketing- und Adtech-Branche herrscht eine große Unsicherheit, weil durch einen Umstieg auf FLoC ganze Branchenzweige wegfallen könnten – zum Beispiel diejenigen Anbieter, die beim Programmatic Advertising dem Nutzer passende Werbung zuordnen.

Viele Werbeunternehmen sehen es zudem kritisch, dass der Werberiese Google mit FLoC in seinem Browser Chrome auch die technische Ausgestaltung der Werbeauslieferung kontrollieren würde. Das hat die britische Aufsichtsbehörde Competition and Markets Authority (CMA) auf den Plan gerufen, die die Neuerungen in Chrome untersucht.

Darüber hinaus gibt es Kritik aus der Branche, weil sich mit FLoC nicht alle Anwendungsszenarien abdecken lassen, für die bisher Cookies zum Einsatz kamen. Es ist zum Beispiel unklar, wie sich mit FLoC Provisionen für Affiliate-Werbung zuordnen oder Retargeting verwirklichen lassen sollen. Letzteres ist die Werbeform, die einen im Netz verfolgt: Hat man sich einmal für Drucker interessiert, bekommt man per Retargeting tage- oder wochenlang Druckerwerbung angezeigt.

Bei beiden Verfahren geht es ja letztendlich darum, einen einzelnen Nutzer über einen längeren Zeitraum wiederzuerkennen, um ihm personalisierte Werbung zu präsentieren beziehungsweise einem Affiliate-Werbepartner eine Provision zukommen zu lassen. Auch setzen einige Lösungen gegen sogenanntes Ad Fraud, also den „Abrechnungsbetrug“ zum Beispiel mit automatischen Klicks auf Anzeigen, auf Cookies.

Es verwundert daher nicht, dass es diverse Alternativvorschläge zu FLoC gibt, unter anderem von Apple und Microsoft. Von Google selbst stammt noch ein weiterer Vorschlag namens Fledge. Wie Branchendienste berichten, soll auch Amazon an einer Alternative zu FLoC arbeiten.

Kommt der „First-Party“-Datenabfluss?

Bei Unternehmen und Publishern stehen Alternativen hoch im Kurs, die unter dem Oberbegriff „First Party Data“ zusammengefasst werden. Das ist ein Euphemismus: Die First Parties, also zum Beispiel die Websites, die ein Surfer besucht, sollen die Daten ihrer Besucher festhalten – und sie an einen zentralen Server übertragen.

Es wird also wie bei den Third-Party-Cookies eine oder mehrere zentrale Stellen geben, die Nutzerdaten Site-übergreifend einsammeln und speichern. Statt eines Third-Party-Cookies, das den einzelnen Surfer wiedererkennbar macht, kommt stattdessen ein anderer Identifier zum Einsatz, den alle teilnehmenden Websites benutzen.

Konkret lässt sich die Funktionsweise einer solchen First-Party-Strategie am besten am Beispiel von Unified ID fassen (UID). Diese Lösung wurde ursprünglich von der Werbeplattform The Trade Desk entwickelt. Mittlerweile hat es seine Spezifikationen in Version 2.0 (UID2) als Open Source auf GitHub veröffentlicht und die Kontrolle an eine Arbeitsgruppe des International Advertising Bureau (IAB) übergeben. Der Wirtschaftsverband IAB sorgt für die Standardisierungen in der Werbebranche. Unter seiner Federführung soll aus Unified ID ein Industriestandard entstehen. The Trade Desk konnte schon Dutzende Partner von Unified ID überzeugen.

Im einzelnen läuft ein typischer Anwendungsfall so ab wie in der Grafik auf S. 87. Damit die First-Party-Site den Anwender (wieder-)erkennen kann, muss er dort eingeloggt sein, zum Beispiel mit seiner E-Mail-Adresse oder seiner Mobilfunknummer. Der Entwurf für den Standard spricht hier Personally Identifiable Information (PII).

Der Website-Betreiber sendet die PII an einen UI Operator, der dazu ein Token zurückliefert, das den Besucher eindeutig identifiziert. Dieses Token speichert der Website-Betreiber in der Folge im Browser des Nutzers oder in einer App als First-Party-Cookie. Es lässt sich dann wie ein Third-Party-Cookie verwenden, um dem Nutzer wiederzuerkennen und ihm zielgerichtet Werbung zukommen zu lassen.

Third-Party-Cookies sind mit einem einzelnen Browser assoziiert. UID2s dagegen, warnt die EFF, „sind mit Personen verbunden, nicht mit Geräten. Das bedeutet, dass ein Werbetreibender, der UID2 von einer Website sammelt, diese mit den UID2s verknüpfen kann, die er über Apps, verbundene Fernsehgeräte und verbundene Fahrzeuge sammelt, die derselben Person gehören.“ Es gebe zudem noch eine Reihe offener Fragen zu UID2, zum Beispiel, wer eigentlich die UID-Dienste betreibt und welche Pflichten den Teilnehmern in Bezug auf die Nutzerdaten auferlegt werden.

Werbeunternehmen trommeln derzeit mit Verve für Unified ID und ähnliche First-Party-Rezepte und versuchen, sie Publishern und anderen Website-Betreibern schmackhaft zu machen. Eher im Stillen dürften sie wohl auch vermehrt andere Trackingverfahren ausbauen, etwa das Browser-Fingerprinting.

Immerhin gibt es stellenweise Gegenbewegungen zur immer größeren Datengier der Online-Werber. Einige Medien haben erkannt, dass nicht jeder Surfer getrackt werden will und bieten sogenannte Pur-Abos an. Für ein paar Euro im Monat erhält man Zugriff auf die Inhalte ohne eingebundenes Tracking und mit sehr viel weniger oder komplett ohne Werbung.

Ein weiterer kleiner Hoffnungsschimmer am Horizont: Einige Medien experimentieren mit Werbeformen, die ohne externe Daten auskommen, die New York Times etwa. Aber solche Vorhaben sind eher die Ausnahme als die Regel. Es ist fraglich, ob sich so etwas auf breiter Basis durchsetzen kann. Kleinere Publisher werden sich kaum eine Datenabteilung, wie sie für die Werbeaussteuerung notwendig ist, leisten können wie die New York Times.

Fazit

FLoC, First Party, Fingerprinting: Es ist noch nicht abzusehen, welche Technik an Stelle der Cookies treten werden – möglicherweise alle parallel. FLoC ist dabei am unkritischsten. Es schützt den Nutzer besser als bisher und es wird für den Nutzer sicherlich Wege geben, die Zuordnung zu Kohorten ganz abzuschalten.

First-Party-Data-Lösungen laufen aus Nutzersicht auf eine Verschlechterung hinaus. Es bleibt abzuwarten, ob technische Mittel alleine helfen werden, sie zu blockieren. Es ist auf jeden Fall eine gute Wahl, den Browser auch heute bereits hochzurüsten, um die eigenen Daten so gut wie möglich zu schützen, indem man zum Beispiel Third-Party-Tracking so gut es geht blockiert. (jo) c't

Weitere Dokumentationen

ct.de/wcff



heise Academy

Egal, ob Newcomer oder Profi: Meistern Sie Ihren Cloud-Betrieb mit unserem Angebot aus Workshops und Webinaren.

Unser Angebot

Cloud Fast Track:
Der schnelle Weg in die Cloud

7. September

WORKSHOP

Jira in der Cloud

21. September

WEBINAR

Sichere Cloud-nutzung

22. – 23. September

WORKSHOP

Requirements-Management
mit Jira & Confluence

28. September

WEBINAR

Cloud Plattformen im Vergleich:
AWS, Azure, Google & Alibaba

6. – 8. Oktober

WORKSHOP

Mehr Informationen: heise-academy.de/cloud

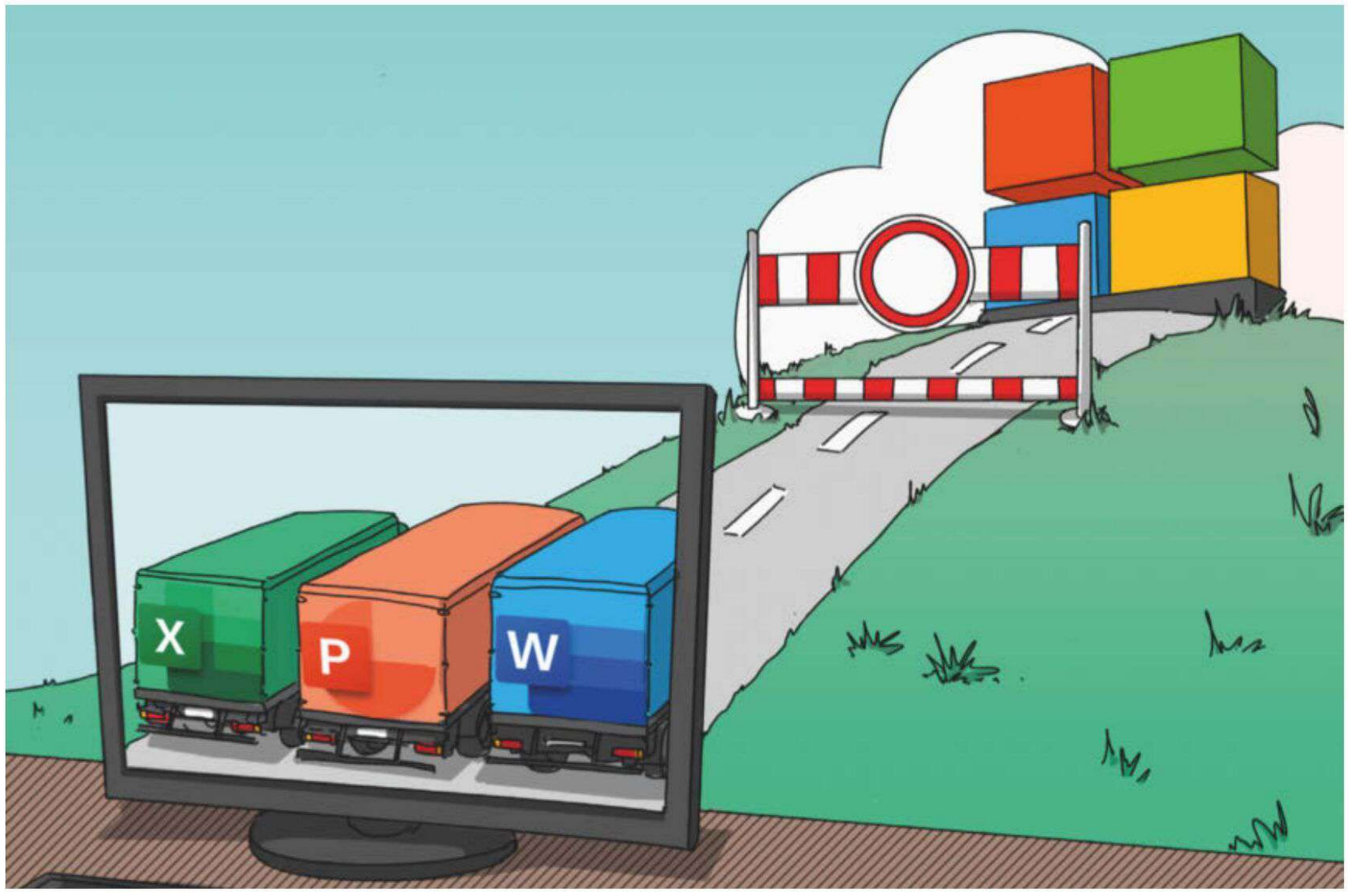


Bild: Thorsten Hübner

Microsoft Office ohne Cloud

Wer die Inhalte seiner Office-Dokumente von Microsofts Servern fernhalten will, muss nicht nur auf das Speichern in der Cloud verzichten, sondern auch auf einige andere Funktionen. Die lassen sich pauschal abschalten.

Von **Stefan Wischner**

Microsoft Office 365, dessen Programmpaket aus Word, Excel, PowerPoint und Outlook inzwischen eigentlich „Microsoft 365 Apps for Business“ heißt, steht zu Recht im Ruf, gerne und ausgiebig mit dem Hersteller zu telefonieren und dabei allerlei Daten zu übermitteln. Das ist besonders bedenklich, wenn es sich nicht nur um anonyme Nutzungs- und Diagnosedaten, sondern um konkrete Inhalte von Word-, Excel- oder PowerPoint-Dateien handelt. Das kollidiert nicht nur mit dem Bedürfnis vieler Nutzer nach Privatsphäre, sondern auch oft mit Unternehmens-Datenschutzbestimmungen oder Arbeitsverträgen. Die Indiskretion von Office, wie wir das Programmpaket in diesem Beitrag

weiterhin nennen wollen, lässt sich aber wirkungsvoll eindämmen. Dazu passt man einige Einstellungen für das Speichern von Dateien an, außerdem schaltet man eine Reihe von Funktionen ab, die allzu freizügig mit Office-Inhalten umgehen. Die folgenden Anleitungen beziehen sich zwar vornehmlich auf die Office-Apps, die im Rahmen eines Microsoft-365-Abos installiert wurden, gelten grundsätzlich aber auch für Office 2019 als Einzel- oder Bestandteil einer Volumenlizenz. Dieser Version fehlen zwar einige der servergestützten Funktionen der aktuellen Office-Programme, aber nicht alle. Außerdem können auch sie Microsofts Cloudspeicher nutzen.

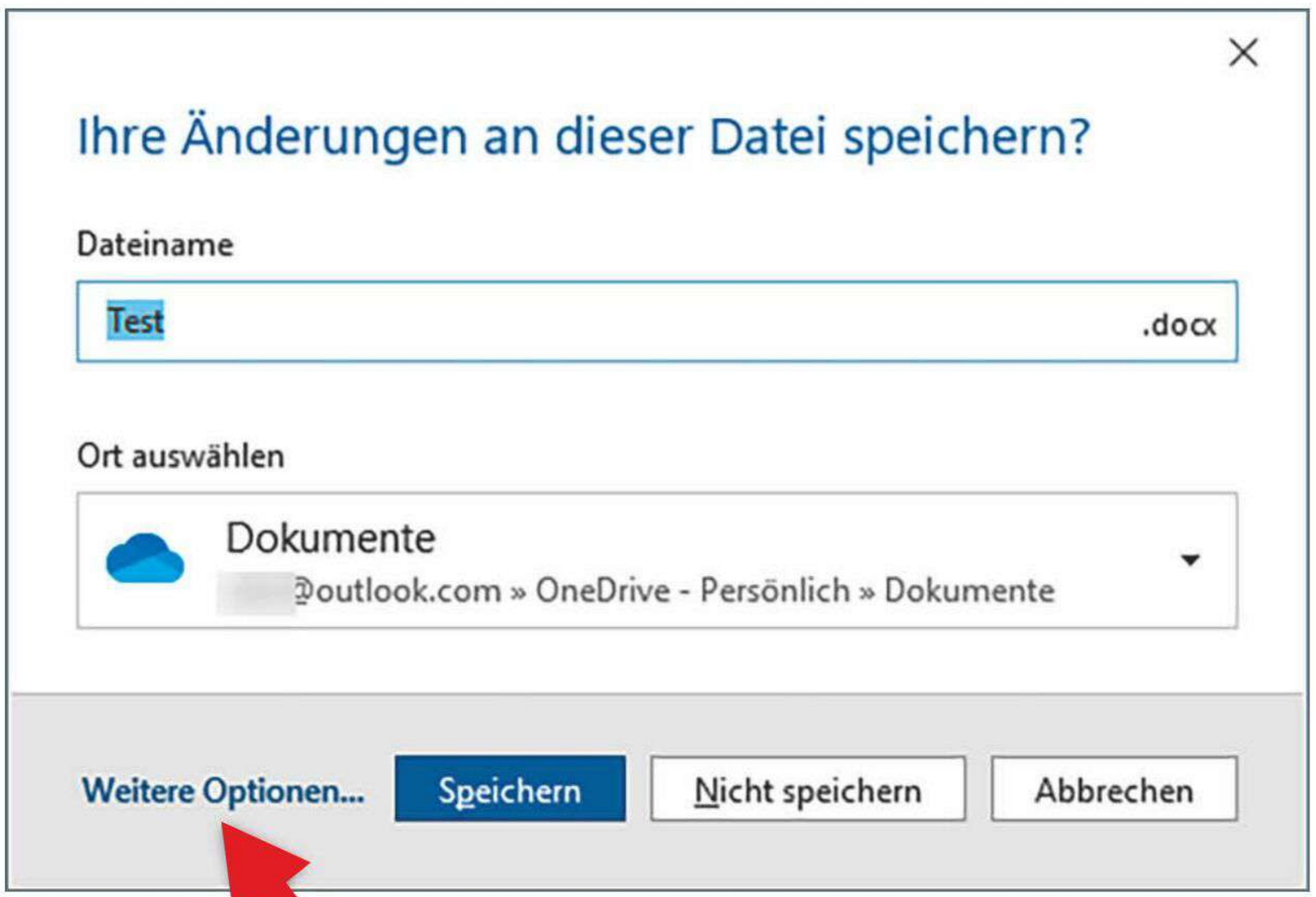
OneDrive-Boykott

Am einfachsten verhindern Sie, dass Office-Dateien in der Cloud gespeichert werden, indem Sie sich nicht auf Microsofts bequeme Voreinstellungen einlassen. Nicht zuletzt aufgrund dieser Defaults unterliegen viele Anwender dem Irrtum, bei Office 365 sei man dazu gezwungen, Dokumente, Tabellen und Präsentationen auf OneDrive oder OneDrive for Business zu speichern.

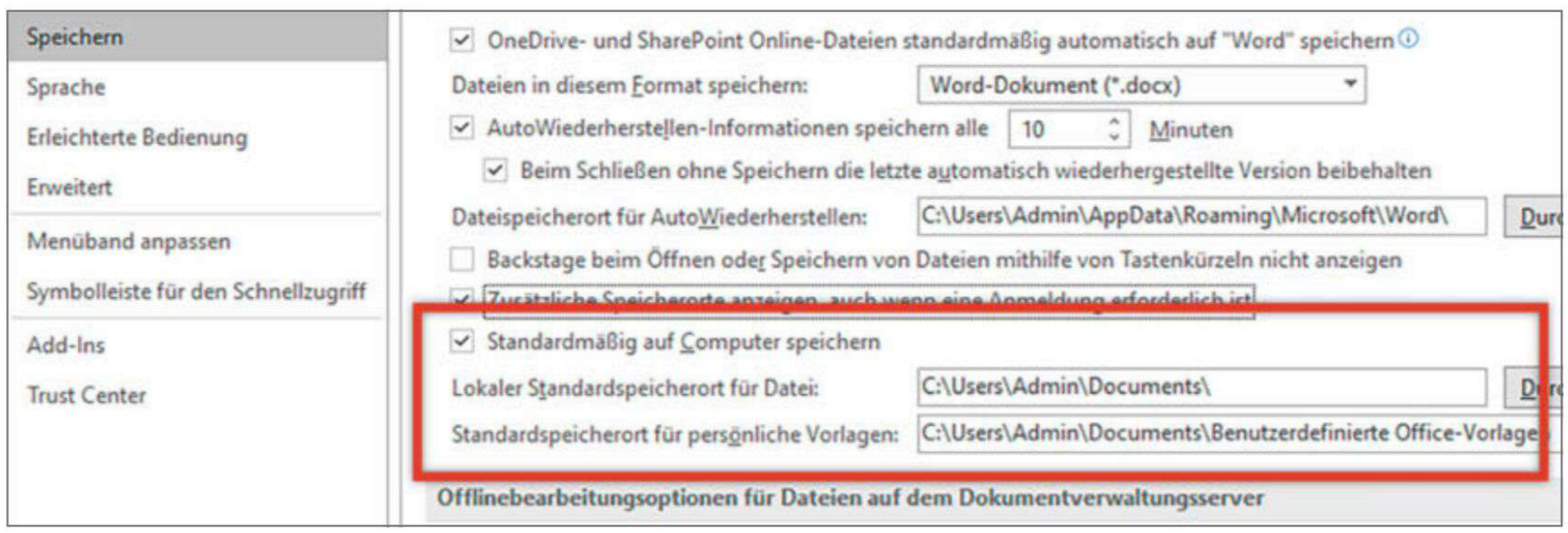
Tatsächlich lassen sich in Word, Excel und PowerPoint Dateien ohne Einschränkungen auf der eigenen Platte oder einem Server im Firmennetz ablegen, ganz so wie in älteren und Abo-losen Office-Versionen. Allerdings hat Microsoft seine Cloudspeicherdienste als Speicherziel inzwischen stark in den Vordergrund gerückt und damit den Blick auf die Optionen zum lokalen Speichern verstellt, etwa in der Backstage-Ansicht. Das ist die von Microsoft nie eingedeutschte Bezeichnung für das formatfüllende Fenster, das unter Windows nach einem Klick auf „Datei“ erscheint und auf macOS nach dem Aufruf bestimmter Dateioperationen aus dem „Datei“-Menü.

Um die gerade bearbeitete Datei ausschließlich auf dem eigenen Rechner oder in einem Netzwerkordner zu sichern, wählen Sie in der Backstage-Ansicht beim Speichern oder Anlegen einer Datei „Dieser PC“ oder „Durchsuchen“ aus dem Abschnitt „Andere Speicherorte“. Bei macOS heißt der Bereich „Auf meinem Mac“. Das öffnet den üblichen Dateiauswahldialog, in dem Sie ein beliebiges Speicherziel wählen können.

Bei manchen Operationen, zum Beispiel dem Sichern wiederhergestellter Dateien oder direkt per Tastenkürzel, wird unter Windows die Backstage-Übersicht übersprungen und es erscheint direkt ein Dateidialog. Bei neueren Office-Versionen ist das jedoch nicht mehr die gewohnte systemeigene Dateiauswahl, sondern ein spezielles Fenster, in dem



Der neue Dateiauswahldialog von Office gibt beim Speichern standardmäßig einen Cloudspeicherordner vor, ...



... was man mit einem Häkchen an passender Stelle im Optionsdialog eines Office-Programms ändern kann.

ein OneDrive-Ordner vorausgewählt ist. Ein unbedachter Klick, und schon liegt die Datei in der Cloud. Zum Systemdialog gelangen Sie, indem Sie auf „Weitere Optionen…“ klicken oder die „Ort auswählen“-Liste aufklappen und „weitere Speicherorte“ wählen. Beim Mac reicht ein Klick links unten auf „Auf meinem Mac“.

Dass die Standardauswahl im neuen Windows-Dateidialog einen Cloudspeicherort zeigt, lässt sich unter Windows leicht ändern: Setzen Sie in einem beliebigen Office-Programm unter „Datei/Optionen/Speichern“ das Häkchen bei „Standardmäßig auf Computer speichern“ und tragen Sie wenn gewünscht im Feld darunter noch einen lokalen Standardpfad ein, der im Speicherdialog zuerst angeboten werden soll. Die Einstellung gilt für alle Office-Programme gleichzeitig. Die Cloudspeicherziele lassen sich auch vollständig aus der Bedienoberfläche der Office-Programme verbannen. Dazu gleich mehr.

Wenn Sie sich entscheiden, Office-Dateien nicht auf OneDrive oder OneDrive for Business zu speichern, fällt das gemeinsame (zeitgleiche) Arbeiten an Dokumenten weg [1], außerdem müssen Sie auf das automatische Speichern [2] und die Versionsverwaltung verzichten.

Meiden sollten Sie auch die Browserversionen von Word, Excel und PowerPoint; diese speichern grundsätzlich in der Cloud und lassen lediglich den zusätzlichen Download von Kopien zu. Gleiches gilt für Dokumente, die Sie in Microsoft Teams anlegen oder dort hochladen. Die liegen nämlich immer auf OneDrive for Business.

Sie hätten auch die Möglichkeit, mit Tools wie Cryptomator, Boxcryptor, VeraCrypt oder passwortgeschützten ZIP-Dateien selbst für eine Ende-zu-Ende-Verschlüsselung zu sorgen, bevor Sie die Dateien auf OneDrive hochladen. Diese Methoden sind aber zumeist unkomfortabel und bringen diverse Funktionseinschränkungen und andere Risiken mit sich. Die zu behandeln wäre Gegenstand eines eigenen Artikels.

Verdeckte Übertragung

Dass Microsoft grundsätzlich die Inhalte von Officedokumenten auf seinem Cloudspeicher mitlesen kann, ist offensichtlich. Nicht jedoch, dass man Auszüge oder komplette Inhalte sogar dann an die Server schickt, wenn man bestimmte Funktionen von Word, Excel oder PowerPoint nutzt. Die verwenden serverbasierte Microsoft-Dienste wie die Azure Cognitive Services oder Microsoft Bing.

Microsoft fasst alle Funktionen, die Inhaltsdaten zu oder von Microsoft-Servern übertragen, unter dem wenig aussagekräftigen Begriff „verbundene Erfahrungen“ zusammen und unterteilt sie in zwei Gruppen:

- Funktionen, die Online-Inhalte herunterladen, dazu aber zumeist mindestens einen Suchbegriff senden. Dazu gehören beispielsweise Online-Bilder, Vorlagen und Piktogramme, Recherche, Cloud-Schriftarten und auch die Hilfefunktion.
- Funktionen, die Inhalte analysieren. Datenschutztechnisch sind das die kritischeren, da sie zum Beispiel Textauszüge oder auch ganze Dokumente an die Microsoft-Server senden, wo die Inhalte unverschlüsselt verarbeitet werden. Das sind zum Beispiel der Übersetzer, die Diktierfunktion, die Excel-Datentypen Aktien und Geographie, die Handschrifterkennung, „Ideen“ in Excel und bestimmte

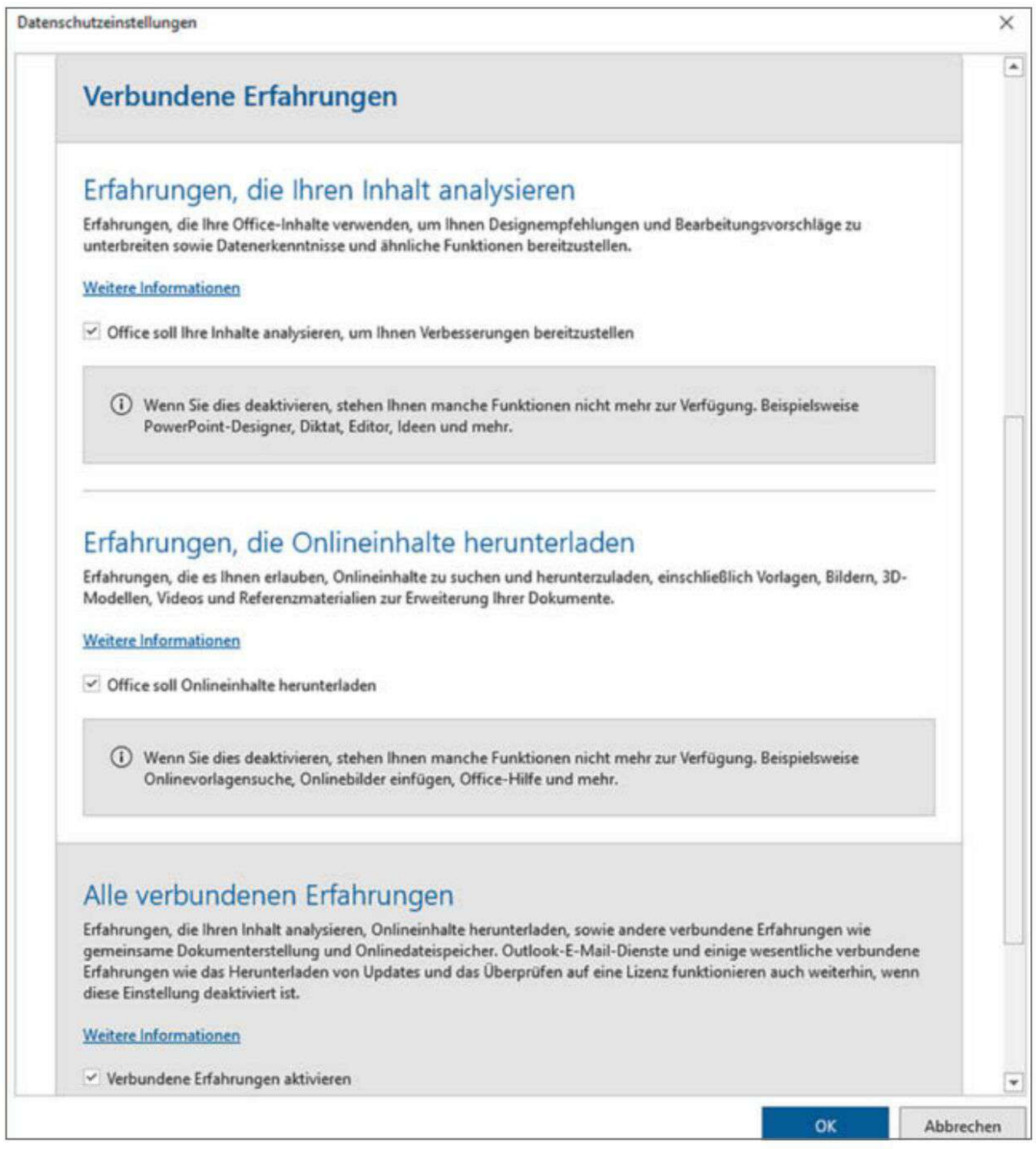
Editor-Funktionen von Word wie Ähnlichkeitsprüfung und Stilanalyse. Eine umfangreiche Aufstellung der betroffenen Funktionen bietet Microsoft unter ct.de/wr9p.

Wo die Daten verarbeitet werden

Die besagten Dienste laufen auf rund um den Globus verteilten Microsoft-Azure-Servern. An welchem Standort die Daten der Nutzer konkret verarbeitet werden, hängt zum einen von der Art des Microsoft-365-Plans (Abonnement) und zum anderen vom Sitz des Lizenzinhabers ab, genauer: von dessen Rechnungsadresse für das Abonnement. Seit 2018 garantiert Microsoft Nutzern einer Unternehmenslizenz, dass ihre Daten auf Servern in ihrem Land oder zumindest innerhalb einer Region (zum Beispiel der EU) gespeichert werden. Das betrifft jedoch nur ruhende Daten, also zum Beispiel auf OneDrive / SharePoint gespeicherte Dateien. Aus einer von Microsoft veröffentlichten Übersicht (siehe ct.de/wr9p) geht zwar hervor, dass die Cognitive Services auch auf EU-Servern laufen. Microsofts Datenschutzerklärungen und Lizenzverträge erlauben die Analyse und Verarbeitung von Daten durch diese Dienste aber auch auf anderen, also auch auf US-Servern. Dass das in der Praxis auch durchaus erfolgen kann, bestätigte uns Microsoft auf Nachfrage.

Besitzern eines privaten Office-Abonnements, zum Beispiel Microsoft 365 Family, garantiert Microsoft die regionale Datenspeicherung jedoch nicht, auch nicht für ruhende Daten. Es ist also möglich, dass die auf OneDrive gespeicherten Daten von Nutzern dieser „Klein-Abos“ auf US-Servern landen.

Unabhängig von Serverstandorten wollen viele Unternehmen und Einzelnutzer überhaupt nicht, dass Inhalte den eigenen Rechner oder das Unternehmensnetzwerk verlassen. Um das zu verhindern, müssen Sie sowohl auf die Cloudspeicher als auch auf die „verbundenen Erfahrungen“ verzichten. Der sicherste Weg ist, diese komplett zu deaktivieren.



Tief versteckt in den Datenschutzeinstellungen der Office-Programme lassen sich die „verbundenen Erfahrungen“ und damit die Übertragung von Inhalten zu Microsoft-Servern und -Diensten deaktivieren.

Verbundene Erfahrungen abschalten

Als Nutzer eines Privat-Abos wie Microsoft 365 Family können Sie die verbundenen Erfahrungen innerhalb von Office lahmlegen. Das geht getrennt für beide Erfahrungs-Arten, also Funktionen, die Daten abrufen und solche, die Inhalte analysieren. Das funktioniert jedoch nur en bloc, also alle Funktionen der jeweiligen Gruppe auf einmal. Das Abschalten der Erfahrungen ist im Microsoft-Konto hinterlegt und gilt somit automatisch für alle Office-Installationen, die unter dem jeweiligen Konto angemeldet sind. Bei Business-Abos steuert hingegen der verantwortliche Administrator diese Einstellungen per Gruppenrichtlinien (siehe ct.de/wr9p); den Nutzern kann er lediglich das Recht einräumen, bestimmte optionale Erfahrungen abzuschalten, etwa die Wetteranzeige in Outlook.

Unter Windows starten Sie ein beliebiges Office-Programm und wählen „Datei/Optionen/Trust Center. In diesem Dialog öffnen Sie „Einstellungen

für das Trust Center…“. Mit einem Klick auf „Datenschutzoptionen“ öffnen Sie den nächsten Dialog und darin wählen Sie „Datenschutzeinstellungen…“. Ein alternativer Weg führt über „Datei/Konto/Einstellungen verwalten“ unter der Überschrift „Kontodatenschutz“. In Office für macOS finden Sie die Einstellungen unter „Datenschutz/Verbundene Erfahrungen verwalten“. Als Nutzer eines Privat-Accounts scrollen Sie im folgenden Fenster bis zum Abschnitt „Verbundene Erfahrungen“ nach unten. Entfernen Sie die Häkchen bei „Office soll Ihre Inhalte analysieren…“ und auf Wunsch auch bei „Office soll Onlineinhalte herunterladen“, um die Übertragung von Inhalten zu und von den Microsoft-Servern zu unterbinden.

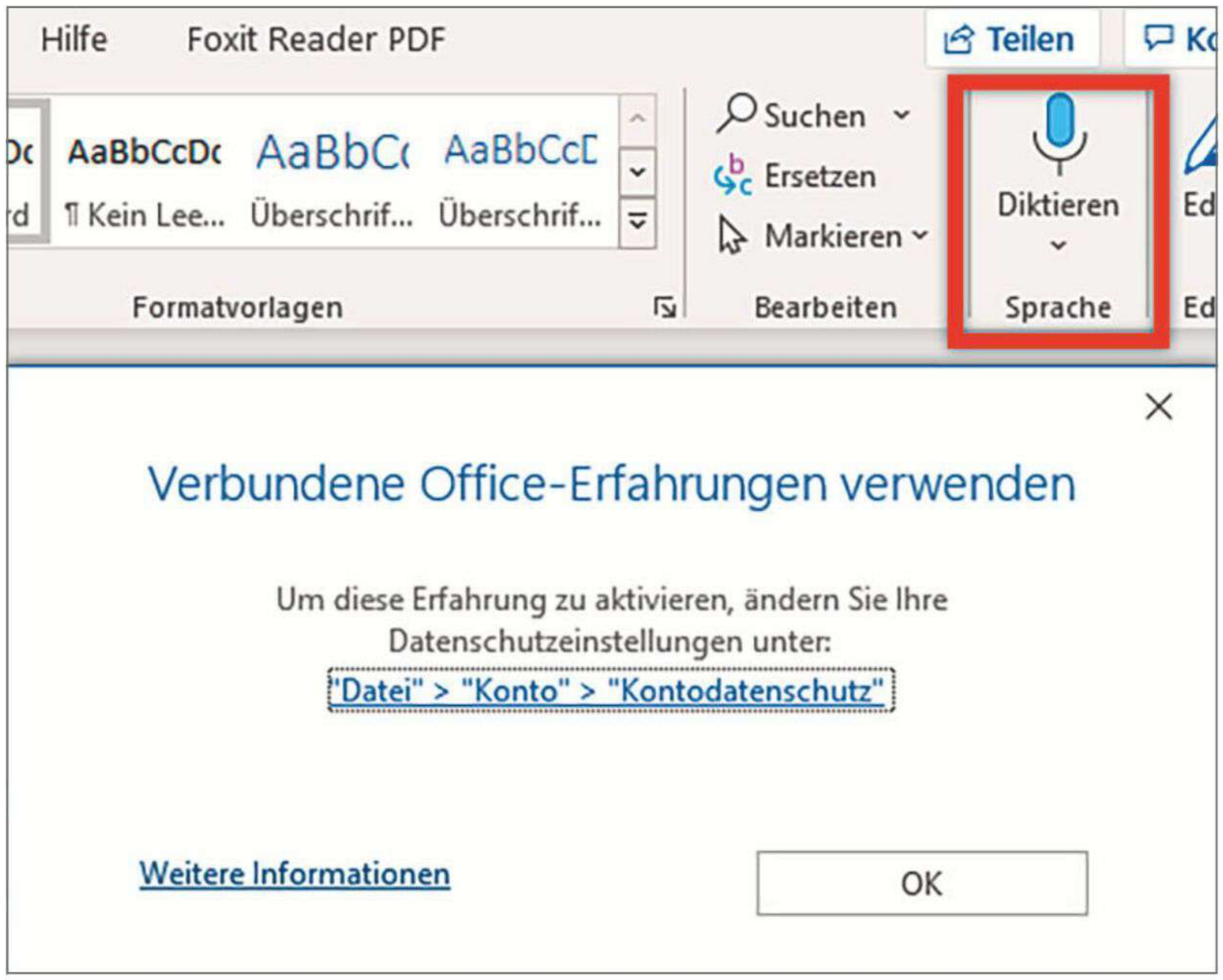
Weiter unten gibt es noch einen dritten, grau hinterlegten Abschnitt namens „Alle verbundenen Erfahrungen“. Nehmen Sie hier das Häkchen weg, hat das denselben Effekt wie das Ausschalten der beiden vorigen Optionen, deaktiviert aber zusätzlich noch die Möglichkeit, Office-Dateien in OneDrive oder OneDrive for Business anzulegen, zu speichern oder von dort zu öffnen. Allerdings ist dieser Schutz sehr schwach. Die Einstellung deaktiviert nämlich nur den Office-internen OneDrive-Zugriff und entfernt die zugehörigen Speicherziele aus der Backstage-Ansicht und den Dateidialogen.

Jedoch hat das Betriebssystem einen eigenen OneDrive-Client, der festgelegte lokale Synchronisationsordner mit dem Cloudspeicher abgleicht. Wenn Sie Office-Dateien im lokalen OneDrive-Ordner sichern, werden sie trotzdem automatisch in die Cloud hochgeladen. Aus Sicht des Office-Programms haben Sie ja lediglich auf die lokale Platte gespeichert. Das lässt sich nur verhindern, indem man auch den systemeigenen OneDrive-Client abschaltet, etwa per Gruppenrichtlinie (siehe ct.de/wr9p).

Die Einstellung „Alle verbundenen Erfahrungen“ deaktiviert auch das Roaming, also die Synchronisation der Datenschutzeinstellungen mit anderen Rechnern, auf denen Office mit demselben Microsoft-Konto verbunden ist. Sie müssen sie also gegebenenfalls auf allen betroffenen Geräten einzeln vornehmen.

Im Rahmen eines Unternehmens-Abos finden Sie in den Datenschutzeinstellungen nur eine Option zum Abschalten der zusätzlichen verbundenen Erfahrungen, vorausgesetzt, der Admin hat das freigeschaltet. Ansonsten begrüßt Sie hier nur ein entsprechender Hinweis.

Jede Veränderung der Einstellungen erfordert einen Neustart aller Office-Programme. Danach erscheint bei dem Versuch, eine der betroffenen Funktionen zu nutzen, eine Meldung, die auf die Beschränkungen der Datenschutzeinstellungen verweist.



Hat man die verbundenen Erfahrungen deaktiviert, quittiert Office (hier: Word) den Aufruf zugehöriger Funktionen, zum Beispiel der Spracheingabe, mit einem Hinweis.

Was Office trotzdem petzt

Der Verzicht auf die Cloud-Speicherung und das Deaktivieren der verbundenen Erfahrungen sollte – so man Microsoft in diesem Punkt vertraut – die Übertragung von Inhalten der Office-Programme an die Microsoft-Server unterbinden, macht die Programme aber nicht komplett mundtot. So werden nach wie vor diverse Diagnosedaten an den Hersteller übermittelt. Dazu dürften neben Fehler- und Absturzberichten zum Beispiel auch (hoffentlich) anonymisierte Statistiken über die Nutzungshäufigkeit von Funktionen gehören [3]. Das lässt sich zumindest bei Enterprise-Versionen von Office per Gruppenrichtlinie oder Registry einschränken oder vollständig unterbinden. Eine Anleitung hierzu finden Sie unter ct.de/wr9p.

Literatur

[1] Stefan Wischner, **Zusammen arbeiten**, c’t Home & Office 2021, S. 82

[2] Stefan Wischner, **Sicherheitsdienste**, Automatische Speicher- und Backup-Funktionen in MS Office, c’t 9/2019, S. 144

[3] Dr. Hans-Peter Schüler, **Microsoft 365**, Zeitgeist 1984, Akribische Anwenderüberwachung durch Microsofts Office-Software, c’t 25/2020, S. 40

Office telefoniert aber auch regelmäßig nach Hause, um nach Updates zu suchen und die Gültigkeit der Lizenz zu überprüfen. Vor allem Letzteres ist der Grund, warum es keine Option ist, Office zum Beispiel per Firewall-Regeln die Internet-Verbindung komplett zu kappen. Zwar funktionieren die lokal installierten Programmmodule (aber natürlich nicht die Browser-Versionen) problemlos offline, so dass man auch zum Beispiel im Flugzeug oder Zug damit arbeiten kann. Nach spätestens 31 Tagen ist jedoch eine zumindest kurze Internetverbindung notwendig.

Kommt die nicht zustande, schaltet Office in einen Read-only-Modus, in dem sich Dateien nicht mehr bearbeiten lassen, bis wieder eine Internetverbindung hergestellt wurde. Microsoft begründet das damit, dass regelmäßig auf Sicherheitsupdates geprüft werden muss, ganz zum Schutz des Anwenders. In erster Linie dürfte es aber um die Kontrolle gehen, ob die Lizenz noch gültig ist. Dazu passt auch das Intervall von 31 Tagen; ein Monat ist nämlich der kleinste Abrechnungszeitraum für Office-365-Abonnements.

Microsoft hat allerdings angekündigt, dass zumindest Nutzer eines Enterprise-Plans (also eines E1- bis E3-Abonnements) demnächst die Option erhalten sollen, das Prüfintervall auf bis zu drei Monate zu verlängern.

Weitere Infos und Anleitungen

ct.de/wr9p

Fazit

Überraschend ist, dass man Inhalte von Office-Dokumenten und -Tabellen nicht nur dann mit Microsoft-Servern teilt, wenn man die Dateien auf OneDrive oder OneDrive for Business speichert. Vor allem viele neue Funktionen übermitteln möglicherweise sensible Inhalte zumindest auszugsweise. Immerhin bietet Microsoft die Möglichkeit, diese Funktionen abzuschalten. Dass damit tatsächlich alle Inhaltsdaten auf dem eigenen Rechner oder im Unternehmen bleiben, ist letztlich Vertrauenssache; eine echte Kontrollmöglichkeit gibt es nicht. (swi) c't

IMMER AUF AUGENHÖHE

2× Mac & i mit 35 % Rabatt testen und Geschenk sichern!



Mac & i – Das Magazin rund um Apple

- Tipps & Workshops
- Hard- & Softwaretipps
- Apps und Zubehör
- inkl. Club-Mitgliedschaft

Für nur 14,40 € statt 21,80 €

NEU: Mit Mac & i Club-Mitgliedschaft exklusive Vorteile genießen



Jetzt bestellen: www.mac-and-i.de/miniabo

leserservice@heise.de 0541 80 009 120

Mac & i. Das Apple-Magazin von c't.



Bild: Andreas Martini

Windows ohne Microsoft-Konto nutzen

Sie verwenden Windows, wollen sich aber nicht mit einem Microsoft-Konto, sondern mit einem herkömmlichen lokalen Konto daran anmelden? Das geht, obwohl Microsoft es gern anders hätte: Windows versucht immer mal wieder, Ihnen das Umstellen der Anmeldung unterzujubeln. Doch Sie können sich dagegen wehren.

Von **Axel Vahldiek**

Schon während der Installation versucht Windows 10, Sie zum Einrichten eines Microsoft-Kontos zu überreden. Im laufenden Betrieb setzt Windows die Versuche fort: Immer mal wieder erscheinen Nachfragen, ob Sie sich nicht doch endlich mit einem Microsoft-Konto anmelden wollen. Doch auch wenn Microsoft Ihnen das gerne einreden würde: Um Windows zu nutzen, brauchen Sie kein Microsoft-Konto. Sie können stattdessen ein herkömmliches lokales Benutzerkonto verwenden.

Das Nachfolgende erläutert zuerst, wie Sie Windows 10 ohne Microsoft-Konto installieren. Anschließend geht es um den laufenden Betrieb: Sie erfahren, wie Sie neue, lokale Benutzerkonten hinzufügen, wie Sie bereits vorhandene Konten von Microsoft-Konto zu lokalem Benutzerkonto umstellen, welche

Apps Sie aus dem Store nutzen können und wie Sie verhindern, dass Mitbenutzer des PCs die Anmeldung auf ein Microsoft-Konto umstellen. Den Abschluss bildet ein besonders rabiater Handgriff, mit dem Sie die Anmeldung an Microsoft-Konten fast komplett lahmlegen.

Ein Tipp aber gleich vorab: Für die erstmalige Anmeldung an ein Microsoft-Konto ist grundsätzlich eine Onlineverbindung erforderlich. Durch das Ziehen des Netzwerksteckers oder Deaktivieren der WLAN-Verbindung umgehen Sie also jegliches Gedrängel. Vor allem während der Installation von Windows kann Ihnen das viel Nerverei ersparen. Auf Dauer stellt der Offlinebetrieb allerdings zugegebenermaßen wohl nur in seltenen Fällen eine ernsthafte Option dar.

Installation: Home

Wie Sie bei der Installation von Windows um ein Microsoft-Konto herumkommen, hängt von der Edition ab: Bei Home geht es anders als bei Pro, Education und Enterprise.

Zuerst zu Home. Während des Installationsablaufs erscheint ein Dialog, in dem der Einrichtungsassistent Ihre E-Mail-Adresse, Ihre Telefonnummer oder Ihren Skype-Namen erfragt. Damit will er Ihr Microsoft-Konto identifizieren. Besitzen Sie kein Konto, können Sie ein neues erstellen. Das Einrichten eines lokalen Kontos hingegen ist nicht vorgesehen, und das ist Absicht: Ein Klick auf „Weitere Informationen“ bringt den Hinweis, dass Sie nach der Installation die Anmeldung von einem Microsoft- auf ein lokales Konto umstellen können. Das ist zwar richtig, doch Microsoft hat bis dahin längst Ihr Konto mit der Installation verknüpft und erkennt letztere danach auch ohne Konto wieder.

Um trotzdem von Anfang an ein lokales Konto zu verwenden, gibt es zwei Ansätze. Der einfachste: Tippen Sie statt E-Mail-Adresse, Telefonnummer oder Skype-Name kurzerhand als Kontoname `windows` ein. Als Kennwort reicht beliebiger Unfug, die Länge ist egal. Das führt zum Hinweis, dass dieses Konto wegen zu häufigen Eingebens eines falschen Kennworts gesperrt sei. Klicken Sie anschließend auf „Weiter“, gelangen Sie zu einem Dialog zum Einrichten eines herkömmlichen lokalen Nutzerkontos. Das funktioniert übrigens auch mit anderen Kontonamen, erfolgreich probiert haben wir `billgates`, `microsoft`, `redmond`, `cortana`, `linux` und `spammer`.

Falls Sie in der Vergangenheit schon mal den Trick verwendeten, die Mailadresse eines existierenden und nicht gesperrten Microsoft-Kontos einzugeben, anschließend aber zehnmal hintereinander ein falsches Kennwort: Das klappt nicht mehr.

Was wie oben bereits erwähnt noch funktioniert: das Kappen der Internetverbindung. Ziehen Sie also vor dem Start der Windows-Installation die LAN-Strippe und lehnen Sie das Verbinden mit einem WLAN ab. Dann landen Sie direkt im Dialog zum Einrichten eines lokalen Kontos. Haben Sie zu spät daran gedacht und sitzen nun doch vor dem Dialog zum Einrichten des Microsoft-Kontos? Drücken Sie Umschalt+F10, woraufhin sich eine Eingabeaufforderung öffnet. Tippen Sie darin entweder das kürzere `ncpa.cpl` oder das leichter zu merkende `control netconnections` ein. Es erscheint ein Fenster mit den vorhandenen Netzwerkverbindungen, deaktivieren Sie die aktiven via Kontextmenü. Schließen Sie dieses Fenster und die Eingabeaufforderung wieder und klicken oben auf den Zurück-Pfeil. Nun können Sie ein lokales Konto einrichten. Der Trick mit dem gesperrten Microsoft-Konto namens „windows“ führt in diesem Fall allerdings schneller ans Ziel, und „windows“ als Kontoname lässt sich auch noch leichter merken als die Befehle zum Deaktivieren der Netzwerkverbindung.



Wenn Sie während der Installation behaupten, dass der Name Ihres Microsoft-Kontos „Windows“ lautet, verweist der Einrichtungsassistent darauf, dass dieses Konto gesperrt sei – und erlaubt Ihnen, ein herkömmliches lokales Konto einzurichten.

Installation: Pro & Co.

Wenn Sie eine Pro-, Education- oder Enterprise-Edition installieren, brauchen Sie keine Tricks zum Einrichten eines lokalen Kontos, sondern müssen bloß an die richtige Stelle klicken: Nachdem Sie gefragt werden, ob Sie den PC „Für persönliche Verwendung“ oder „Für eine Organisation“ einrichten, erscheint unabhängig von der Auswahl im nächsten Dialog ein

zusätzlicher, aber unscheinbarer Link, der bei Home fehlt. Bei Auswahl „Für persönliche Verwendung“ heißt er „Offlinekonto“.

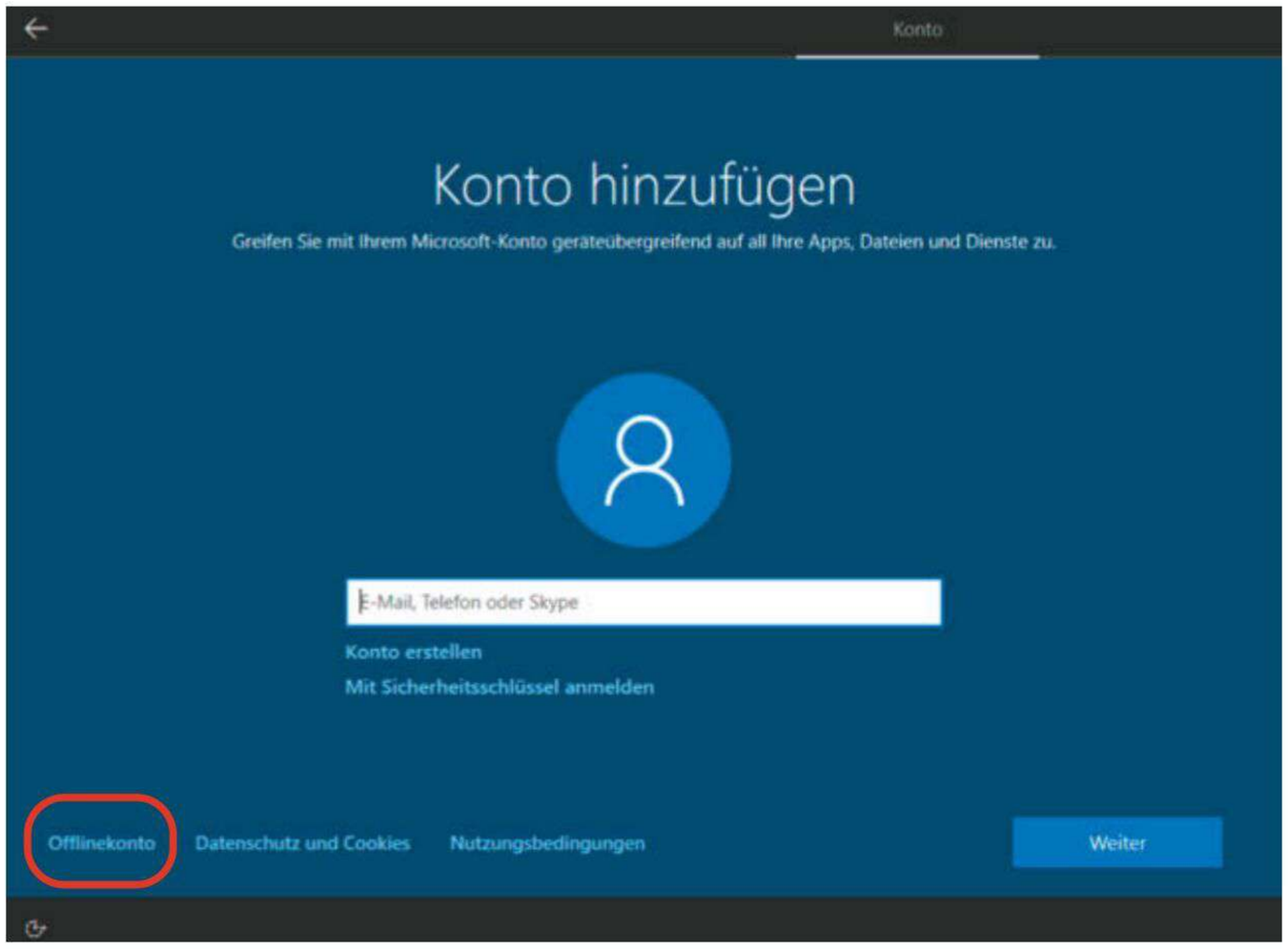
Als Nächstes versucht Windows, Sie doch noch zu einem Microsoft-Konto zu überreden. Unter anderem behauptet es, dass Sie sich ohne so eines auf eine „Eingeschränkte Erfahrung“ gefasst machen müssten. Das ist Humbug, Windows funktioniert mit einem lokalen Konto genauso wie mit einem Microsoft-Konto. Sie verzichten halt nur auf die zusätzlichen Clouddienste, aber darum geht es ja. Klicken Sie also auf den Link „Eingeschränkte Erfahrung“, dann können Sie ein lokales Konto erstellen.

Unbeaufsichtigte Installation

Es gibt einen weiteren Weg zum lokalen Konto, der bei allen Editionen gleichermaßen gangbar ist, und zwar unabhängig vom Bestehen einer Onlineverbindung. Verwenden Sie eine Antwortdatei, die alle während der Installation auftauchenden Fragen an Ihrer Stelle beantwortet. Damit können Sie automatisiert ein lokales Konto einrichten lassen und kommen so um Microsofts Überredungsversuche herum. So eine Datei zu erstellen ist allerdings nicht ganz trivial, die Anleitung dazu füllt einen eigenen Artikel [1].

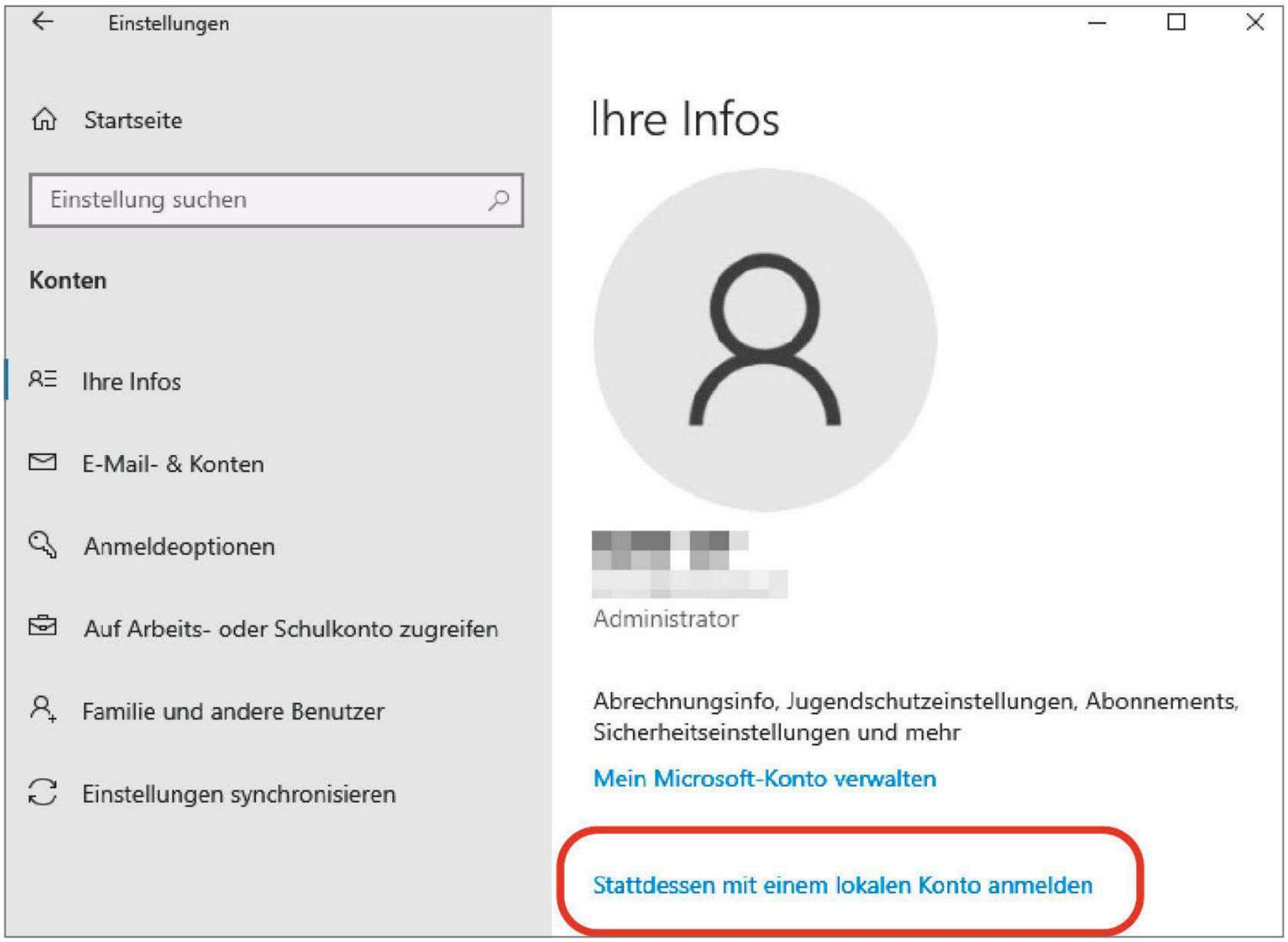
Sie können auch von c’t vorgefertigte Antwortdateien verwenden. Sie finden via ct.de/wfgu ein Zip-Archiv mit gleich zwei Antwortdateien: Autounattendx64.xml sowie Autounattendx86.xml – Obacht, bitte erst diesen Abschnitt zu Ende lesen. Die beiden Dateien sorgen dafür, dass Sie während einer Installation nur noch nach dem Installationsschlüssel und dem Installationsziel auf dem Datenträger gefragt werden. Anschließend läuft alles automatisch durch. Sämtliche Spracheinstellungen werden auf „de-de“ gesetzt, in der Gruppe der Administratoren wird ein Konto namens „ctleser“ angelegt und die Nachfragen zu „Spracherkennung“, „Standort“, „Mein Gerät suchen“, „Umfang der Diagnosedaten“, „Freihand- und Eingabeerkennung verbessern“, „Mithilfe von Diagnosedaten angepasste Erfahrungen erhalten“ und „Apps Werbe-ID verwenden lassen“ werden abgelehnt. Wenn die Installation durch ist, erscheint noch ein Dialog zum Ändern des bislang leeren Kennworts für das Konto. Wollen Sie keines vergeben, lassen Sie das Eingabefeld leer.

Sie können die XML-Dateien anpassen, öffnen Sie sie dazu einfach in einem Texteditor wie Notepad. Wenn Sie in Österreich oder in der Schweiz wohnen, ändern Sie per Suchen und Ersetzen alle „de-de“ zu „de-at“ beziehungsweise „de-ch“. Den Namen „ctleser“ können Sie ebenfalls per Suchen und Ersetzen anpassen. Falls Sie anderes anpassen wollen, bleibt allerdings nur der erneute Verweis auf [1].



Während der Installation von Windows 10 Pro, Education und Enterprise führt der unscheinbare Link „Offlinekonto“ zum Einrichtungsdialog für ein lokales Konto.

Sollten Sie bislang ein Microsoft-Konto zum Anmelden an Windows verwenden, das künftig aber nicht mehr wollen, stellen Sie das in den Einstellungen unter „Konten“ um.



Um eine der XML-Dateien zu verwenden, entscheiden Sie zuerst, ob Sie eine 64- oder 32-Bit-Version von Windows installieren wollen. Bei 64 Bit wählen Sie die Datei Autounattendx64.xml aus und kopieren sie auf einen USB-Stick in dessen Wurzelverzeichnis. Es darf durchaus jener USB-Stick sein, vom dem Sie Windows installieren. Wichtig: Benennen Sie die Datei dort um in Autounattend.xml. Achten Sie darauf, sich nicht zu vertippen, denn mit anderen Namen funktioniert es nicht. Lassen Sie den Stick während der gesamten Installation angestöpselt. Bei einer 32-Bit-Installation verfahren Sie analog mit der Datei Autounattendx86.xml.

Anmeldung von Microsoft-Konto trennen

Falls Sie bereits ein Microsoft-Konto für die Anmeldung an Windows nutzen, das aber künftig nicht mehr wollen, können Sie die Verbindung trennen. Öffnen Sie dazu die Einstellungen (Windows+I drücken oder auf das Zahnrad links unten im Startmenü klicken). Unter „Konten“ finden Sie hier direkt Ihr Konto und darunter einen Link namens „Stattdessen mit einem lokalen Konto anmelden“.

Es startet ein Assistent, der erst das Kennwort beziehungsweise die PIN Ihres Microsoft-Kontos wissen will. Anschließend fragt er Benutzername, Kennwort und Kennworthinweis für das lokale Konto ab, mit dem Sie sich künftig anmelden. Sie können als Benutzernamen einen anderen als den vorgegebenen eintragen, doch beachten Sie dann, dass Ihr Nutzerprofil unter C:\Benutzer von der Namensänderung nicht betroffen ist, es heißt also weiterhin wie zuvor. Zum Schluss meldet Sie Windows einmal ab und wieder an, dann ist die Umstellung abgeschlossen.

Haben Sie sich in der Vergangenheit zwar nicht an Windows, wohl aber im Store oder an Apps angemeldet, hat Windows die dazugehörigen Informationen gespeichert. Löschen können Sie diese in den Einstellungen unter „Konten/E-Mail- & Konten“. Hier

können Sie bei jedem gespeicherten Konto nach einem Klick darauf nicht nur umstellen von „Microsoft-Apps dürfen mich anmelden“ auf „Apps müssen zur Verwendung dieses Kontos meine Zustimmung anfordern“, sondern das Konto auch entfernen.

Sie können ein überflüssig gewordenes Microsoft-Konto übrigens auch komplett löschen, doch das ist nicht trivial. Denn das erfordert diverse Bestätigungen, und zwar aus gutem Grund. So soll unter anderem verhindert werden, dass jemand unberechtigt ein fremdes Konto schließt. Außerdem könnten jede Menge persönliche Daten beim Löschen verloren gehen, etwa Mails, Chatverläufe und Kontakte, aber auch Spielfortschritte. Schließlich könnten auch Guthaben und Abonnements etwa für Office 365 im Konto hinterlegt sein. Einen Assistenten zum Löschen hat Microsoft auf seiner Website veröffentlicht, zu finden über ct.de/wfgu.

Neues Nutzerkonto

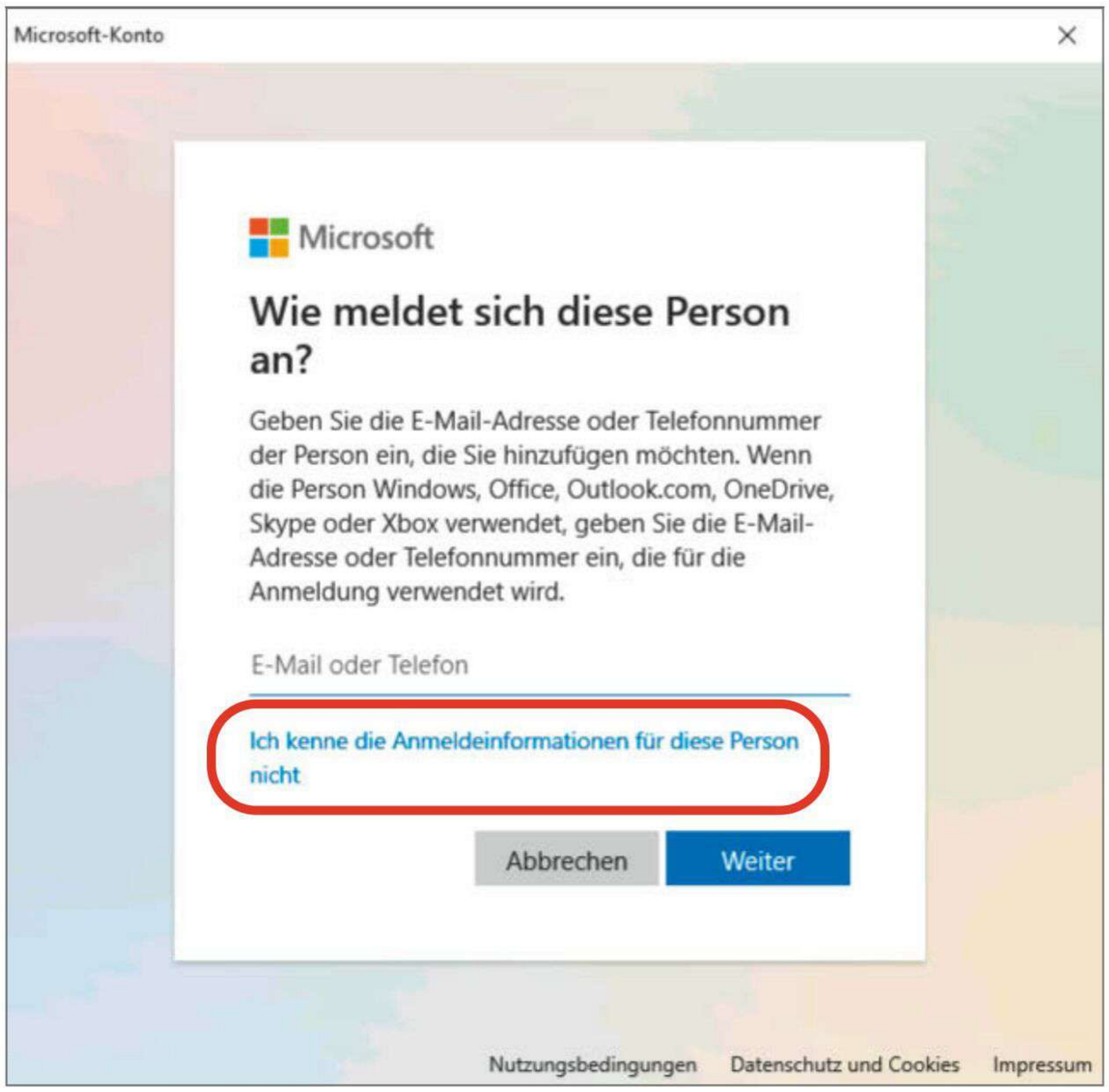
Windows gibt sich viel Mühe, um zu verhindern, dass Sie einer Installation ein weiteres lokales Konto hinzufügen – alle weiteren Konten sollen nach Microsofts Willen Microsoft-Konten sein. Das führt dazu, dass die schnellste und einfachste Methode zum Erstellen eines lokalen Kontos das Eintippen eines Kommandozeilenbefehls ist. Drücken Sie Windows+X und wählen Sie (je nachdem, was vorhanden ist) „Eingabeaufforderung (Administrator)“ oder „Windows PowerShell (Administrator)“. Dort tippen Sie Folgendes ein, um ein neues Konto beispielsweise namens „ctleser“ anzulegen.

```
net user ctleser /add
```

Den Namen können Sie anpassen. Verwenden Sie nur Buchstaben und Ziffern. Falls Sie partout ein Leerzeichen im Namen wollen, müssen Sie den Namen in Anführungsstrichen angeben (`net user "Bill Gates" /add`).

Auch per Mausklick können Sie ein lokales Konto erstellen, doch ist das oft umständlicher, als den genannten Befehl einzutippen. Den Assistenten finden Sie in den Einstellungen unter „Konten/Familie und andere Benutzer/Diesem PC eine andere Person hinzufügen“. Der einfachste Trick, Sie ahnen es schon, ist wie bei der Installation auch hier das vorübergehende Trennen der Internetverbindung, dann können Sie ein lokales Konto erstellen.

Mit einer bestehenden Onlineverbindung hingegen scheint der Konto-Assistent grundsätzlich nur zum Erstellen von Microsoft-Konten bereit zu sein, denn er bietet als Schaltflächen nur „Abbrechen“ und „Weiter“ an. Doch es gibt hier auch den Link „Ich kenne die Anmeldeinformationen für diese Person nicht“. Mit dem landen Sie in einem Dialog zum Erstellen eines neuen Microsoft-Kontos – und oberhalb der Schaltflächen finden sich mehrere Links, deren unterer „Benutzer ohne Microsoft-Konto hinzufügen“ endlich ans Ziel führt. Das mag etwas absurd klingen, ist aber der offiziell von Microsoft empfohlene Weg zum Erstellen eines lokalen Kontos (siehe ct.de/wfgu).



Wenn Sie in Windows ein weiteres herkömmliches lokales Konto einrichten wollen, klicken Sie im Assistenten auf den unteren Link.

Gequengel abstellen

Gelegentlich wird Sie Windows 10 nach dem Hochfahren mit der Frage begrüßen, ob Sie nicht endlich ein Microsoft-Konto zur Anmeldung verwenden wol-

Literatur

[1] Axel Vahldiek, **Frag nicht, mach hin!**, Mit Antwortdateien automatisiert Windows installieren, c’t 25/2018, S. 148

[2] Axel Vahldiek, **Dienstliches auf dem Privat-PC schützen**, c’t Windows 2021, S. 26

Downloads und Dokus

ct.de/wfgu

len. Ein „Nein“ ist dabei nicht vorgesehen, die einzige Schaltfläche heißt „Weiter“ und führt zur Umstellung auf das Microsoft-Konto. Der Versuch, den Dialog per Taskmanager abzuschießen, scheitert daran, dass sich der Konto-Dialog stets ganz nach vorn drängelt und so selbst den Taskmanager überdeckt. Die einzige Alternative ist der Klick auf einen Link, der „In drei Tagen erinnern“ heißt. Dann erscheint der Dialog nach dieser Zeitspanne erneut, und wenn Sie dieses Mal statt auf „Weiter“ auf „Später erinnern“ klicken, ist erst mal wieder für eine Weile Ruhe.

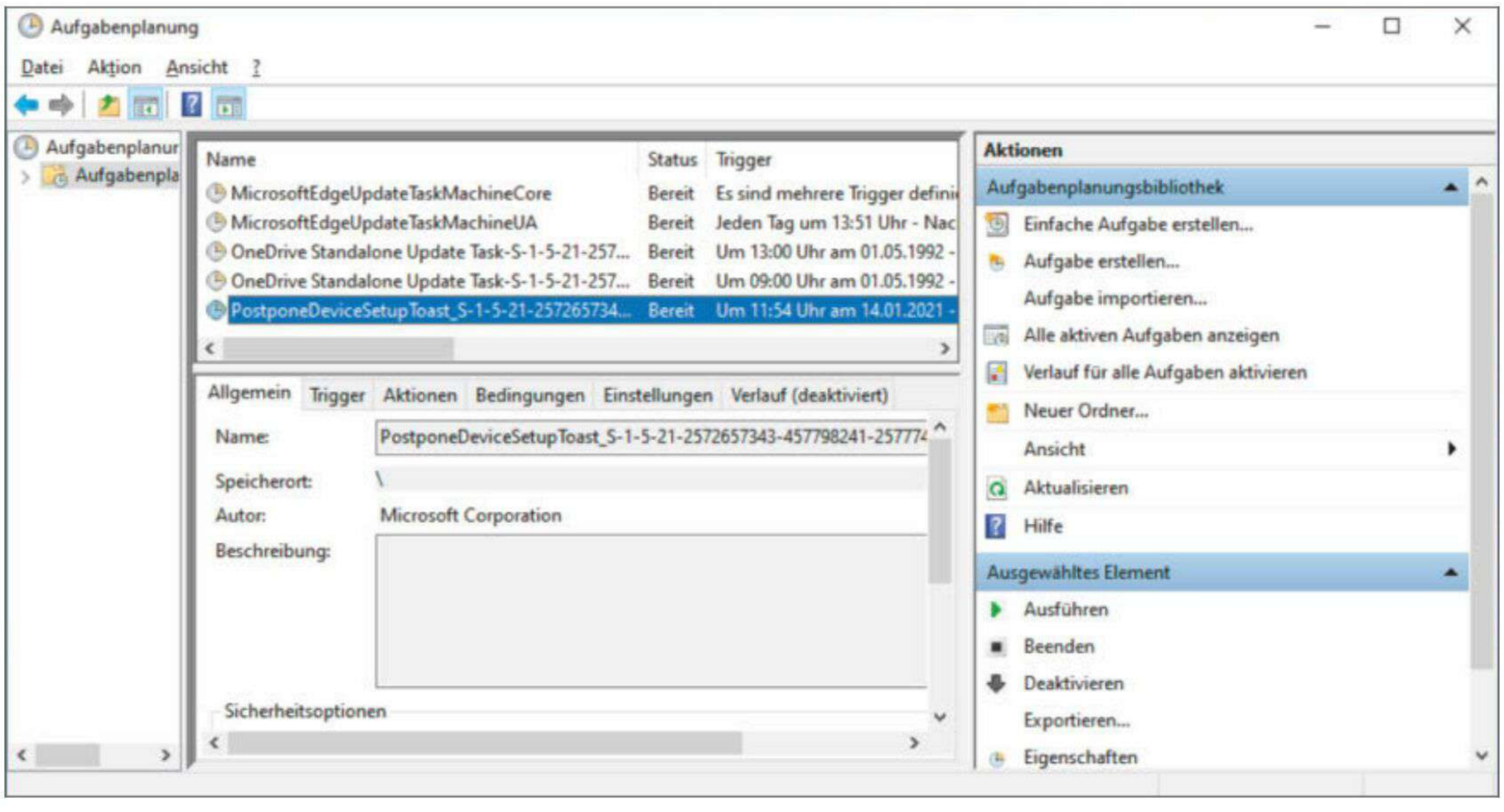
Ganz verhindern lassen sich solche Nachfragen nicht, denn Microsoft kann per Windows Update weitere nachladen. Aber immerhin können Sie verhindern, dass der weggeklickte Dialog noch ein weiteres Mal erscheint. Drücken Sie die Windows-Taste und geben Sie buchstabenweise so lange `Aufgabenplanung` ein, bis der gleichnamige Suchtreffer erscheint. In der Aufgabenplanungsbibliothek finden Sie eine Aufgabe, die derzeit „PostponeDeviceSetupToast …“ heißt. Der Name mag jedoch schon nach dem nächsten Windows-Update wieder anders lauten. Was Microsoft nicht so leicht ändern kann: In der Spalte „Trigger“ ist ein Termin in drei Tagen genannt. Löschen Sie die Aufgabe via Kontextmenü, dann erscheint die Erinnerung nicht erneut.

Theoretisch bietet Windows 10 übrigens eine Option, damit solche Nachfragen nicht mehr auftauchen: Entfernen Sie in den Einstellungen unter „System/Benachrichtigungen und Aktionen“ das Häkchen vor „Möglichkeiten zum Abschließen der Einrichtung meines Geräts für die optimale Nutzung von Windows vorschlagen“. In der Praxis hilft das aber nicht, weil Microsoft auch diese Option gelegentlich bei Updates wieder reaktiviert.

Store und Apps ohne Microsoft-Konto

Die weit verbreitete Annahme, dass sich Apps aus dem Windows-eigenen Store nur mit einem Microsoft-Konto herunterladen lassen, ist schon seit einiger Zeit nicht mehr korrekt. Bei aktuellen Windows-10-Versionen können Sie Gratis-Apps problemlos ohne Microsoft-Konto bekommen. Der Store bittet Sie zwar nach einem Klick auf „Herunterladen“ unter der Überschrift „Geräteübergreifend verwenden“ darum, sich mit einem Microsoft-Konto anzumelden, doch dort prangt ausnahmsweise neben der „Anmelden“-Schaltfläche eine namens „Nein, danke“.

Auch die bei Windows mitgelieferten Apps wie „Alarm & Uhr“, „Wetter“, „Fotos“, „Karten“ und den Browser „Edge“ können Sie ohne ein Microsoft-Konto nutzen. Falls ein Anmeldedialog erscheint, reicht es aus, ihn über das Kreuz oben rechts zu schließen, notfalls die App danach erneut starten. Ausnahmen sind reine Cloud-Apps wie OneDrive und Skype, die nur mit Microsoft-Konto funktionieren.



Nachfragen, ob Sie nicht doch endlich ein Microsoft-Konto verwenden wollen, können Sie zwar nicht ganz verhindern, weil Windows sie per Update nachlädt. Das Wiederholen so einer Nachfrage können Sie aber unterdrücken, indem Sie die dazugehörige Aufgabe löschen.

Mitbenutzer-Falle vermeiden

Es gibt eine Falle, von der Sie wissen sollten, wie sie aussieht und wie Sie sie umgehen. Auch Mitbenutzer Ihres Benutzerkontos könnten sich mit einem Microsoft-Konto anmelden und bei der Gelegenheit die Windows-Anmeldung darauf umstellen. Es gab durchaus schon den Fall, dass ein Vater seinen Sohn an den PC ließ. Der Sohn, der bereits ein eigenes Microsoft-Konto besaß, wollte auf Papas PC ein Spiel aus dem Store laden, gab dafür seine Zugangsdaten ein und klickte auf „Weiter“. Als Nächstes passierte, was der Vater unbedingt verhindern wollte: Die Anmeldung war umgestellt, und das nicht mal auf das Microsoft-Konto des Vaters, sondern auf das des Sohnes.

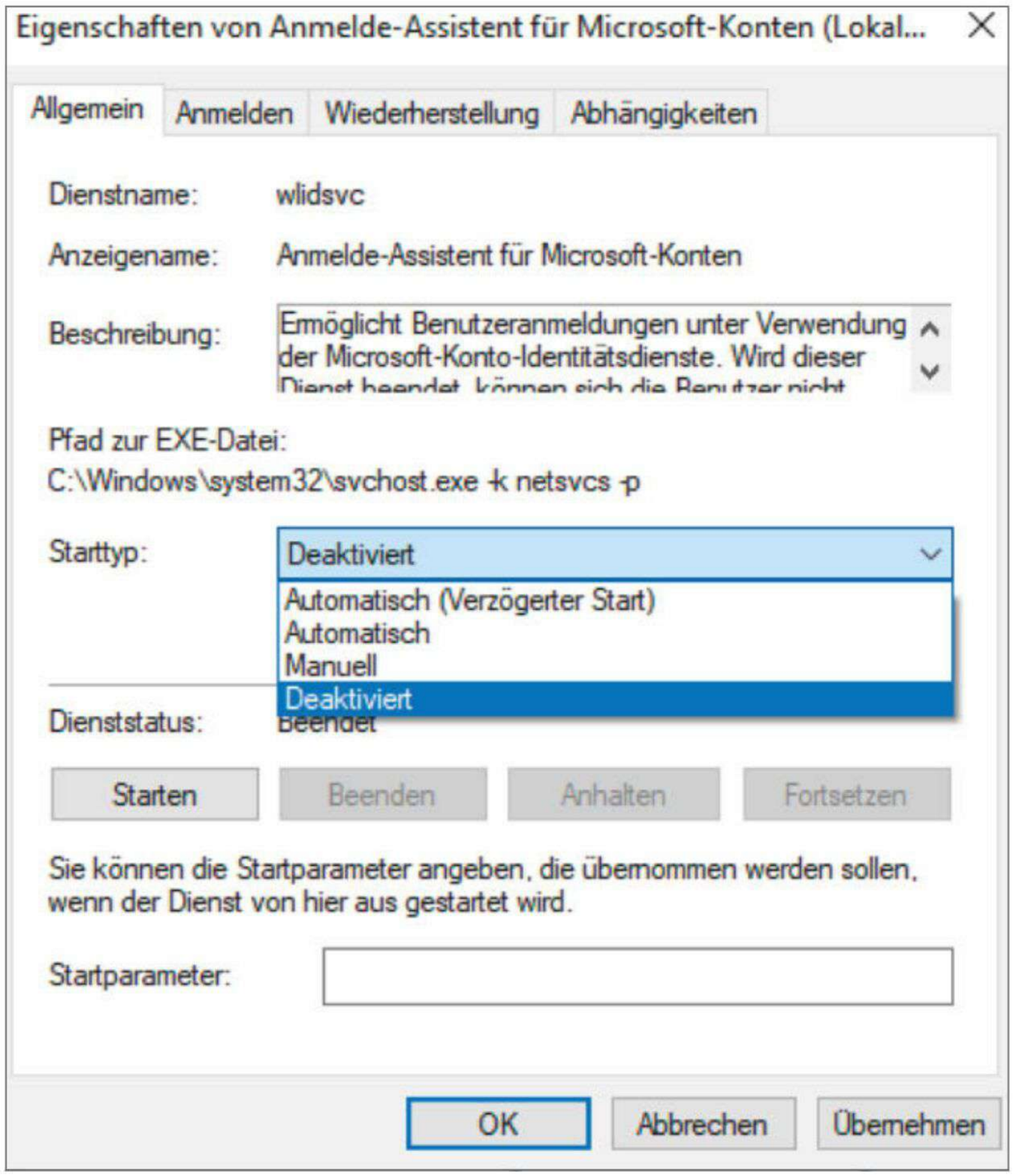
Es gibt mehrere Möglichkeiten der Abhilfe. Empfehlenswert ist, dem Nachwuchs separate Nutzerkonten einzurichten. Wenn Sie auf Ihrem privaten PC sensible Daten speichern, sollten Sie diese zudem verschlüsseln. Sofern Sie Windows 10 Pro, Education oder Enterprise nutzen, gelingt das mit Bordmitteln, und zwar so, dass Mitbenutzer den PC trotzdem ohne Kennwort nutzen können. Die Handgriffe dazu haben wir in [2] zusammengetragen.

Die rabiate Methode

Wenn Sie sicherstellen wollen, dass sich an Ihrem PC niemand an einer App oder an Windows mit einem Microsoft-Konto anmelden kann, gibt es noch einen besonders rabiaten Weg. Rabiat ist er vor allem deshalb, weil Sie, wenn Sie ihn verfolgen, später immer mal wieder Fehlermeldungen zu sehen bekommen, denn damit endet anschließend jeder Anmeldeversuch an ein Microsoft-Konto. Das gilt auch für andere Nutzer des PCs. Alles andere funktioniert aber wie gewohnt weiter. Der Trick besteht darin, den zum Anmelden nötigen Assistenten lahmzulegen (was sich aber bei Bedarf rückgängig machen lässt).

Hinter diesem Assistenten steckt ein Windows-eigener Dienst. Zum Deaktivieren des Dienstes drücken Sie die Windows-Taste und tippen `Dienste` so lange buchstabenweise ein, bis der gleichnamige Suchtreffer erscheint. Suchen Sie in der Liste der Dienste jenen namens „Anmelde-Assistent für Microsoft-Konten“. Wählen Sie aus dessen Kontextmenü „Eigenschaften“ und klicken Sie darin auf die Schaltfläche „Beenden“. Anschließend ändern Sie das Pull-down-Menü „Starttyp“ von „Automatisch“ auf „Deaktiviert“. Nach einem Klick auf „Übernehmen“ sind keine Anmeldungen per Assistent mehr möglich. Beachten Sie bitte, dass Windows das Deaktivieren des Dienstes beim Upgrade auf die nächste Windows-10-Version rückgängig machen könnte. Es reicht dann aber aus, das Deaktivieren zu wiederholen.

Die einzigen Anmeldungen an Microsoft-Konten, die danach noch funktionieren, sind Anmeldungen im Browser, da diese nicht über den Assistenten laufen. Doch das macht in diesem Fall nichts, denn per Browser lässt sich die Windows-Anmeldung nicht auf ein Microsoft-Konto umstellen. Und darum geht es ja. (axv) c't



Um Sie an ein Microsoft-Konto anzumelden, nutzt Windows einen Assistenten. Dahinter steckt ein Dienst, und den können Sie lahmlegen. Dann scheitert jeder Anmeldeversuch mit einer Fehlermeldung.

Halten Sie Ihre Prozesse im Takt



Exklusiver Frühbucher-Rabatt!

heise Academy

Werden Sie mit unseren Workshops zum Master Ihrer Entwicklungsprozesse.

Unser Angebot

Powerkurs vSphere-Administration
6. – 10. September
WORKSHOP

Container managen
mit Kubernetes & Rancher
9. – 10. September
WORKSHOP

Container-Orchestrierung
mit Kubernetes
20. – 23. September
WORKSHOP

Elastic Stack Fundamentals
5. – 7. Oktober
WORKSHOP

Sicheres Single-on mit Kerberos
11. – 13. Oktober
WORKSHOP

Continous Integration
mit Jenkins
12. – 13. Oktober
WORKSHOP

Mehr Informationen: heise-academy.de/devops



Zeiterfassung per Fingerscan?

Nicht alles, was in puncto Arbeitsorganisation Zeit und Kosten spart, ist rechtlich auch statthaft. Ein Zwang zum Abgeben eines Fingerabdrucks fürs Ein- und Ausloggen bei der Arbeit kollidiert mit dem besonderen gesetzlichen Schutz, dem biometrische Daten unterliegen.

Von **Verena Ehrl**

Bevor sich die Auswertung von DNA-Spuren durchsetzte, galten Fingerabdrücke als hochwichtige Schlüsselindizien für die forensische Personenidentifikation – wie jeder Krimileser weiß. Der daktyloskopische Identitätsnachweis, also das Zuordnen der individuellen Hautlinienmuster an den Fingern, ist bereits seit Mitte des 19. Jahrhunderts bekannt. Digitale Auswertungssysteme (AFIS) dienen heute der Merkmalsextraktion und -speicherung sowie dem Vergleichen von Fingerabdrücken.

Was der Kriminalistik reicht, ist dem modernen Smartphonenutzer billig – und so nehmen Mobiltelefone mithilfe optischer Sensoren millionenfach Fingerabdrücke zum Entsperren und für Authentifizierungszwecke bei Anwendungen entgegen. Wenn diese Methode so alltäglich und populär geworden

ist, warum sollten dann nicht auch Arbeitgeber sie für die vorgeschriebene Zeiterfassung ihrer Mitarbeiter einsetzen? Geeignete Scanner-Terminals, die für Alltagszwecke hinreichend zuverlässig funktionieren, sind auf dem internationalen Markt günstig zu haben. Es gibt sogar laientaugliche Stand-alone-Geräte mit lokaler Speicherung, die ohne Netzwerkeinbindung auskommen. Der biometrische Ansatz verhindert ein stellvertretendes Ein- und Ausloggen durch Kollegen – jedenfalls solange niemand das Scannersystem unter Einsatz massiver krimineller Energie überlistet. Zudem bringt das Konzept noch einen für Arbeitgeber charmanten Nebeneffekt mit sich: Ein schneller Fingertipp spart gegenüber anderen Authentifizierungsverfahren wertvolle Arbeitszeit.

Schnell und bequem verdatet

Es ist nicht ins Belieben eines Arbeitgebers gestellt, ob er für seine Mitarbeiter eine Zeiterfassung betreibt. Vielmehr hat der Europäische Gerichtshof (EuGH) in einem Grundsatzurteil 2019 festgestellt, dass Unternehmen verpflichtet sind, mithilfe geeigneter Erfassungssysteme die Arbeitszeit ihrer Mitarbeiter zu protokollieren [1].

In vordigitalen Zeiten dienten Stempeluhren am Werkseingang diesem Zweck. Heute gibt es viele Wege der computergestützten Zeiterfassung. Sie soll nicht nur dem Arbeitgeber Kontrolloptionen verschaffen, sondern auch dem Arbeitnehmer den Nachweis geleisteter Arbeitsstunden ermöglichen; zudem ist sie versicherungstechnisch relevant.

Eine Radiologiepraxis in Berlin, die zu einem bundesweit tätigen Konzern gehört, ersetzte 2018 die zuvor auf ausgedruckten Dienstplänen und Handnotizen beruhende Arbeitszeiterfassung für ihre Mitarbeiter durch ein digitales System („ZEUS“), das mit einem Fingerabdruckscanner arbeitete. Dieses speicherte allerdings nicht komplette Fingerabdrücke, sondern wertete nur die sogenannten Minutien aus, also signifikante Linienverzweigungen. Daraus erzeugte die Software einen Zahlencode, der weder eine Rekonstruktion der Minutien noch des eigentlichen Abdrucks erlauben sollte. Der Praxisbetreiber informierte die Beschäftigten per E-Mail über das neue System.

Ein dort angestellter 57-jähriger medizinisch-technischer Radiologieassistent (MTRA) verweigerte die Benutzung des Scanners. Er bestand darauf, geplante und geleistete Arbeitsstunden weiterhin manuell einzutragen. Im Herbst 2018 und im Frühjahr 2019 erhielt er deswegen je eine Abmahnung mit dazugehörigem Eintrag in seiner Personalakte.



Bild: Centor & Cia., Bogotá/Kolumbien

Zur biometrisch gestützten Zeiterfassung bieten Hersteller in aller Welt Systeme jeden Zuschnitts an. Für Kleinunternehmen gibt es sogar preisgünstige Stand-alone-Geräte, deren Einrichtung und Betrieb keinerlei Netzwerkkenntnisse erfordern.

Abdruckverweigerer klagt

Er klagte dagegen vor dem Arbeitsgericht (ArbG) Berlin [2]; das gab ihm auf Grundlage von Art. 9 der europäischen Datenschutz-Grundverordnung (DSGVO) und § 26 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) Recht. Der Arbeitgeber legte Berufung ein. Das Landesarbeitsgericht (LAG) Berlin-Brandenburg wies diese Berufung im Juni 2020 zurück [3]: Es stellte sich wie schon die Vorinstanz auf die Seite des Mitarbeiters.

Daktyloskopische Daten, auch die aus Fingerabdrücken gewonnenen numerischen Minutien-Kenncodes, sind personenbezogene Daten im Sinne von Art. 4 DSGVO. Als biometrische Daten gehören sie sogar zu den Kategorien sensibler Daten, für die nach Art. 9 DSGVO ein besonderer Schutz gilt. Dem gleichen Schutz unterliegen unter anderem Daten zu ethnischer Herkunft, politischen Meinungen und Religionszugehörigkeit sowie Gesundheitsdaten

oder Daten zum Sexualleben. Bereits die reduzierten Daten, mit denen das System der Radiologiepraxis arbeitete, reichten dem Gericht zufolge aus, um den besonderen Schutz nach Art. 9 DSGVO auszulösen.

Risikoabwägung

In Erwägungsgrund 51 zur DSGVO heißt es: „Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können." Das Grundrecht, um das es hier geht, betrifft die informationelle Selbstbestimmung und bildet das Fundament des deutschen Datenschutzrechts. Das Bundesverfassungsgericht (BVerfG) hat es aus Art. 2 Abs. 2 des Grundgesetzes (GG) in Verbindung mit Art. 1 entwickelt: Jeder Mensch soll selbst bestimmen können, welche Informationen über ihn erhoben, verarbeitet und gespeichert werden.

Die Verarbeitung gewöhnlicher personenbezogener Daten wie Namen, E-Mail-Adresse oder Telefonnummer berührt zwar auch dieses Grundrecht, bildet aber keinen so tiefen Eingriff wie der Umgang mit biometrischen Daten, etwa zu Fingerabdrücken, Iris und Retina, Gesichtsgeometrie, DNA sowie Hand- und Unterschriften. Deren Verarbeitung ist verboten – sofern nicht einer der klar umrissenen Ausnahmefälle vorliegt. Dabei geht der Gesetzgeber von einer Risikoabwägung aus: Welche Folgen könnte es haben, wenn die besagten Daten öffentlich werden? Um möglicherweise existenzgefährdende Folgen für Betroffene auszuschließen, geht Schutz vor Verarbeitung.

Eine Verarbeitung der Fingerabdruckdaten wäre im Fall der Radiologiepraxis statthaft gewesen, wenn der Betreiber nachgewiesen hätte, dass seine Maßnahme „erforderlich" war, damit er seine Rechte und Pflichten als Arbeitgeber wahrnehmen konnte. Dann hätte eine Ausnahme nach Art. 9 Abs. 2b DSGVO gegriffen. Im Prozess hatte er argumentiert, das strittige System sei in allen Praxen des Konzerns eingeführt worden, da es bei anderen Erfassungsverfahren wiederholt zu Unregelmäßigkeiten gekommen sei. Derlei Missbräuche waren in der Berliner Praxis, um die es ging, aber nicht bekannt. Auch dem klagenden MTRA hatte niemand vorgeworfen, er habe Einträge gefälscht. Das LAG hielt fest, dass „ein biometrisches Zeiterfassungssystem … in aller Regel nicht erforderlich" im Sinne des genannten Paragrafen ist, und sah auch im konkreten Fall keine Erfordernis. In anderen Zusammenhängen können vergleichbare Maßnahmen hingegen durchaus als zulässig gelten: So kann eine Zutrittskontrolle für Hochsicherheitsbereiche verbindliche Gesichtskontrolle oder Fingerscan erfordern (§ 26 Abs. 3 BDSG).

Art. 9 DSGVO: Verarbeitung besonderer Kategorien personenbezogener Daten

(1) … die Verarbeitung von … biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person … ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt …,

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann …, …

Fast freiwillige Einwilligungen

Es hätte nur einen anderen Weg gegeben, die biometriegestützte Zeiterfassung datenschutzrechtlich reinzuwaschen: Die Betroffenen hätten ausdrücklich einwilligen müssen (Art. 9 Abs. 2a DSGVO) – was nicht der Fall war. Eine solche Einwilligung hätte zudem freiwillig erfolgen müssen, um wirksam zu sein. Jeder der Mitarbeiter hätte konkret darauf hingewiesen werden müssen, welche Folgen seine Einwilligung hat. Auch Hinweise auf die Freiwilligkeit und auf das Recht, die Einwilligung jederzeit risikofrei widerrufen zu können, wären nötig gewesen. Etwas leichter haben es die Arbeitgeber in Unternehmen mit Betriebsräten. Die Einwilligung kann dann durch eine Dienstvereinbarung nach § 26 Abs. 4 BDSG ersetzt werden, die für die Arbeitnehmer bindend ist. Das geht jedoch nicht, ohne dass der Betriebs-/Personalrat an dieser Vereinbarung beteiligt worden ist und ihr zugestimmt hat. (psz) c't

Literatur

[1] EuGH, Urteil vom 14.5.2019, Az. C-55/18: heise.de/s/dXDP

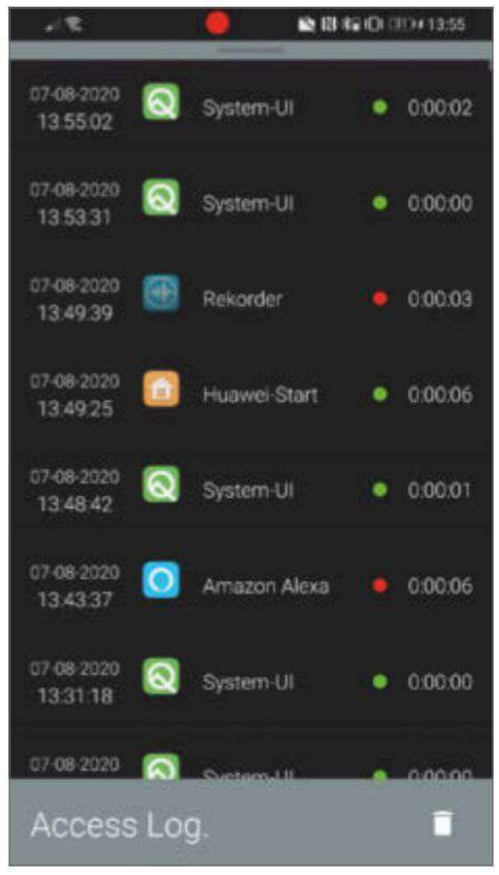
[2] ArbG Berlin, Urteil vom 16.10.2019, Az. 29 Ca 5451/19: heise.de/s/3EjZ

[3] LAG Berlin-Brandenburg, Urteil vom 4.6.2020, Az. 10 Sa 2130/19: heise.de/s/jpGj

Spionageschutz mit Access Dots

Unter Android bekommt man normalerweise nichts davon mit, wenn eine App Kamera, Mikrofon oder Standort anzapft. Access Dots zeigt eine virtuelle LED in der Statusleiste an, solange ein Zugriff erfolgt – vergleichbar mit der Kamera-LED am Notebook.

Von **Ronald Eikenberg**



Hat man einer Android-App einmal die Berechtigungen für Kamera, Mikrofon und Standort erteilt, kann sie damit machen, was sie will: Apps können etwa im Hintergrund laufen und unbemerkt Fotos oder gar Videos aufzeichnen. Auch Gespräche lassen sich so belauschen. Eine Kontrollmöglichkeit gibt es nicht, denn eine Kamera-LED, die den Zugriff signalisiert, fehlt. Apple hat das Problem bereits gelöst und zeigt seit iOS 14 bei aktiver Kamera einen farbigen Kreis in der Statusleiste an. Mit der kostenlosen App „Access Dots“ gibt es diese sinnvolle Funktion jetzt auch für Android.

Nach dem ersten Start muss man die App in den Geräteeinstellungen als sogenannte Bedienungshilfe (Accessibility Service) aktivieren, damit sie andere Apps überwachen darf. Öffnet man anschließend etwa die Kamera-App des Smartphones, erscheint in der Statusleiste ein grüner Kreis, beim Mikrofonzugriff ist der Kreis orange. Zapft eine App den Standort an, leuchtet der Kreis hellblau. Wenn der Punkt trotz aktivierter Bedienungshilfe nicht erscheint, dann ist wahrscheinlich das Energiemanagement des Geräts Schuld: In diesem Fall muss in den Energiespar-Einstellungen eine Ausnahme definiert werden.

Im Test signalisierte Access Dots zuverlässig und ohne Verzögerung, wenn eine App Kamera, Mikro oder Standort nutzte. Auch die Kamerazugriffe unseres Test-Trojaners „Spycam“, der unbemerkt im Hintergrund Fotos schießt, wurden zuverlässig angezeigt. Wer möchte, kann die Statusfarben beliebig ändern und die Position des Punkts einstellen. Mit der Gratis-Version kann man hierfür die vier Bildschirmecken auswählen. Wer ein „Support Dev Pack“ als In-App-Kauf erwirbt (ab 2,39 Euro), der kann die Position sogar pixelgenau bestimmen. So konnten wir den Punkt präzise neben der Frontkamera platzieren, ähnlich der Kamera-LED der Notebook-Webcam. Zudem fällt mit dem Kauf das Werbebanner auf der Einstellungsseite weg und man unterstützt nicht zuletzt die Weiterentwicklung der App.

Äußerst nützlich ist auch das „Access Log“, in dem Access Dots alle Zugriffe auf notiert. Dort erfährt man nicht nur Zeitpunkt und Dauer, sondern auch, welche App zugegriffen hat. Damit lassen sich Spione leicht überführen. Wünschenswert wäre jedoch eine Filterfunktion: Wer sein Smartphone oder Tablet per Gesichtserkennung entsperrt, findet dort etliche Einträge von System-UI. Dadurch besteht die Gefahr, dass eine spionierende App in der Masse untergeht.

Fazit

Access Dots ist so simpel wie effektiv. Im Test funktionierte die App zuverlässig und ohne Verzögerung. Es ist beruhigend, zu wissen, wann Kamera, Mikrofon oder Standort angezapft werden – und von welchen Apps. Wir wollten den bunten Punkt schon nach kurzer Zeit nicht mehr missen. (rei) c't

Access Dots bei Google Play

ct.de/wc12

Access Dots	
Privacy-App	
Anbieter	IJP
Systemanforderungen	Android 7 oder höher
Preis	Basis-Version **kostenlos**



Bild: Thorsten Hübner

Lauschangriff mit optischem Teleskop

Selbst schalldichte Fenster schützen nicht vor neugierigen Mithörern. Forscher haben feinste Lichtschwankungen einer Bürolampe von außen aufgenommen und in Sprache zurückübersetzt.

Von **Arne Grävemeyer**

Der Vorsitzende im kargen Besprechungsraum ermahnt die Anwesenden: „Nichts von dem heute Gesagten darf diesen Raum verlassen.“ Er hat noch gar nicht wieder Luft geholt, da hat das Leuchtmittel in der Hängelampe seine Worte bereits in Licht kodiert und durchs Fenster sichtbar ausgestrahlt. Und diese Lampe ist nichts Außergewöhnliches: Sie beherbergt beispielsweise eine herkömmliche LED-Leuchte mit E27-Gewinde und zwölf Watt Leistung.

Viele indirekte Abhörtechniken sind in den vergangenen Jahren bekannt geworden. Sie nutzen manipulierte Geräte im Raum oder sie arbeiten mit Lasermikrofonen oder mit hochauflösenden Kameras. Forscher an der Ben-Gurion-Universität des Negev in Israel haben 2020 eine Technik demonstriert, die

Raumschall einfach durch die Beobachtung einer hängenden Deckenlampe im Besprechungsraum mit einem Teleskop von außerhalb aufnimmt. Der weitere technische Aufwand und auch die erforderliche Rechnerleistung sind gering.

Schallwellen in einem Konferenzraum sind Druck- und Dichteschwankungen der Luft. Sie wirken nicht nur auf die Trommelfelle der Anwesenden oder auf Mikrofone ein, sondern auf vielerlei Objekte. Beispielsweise versetzen Schallwellen die unterschiedlichsten Membranen in Vibrationen, etwa die Folie einer Chipstüte, oder sie erzeugen Wellen in einem Glas Wasser. Solche Vibrationen lassen sich beobachten und in Schallwellen zurückübersetzen (siehe S. 111). Ähnlich wirken sich Schallwellen auf Lautsprechermembranen aus, das ist keine Überraschung. Weniger offensichtlich ist, dass Bewegungssensoren etwa in Smartphones schon auf Schallwellen reagieren. Ein manipuliertes Handy kann bei abgeschaltetem Mikrofon immer noch diese Schwingungen aufzeichnen, um daraus später eine Besprechung zu rekonstruieren. Sogar die feine Mechanik einer Festplatte reagiert auf Schall und hat dadurch bereits Forschern als Abhörinstrument gedient (siehe S. 112).



Von einer Fußgängerbrücke aus nahmen die Forscher die Deckenleuchte eines Büros im dritten Stock ins Visier. Aus 25 Meter Entfernung konnten sie damit Gesprächsinhalte belauschen.

Lamphone ist ein passives Verfahren

Viele dieser Möglichkeiten erfordern vom Abhörer zunächst, manipulierte Geräte in Hörweite zu platzieren. Ein Lasermikrofon kommt zwar ohne Eingriffe im Raum aus, der Angreifer muss allerdings aktiv einen Laserstrahl von außen auf eine geeignete Membran richten. Mit optischen Sensoren lassen sich solche Laserstrahlen und deren Reflexionen aber erkennen, um dann den Abhörversuch zu unterbinden.

Die meisten der angesprochenen Abhörtechniken zeichnen Vibrationen auf, die sich in einem zweiten Schritt später mit hoher Rechenleistung wieder in akustische Signale zurückübersetzen lassen. Das jetzt verwirklichte Verfahren einer Gruppe um den Informatiker Ben Nassi ist dagegen passiv, funktioniert auf Entfernung von außerhalb des Besprechungsraums und liefert Ergebnisse in Echtzeit.

Ihre Deckenlampen-Technik nennen die Forscher Lamphone. Ihre Idee: Auftreffende Schallwellen versetzen das Leuchtmittel einer frei schwingenden Hängelampe in Vibrationen. Im Labor statteten die Wissenschaftler eine solche Lampe mit einem Gyroskop aus und maßen bei verschiedenen Lautstärken und Tonfrequenzen Schwingungen um wenige Milligrad, was für die hängende Leuchte im Versuchsaufbau Wegstrecken zwischen 300 und 950 Mikrometer bedeutete.

Für den Beobachter stellten diese Schwankungen Entfernungsunterschiede dar, die im Versuch deutlich messbare Helligkeitsunterschiede hervorriefen. Die offensichtlich im Raum hängende Lampe wird zum mechanisch-optischen Wandler. Um die Helligkeitsschwankungen zu erkennen, nutzten die Forscher Teleskope mit Objektivdurchmessern von 10, 20 und 35 Zentimeter. Auf diese pflanzten sie einen Fotodetektor Thorlab PDA100A2 mit schaltbarer Verstärkung, dessen Fotodiode auftreffendes Licht in eine elektrische Spannung überträgt. Diese Spannung digitalisierte ein 16-Bit-Analog-Digital-Wandler NI-9223 von National Instruments.

In der Entwicklungsumgebung LabVIEW, die echtzeitfähige National-Instruments-Hardware unterstützt, schrieben sie ein Skript, das einen eigenen Equalizer implementierte. Damit gelang es den Forschern, Sprachsignale zu verdeutlichen und beispielsweise hochfrequente Konsonanten etwas hervorzuheben. Zudem bauten sie in ihr Programm eine Rauschunterdrückung ein. Die filtert beispielsweise das Lichtflimmern aus, das mit der doppelten Frequenz der Netz-Wechselspannung auftritt. Letztlich zeigten sie in Versuchen, dass sich mit dem Versuchsaufbau auch überlagerte Tonhöhen erkennen lassen. Beispielsweise erzeugten sie an der Hängelampe parallel fünf Sinuswellen auf 520, 580, 640, 710 und 760 Hertz, die sich anschließend im Spektrogramm wiederfanden.

Per Teleskop abgehört

Mit dieser Konfiguration ließ sich dann ein realitätsnäheres Szenario verwirklichen: Die Forscher visierten mit ihren Teleskopen von einer Fußgängerbrücke aus die Deckenleuchte in einem Konferenzraum im dritten Stock eines nahen Gebäudes an, Entfernung etwa 25 Meter Luftlinie. Im Büro spielten sie zwei Musikstücke ab, „Clocks“ von Coldplay und „Let it Be“ von den Beatles, sowie ein bekanntes Zitat von Donald Trump („We will make America great again“).

Der beobachtete Büroraum ist außer durch das handelsübliche Fensterglas noch durch eine Vorhangfassade geschützt, die das Licht der anvisierten Lampe etwas dämpft. Zudem waren die Abhörer auf der Brücke von Straßenlärm umgeben. Unter der Brücke befinden sich Gleise und eine Bahnstation, der Zugverkehr versetzte die Brücke selbst in Schwingungen.

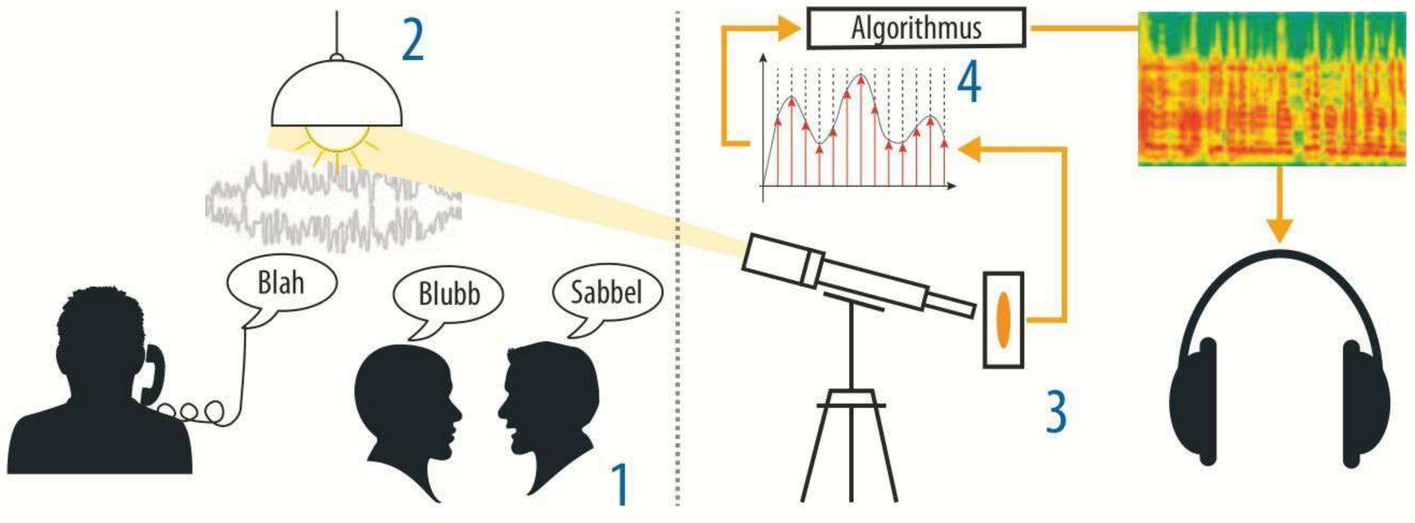
Bei der Analyse der Ergebnisse mussten sich die Forscher nicht auf ihre eigenen subjektiven Eindrücke verlassen. Sowohl Shazam als auch SoundHound erkannten beide Musikstücke, wie sie der Equalizer wiedergab, nach wenigen Sekunden eindeutig. Den Trump-Ausspruch transkribierte Googles Cloud-Speech-to-Text-API akkurat und in Echtzeit. Damit lässt sich Lamphone als Abhörtechnik sogar automatisieren und könnte belauschte Gespräche nicht nur aufnehmen, sondern direkt protokollieren.

Größere Entfernung möglich

Wie bei vielen Abhörtechniken, die Wissenschaftler in den vergangenen Jahren wissenschaftlich belegt und demonstriert haben, denkt man unwillkürlich an deren Einsatz für politische oder wirtschaftliche Spionage. Tatsächlich arbeitete das Team an der Ben-Gurion-Universität unabhängig und mit vergleichsweise kleinem Budget. Ben Nassi und seine Kollegen haben ihr Lamphone 2020 erstmals öffentlich

Jedes Wort ein leichtes Flackern

Ein Lamphone-Angriff: Geräusche und Gespräche im abgehörten Raum (1) erzeugen Schwingungen einer hängenden Deckenlampe (2). Der Lauscher beobachtet die daraus resultierenden Lichtschwankungen mit einem Teleskop (3), leitet das Signal auf einen optischen Sensor und wandelt es digital um (4). Daraus lassen sich wieder akustische Signale erzeugen.



Literatur

[1] The Visual Microphone: Passive Recovery of Sound from Video; Abe Davis, Michael Rubinstein, Neal Wadhwa, Gautham J. Mysore, Frédo Durand und William T. Freeman; Juli 2014, ACM Transactions on Graphics

[2] Gyrophone: Recognizing Speech from Gyroscope Signals; Yan Michalevsky und Dan Boneh, Stanford University; Gabi Nakibly, National Research & Simulation Center; August 2014, 23. USENIX Security Symposium

[3] SPEAKE(a)R: Turn Speakers to Microphones for Fun and Profit; Mordechai Guri, Yosef Solewicz, Andrey Daidakulov und Yuval Elovici; November 2016, Cryptography and Security (cs.CR)

[4] Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone; Andrew Kwong und Kevin Fu, University of Michigan, Wenyuan Xu, Zhejiang University; Mai 2019; Proceedings of the 40th Annual IEEE Symposium on Security & Privacy

[5] Lamphone: Real-Time Passive Sound Recovery from Light Bulb Vibrations; Ben Nassi, Yaron Pirutin, Adi Shamir, Yuval Elovici und Boris Zadov; Juni 2020; Cryptology ePrint Archive

Kamera belauscht Chipstüte

Die Vibrationen, die Schallwellen an alltäglichen Gegenständen hervorrufen, lassen sich mit Highspeed-Kameras aufzeichnen. Das zeigte ein Team um Abe Davis am MIT 2014. Die Forscher nahmen durch ein geschlossenes Fenster beispielsweise Pflanzenblätter auf, Chipstüten oder ein Glas mit Wasser. Die aus den Bildern rekonstruierten Schwingungen ließen sich in Worte zurückübersetzen oder in Musiktitel, die Shazam wiedererkannte.

Allerdings ist die Erkennung hoher Frequenzen durch die Bildrate der Highspeed-Kamera begrenzt. Den Forschern gelangen hohe Erkennungsraten auf Entfernungen bis zu vier Meter. Für die Verarbeitung der hohen Bildrate benötigten sie eine vergleichsweise große Rechnerleistung.



Bild: MIT

Eine unverdächtige Chipstüte dient der Highspeed-Kamera hinter der schalldichten Glasscheibe als Membran und damit als Verräterin der Geräuschkulisse.

Lasermikrofon

Die Technik des Lasermikrofons ist bereits seit den Achtzigerjahren erforscht. Der Angreifer richtet einen Laserstrahl auf eine Membran. Deren Schwingungen lassen sich über die Laufzeitmessung von Laserstrahl und Reflexion berechnen. Als Membran können eine Vielzahl von Gegenständen dienen, von der Chipstüte bis zur Fensterscheibe. Das Lasermikrofon ist mittlerweile eine weithin bekannte Spionagetechnik, um Gespräche von außerhalb eines Raumes mitzuschneiden.

heise Academy
Neue Online-Kurse für IT-Professionals

Web Application Security
Das Security-Training für Entwickler und Webmaster
▸ 82 Videos, 9:30 Std. Spielzeit

Angriffsszenarien im Netzwerk
Der Intensivkurs für die richtigen Verteidigungsstrategien
▸ 71 Videos, 6:30 Std. Spielzeit
Gratis-Lektionen aus allen Kursen anschauen unter:
heise-academy.de

Festplattenkopf vibriert

Magnetische Festplatten haben eine feine Mechanik, um eine hohe Speicherdichte bieten zu können. 2019 zeigte ein Team um Kevin Fu an der University of Michigan, dass der Schreib-Lese-Kopf auf Schallwellen reagiert. Damit lässt sich dessen Mechanik als Mikrofon für Gespräche in unmittelbarer Nähe zur Festplatte einsetzen. Zudem konnten die Forscher zum Teil auf Funktionen der Firmware wie etwa das Position Error Signal zurückgreifen, das feinste Abweichungen zur Spur erkennt. Angesichts der Abtastrate von 15 bis 30 Kilohertz lassen sich allein mit diesen Daten Audioaufnahmen erzeugen. Selbst ein eingeschalteter Lüfter störte das heimliche Mitschneiden von Gesprächen nicht.

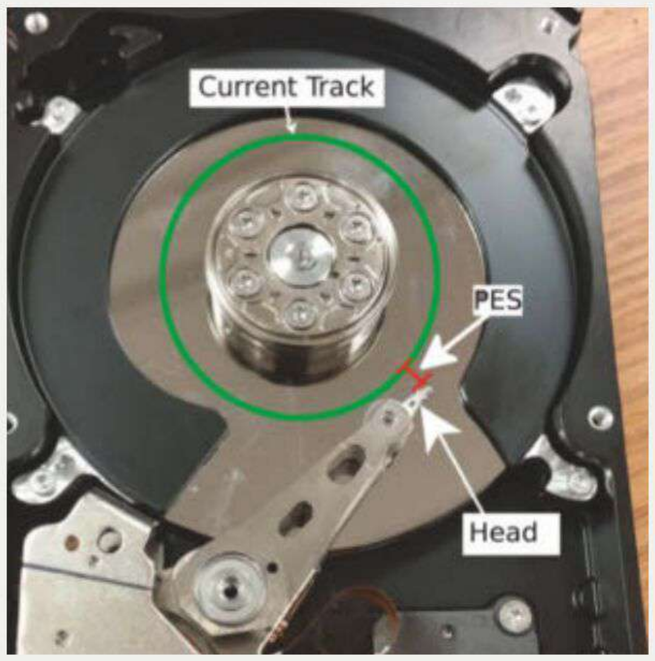


Bild: University of Michigan

Das Position Error Signal (PES) misst die Abweichung des Schreib-Lese-Kopfes von der Spurmitte.

Das Gyroskop zeichnet auf

Wenn eine Smartphone-Anwendung oder eine Website auf Mikrofon oder Kamera zugreifen will, verlangen iOS und Android die explizite Freigabe; für das interne Gyroskop allerdings nicht. 2014 zeigte ein Team um Yan Michalevsky an der Stanford University, dass ein Smartphone damit aber Schallwellen in seiner Umgebung aufzeichnen kann. Angesichts der Abtastrate von bis zu 200 Hertz konnten die Forscher zwar nur einen kleinen Teilbereich des Spektrums menschlicher Stimmen (80 Hertz bis über 10 Kilohertz) abdecken. Es gelang ihnen aber, den Sprecher und mittels neuronaler Netze auch einzelne Wörter zu erkennen. Durch die Erkennung von Schwingungen in drei Achsen lasse sich zudem die Richtung eines Geräuschs bestimmen und dadurch auch unterschiedliche Sprecher unterscheiden.

Die Genauigkeit der Spracherkennung verbesserte sich deutlich, sobald eine attackierende Anwendung einige Sprachbeispiele vom Hauptnutzer gesammelt hatte und damit sprecherabhängig die Worterkennung optimierte. Insbesondere das Abhören von Ziffernfolgen wie beispielsweise einer Kreditkartennummer wurde damit möglich. Die sprecherabhängige Worterkennung steigerten die Forscher zudem, indem sie zugleich auf die Gyroskope mehrerer Smartphones in einem Raum zugriffen. Eine wirksame Abwehrmaßnahme wäre es laut Studie bereits, die Abtastrate des Gyroskops auf maximal 20 Hertz zu begrenzen.

Lautsprecher dient als Mikrofon

Jeden Kopf- oder Ohrhörer kann ein Angreifer in ein Mikrofon umfunktionieren; damit lassen sich dann Gespräche in der Umgebung belauschen. Eine entsprechende Malware hat ein Team um Mordechai Guri von der Ben-Gurion-Universität des Negev bereits 2016 vorgestellt. Lautsprecher und Mikrofone sind letztlich sehr ähnlich aufgebaut. Während ein Lautsprecher durch das magnetische Feld elektrischer Signale eine Membran zum Schwingen bringt, reagiert die Membran eines Mikrofons umgekehrt auf die Druckschwankungen des Schalls und setzt diese in elektrische Impulse um. Tatsächlich enthalten die Chipsätze einiger Soundkarten sogar eine Option zum Funktionswechsel bei Audioports. Ein Angreifer müsste seinen Kopfhörer daher nicht einmal in den Audioeingang umstöpseln, um ihn als Behelfsmikrofon zu missbrauchen.

Mit ihrer Malware konfigurierten die Forscher heimlich die Funktion eines Audioausgangs um. Das funktionierte in Versuchen auch dann, wenn das interne Mikrofon des Computers ausgeschaltet war. Die Klangqualität insbesondere aufgenommener Gespräche ist im Vergleich besser als bei indirekten Methoden. Der Angreifer kann so nicht nur Gesprächsinhalte, sondern auch Stimmen erkennen.

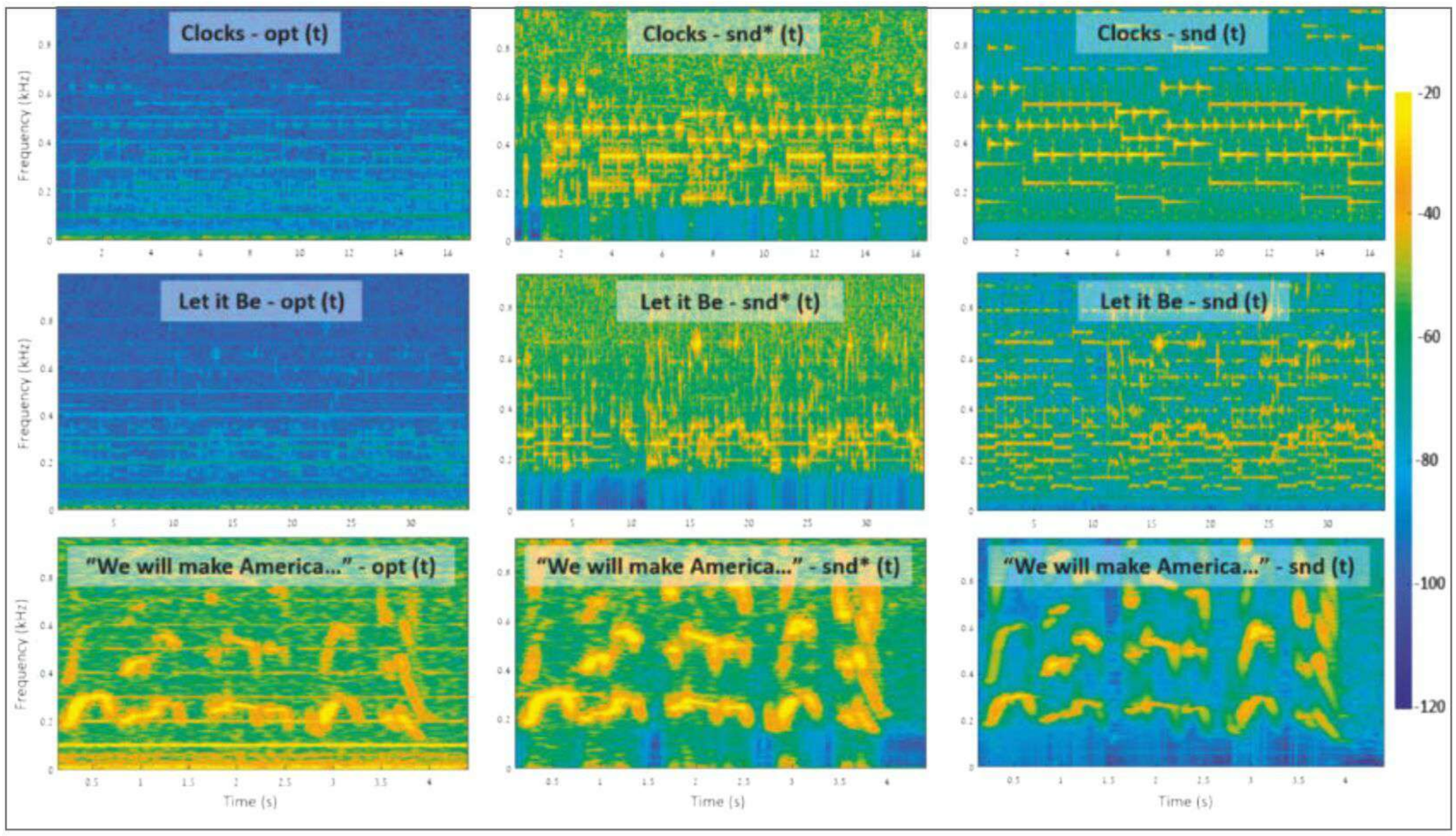


Bild: Ben-Gurion-Universität

Rechts Originalaufnahmen (snd(t)), links die digitalisierten optischen Signale (opt (t)), in der Mitte die im Equalizer wiederhergestellten akustischen Signale (snd* (t)): Die Musiktitel wurden von Shazam wiedererkannt, den Trump-Ausspruch transkribierte das Google-Sprach-API akkurat.

gemacht. Dass gut budgetierte Geheimdienste eine solche oder ähnliche Technik bereits zuvor eingesetzt haben, ist gar nicht so unwahrscheinlich.

„Mit einer höherwertigen Ausstattung lässt sich die Abhörentfernung sicher noch deutlich erweitern“, sagt Ben Nassi. So zeigte sich in den Tests, dass die Lauschergebnisse des Teleskops mit dem größten Objektivdurchmesser die beste Qualität aufwiesen. Ein lichtstärkeres Teleskop, das also einen noch größeren Objektivdurchmesser aufweist, liefert genauere Bilder. Damit sind dann auch größere Abhörentfernungen realisierbar.

Außerdem erwarten die Forscher, dass sich das Signal-Rausch-Verhältnis durch Fotosensoren mit breiterem Ausgangsbereich verbessern lässt. Eine zweite Möglichkeit wäre es, dasselbe optische Signal von mehreren Sensoren mit verschiedenen Abtastraten analysieren zu lassen.

Schließlich ist im Versuch lediglich ein 16-Bit-Analog-Digital-Wandler mit einem Eingangsbereich von -10 bis +10 Volt zum Einsatz gekommen. Damit ergibt sich als kleinster Spannungsschritt etwa ein Wert von 305 Mikrovolt. Ein 32-Bit-Wandler könnte die Schrittweite rein rechnerisch auf ein Nanovolt absenken und so die Empfindlichkeit des Abhörsystems um einige Größenordnungen erhöhen. Damit sollten sich noch feinere Vibrationen einer hängenden Leuchte detektieren lassen. Die Genauigkeit der Abhörergebnisse lässt sich so weiter steigern.

Darüber hinaus weisen die Forscher auf ihr nur kurzes LabVIEW-Skript hin. Durch den Einsatz von neuronalen Netzen beispielsweise ließe sich die Rauschunterdrückung noch deutlich verbessern.

Schutzmaßnahmen

Auf der anderen Seite sehen die Forscher Maßnahmen, um Lamphone-Attacken wirksam abzuwehren. Dazu zählen natürlich dichte Vorhänge oder wenigstens lichtschwächere Leuchtmittel. Für die Verantwortlichen, die Besprechungen nicht bei gedämpftem Licht oder in fensterlosen Räumen abhalten wollen, lautet der Rat, schwerere Lampen einzusetzen. Die würden aufgrund ihrer Masse zumindest weniger vibrieren.

Anstatt nun aber Leuchtmittel nach Gewicht zu kaufen, sollten Architekten für sensible Besprechungsräume künftig besser auf Hängelampen verzichten und stattdessen feste Strahler und indirekte Beleuchtung vorsehen. Ob damit Lamphone-Attacken schon abgewehrt sind, ist allerdings nicht sicher. Das Team um Nassi unternimmt inzwischen Versuche, Besprechungen durch die Fernbeobachtung von dekorativen LED-Blumen zu belauschen. (agr) c't

Video:
Per Teleskop belauscht
ct.de/wzvf

Was Sie über Kryptografie wissen müssen

Weil das Internet vor potenziellen Lauschern nur so wimmelt, müssen Menschen Nachrichten verschlüsselt übertragen. Dass das geht, verdankt die Menschheit den Errungenschaften der Kryptologie, an denen sich auch heutige Supercomputer die Zähne ausbeißen. Eine Einführung auch für Nicht-Mathematiker.

Von **Jan Mahn**



Verschlüsseln statt Vertrauen

Wider die Lauschangriffe	114
(A-)symmetrische Verschlüsselung	116
Sicher durch Falltürfunktionen	122
Wie kryptografische Hashes funktionieren	126
Sichere Kommunikation	132

Bild: Albert Hulm

Es ist eine typische Szene in vielen Kriminalfilmen und Thrillern der letzten Jahre: Der Computer eines Verdächtigen wurde sichergestellt, große Freude beim Ermittlerteam. Doch dann die Ernüchterung, die Daten sind natürlich verschlüsselt. Ein Fall für die Kriminaltechnik; Auftritt für eine Figur, die alle Nerd-Klischees erfüllt, in wenigen Szenen sehr viel Kaffee trinkt und mit hektischem Tippen auf einer Notebooktastatur die Daten wiederherstellt. Mehr als einen Tag lässt sich ein solcher Hacker im Film von der vermeintlich sicheren Verschlüsselung selten aufhalten.

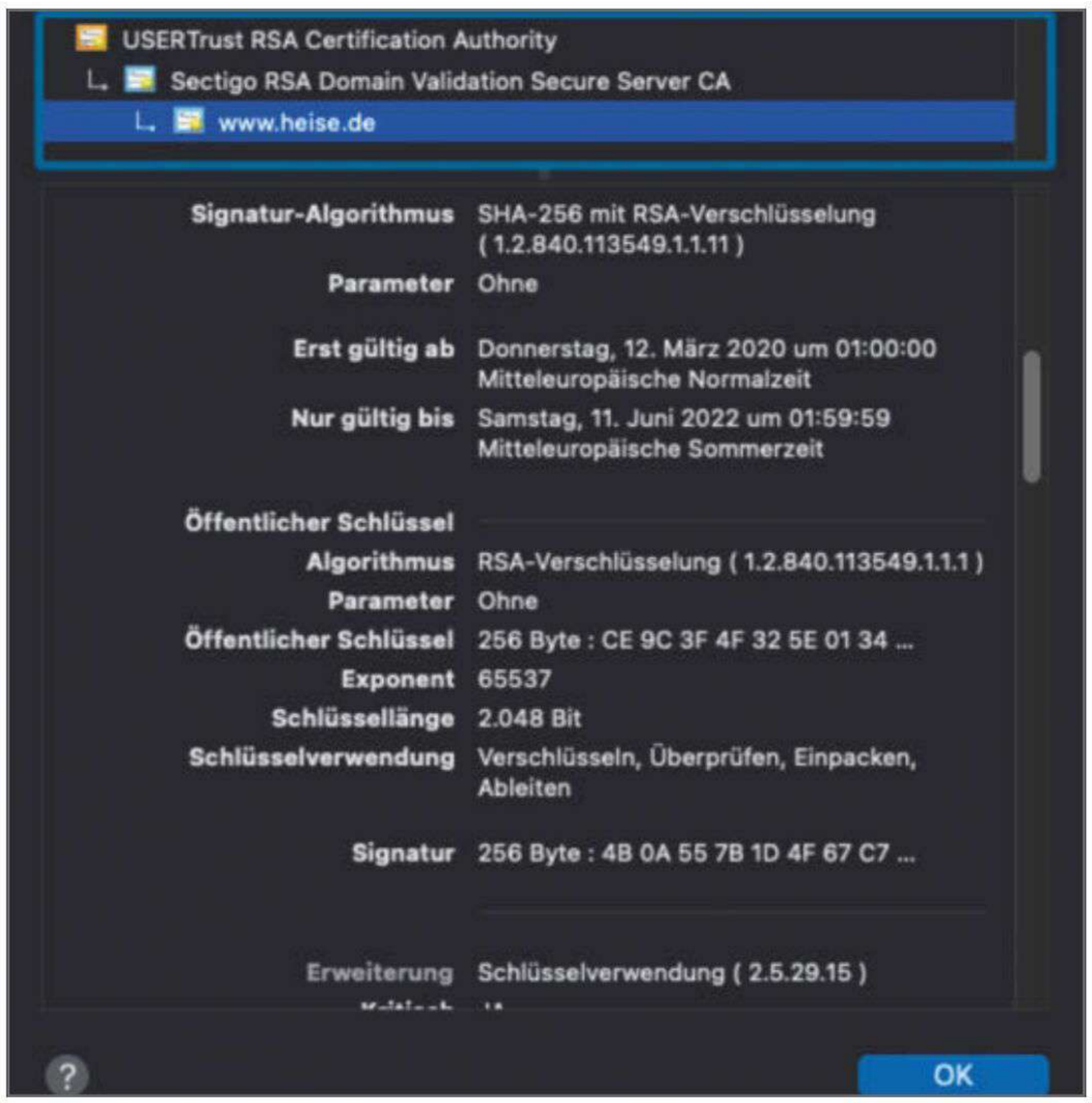
Solche Geschichten prägen das Bild, das Laien von IT-Sicherheit haben: Vor dem neugierigen Partner, den eigenen Kindern oder einem Gelegenheitseinbrecher kann man sich mit Verschlüsselung vielleicht schützen, doch gegen Polizei und Geheimdienst hat man ohnehin keine Chance. Schließlich haben NSA, BND und Mossad doch Superhirne und -computer und können, wenn sie wollen, eh alles entschlüsseln, was auf dem Computer und im Internet passiert. Dieses Misstrauen in die Technik führt zu verhängnisvollen Fehlannahmen. Wenn man keine Chance, gegen „die da oben“ habe, brauche man den Aufwand überhaupt nicht zu treiben, zum Beispiel verschlüsselt zu kommunizieren oder Daten auf der Festplatte mit einer Laufwerksverschlüsselung zu sichern.

In Wahrheit sind moderne Verschlüsselungsverfahren sicherer, als es unseren Geheimdiensten lieb ist. Sofern in den Implementierungen keine mutwilligen Schwächen versteckt sind, sind die Verfahren nach den Erkenntnissen aus jahrzehntelanger Forschung nicht zu knacken. Angriffe gelingen Geheimdiensten vor allem über Viren und soziale Betrügereien (Phishing). Ab Seite 6 lesen Sie, wie Sie möglichst viele Teile Ihrer Kommunikation verschlüsselt abwickeln. Doch was passiert eigentlich genau im Hintergrund, wenn eine Software eine Sitzung mit TLS absichert, Ihr Mailprogramm mit PGP verschlüsselt? Wie werden zwischen Browser und Server Schlüssel über eine unsichere Leitung ausgetauscht? Und warum kann man mit dem heutigen Wissen davon ausgehen, dass auch gigantische Rechenanlagen der Geheimdienste Jahre brauchen, sicher verschlüsselte Informationen wieder lesbar zu machen?

Die folgenden Artikel sollen Antworten auf diese Fragen liefern und richten sich ausdrücklich nicht nur an Mathematiker, sondern an alle Computernutzer. Ab Seite 116 erfahren Sie, was symmetrische und asymmetrische Verfahren ausmacht und wie sie gemeinsam für den Schutz von Geheimnissen im Internet verantwortlich sind. Warum auch Superrechner ein Problem bekommen, wenn sie die Multiplikation von zwei Primzahlen umkehren sollen, erfahren Sie ab Seite 122 – diese Erkenntnisse sind entscheidend für das Vertrauen in asymmetrische Verschlüsselung mit RSA.

Neben dem Verschlüsseln spielt auch das Hashen von Nachrichten eine entscheidende Rolle. Bei digitalen Unterschriften, der Sicherheit von Datei-Downloads und Kennwörtern und spätestens bei Blockchains ist es entscheidend, eine beliebig lange Zeichenkette auf einen kurzen Hash abzubilden. Wie es Hashfunktionen schaffen, eine zufällig wirkende, aber reproduzierbare Zeichenkette zu generieren, erfahren Sie ab Seite 126.

Angst vor höherer Mathematik müssen Sie nicht haben. Viele der Beispiele können Sie sogar mit Zettel, Stift und Kenntnis der Grundrechenarten nachvollziehen. Das ist schon die wichtigste Erkenntnis rund um die Kryptografie: Damit ein Verfahren sicher ist, darf es nicht so gestaltet sein, dass es niemand versteht! Das wäre „security by obscurity“ – ein erwiesenermaßen erfolgloser Ansatz. (jam) c't



Kryptografie begegnet jedem Internetnutzer täglich. Öffnet man eine Website über HTTPS, kommen asymmetrische Verschlüsselung, Schlüsselaustausch und Hashes zum Einsatz.

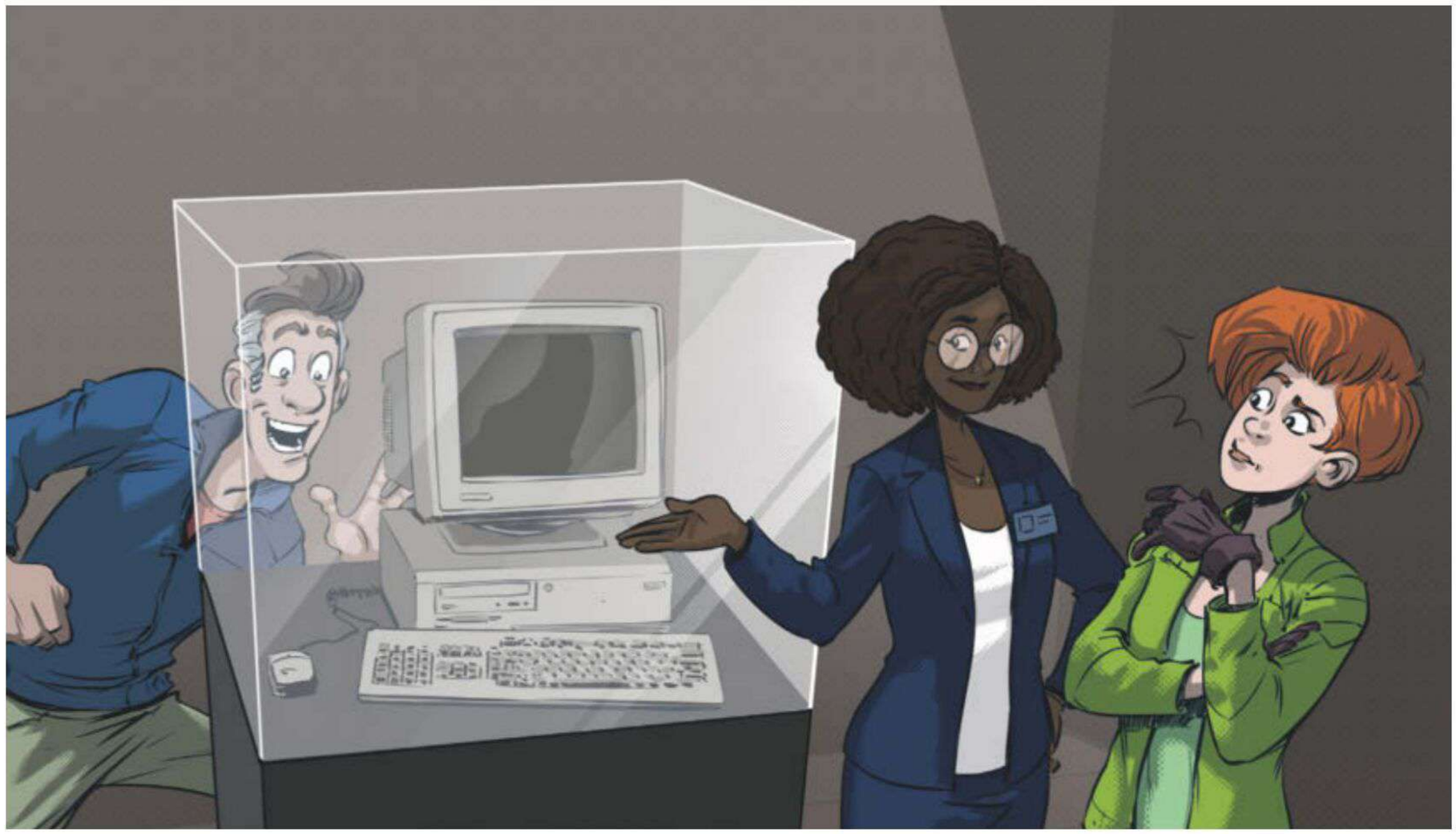


Bild: Albert Hulm

(A-)symmetrische Verschlüsselung

Möchten zwei Partner sicher kommunizieren, müssen sie die Nachrichten verschlüsseln und dazu Schlüssel austauschen. Mit der Zeit wurden die Verfahren dazu immer raffinierter – asymmetrische Verschlüsselung macht sichere Übertragungen im Internet erst möglich.

Von **Jan Kopia**

Vom römischen Feldherren Caesar ist überliefert, dass er bereits ein Verschlüsselungsverfahren verwendet hat, das militärische Nachrichten so verschlüsselt, dass nur Empfänger sie lesen konnten. Dahinter verbarg sich ein sehr einfaches symmetrisches Prinzip, bei dem der Klartext direkt auf den verschlüsselten Text abgebildet werden konnte. Durch Verschieben des Alphabets um drei Stellen wurde etwa aus einem A so ein D, aus einem B ein E. Der Empfänger musste nur wissen, um wie viele Stellen der Sender verschoben hat und die Verschiebung umkehren.

Der Text war damit für denjenigen unlesbar, der dieses System nicht durchschaut hatte. Diese Form der Verschlüsselung ist auch als Verschiebechiffre bekannt und wurde historisch betrachtet häufig verwendet, um Inhalte geheim zu halten. Dabei ist das Verfahren leicht zu knacken, wenn man sich die Buchstabenhäufigkeit der Sprache anschaut, in der ein Text verfasst wurde. In der deutschen Sprache kommt

der Buchstabe E mit etwa 17 Prozent am häufigsten vor, gefolgt vom Buchstaben N mit etwa 9 Prozent, dem I mit 6 bis 7 Prozent. Weitere Analysen, etwa der Buchstabenhäufigkeit beim ersten Wort eines Satzes, lassen noch leichtere Rückschlüsse zu.

Eine Verschiebechiffre ist ein symmetrisches Verfahren, weil der Sender sowie der Empfänger den gleichen Schlüssel brauchen (im Beispiel ist der Schlüssel „3“). Ähnliche Verfahren dienten nach dem Caesar-Verfahren immer wieder als Grundlage für Kryptografie. Erst mit der Erfindung elektrischer Übertragungen hat sich ein größerer Grad an Raffinesse entwickelt. Bis dahin wurden lediglich Zeichen entweder rotiert oder durch ein anders sortiertes Alphabet (zum Beispiel mit einer Chiffrierscheibe) ersetzt.

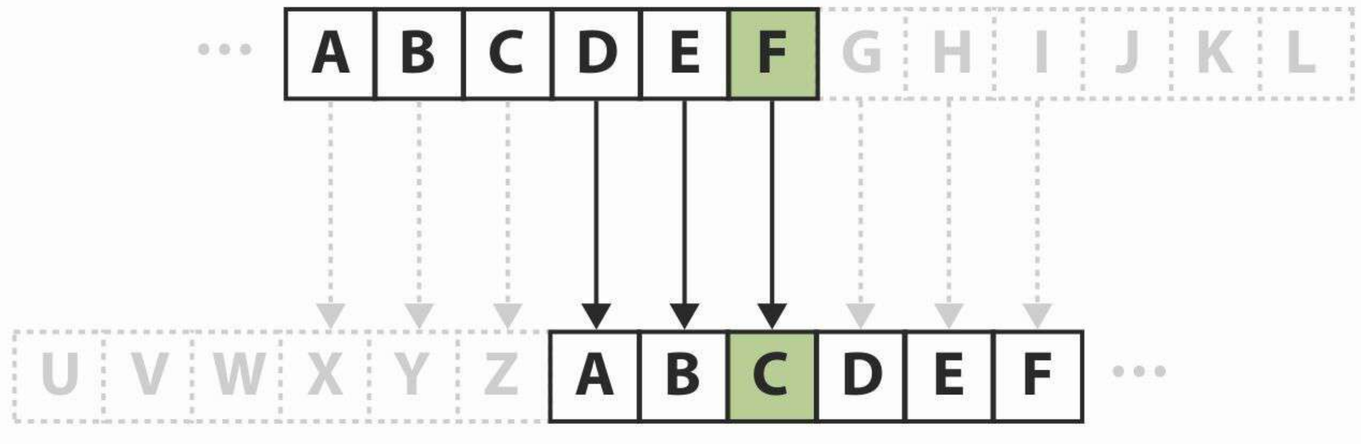
Die Kryptoanalyse nahm ab dem ersten Weltkrieg Fahrt auf. Dort entschieden sich ganze Schlachten auf Basis weniger Informationen. Es entstanden zahlreiche Systeme, die auch in elektromechanische Kryptografiemaschinen umgesetzt wurden. In Deutschland ist vor allem die Enigma bekannt, die mechanisch die Rotation durch Walzensätze umsetzt. Der Trick dabei ist, dass die Walzen sich bewegen und daher einen Buchstaben nicht immer auf denselben anderen Buchstaben abbilden. Dadurch scheitern einfache Verfahren zur Erkennung von Buchstabenhäufigkeiten. Den Engländern gelang es trotzdem, die Nachrichten der Enigma zu entschlüsseln. Möglich wurde das durch aufwendige mathematische Analysen, für die später auch abgefangene Enigma-Maschinen genutzt werden konnten. Eine Voraussetzung war die Kenntnis der elektrischen Verdrahtung sowie die Walzenanzahl in der Maschine. Sind diese Punkte nicht bekannt, ist das eingesetzte Verfahren der Enigma nur mit großen Rechenleistungen zu bewältigen, die erst heutige Computertechnik bietet. Tatsächlich wurden einige im zweiten Weltkrieg mit Enigma verschlüsselte Texte erst 2005 erfolgreich entschlüsselt.

Moderne symmetrische Verfahren

Jahrzehnte später, digital arbeitende Computer hatten inzwischen elektromechanische Geräte ersetzt, wurde 1976 das Verfahren „Data Encryption Standard“ (DES) zur behördlichen Verschlüsselung in den USA entwickelt. Es basiert auf einem Block-Chiffre-Verfahren, das so heißt, weil es einen Block von Zeichen des Klartexts in einen Block von Zeichen eines Geheimtextes umwandelt: Der Sender zerlegt eine Nachricht in 64-Bit-Blöcke, zerlegt diese in eine linke und eine rechte Hälfte und chiffriert diese in 16 Durchläufen auf Basis eines 56 Bit langen Schlüssels. Mathematisch kommen sogenannte Permutationen (Vertauschungen) und ein Feistel-Netzwerk, benannt nach dem IBM-Mitarbeiter Horst Feistel, zum Einsatz. Von ihm stammt die Idee mit den 32-Bit-Halbblöcken. Dasselbe Verfahren nutzt der Empfänger zum Entschlüsseln, wobei er die Reihenfolge einfach umdreht und den Rundenzähler rückwärts zählt. Auch DES ist

Verschiebechiffre

Die Verschiebechiffre (auch Caesar-Verschlüsselung) ist die einfachste symmetrische Verschlüsselung. Zum Verschlüsseln werden die Buchstaben des Alphabets auf ein verschobenes Alphabet abgebildet. Wer weiß, um wie viele Stellen verschoben wurde, kann den Text wieder entschlüsseln.



also eine symmetrische Verschlüsselung und wurde ab den Achtzigern viel benutzt.

Die wesentliche Schwäche von DES ist die Schlüssellänge von nur 56 Bit. Der Inhalt der Nachrichten kann mit einem modernen Rechner und bloßem Ausprobieren (Brute-Force-Attacke) in einigermaßen kurzer Zeit entschlüsselt werden. Nur unwesentlich verbessert wurde das Verfahren mit 3DES (Triple DES). Anstatt sich ein neues Verfahren zu überlegen, wird DES einfach nacheinander mit drei verschiedenen Schlüsseln ausgeführt, was die Schlüssellänge auf 168 Bit anhebt. DES und 3DES werden heute noch teilweise in der Verschlüsselung von Funkverbindungen verwendet, gelten jedoch im Sinne sicherer Kryptografie als ungeeignet.

Als Nachfolger von DES trat im Jahr 2000 der Advanced Encryption Standard (AES) als sicheres symmetrisches Verschlüsselungsverfahren an [1]. Es basiert ebenfalls auf Blöcken. Zum Einsatz kommt der Rijndael-Algorithmus, der mit variablen Schlüssellängen von 128, 160, 192, 224 oder 256 Bit arbeitet. AES findet bis heute Anwendung in verschiedenen Protokollen, die alltäglich genutzt werden. Dazu gehören die Verschlüsselung von WLAN-Verbindungen mit WPA2 oder die Kommunikation über SSH. AES gilt ab einer Schlüssellänge von 192 Bit bis heute als sicher, da das Knacken per Brute-Force-Attacke trotz der Rechenleistung moderner Hardware eine erhebliche Zeit in Anspruch nehmen würde.

Das Problem mit den Schlüsseln

Alle symmetrischen Verfahren haben allerdings dasselbe Problem: Die übermittelte Nachricht wird mit demselben Schlüssel entschlüsselt, mit dem sie auch verschlüsselt wurde. Beide Partner müssen sich also ein gemeinsames Geheimnis teilen.

Das macht die Verfahren nicht grundsätzlich unsicher, aber die Tatsache, dass ein Schlüssel den Weg vom Sender zum Empfänger finden muss, birgt das Risiko, dass er abgefangen werden könnte. Viele Nutzer werden separate Übertragungswege für gemeinsame Geheimnisse kennen und schon genutzt haben – man verschickt zum Beispiel ein sicher mit AES-256 verschlüsseltes ZIP-Archiv als E-Mail-Anhang und überträgt das Kennwort separat in einer (unverschlüsselten) SMS oder diktiert es am Telefon. Das ist umständlich und auch nicht absolut sicher. Das wäre es nur, wenn der Übertragungsweg für das Kennwort nicht abgehört werden könnte – man müsste das Gegenüber zum Beispiel allein und ohne möglicherweise mithörendes Handy auf einem Golfplatz treffen und ihm das Kennwort zuflüstern. Dann könnte man aber auch gleich einen Stick mit der Zip-Datei übergeben.

Dieses Problem war Anlass für eine neue Idee, die erst in den 70ern des letzten Jahrhunderts aufkam: 1974 erdacht und 1978 veröffentlicht, entstand eines der ersten asymmetrischen Verfahren durch die Mathematiker Merkle und Hellman („Merkle-Hellman-Kryptosystem“), gefolgt von dem in 1976 von Whitfield Diffie und Martin Hellman veröffentlichten Diffie-Hellman-Schlüsselaustausch. Ziel war der Austausch eines geheimen Schlüssels über einen unsicheren Kanal, ohne eine Kompromittierung befürchten zu müssen. Merkle, Hellman und Diffie gelten damit als Pioniere der asymmetrischen Kryptografie. 1977 folgte das asymmetrische Verschlüsselungsverfahren RSA, benannt nach den Anfangsbuchstaben der Erfinder Rivest, Shamir und Adleman. Das Verfahren löste gleich mehrere Probleme: Schlüsselübertragung, Verschlüsseln, Entschlüsseln und Signieren.

Allen asymmetrischen Verfahren liegt die Idee zugrunde, geheime Informationen über öffentliche Kanäle zu übertragen, ohne das Schutzniveau des Schlüssels oder des Inhalts zu beeinträchtigen. Man bezeichnet diese Verfahren als Public-Key-Kryptografie, weil es bei allen Verfahren einen öffentlichen Schlüssel, also eine öffentliche Teilinformation gibt, die jeder einsehen kann. Diese kann problemlos über das Internet oder sonstige Kanäle (zum Beispiel per Funk oder Telefon) übertragen werden.

Die Grundprinzipien asymmetrischer Verschlüsselung sind:

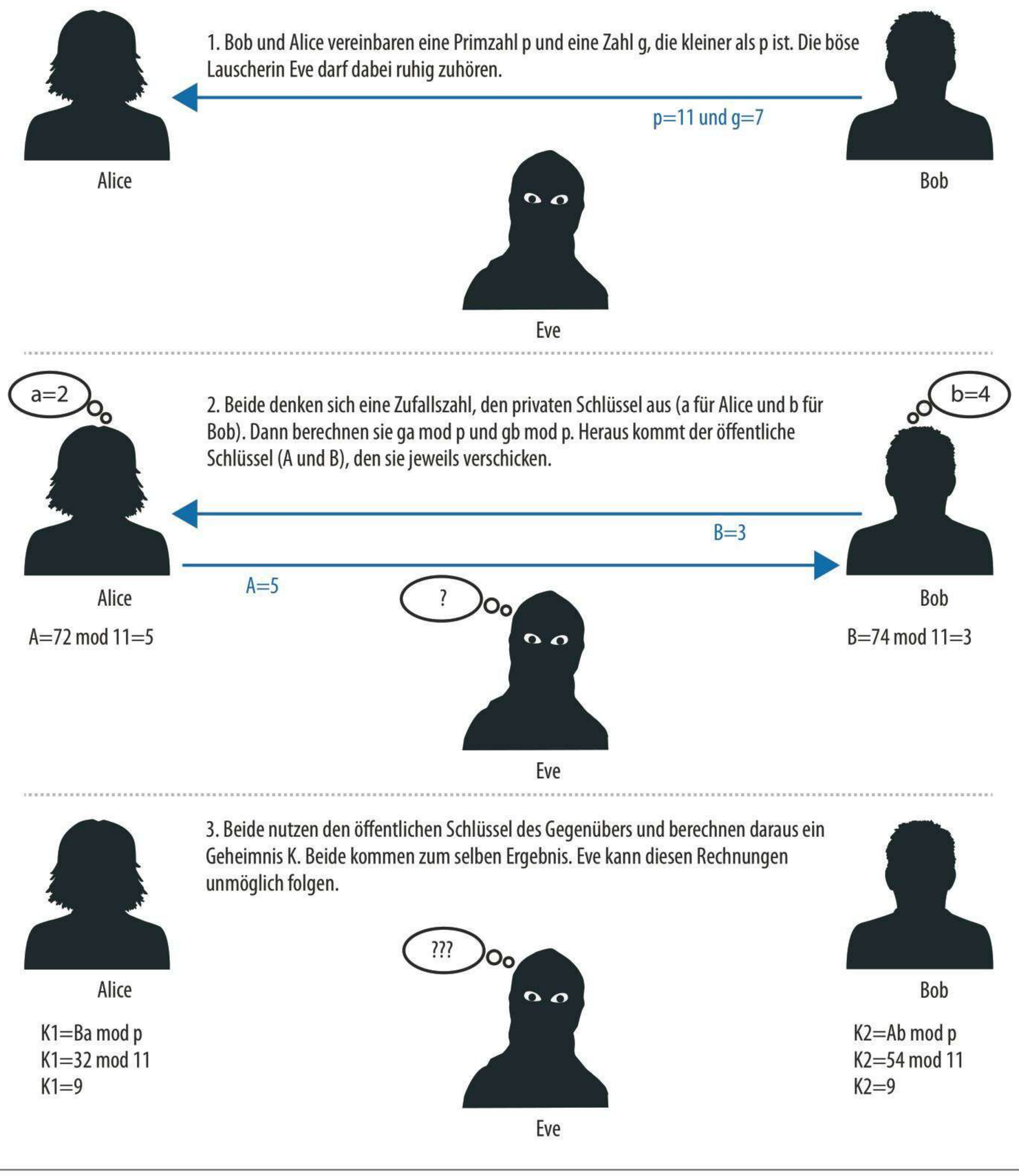
- Jeder Kommunikationspartner hat zwei Schlüssel: Einen öffentlichen Schlüssel und einen privaten Schlüssel. Beide Schlüssel zusammen werden als Schlüsselpaar bezeichnet.
- Der öffentliche und der private Schlüssel sind mathematisch verwandt – sie werden gemeinsam generiert, wobei irgendeine Form von Zufall zum Einsatz kommt.
- Den öffentlichen Schlüssel darf jeder sehen, er kann problemlos übertragen werden.
- Der private Schlüssel wird unter allen Umständen geheim gehalten, also wirklich niemandem verraten.
- Nachrichten werden mit dem öffentlichen Schlüssel des Kommunikationspartners verschlüsselt und können nur mit dessen privatem Schlüssel – und damit nur von ihm – wieder entschlüsselt werden.

Es gibt noch eine weitere wichtige Anwendung von asymmetrischer Kryptografie, die durch die Schlüsselpaare nebenbei abfällt: Durch den privaten Schlüssel kann man eine digitale Signatur erzeugen. Nur der Besitzer eines privaten Schlüssels kann eine solche Signatur produzieren, aber jeder, der den öffentlichen Schlüssel besitzt, kann sie überprüfen. Damit gleicht eine solche Signatur einer Unterschrift.

Zum Signieren verschlüsselt man die Nachricht (oder einen Hash davon – siehe Seite 126) mit dem

Diffie-Hellman-Schlüsselaustausch

Um ein gemeinsames Geheimnis für weitere Verschlüsselung auszuhandeln, führen Alice und Bob einen Schlüsselaustausch nach Diffie und Hellman aus. Die Leitung, über die sie kommunizieren, ist ungeschützt, sodass die Lauscherin Eve zuhören kann. Aus den übermittelten Daten kann sie aber nicht auf das gemeinsame Geheimnis schließen.



eigenen privaten Schlüssel. Das Ergebnis wird als Signatur bezeichnet und an die Nachricht angehängt. Jeder Empfänger, der den öffentlichen Schlüssel besitzt, kann dann die Korrektheit der Signatur prüfen: Falls er sie mit dem öffentlichen Schlüssel wieder entschlüsseln kann, weiß er, dass der Inhaber des privaten Schlüssels die Signatur erzeugt haben muss. Und falls die entschlüsselte Signatur mit der Nachricht (oder ihrem Hash) übereinstimmt, kann die Nachricht nicht manipuliert worden sein. Die Nachricht ist damit authentisch und nicht abstreitbar.

Asymmetrische Verfahren

Häufig verwendete asymmetrische Verfahren sind vor allem RSA und der Diffie-Hellman-Schlüsselaustausch. Der Diffie-Hellman-Schlüsselaustausch löst das Problem des sicheren Austauschs eines Schlüssels. Die Idee besteht darin, dass sich die beiden Partner über eine ungesicherte Verbindung auf einen Schlüssel einigen, aber ein Unbefugter aus diesen Nachrichten nicht auf den geheimen Schlüssel schließen kann. Das klingt nach Magie, ist aber nur Mathematik. Voraussetzung für den Schlüsselaustausch sind sogenannte Einwegfunktionen – wie sie funktionieren, lesen Sie ab Seite 122.

Diffie-Hellman mit Bob und Alice

Die klassischen Beispielpersonen für Kryptografie-Erklärungen heißen seit jeher Alice und Bob. Der böse Lauscher oder die böse Lauscherin heißt meist Eve. Alice und Bob, die Nachrichten über eine unsichere Verbindung austauschen wollen und dafür ein gemeinsames Geheimnis brauchen, einigen sich zunächst öffentlich auf eine gemeinsame Primzahl p und den sogenannten Generator, eine natürliche Zahl mit dem Namen g, die kleiner als p ist. Wer wem die Zahlen vorschlägt, ist unerheblich. Sie können bedenkenlos über unsichere Kanäle geschickt werden oder in der Krypto-Software hartkodiert sein.

Für ein Beispiel reichen sehr kleine Zahlen, etwa p = 11 und g = 7, reale Anwendungen benötigen größere Zahlen, um Brute-Force-Angriffe zu verhindern.

Alice beginnt und denkt sich als privaten Schlüssel eine Zahl a aus, die größer als 1 und kleiner als p ist. Auch Bob überlegt sich eine solche Zahl (b). Unter keinen Umständen werden diese privaten Schlüssel verschickt! Im Beispiel nimmt Alice a = 2 und Bob b = 4.

Alice beginnt und berechnet folgende einfache Gleichung für den öffentlichen Schlüssel A:

$$A = g^a \mod p$$

Für die Beispielwerte also:

$$A = 7^2 \mod 11 \quad \Rightarrow \quad A = 5$$

Diesen Wert A schickt sie Bob. Der generiert sich zunächst einen öffentlichen Schlüssel (B) mit derselben Formel und schickt ihn an Alice:

$$B = 7^4 \mod 11 \quad \Rightarrow \quad B = 3$$

Jetzt folgt der wahre Kern des Verfahrens: Beide Partner setzen die erhaltenen öffentlichen Schlüssel des anderen in eine Gleichung ein, um den gemeinsamen Schlüssel K zu erhalten. Alice nimmt die Gleichung:

$$K_A = B^a \mod p$$

Und Bob äquivalent:

$$K_B = A^b \mod p$$

Beide nutzen also den öffentlichen Schlüssel des Gegenübers und als Exponenten ihren eigenen privaten Schlüssel.
Heraus kommt für Alice:

$$K_A = 3^2 \mod 11 \quad \Rightarrow \quad K_A = 9$$

Und für Bob:

$$K_B = 5^4 \mod 11 \quad \Rightarrow \quad K_B = 9$$

Beide können jetzt mit der 9 als gemeinsamem Geheimnis arbeiten. Es lohnt sich, diese Schritte einmal mit Stift und Zetteln nachzuspielen und mit eigenen Zahlen nachzurechnen. Beeindruckend zu sehen ist, dass ein Zuschauer, der die geheimen Schlüssel nicht gesehen hat, keine Chance hat, den Rechnungen zu folgen. In der Realität sind die Zahlen wesentlich größer – viel größer. Um die Sicherheit des Verfahrens zu erhöhen, gibt es auch an den Generator g noch weitere Anforderungen.

Sicher mit RSA

RSA ist mathematisch komplexer als ein Diffie-Hellman-Schlüsseltausch. Es basiert auch auf Einwegpermutationen mit Falltür. Dabei geht es um die Zerlegung großer Zahlen in ihre Primfaktoren, was rechnerisch ein großes Problem darstellt. Umgekehrt ist es leicht, Primfaktoren zu großen Zahlen zu multiplizieren. In Kombination ist das gut geeignet, um Daten leicht zu verschlüsseln, aber die Verschlüsselung nur schwer knacken zu können. Wie das im Detail funktioniert, lesen Sie ab Seite 122.

Die Sicherheit der Schlüssel hängt dabei von der Faktorisierung der großen Zahl ab. So bestimmt die Schlüsselgröße auch die Verschlüsselungsstärke: Mit der Schlüssellänge nimmt die Verschlüsselungsstärke zu. RSA-Schlüssel haben typischerweise eine Länge von 1024, 2048 oder 4096 Bit.

Weitere asymmetrische Verfahren sind der 1991 entwickelte Digital Signature Algorithm (DSA) sowie die Verfahren, die auf elliptischen Kurven basieren (ECC): Elliptic-Curve Diffie-Hellman (ECDH) und Elliptic Curve Digital Signature Algorithm (ECDSA). Während DSA keine wesentlichen Neuerungen brachte, wurde mit der Einführung von ECDH/ECDSA das Sicherheitsniveau von kryptografischen Verfahren bei gleichzeitiger Reduktion des Ballasts erhöht. So lässt sich laut NIST (dem US-Pendant zum deutschen DIN) mit 160 Bit Schlüssellänge ein ähnliches Sicherheitsniveau erreichen wie mit 1024 Bit bei RSA oder herkömmlichem Diffie-Hellman. Kürzere Schlüssel führen im Allgemeinen zu weniger Berechnungsaufwand und damit schnellerer Ausführung, obwohl die Kalkulationen selbst durchaus komplexer sind. ECC wird beispielweise beim neuen Personalausweis in Deutschland oder bei TLS eingesetzt.

Symmetrische und asymmetrische Verfahren sind keine Konkurrenten. Keins ist besser als das andere – sie lösen unterschiedliche Probleme und arbeiten auch gut im Team.

Die Mischung machts

Bei asymmetrischen Verfahren muss man keinen geheimen Schlüssel übertragen – ein Vorteil gegenüber symmetrischen Verfahren. Die Ver- und Entschlüsselung kostet jedoch etwas mehr Rechenkapazität. Große Datenmengen oder schnell auszuführende Verschlüsselung beim konstanten Übertragen von Daten wie dem Surfen im Internet, wird daher vorzugsweise mit symmetrischen Verfahren realisiert. In der Praxis werden einfach beide Verfahren kombiniert: Bei hybriden Verschlüsselungen kommt das asymmetrische Verfahren lediglich zum Tausch des geheimen Schlüssels zum Einsatz. Dieser geheime Schlüssel wird dann für eine symmetrische Verschlüsselung verwendet. Beispiele sind unter anderem die E-Mail-Verschlüsselung mit PGP, bei der der Klartext zunächst mit einem symmetrischen Schlüssel verschlüsselt wird und dieser dann mit dem öffentlichen Schlüssel des Empfängers. Beide Informationen können nun sicher übertragen werden. Der Empfänger geht den Weg rückwärts und entschlüsselt erst den symmetrischen Schlüssel mit seinem privaten Schlüssel und kann dann den eigentlichen Text mit einem symmetrischen Verfahren entschlüsseln. Hierbei kommen zum Beispiel RSA und AES zum Einsatz. Auf ähnliche Art und Weise wird der Session Key im Webbrowser mittels TLS ausgehandelt und dann genutzt, um den Datenstrom symmetrisch zu verschlüsseln.

Verschlüsselung muss sich ständig der Realität anpassen und kein Verfahren wird ewig halten. Schließlich werden auch die Rechner immer leistungsstärker und es wird wahrscheinlicher, dass man verschlüsselte Nachrichten in endlicher Zeit knacken kann. Wer den Überblick behalten will, welche Algorithmen und Bitlängen aktuell als sicher gelten, sollte alle paar Jahre einen Blick in Standards wie TR-02102 des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), SP-800 des amerikanischen NIST oder die Reports des europäischen ECRYPT-CSA werfen (alle Dokumente zu finden über ct.de/w1y5).

In den letzten Jahren ist das Bewusstsein für verschlüsselte Kommunikation bei den Betreibern von Diensten zum Glück stark gestiegen. Noch vor wenigen Jahren war HTTPS im Web keine Normalität, nun warnt jeder Webbrowser bei unverschlüsselten HTTP-Verbindungen. Das soll unbedarfte Nutzer bewusst verstören und so die Seitenbetreiber animieren, HTTPS einzusetzen, wenn sie keine Besucher verlieren wollen. (jam) c't

Literatur

[1] Oliver Lau, **Spezialkommando**, Schnelle AES-Chiffres mit Intrinsics, c't 14/2013, S. 174

Standards

ct.de/w1y5



Bild: Albert Hulm

Sicher durch Falltürfunktionen

Große Primzahlen miteinander zu multiplizieren ist für Computer keine Herausforderung. Aus dem Ergebnis der Multiplikation wieder auf die Primzahlen zu schließen dagegen schon – auch für Supercomputer. Solange das so bleibt, ist asymmetrische Verschlüsselung wie RSA sicher.

Von **Wilhelm Drehling**

Die Zahlen 3323 und 2281 sind Primzahlen. Sie zu multiplizieren ist keine große Herausforderung und zur Not mit Zettel und Stift ganz ohne Taschenrechner zu schaffen: 7.579.763 ist das Ergebnis. Stellt man einem Menschen dagegen die Aufgabe, die zwei Primzahlen zu finden, die multipliziert 7.579.763 ergeben, vergeht den meisten selbst mit einem Taschenrechner der Spaß. Um die passenden Primzahlen zu finden, muss man nämlich wohl oder übel ausprobieren: Kann man die Zahl durch 3 teilen? Nein. Auch nicht durch 5, 7, 11 oder 13? Sehr viele Probedivisionen sind nötig, bis man

endlich bei der Primzahl 2281 angekommen ist und sogleich weiß, dass 2281 und 3323 die gesuchten Primfaktoren sind.

Weil der Hinweg einer solchen Primzahlmultiplikation so einfach, der Rückweg, also die Faktorisierung, aber so aufwendig ist, spricht man von einer Falltürfunktion. Diese Funktionen gehören zu den Einwegfunktionen und tun das, was ihr Name verspricht: In eine Richtung sind sie einfach zu berechnen, doch der Rückweg ist nicht möglich, solange man eine zusätzliche Information, die sogenannte Falltürinformation, nicht kennt. Eine Falltürfunktion im Alltag findet man an jeder Hauswand: Der Postbote wirft ohne Mühe einen Brief in einen Briefkasten. Ihn herauszubekommen ist schwierig, es sei denn, man hat den Schlüssel zu dem Briefkasten.

RSA: Sicher durch Primzahlen

Schwer zu knacken soll auch Verschlüsselung digitaler Kommunikation sein. Daher nutzt das asymmetrische Verschlüsselungsverfahren RSA genau dieses mathematische Problem, das Faktorisierungsproblem. Wie asymmetrische Verfahren wie RSA funktionieren und welche Relevanz sie im Alltag haben, erfahren Sie ab Seite 114. Ein Nutzer, der ein Schlüsselpaar aus öffentlichem und privatem Schlüssel braucht, lässt den Computer zwei große Primzahlen p und q zufällig suchen, die die gleiche Größenordnung haben, aber nicht zu nah beieinander liegen. Das Ergebnis der Multiplikation p·q wird RSA-Modul (N) genannt und ist der wesentliche Bestandteil des öffentlichen Schlüssels, den man mit der ganzen Welt teilen darf.

Zugegebenermaßen ist das etwas vereinfacht – um ganz genau zu sein, wird noch die Eulersche-Funktion von N berechnet und eine zu (N) teilerfremde Zahl e bestimmt, um den öffentlichen Schlüssel zu bilden. Der private Schlüssel besteht ebenfalls aus N und der Komponente d, die man mit Kenntnis von (N) und e berechnet. Das ist aber nicht der Kern der Sache: Entscheidend für die Sicherheit ist die Primzahlmultiplikation p·q. Sobald es gelänge, diese aus dem öffentlich zugänglichen N zu rekonstruieren, könnte ein Angreifer den privaten Schlüssel generieren und RSA wäre unbrauchbar.

Die Länge zählt

Wie lange es dauert, die passenden Primzahlen durch Ausprobieren zu finden, hängt von der Länge der multiplizierten Primzahlen und der Hardware ab, die potenzielle Angreifer zur Verfügung haben.

Als Rivest, Shamir und Adleman RSA 1977 entwarfen, gingen sie von der damals verfügbaren Hardware aus und kamen zu dem Schluss, dass es schon ausreiche, zwei Primzahlen mit 100 Stellen miteinander zu multiplizieren. Mit der ihnen bekannten Hardware war es dann unvorstellbar, solange alle möglichen Kombinationen zu prüfen, bis man auf die verwendeten Primzahlen stoßen würde.

In ihren Berechnungen kamen sie zum Ergebnis, dass ein damals aktueller Computer 3,8 Milliarden Jahre dafür brauchen würde, über einen solchen Brute-Force-Angriff, also stumpfe Gewalt, die pas-

Table 1

Digits	*Number of operations*	*Time*
50	1.4×10^{10}	3.9 hours
75	9.0×10^{12}	104 days
100	2.3×10^{15}	74 years
200	1.2×10^{23}	3.8×10^{9} years
300	1.5×10^{29}	4.9×10^{15} years
500	1.3×10^{39}	4.2×10^{25} years

We recommend that n be about 200 digits long. Longer or shorter lengths can be used depending on the relative importance of encryption speed and security in the application at hand. An 80-digit n provides moderate security against an attack using current technology; using 200 digits provides a margin of safety against future developments. This flexibility to choose a key-length (and thus a level of security) to suit a particular application is a feature not found in many of the previous encryption schemes (such as the NBS scheme).

Vor mehr als 40 Jahren empfahlen die Erfinder von RSA eine optimale Länge von 200 Ziffern [1].

senden Primzahlen zu finden. Auf Seite 123 sehen Sie einen Auszug aus der originalen Arbeit mit den Berechnungen zur Laufzeit. Doch die Computertechnik entwickelte sich bekanntlich weiter und über einige Jahrzehnte galt das Moore'sche Gesetz, nach dem sich die Leistungsfähigkeit von Prozessoren nach etwa 18 Monaten verdoppelt. Damit stimmten die Annahmen aus den 70ern schnell nicht mehr.

Und so ist es nicht überraschend, dass Forscher sehr bald begannen, das RSA-Kryptosystem mithilfe der jeweils aktuellen Hardware anzugreifen. Überzeugt, dass die eingesetzte Falltürfunktion ausreichend sicher sei, rief RSA Security, das Unternehmen von Rivest, Shamir und Adleman, 1991 die RSA-Factoring-Challenge ins Leben und lobte Preisgelder von bis zu 200 000 US-Dollar aus. Zu knacken waren 54 verschiedene RSA-Module zwischen 330 Bit (N mit 100 Stellen) und 2048 Bit (N mit 617 Stellen) Länge. 2007 beendeten die Organisatoren die Challenge vorzeitig, da sich langsam abzeichnete, dass die wirklich großen Zahlen beinahe unmöglich zu lösen sein werden und RSA ausreichend sicher ist. Genau das zu beweisen war das Ziel des Wettbewerbs.

Eine kleine rege Community aus Wissenschaftlern hat dennoch nicht aufgegeben – obwohl kein Preisgeld mehr winkt – und wendet Tausende Prozessorjahre auf, um diese großen Zahlen aus dem Wettbewerb in ihre Primzahlen aufzulösen. Ein Team um den französischen Informatiker Paul Zimmermann schaffte es im Februar 2020, die bisher höchste Zahl aus dem Wettbewerb aufzulösen. Den Forschern gelang die Zerlegung von RSA-250, also einer 829 Bit langen Zahl. Selbst mit einem leistungsstarken, 2000 Euro teuren Intel Xeon Gold 6130 mit 2,1 GHz benötigt man dafür ungefähr 2700 Prozessorjahre.

Dass selbst große Supercomputer kaum eine Chance haben, zeigt die Auflösung des etwas kleineren RSA-232 (768 Bit). Russischen Wissenschaftlern gelang am 17. Februar 2020 mithilfe der beiden Supercomputer „Lomonosov" und „Zhores", die Zahl mit beträchtlichem Aufwand zu knacken. Umgerechnet auf einen Intel Xeon Gold entpricht die aufgewendete Rechenleistung knapp 50 Prozessorjahren.

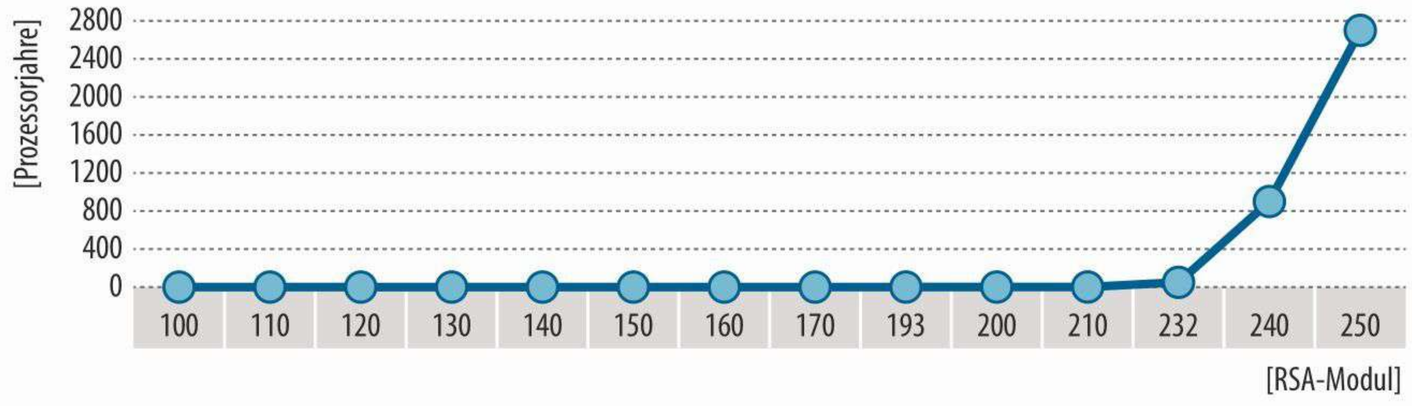
Zum heutigen Zeitpunkt gilt RSA mit einer Länge von 2048 Bit noch gerade so als sicher. Das entspricht einer Länge von 617 Dezimalstellen für N. Jede Primzahl hat dann eine Länge von ungefähr 308 Stellen, und auch Superrechner, die im Cluster zusammen am Faktorisieren arbeiten, sind noch weit von einem Erfolg entfernt. 2048 Bit sollte man dennoch in heutiger Kommunikation als absolute Untergrenze betrachten, um auch für die Zukunft gerüstet zu sein. Mittlerweile empfiehlt unter anderem das BSI, für Zertifikate auf Schlüssellängen von 4096 Bit zu setzen.

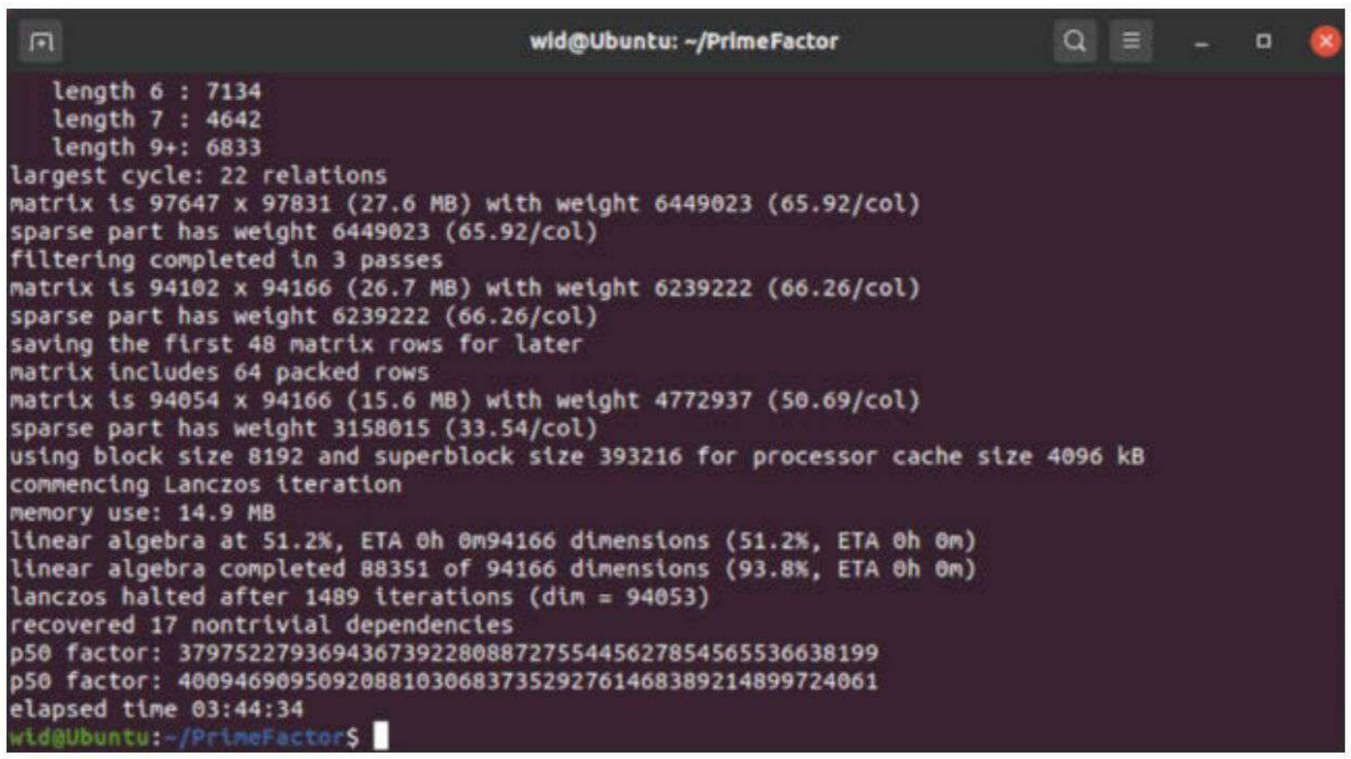
Probieren und probieren lassen

Sollten Sie beim Lesen immer noch nicht glauben, dass Computer bei dieser vermeintlich einfachen Aufgabe wirklich so lange brauchen, können Sie das

RSA Factoring Challenge

Ein RSA-Modul ist die Multiplikation zweier sehr großen Primzahlen. In der „RSA Factoring Challenge" sind 54 Module von der RSA Company ausgeschrieben worden. Diese reichen von RSA-100 (330 Bit) bis RSA-617, welches dem Standard von 2048 Bit entspricht. Wissenschaftler knackten in den letzten zwei Jahrzehnten die kleinsten 23.





Die Kombination der beiden Spezialwerkzeuge MSIEVE und GMP-ECM auf unserem Test-PC konnte in 3 Stunden und 44 Minuten RSA-100 knacken.

Faktorisieren auch selbst am PC ausprobieren. Ein recht anschauliches Programm für Windows ist das für Lehrzwecke entwickelte kostenlose „Mathematik alpha“ (siehe ct.de/w4xv). Für Linux und macOS bietet sich auf den ersten Blick das Kommandozeilenwerkzeug `factor` an – ein Relikt aus den Linux-Anfangstagen. Doch hier ist eine Tücke versteckt: In vielen Distributionen wird eine Version ausgeliefert, die ohne die Bibliothek „GNU MP Bignum Library“ kompiliert wurde und daher nur mit Zahlen bis 2^{128} klarkommt.

Wenn Sie einen Windows-PC für einige Tage entbehren können, können Sie ihn mit einer Zahl aus der „RSA Factoring Challenge“ gut beschäftigen. Die kleinste Herausforderung des Wettbewerbs ist die „RSA-100“, eine 100-stellige Zahl. Unser Test-PC mit einem AMD Ryzen 5 2400G brauchte sechs Tage, um 37975227936943673922808872755445627854565536638199 und 400946909509208810306837352927614683892148997240 61 als die beiden Primzahlen aufzuspüren.

Schneller mit System

Stumpfes Ausprobieren ist ganz offensichtlich nicht der Weisheit letzter Schluss und so sind viele neue Verfahren entstanden, die Beschleunigung versprechen – eingesetzt werden sie gern auch in Kombination. Eine der allerersten Angriffsmöglichkeiten ging von dem Lehmann-Algorithmus aus. Entwickelt im Jahr 1974 riet dieser Algorithmus Primzahlen geringfügig schneller als einfache Probedivisionen.

Wirkliche Verbesserung versprach damals das Pollard-Rho-Verfahren, welches auch im Programm von „Mathematik alpha“ Zahlen zwischen 15 und 20 Ziffern am schnellsten auflöst. Der Vorteil des Systems geht bei größeren Zahlen aber verloren. Andere Verfahren wie p–1 oder die Fermat-Faktorisierung hatten für einen gewissen Zeitraum ihre Daseinsberechtigung.

Für Zahlen bis 100 Stellen gilt bis heute das quadratische Sieb als das schnellste Vorgehen. Mit dessen Hilfe gelang 1994 zum Beispiel die Auflösung von RSA-129. Die Verbesserung davon ist das MPQS-Verfahren. Diese hochanspruchsvolle Methode „siebt“ Zahlen nach gewissen Faktoren aus, baut dafür Zehntausende an Gleichungen und löst diese wiederum, um andere Faktoren zu bestimmen.

Ein solches Sieb-Werkzeug ist MSIEVE. Setzt man dieses in Kombination mit dem elliptischem GMP-ECM auf RSA-100 aus der Challenge an, dauert die Auflösung knappe drei Stunden auf der gleichen Test-Hardware. Als Vergleich: Die Zahl wurde 1991 in mehreren Tagen mit einem quadratischen Sieb zerlegt. RSA-110 mit nur zehn Stellen mehr brauchte einen Monat und RSA-120 sogar schon drei Monate.

Die Zukunft

Bessere Algorithmen als Brute Force beschleunigen zwar das Faktorisieren, große Module sind aber noch immer nicht in endlicher Zeit zu knacken – auch nicht für BND, NSA oder andere Profis mit gigantischem Budget. Solange niemand wider Erwarten eine ultimative Abkürzung findet, um die Einwegfunktion geschickt zurückzurechnen oder anderweitig an die Falltürinformation zu gelangen, bleibt RSA also sicher.

Ändern wird sich das vermutlich erst mit leistungsstarken Quantencomputern. Für die existiert theoretisch ein Verfahren, mit dem man das Faktorisierungsproblem und den diskreten Logarithmus, ein weiteres Falltürproblem, plötzlich in endlicher Zeit auflösen kann – der sogenannte Shor-Algorithmus. Bisher fehlt es aber an der Hardware, die dieses theoretische Konzept umsetzen kann. Asymmetrische Falltürfunktionen haben ab dann eine schwere Zeit, und Alternativen sind gefragt, die andere mathematische Probleme einsetzen. Bis es so weit ist, schützt RSA daher weiterhin Kommunikation und Privatsphäre im Internet. (wid) c't

Literatur

[1] R. L. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, 1978: https://people.csail.mit.edu/rivest/Rsapaper.pdf

Software zum Faktorisieren und RSA-Paper

ct.de/w4xv



Bild: Albert Hulm

Wie kryptografische Hashes funktionieren

Hashes begegnen Computernutzern überall, auch wenn sie sich nicht für IT-Security interessieren. Mit ihnen werden Downloads überprüft und Daten identifiziert. Sie schützen Passwörter und verketten Blockchains. Aber was sind Hashes, wie leisten sie all das und wie berechnet man sie?

Von **Sylvester Tremmel**

Als Hash oder Hashwert bezeichnet man – wenig überraschend – die Ausgabe einer Hashfunktion. Der Name leitet sich wohl von der englischen Bezeichnung „hash“ für ein ungeordnetes Durcheinander ab, weil die Ausgaben typischer Hashfunktionen möglichst chaotisch sind. Klassischerweise nutzt man Hashes als Indexwerte für Hashtabellen, aber sie haben auch für viele andere Dinge Verwendung gefunden – oft in Varianten, die auf den jeweiligen Zweck spezialisiert sind. Im Kontext von IT-Security sind mit „Hashes“ in der Regel kryptografische Hashfunktionen gemeint, um die es in diesem Artikel gehen soll.

Eine kryptografische Hashfunktion nimmt beliebig viele Daten entgegen und generiert daraus eine kurze Bitfolge fester Länge. Die Hashfunktion MD5 generiert zum Beispiel immer Hashes mit 128 Bit Länge, die Funktion SHA-256 liefert – wie der Name nahelegt – 256-Bit-Hashes. Egal, wie viele Eingabedaten es sind, die Ausgabe ist immer gleich lang. Berechnet wird diese Ausgabe streng deterministisch: Füttert man zweimal dieselben Daten in eine Hashfunktion, entsteht exakt dieselbe Bitfolge.

Pre-Image Resistance

Diese Bitfolge darf nichts über die Eingabedaten verraten. Idealerweise ist die Ausgabe von Hashfunktionen nicht von gleichverteilten Zufallszahlen zu unterscheiden: Alle Ausgaben sind gleich wahr-

scheinlich. Außerdem soll sich, wenn sich auch nur ein Bit der Eingabe ändert, jedes Bit der Ausgabe mit 50 Prozent Wahrscheinlichkeit ebenfalls ändern. Durch diesen sogenannten Lawineneffekt ergibt sich selbst bei kleinsten Eingabe-Änderungen ein völlig anderer Hashwert. Wer nur diesen Output kennt, kann keinerlei Rückschlüsse auf die Eingabe ziehen.

Das Konzept ähnelt dem vom Einwegfunktionen (siehe S. 122) und wird „pre-image resistance“ (Sicherheit gegen Urbildangriffe) genannt. Es soll praktisch unmöglich sein, die Eingabe (Urbild, englisch pre-image) zu berechnen, die einen gegebenen Hashwert (Bild) produziert hat. Genau genommen soll es keinen schnelleren Weg geben als ausprobieren, also eine Brute-force-Attacke: Wer das Urbild eines 128-Bit-Hashes errechnen will (man spricht auch vom Invertieren eines Hashes), muss 2^{128} Hashes ausprobieren – praktisch undurchführbar. Umgekehrt soll es einfach sein: Einen einzelnen Hashwert von ein paar Byte Eingabedaten kann auch ein Mikrocontroller in Sekundenbruchteilen berechnen.

Aufgrund der Sicherheit gegen Urbildangriffe eignen sich Hashfunktionen beispielsweise dazu, Passwörter zu schützen: Ein Anbieter speichert dafür Kundenpasswörter nicht direkt in einer Datenbank, sondern nur deren Hashes. Wenn sich ein Kunde später anmelden will, wird der Hash des angegebenen Passwortes berechnet und mit dem gespeicherten verglichen. Stimmen beide Hashes überein, hat der Kunde das korrekte Passwort angegeben.

Erbeutet ein Angreifer die Datenbank, findet er darin nur die Hashwerte und kann aus ihnen nicht auf die Passwörter schließen – und sie damit auch nicht bei anderen Diensten ausprobieren. Das gilt zumindest, wenn gute Passwörter zum Einsatz kommen. Weil das leider oft nicht der Fall ist, muss man weitere Maßnahmen ergreifen (siehe Kasten „Salz und Argon“).

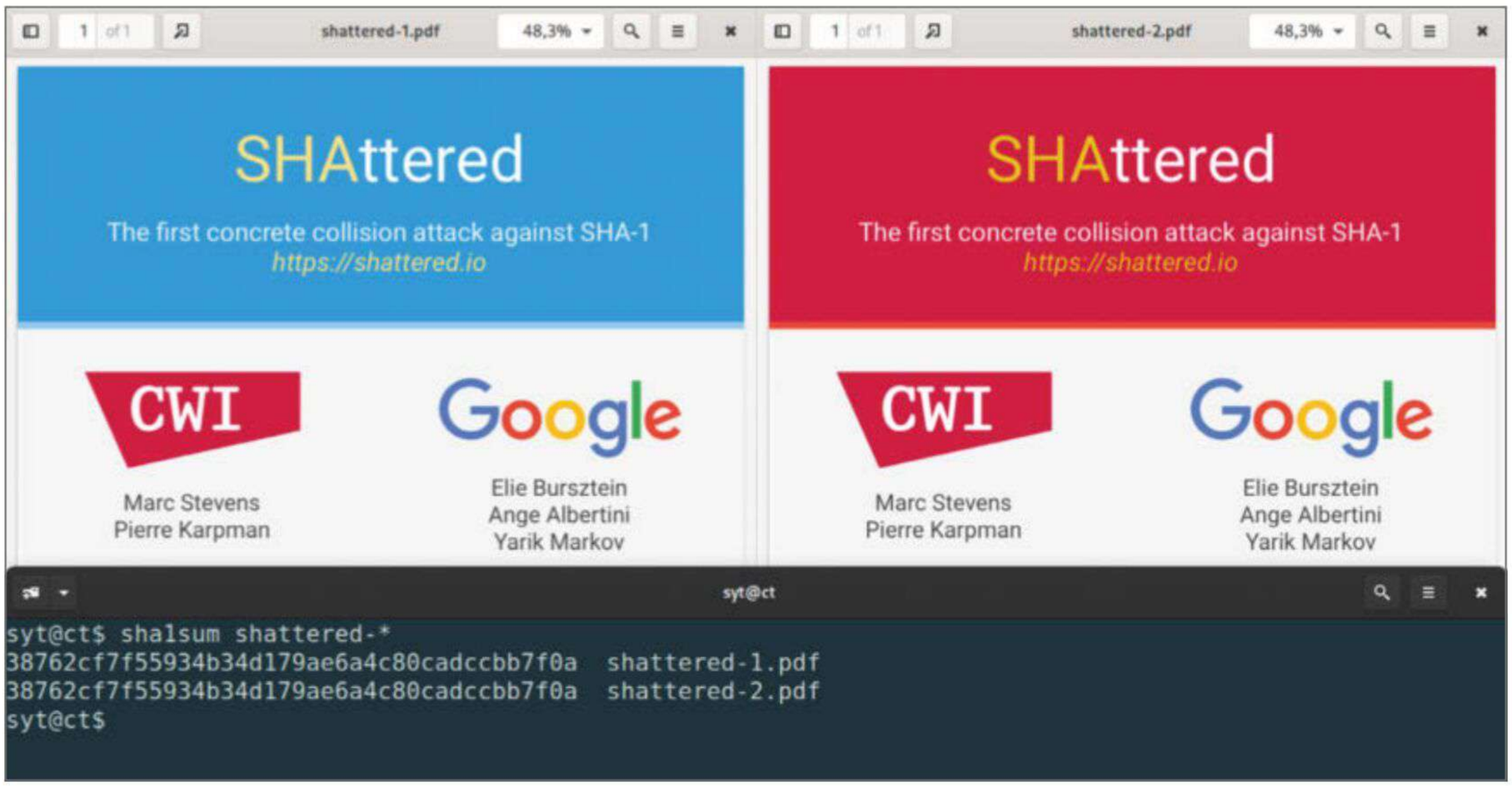
Salz und Argon

Um Eingabedaten zu finden, die einen bestimmten 128-Bit-Hashwert erzeugen, muss man unmögliche 2^{128} Hashes berechnen. Das gilt allerdings nur, wenn man nichts über die Eingabedaten weiß. Über die Eingabedaten von Passwort-Hashes weiß ein Angreifer in der Regel aber recht viel: Allzu oft sind sie nämlich „password“, „12345“ oder einige Wörter aus dem Wörterbuch plus ein paar Ziffern. Die Zahl der Möglichkeiten liegt in diesem Fall weit, weit unter 2^{128}.

Angreifer testen daher nicht irgendwelche Eingaben, sondern systematisch solche, die Menschen gerne als Passwörter verwenden – ein sogenannter Wörterbuchangriff. Diese Hashes können Angreifer auch vorsorglich berechnen. Wenn sie später eine Datenbank mit Passwort-Hashes erbeuten, schlagen sie die Hashwerte in dem selbst berechneten Datensatz nach und erfahren so die Passwörter.

Um das zu verhindern, kann man jedes Passwort mit einer zufälligen Zeichenkette kombinieren, bevor man den Hash berechnet. Diese Zeichenkette heißt „Salt“, also „Salz“, und man speichert sie zusammen mit dem Hashwert ab. Auch wenn ein Angreifer das Salz erfährt, nützen ihm Tabellen mit bekannten Hash-Werten nichts mehr, weil er für jeden einzelnen Salz-Wert eine neue Tabelle bräuchte.

Trotzdem lassen sich gerade schlechte Passwörter auch mit Salz noch in akzeptabler Zeit finden, einfach weil man mit moderner Hardware sehr schnell Hashes ausprobieren kann. Hashfunktionen sollen schließlich leicht zu berechnen sein. Dagegen hilft, Passwort-Hashes mit speziellen Schlüsselableitungsfunktionen wie „Argon2“ zu berechnen, die absichtlich CPU-Zeit, RAM oder beides beanspruchen. Der Ressourcenaufwand für Nutzer bleibt so klein, dass er kaum bemerkt wird, aber für einen Angreifer, der Milliarden mögliche Passwörter testen muss, wird es unbezahlbar. Neben Argon2 sind noch eine Reihe ähnlicher Funktionen verbreitet, etwa PBKDF2, bcrypt oder scrypt.



Zwei offensichtlich verschiedene PDF-Dateien haben den gleichen SHA-1-Hash. Diese Kollision, „SHAttered“ genannt, ist einer der Sargnägel für die kryptografische Sicherheit von SHA-1.

Schwache Kollisionen

Damit sich eine Hashfunktion zur Überprüfung von Downloads oder digitalen Unterschriften eignet, muss sie aber noch mehr können. Es soll unmöglich sein, einen zweiten Datensatz zu finden, der den gleichen Hashwert ergibt, wie das Original. Andernfalls könnten Downloads oder signierte Dateien unerkannt manipuliert oder ausgetauscht werden. Ein Hashwert soll Daten also eindeutig identifizieren.

Daten, die man über ihren Hash identifiziert, können auch selbst einen Hash von anderen Daten enthalten. So lassen sich Ketten aufbauen, in denen sich kein Element ändern lässt. Das würde schließlich den Hash dieses Elements ändern und der diente wiederum als Eingabe eines anderen Hashes und so weiter. Solche Hashketten sind auch die „chains“ von Blockchains.

Mathematiker horchen bei „eindeutig identifizieren“ allerdings auf: Eine Funktion, die beliebig lange Eingabedaten auf eine beschränkte Menge an Ausgaben abbildet, kann das nicht eindeutig tun; es gibt einfach mehr mögliche Eingaben als Ausgaben. Streng genommen sind Hashfunktionen daher nur „kollisionsresistent“. Das heißt, dass es zwar Eingaben gibt, die denselben Hashwert produzieren, man diese aber praktisch nicht finden kann.

Zum Prüfen von Dateihashes genügt die sogenannte „schwache Kollisionsresistenz“, die präziser als „second pre-image resistance“ bezeichnet wird. Zu einer vorhandenen Eingabe (also einer bestimmten Datei), die einen bestimmten Hashwert produziert, darf man keine andere Eingabe finden, die denselben Hashwert produziert. Man darf also zu einem bekannten Urbild kein zweites finden. Sonst könnte ein Angreifer zum Beispiel einen harmlosen Download durch Malware ersetzen, die denselben Hashwert hat und dadurch valide aussieht. Bezeichnend für schwache Kollisionsresistenz ist, dass ein Urbild vorgegeben ist (der wahre Download) und der Angreifer ein zweites, dazu passendes finden muss.

Starke Kollisionen

Die sogenannte starke Kollisionsresistenz (oft auch nur „Kollisionsresistenz“ genannt) erlaubt dem Angreifer hingegen, beide Urbilder zu wählen. Auch dann darf er kein Paar von Eingaben finden, die denselben Hashwert haben. Starke Kollisionsresistenz ist beispielsweise bei digitalen Signaturverfahren wichtig. Signaturen nutzen Hashes, um Dokumente zu identifizieren und dürfen jeweils nur zu genau einem Dokument passen.

Beide Eingaben anpassen zu dürfen, bietet relativ viel Angriffsfläche, was zu Problemen in der Praxis führt: Einige Hashverfahren, zum Beispiel MD5 oder SHA-1, werden nicht mehr als sicher angesehen, weil sie insbesondere gegen Kollisionsangriffe weniger Widerstand leisten, als man anfänglich annahm.

Starke Kollisionsresistenz ist aber auch prinzipiell problematisch: Auch eine perfekte Hashfunktion mit 160 Bit Output bietet nicht etwa 160 Bit starke Kollisionsresistenz, sondern nur 80 Bit. Das heißt, dass ein Angreifer, der beide Eingabewerte frei modifizieren kann, nur etwa 2^{80} Hashwerte berechnen muss, um eine Kollision zu finden. Er muss nämlich nicht eine bestimmte Kollision mit einem bestimmten Hash finden, sondern irgendeine Kollision mit irgendeinem Hash.

Die zugrunde liegenden Wahrscheinlichkeiten sind dieselben wie beim Geburtstagsparadoxon: Dass in einem Raum mit 20 oder 30 Menschen jemand an einem bestimmten Tag Geburstag hat, ist eher unwahrscheinlich. Viel höher ist aber die Wahrscheinlichkeit, dass zwei beliebige Personen in diesem Raum am selben Tag Geburtstag haben. Schon in einem Raum mit 23 Personen übersteigt sie 50 Prozent.

2^{80} Hashes ausprobieren zu müssen ist dramatisch weniger Aufwand als 2^{160} Hashes. Umso schlimmer, wenn Schwächen des Algorithmus diese Sicherheit dann weiter reduzieren: Wie man mittlerweile weiß, bietet SHA-1 höchstens eine Sicherheit von circa 2^{63} Bit gegen Kollisionsangriffe [1].

Bauanleitung

Aber wie programmiert man eine Funktion, die streng deterministisch ist und dennoch zufällig wirkenden Output produziert; die Urbild- und kollisionsresistent ist, sich aber trotzdem über beliebig große Eingaben leicht berechnen lässt?

Die heutzutage gebräuchlichsten Hashfunktionen basieren auf der Merkle-Damgård-Konstruktion (siehe Schaubild). Deren Prinzip ist einfach: Die Berechnung startet mit einem definierten internen Zustand (Initialisierungsvektor, IV). Eine mehrfach angewandte Funktion durchmischt diesen Zustand möglichst chaotisch. Die eigentlichen Eingabedaten werden blockweise ebenfalls in diese Funktion gegeben und dadurch mit in den Zustand gemischt.

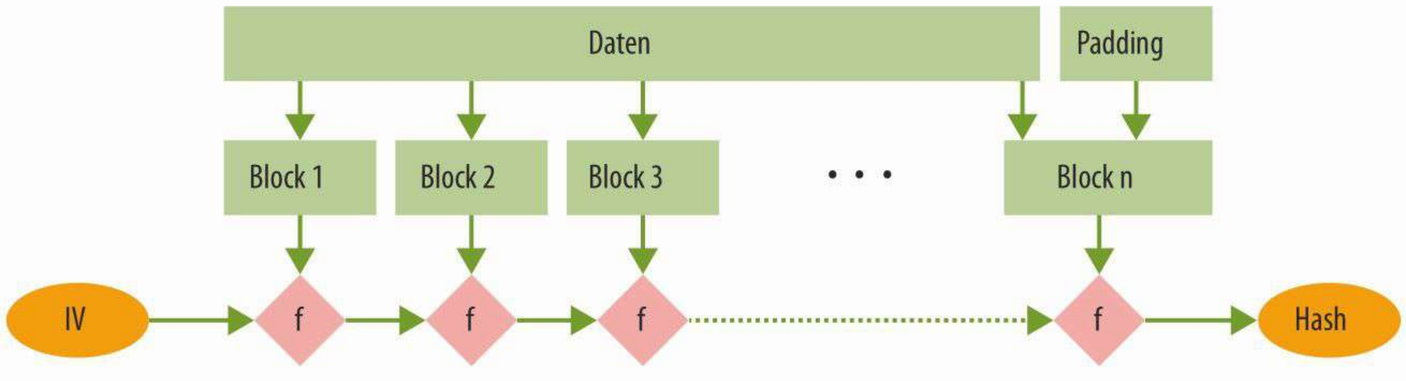
Weil die Funktion einen Zustand aus n Bits zusammen mit einem Eingabeblock von m Bits auf einen neuen Zustand von n Bits verdichtet, nennt man sie Kompressionsfunktion. Damit sich passende Blöcke bilden lassen, werden die Eingabedaten verlängert (Padding), bis sie einem Vielfachen der Blockgröße entsprechen. Die Ausgabe des letzten Aufrufs der Kompressionsfunktion ist der Hashwert.

In der Praxis kommt noch hinzu, dass man die Eingabedaten vor Anwendung der Kompressionsfunktion aufbereitet. Eventuell wird auch der finale Zustand noch bearbeitet, bevor er als Hashwert dient; aber im Prinzip arbeiten MD5, SHA-1, alle SHA-2-Varianten und auch einige weniger bekannte Hashfunktionen nach dem beschriebenen Prinzip.

Die Qualität einer Merkle-Damgård-Hashfunktion hängt davon ab, wie gut die Kompressionsfunktion den Zustand durchmischt. Schwächen der Hashfunktion beruhen häufig auf Schwächen ihrer Kompres-

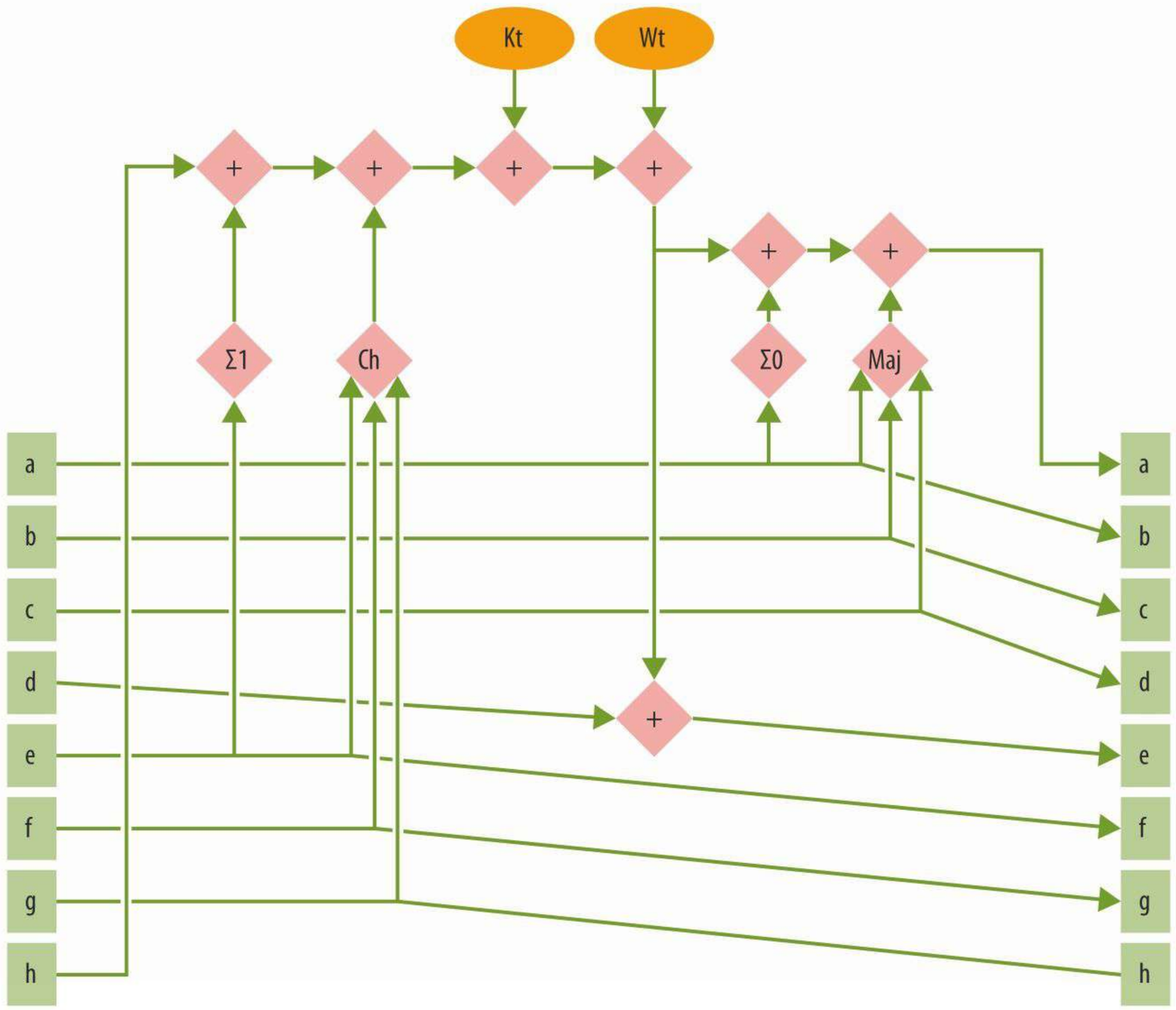
Merkle-Damgård-Konstruktion

Die gebräuchlichsten Hashfunktionen basieren auf dieser Konstruktion. Die Eingabedaten werden dabei auf passende Länge gebracht (Padding) und dann blockweise in eine Kompressionsfunktion (f) gegeben, die sie mit der Ausgabe der vorherigen Kompression verrechnet. Beim ersten Aufruf wird stattdessen ein fester Wert (IV) genutzt, die Ausgabe des letzten Aufrufs von f ist – vereinfacht gesagt – der berechnete Hashwert.



SHA-256

Die Kompressionsfunktion von SHA-256 besteht aus 64 Runden. Im Wesentlichen werden in jeder Runde die Zustandsvariablen (a–h) um eins verschoben (a wird zu b, b zu c etc.). Allerdings werden die Variablen a und e auf Werte gesetzt, die über verschiedene Funktionen aus dem gesamten Zustand berechnet werden. In diese Rechnung fließt pro Runde auch eine Konstante (Kt) ein, wie auch – ganz wichtig – ein Teil vom aktuellen Block der zu hashenden Daten (Wt).



sionsfunktion. Moderne Hashes wie SHA-256 benutzen daher deutlich komplexere Kompressionsfunktionen als ältere wie MD5 oder SHA-1 (siehe Grafik).

In die Verlängerung

Ein prinzipielles Problem haben allerdings alle Merkle-Damgård-Hashfunktionen: Length-Extension-Attacken. Weil der gesamte interne Zustand letztlich in den Hashwert mündet, lässt sich die Berechnung fortsetzen. Man nutzt den Hashwert sozusagen als internen Zwischenzustand und führt das Merkle-Damgård-Schema einfach mit mehr Eingabedaten fort. Konkret kann ein Angreifer, der die Länge und den Hashwert von Eingabedaten kennt, auch den Hashwert berechnen, der entsteht, wenn man etwas an die Eingabedaten anhängt. Er kann das, wohlgemerkt, ohne die Eingabedaten an sich zu kennen.

Length-Extension-Attacken sind zum Beispiel ein Problem, wenn Hashfunktionen als Message-Authentication-Codes (MAC) missbraucht werden:

```
Hash($Key + $Nachricht) # Bad MAC!
```

Den Schlüssel `$Key` kennt ein Angreifer nicht und kann ihn aufgrund der Sicherheit gegen Urbildangriffe auch

Hashes und Verschlüsselungen

Hashfunktionen sind etwas grundlegend anderes als Verschlüsselung, weil niemand einen Wert ent-hashen können soll. Meist ist es deshalb falsch, von „verschlüsselten Passwörtern“ und Ähnlichem zu reden.

Trotzdem gibt es interessante Wechselbeziehungen zwischen Hashes und Verschlüsselungen. Kompressionsfunktionen müssen nicht neu erfunden werden; stattdessen kann man auch symmetrische Blockchiffren nutzen. Zum Beispiel verschlüsselt man – vereinfacht gesagt – einen internen Zustand mehrfach, wobei jede Verschlüsselung Stücke der zu hashenden Daten als Schlüssel nutzt.

Andersherum ist es auch möglich, aus kryptografischen Hashfunktionen symmetrische Blockchiffren zu bauen, zum Beispiel über Feistel-Netzwerke. Die Daten werden dafür blockweise verarbeitet und jeder Block wird zweigeteilt. Jeweils eine Hälfte wird zusammen mit einem Schlüssel gehasht und der Hashwert dann mit der anderen Hälfte des Datenblocks verrechnet (per exklusivem Oder, XOR). Danach vertauscht man die beiden Hälften und wiederholt das Ganze mehrfach. Das Resultat ist ein Algorithmus, der sich – wenn man den Schlüssel kennt – rückabwickeln lässt, obwohl die Hashes selbst nicht invertierbar sind.

nicht extrahieren. Aber auch ohne ihn (oder die Nachricht) zu kennen, kann ein Angreifer über eine Length-Extension etwas an die Nachricht anhängen und einen neuen, gültigen MAC berechnen.

Gegen dieses konkrete Problem helfen bessere MACs, die durchaus auf Hashfunktionen beruhen können. Ein beliebtes Schema ist HMAC, bei dem – im Prinzip – schlicht der Hash eines Hashes berechnet wird:

```
Hash($Key + Hash($Key + $Nachricht))
```

Die Eingabedaten des äußeren Hashes könnte ein Angreifer zwar per Length-Extension fortsetzen, aber das erlaubt ihm nicht, die Nachricht zu verlängern. Dafür müsste er den inneren Hash kennen und das ist – wieder aufgrund der Sicherheit gegen Urbildangriffe – nicht möglich.

Vor Length-Extension-Attacken im Allgemeinen schützt es, nicht den gesamten internen Zustand in den finalen Hash einfließen zu lassen. Seltenere SHA-2-Varianten wie SHA-384 oder SHA-512/256 machen das.

Literatur

[1] Jürgen Schmidt, Warum SHAttered wichtig ist: https://heise.de/-3634341

Alles neu macht SHA-3

Unter anderem aufgrund von Length-Extension-Attacken ist man in letzter Zeit aber etwas misstrauischer gegenüber Merkle-Damgård-Konstruktionen geworden. Es sind zwar keine praktisch relevanten Angriffe gegen SHA-2 bekannt, aber die Hashfunktionen der SHA-3-Familie sind trotzdem anders aufgebaut: Sie nutzen eine sogenannte Sponge-Konstruktion. Auch dabei wird eine Funktion wiederholt angewandt, aber die Eingabedaten werden immer nur mit einem Teil des internen Zustands verrechnet. Die Ausgabe wird – anders als bei Merkle-Damgård – iterativ produziert, indem man weiter die interne Funktion wiederholt anwendet, aber zwischen den Anwendungen Teile des Zustandes ausliest. Das verhindert Length-Extension-Attacken und erlaubt Hashes einstellbarer Länge.

Das US-amerikanische National Institute of Standards and Technology (NIST), das für viele kryptografische Standards maßgeblich ist, hat SHA-3 schon 2015 standardisiert. Trotzdem sind Hashfunktionen der SHA-2-Familie – und damit Merkle-Damgård-Konstruktionen – aktuell noch deutlich weiter verbreitet. Sie erledigen die vielfältigen Aufgaben kryptografischer Hashes gut und effizient, haben – soweit man weiß – keine relevanten Schwächen und müssen daher auch nicht durch SHA-3 ersetzt werden. Die Security-Gemeinschaft ist dennoch froh über SHA-3. Falls sich in Zukunft Probleme mit SHA-2 zeigen sollten, hat man schon eine kompatible und gut durchdachte Alternative in petto. (syt) c't

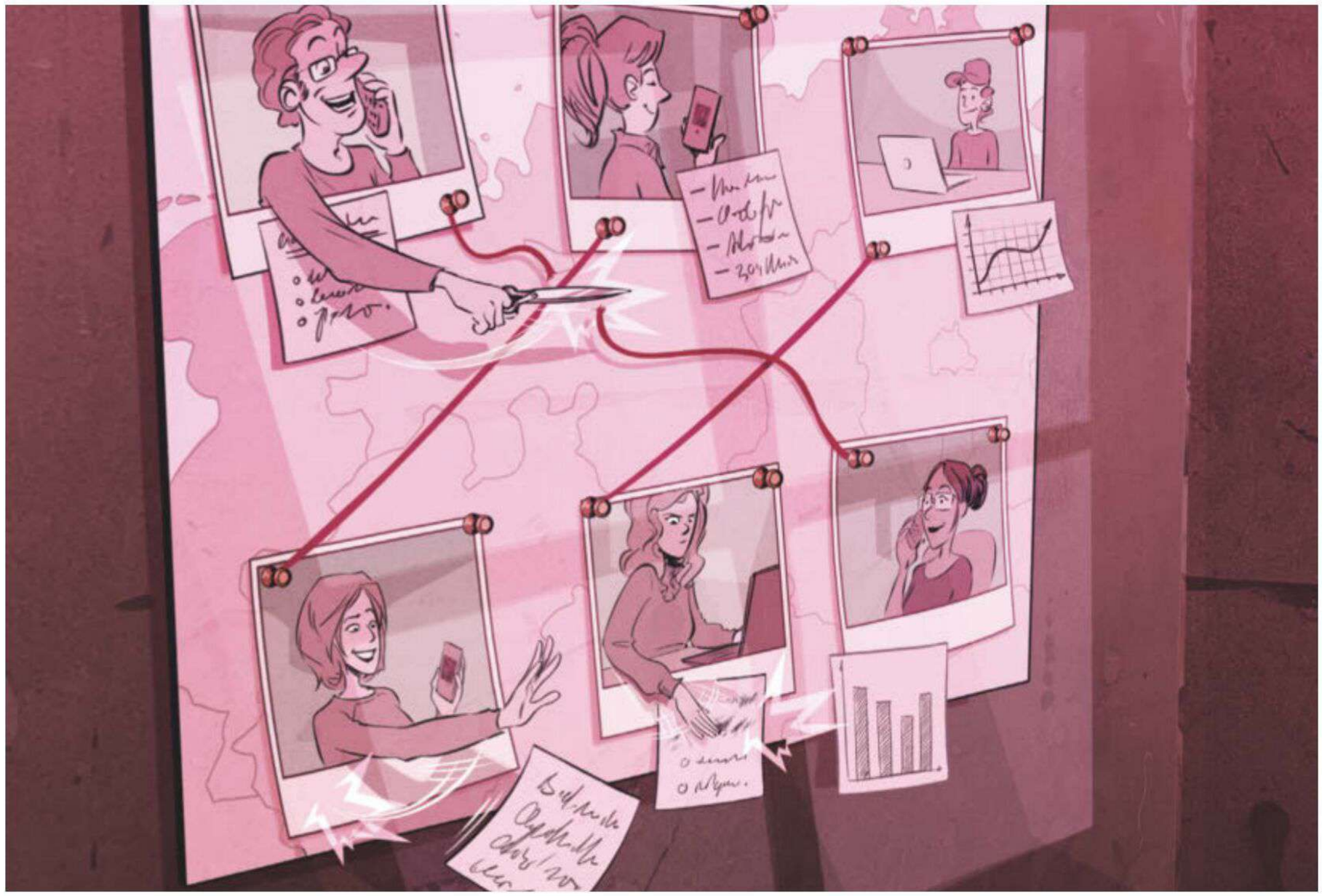


Bild: Albert Hulm

Sichere Kommunikation

Ende-zu-Ende-Verschlüsselung klingt nach absoluter Sicherheit, aber bei vielen Implementierungen gibt es noch Luft nach oben. Mit dem Boom von Messengern kamen neue Verfahren auf, die sogar dann noch Sicherheiten bieten, wenn Kommunikationspartner unterwandert werden.

Von **Sylvester Tremmel**

Eine Nachricht abhör- und manipulationssicher zu verschicken, ist eigentlich gar nicht kompliziert: Man einigt sich mit dem Korrespondenten auf einen Schlüssel und chiffriert damit die Nachricht. Passende Verfahren sind altbekannt. Aber wie einigt man sich mit seinem Gesprächspartner auf einen Schlüssel? Das muss ebenfalls abhör- und manipulationssicher geschehen und die Katze beißt sich in den Schwanz.

Über Jahrtausende wurden verschiedenste Tricks angewandt, um den Schlüssel zu transportieren. Seit den 1970er-Jahren sind bestimmte mathema-

tische Tricks beliebt: Asymmetrische Kryptosysteme, auch Public-Key-Verfahren genannt, funktionieren mit zwei verschiedenen Schlüsseln – einem öffentlichen zum Verschlüsseln und einem dazu passenden privaten Schlüssel zum Entschlüsseln (siehe S. 116). Nachrichten, die mit dem öffentlichen Schlüssel chiffriert wurden, können nur mit dem privaten entschlüsselt werden. Außerdem lässt sich der private Schlüssel nicht aus dem öffentlichen rekonstruieren. Das ist der entscheidende Punkt, weil man so seinen öffentlichen Schlüssel ruhigen Gewissens an potenzielle Gesprächspartner verteilen kann.

Die fortschreitende Verbesserung von Computern erzwingt zwar gelegentliche Anpassungen an den Krypto-Verfahren und Quantencomputer bedrohen manche Verfahren grundsätzlich. Aber in der Praxis lösen Public-Key-Verfahren das Problem des Schlüsselaustauschs. Man kann die beiden Schlüssel nutzen, um Nachrichten sicher zu (de-)chiffrieren, oder um sich über Verfahren wie einen Diffie-Hellman-Schlüsselaustausch abhörsicher auf ein gemeinsames Geheimnis zu einigen und es als Schlüssel für herkömmliche – symmetrische – Verschlüsselungsverfahren zu nutzen. Durch Standards wie OpenPGP sind Public-Key-Verfahren für jedermann verfügbar. Also gibt es nichts mehr zu tun?

Identitätsfragen

Leider doch: Über die Jahre und mit der zunehmenden Verbreitung von Public-Key-Verfahren haben sich diverse Unzulänglichkeiten herauskristallisiert. Eine davon ist **Authentifizierung**. Also die Garantie, dass man mit dem beabsichtigten Gegenüber spricht und nicht einem Angreifer, der sich zwischen die Korrespondenten geschaltet hat. Public-Key-Verfahren bieten dafür digitale Signaturen, die beweisen, dass eine Nachricht vom Besitzer eines bestimmten privaten Schlüssels kommt. Üblicherweise kombiniert man die Signatur mit der Verschlüsselung der Nachricht, sodass nur der Kommunikationspartner den Ursprung der Nachricht sicher nachweisen kann.

Dafür müssen die beiden Korrespondenten aber sicher den öffentlichen Schlüssel ihres Gegenübers kennen. Wenn ein Angreifer es schafft, seinen eigenen öffentlichen Schlüssel als den eines Partners auszugeben, dann kann er natürlich auch die passenden Signaturen erstellen. Eine Möglichkeit dieses Problem anzugehen, sind vertrauenswürdige Zertifizierungsstellen, die für die Korrektheit des Schlüssels bürgen. Diese Methode kommt zum Beispiel bei der HTTPS-Verschlüsselung von Webseiten oder der S/MIME-Verschlüsselung von E-Mails zum Einsatz.



Viele Messenger erlauben Fingerabdrücke – Signal nennt sie „safety numbers" – semiautomatisch abzugleichen.

Allerdings muss man der Zertifizierungsstelle vertrauen. Das ist grundsätzlich schlecht – Verschlüsselung soll Vertrauen unnötig machen – und auch praktisch haben Zertifizierungsstellen schon mehrfach grobe Fehler gemacht. Viele Messenger und auch manche Systeme für PGP-verschlüsselte E-Mails setzen daher auf eine andere Methode: TOFU und das Prüfen von Fingerabdrücken. „TOFU" steht für „Trust on first use" und bedeutet, anfänglich einfach anzunehmen, dass der öffentliche Schlüssel

korrekt ist. So kann sich ein Angreifer immerhin nicht nachträglich in eine Kommunikation einschalten, er muss schon beim erstmaligen Nachschlagen des öffentlichen Schlüssels eine Fälschung untergeschoben haben.

Um auch das zu verhindern, kann man – wenn man sich einmal real sieht – die Fingerabdrücke von Schlüsseln vergleichen. Stimmen sie überein, dann hat man sicher den wahren Schlüssel. Um den Abgleich möglichst einfach zu machen, können ihn viele Messenger semiautomatisch durchführen – zum Beispiel über das gegenseitige Scannen von QR-Codes – und merken sich, welche Kontakte verifiziert wurden. Ändert sich ein Fingerabdruck später, schlägt der Messenger Alarm.

Ich wars nicht

Mit der Authentifizierung geht allerdings eine häufig unerwünschte Eigenschaft einher: Kommunikation kann nicht abgestritten werden. Eine mit einem privaten Schlüssel signierte Nachricht kommt ohne jeden Zweifel vom Besitzer dieses Schlüssels. Das lässt sich auch nachträglich prüfen und wird problematisch, wenn zum Beispiel staatliche Stellen einen Kommunikationspartner unterwandern und so an alte Nachrichten im Klartext gelangen. Die tragen Signaturen vom privaten Schlüssel des Absenders und liefern so auch Beweismaterial gegen ihn. Der Angreifer kann die Signaturen leicht prüfen, weil er dazu nur den öffentlichen Schlüssel des Absenders braucht – und der ist eben öffentlich. Es ist umstritten, ob **Abstreitbarkeit** einen praktischen Nutzen hat, gerade gegenüber Stellen, die im Zweifel nicht an gerichtsfesten Beweisen interessiert sind. Zumindest in Rechtsstaaten hilft es aber, Kommunikation bestreiten zu können.

Authentifizierung und Abstreitbarkeit scheinen sich nur auf den ersten Blick zu widersprechen: Tatsächlich wollen Gesprächspartner vornehmlich, dass sie in einer Konversation *aktuell* sicher sein können, mit dem richtigen Korrespondenten zu reden. Sie wollen es nicht nachträglich für bereits vergangene Gespräche beweisen. Die Lösung ist daher ein System, das den Signaturschlüssel regelmäßig wechselt, und zwar so, dass sich keine Rückschlüsse auf frühere Schlüssel ziehen lassen. Man spricht auch von Schlüsselrotation. Wenn ein Gesprächspartner kompromittiert wird, können so aus dem aktuellen Schlüssel keine früheren abgeleitet werden, und alte, vom Angreifer aufgezeichnete Konversationen, lassen sich nicht sicher zuordnen. Voraussetzung dafür ist, dass ausgediente Schlüssel auch gelöscht werden.

Perfekte Geheimhaltung

Wenn Schlüsselrotation nicht (nur) bei Signaturen, sondern auch bei der Verschlüsselung selbst zum Einsatz kommt, kann sie eine noch wichtigere Eigenschaft garantieren: **Folgenlosigkeit**, oft auch **(Perfect) Forward Secrecy** (PFS oder FS) genannt. PFS schützt vor dem oben bereits skizzierten Szenario: Ein Angreifer kann die Verschlüsselung nicht brechen, zeichnet die Chiffrate aber trotzdem auf. Geheimdienste wie die NSA tun das in großem Stil. Wenn nun, vielleicht Jahre später, der private Schlüssel eines Kommunikationspartners bekannt wird, können damit die jahrelang aufgezeichneten Übertragungen allesamt entschlüsselt werden. PFS verhindert das, weil die Schlüssel wechseln. Der Jahre später kompromittierte Schlüssel verrät nichts über frühere Schlüssel und die von ihnen geschützten Nachrichten bleiben sicher verschlüsselt.

PFS kommt heutzutage bei TLS zum Einsatz und damit automatisch bei vielen Transportverschlüsselungen. Bei Ende-zu-Ende-Verschlüsselungen ist es weniger selbstverständlich: Bei den E-Mail-Verschlüsselungen S/MIME und OpenPGP sind häufige Schlüsselrotationen umständlich und bleiben dem Benutzer überlassen. In der Praxis kommen sie daher kaum vor und E-Mails sind nicht durch PFS geschützt. Manche Messengerprotokolle unterstützen PFS ebenfalls nicht, Threema etwa nutzt PFS nur in der Transportverschlüsselung zwischen Client und Server, nicht in der Ende-zu-Ende-Verschlüsselung zwischen den Clients.

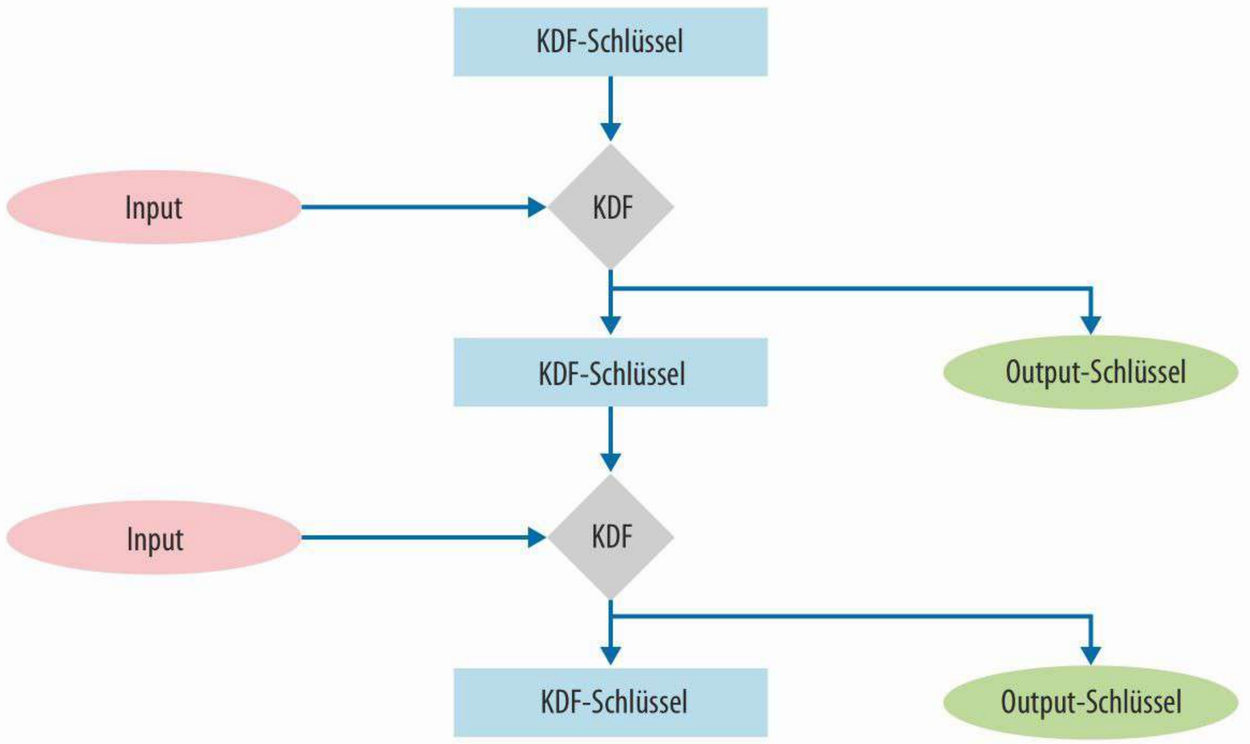
Double Ratchet

Der Messenger Telegram unterstützt PFS in seinen geheimen Chats, in denen etwa alle 100 Nachrichten oder einmal pro Woche der Schlüssel gewechselt wird. Bei den meisten anderen Messengern hat sich das Signal-Protokoll (oder Abwandlungen davon) als Quasi-Standard durchgesetzt. Das Protokoll verschlüsselt jede einzelne Nachricht mit einem neuen Schlüssel. Zentrales Element dafür ist der Double-Ratchet-Algorithmus. Er besteht aus symmetrischen und asymmetrischen Ratschen, also Komponenten, die sich nur in eine Richtung bewegen können.

Die symmetrischen Ratschen basieren auf KDF-Ketten (siehe Grafik gegenüber). Für die Inputs der

KDF-Kette

Aus einer Schlüsselableitungsfunktion (key-derivation function, KDF) lässt sich eine Kette knüpfen. Jede Anwendung der KDF generiert einen neuen Output-Schlüssel, der etwa genutzt werden kann, um Nachrichten zu verschlüsseln, und einen neuen Schlüssel für die Kette selbst. KDFs sind wie Hash-Funktionen nicht umkehrbar: Aus einem bekannten Kettenstand lassen sich keine früheren Output- oder KDF-Schlüssel errechnen. Falls die Inputs nicht vorhersagbar sind, lassen sich aus einem bekannten Zustand auch keine zukünftigen Zustände errechnen.



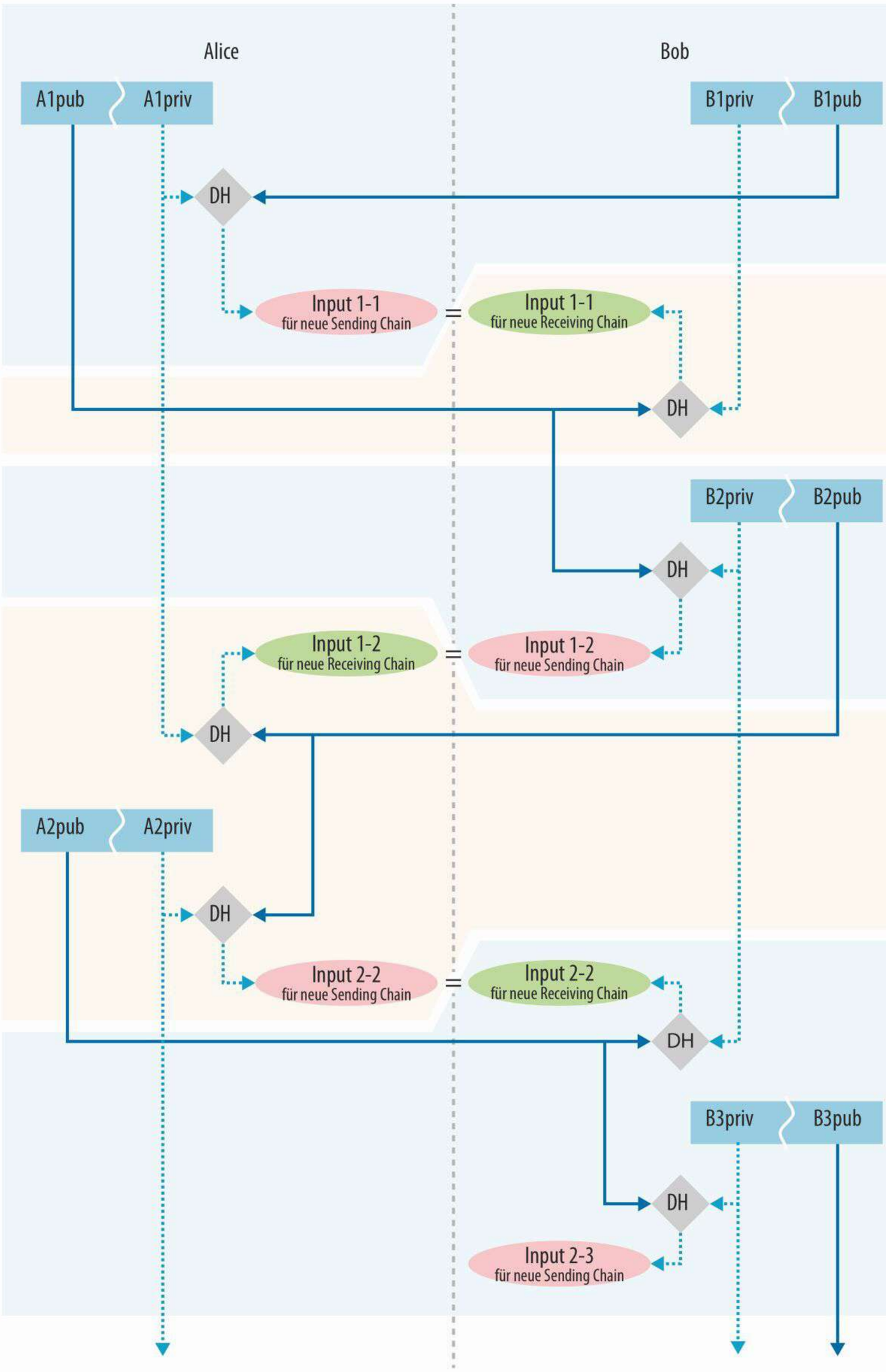
Ketten werden feste Werte genutzt. Für jede zu übermittelnde Nachricht vollzieht der Sender einen Kettenschritt und nutzt den Output-Schlüssel zum Verschlüsseln der Nachricht. Der ebenfalls entstandene neue KDF-Schlüssel ersetzt den alten. Der Empfänger hat eine Kopie der Kette, vollzieht ebenfalls einen Schritt und nutzt den entstandenen identischen Output-Schlüssel zum Entschlüsseln. Alte Schlüssel werden verworfen und die Ketten lassen sich nicht zurückrechnen, was PFS herstellt.

Zum Senden in die andere Richtung nutzen die Partner ein zweites Kettenpaar, sodass sich überschneidend gesendete Nachrichten nicht stören. Bleibt die Frage, wie Kommunikationspartner zu den identischen KDF-Ketten kommen. Dafür ist die asymmetrische Diffie-Hellman-Ratsche (DH-Ratsche, siehe Grafik auf S. 136) zusammen mit einer weiteren KDF-Kette – der Root-Chain – zuständig. Beide Partner haben dieselbe Root-Chain. Jedes Mal, wenn die Kommunikationsrichtung wechselt, denkt sich der Sender in der DH-Ratsche ein neues Schlüsselpaar aus und nutzt es als Input, um einen Schritt mit der Root-Chain zu machen. Mit dem Output-Schlüssel der Root-Chain beginnt er eine neue KDF-Kette zum Senden. Über die DH-Ratsche kann der Empfänger ebenfalls denselben Input in seine Kopie der Root-Chain geben und so eine passende neue KDF-Kette zum Empfangen erstellen.

Mit jeder Umkehr der Kommunikationsrichtung wechseln Sender und Empfänger also die genutzten KDF-Ketten. Das DH-Ratchet garantiert so PFS, aber das konnten ja schon die Ketten selbst bereitstellen. Wichtiger ist etwas anderes: **Post-Compromise Security** (PCS). Diese auch als **Selbstheilung** oder **Future Secrecy** bezeichnete Fähigkeit ist das Gegenstück zu PFS. Falls ein Kommunikationsteilnehmer kompromittiert wird, schützt PFS vergangene Kommunikation. Zukünftige kann der Angreifer aber für alle Zeit mitlesen (sofern er nicht bemerkt wurde), selbst wenn er den Zugriff auf den Ge-

Diffie-Hellman-Ratchet

Die Diffie-Hellman-Ratsche ist die übergeordnete Ratsche des Double-Ratchet-Algorithmus. Die sekundären Ratschen befinden sich in den angedeuteten Sending und Receiving Chains.



Alice und Bob generieren jeweils ein Schlüsselpaar aus einem privaten und einem öffentlichen Schlüssel. Im diesem vereinfachten Beispiel gibt zuerst Bob seinen öffentlichen Schlüssel an Alice weiter. Über einen Diffie-Hellman-Schlüsselaustausch (DH) generiert Alice daraus zusammen mit ihrem privaten Schlüssel einen eindeutigen, geheimen Wert, mit dem sie ihre Sending Chain initialisiert.
In Wirklichkeit wird das DH-Ratchet komplizierter über mehrere DH-Schlüsselaustausche initialisiert (X3DH, siehe ct.de/wa6f), damit die anfängliche Kommunikation auch umgekehrt und asynchron erfolgen kann.

Nun sendet Alice ihren öffentlichen Schlüssel an Bob. Der kann, wiederum per DH, zusammen mit seinem eigenen privaten Schlüssel den gleichen geheimen Wert errechnen, den er nutzt, um seine Receiving Chain zu initialisieren. Von nun an kann Alice über ihre Sending Chain Nachrichten chiffrieren, die Bob über seine Receiving Chain entschlüsseln kann.

Gleich darauf generiert Bob ein neues Schlüsselpaar und nutzt Alices öffentlichen und seinen neuen privaten Schlüssel, um einen weiteren Wert per DH zu errechnen. Damit initialisiert er seine eigene Sending Chain, den öffentlichen Schlüssel des neuen Paares schickt er wieder an Alice.

Mit Bobs neuem öffentlichen Schlüssel und ihrem eigenen privaten kann Alice eine passende Receiving Chain aufsetzen. Von nun an kann auch Bob Nachrichten an Alice über passende Chains verschlüsseln.
Alice generiert außerdem sofort selber ein neues Schlüsselpaar und nutzt Bobs soeben erhaltenen öffentlichen und ihren neuen privaten Schlüssel, um eine neue Sending Chain aufzusetzen.

Sowie Bob Alices neuen öffentlichen Schlüssel erhält, setzt er eine passende Receiving Chain auf, generiert selbst wieder ein neues Schlüsselpaar und zusammen mit Alices neuem Schlüssel eine eigene neue Sending Chain.
So führen die beiden Partner immer wieder neue Sending Chains ein und legen passende Receiving Chains an. Solange die Nachrichten nur in eine Richtung fließen, werden die gerade aktuellen Chains genutzt. Mit jedem „Richtungswechsel" der Kommunikation werden neue Chains angelegt.

sprächsteilnehmer wieder verliert. Schließlich lassen sich die symmetrischen Ratschen (und andere Schlüsselrotationssysteme) leicht „nach vorne“ bewegen. Aus einem einmal bekannten Kettenzustand kann der Angreifer alle zukünftigen Output-Schlüssel selbst errechnen.

Die neuen Schlüsselpaare im DH-Ratchet denken sich die beiden Partner aber aus, sie lassen sich nicht vorhersagen. Wenn ein Angreifer also den Zugriff auf einen Kommunikationspartner verliert, so kann er nur so lange weiter mitlesen, wie die ihm bekannten symmetrischen Ratschen genutzt werden. Sobald aber ein ganzer DH-Schritt erfolgt, sind beide Kettenpaare ausgetauscht und der Angreifer ist wieder ausgesperrt. Die Verschlüsselung hat sich selbst geheilt.

Jenseits der Verschlüsselung

Der Double-Ratchet-Algorithmus nutzt die wechselnden Schlüssel auch zur Authentifizierung und erreicht so Abstreitbarkeit, zumindest in Bezug auf den Nachrichteninhalt. Angreifer könnten aber zum Beispiel den Anbieterserver kompromittieren und dadurch immerhin erfahren, wer mit wem Nachrichten austauscht. Manche Messenger – etwa WhatsApp oder Telegram – analysieren sogar das komplette Telefonbuch ihrer Nutzer und schaffen damit attraktive Angriffsziele. Diverse Messenger versuchen aber, möglichst wenig Metadaten zu sammeln und gesammelte Daten möglichst schnell zu löschen. Löschversprechen muss man als Nutzer allerdings vertrauen, weswegen es besser ist, wenn Messenger Daten gar nicht erheben. Zum Beispiel Threema, Conversations (XMPP) oder Element (Matrix) nutzen IDs, statt die Nutzer um ihre Telefonnummern zu bitten. Signal treibt dagegen viel Aufwand, damit ihre Server die Telefonnummern nicht erfahren (siehe S. 34).

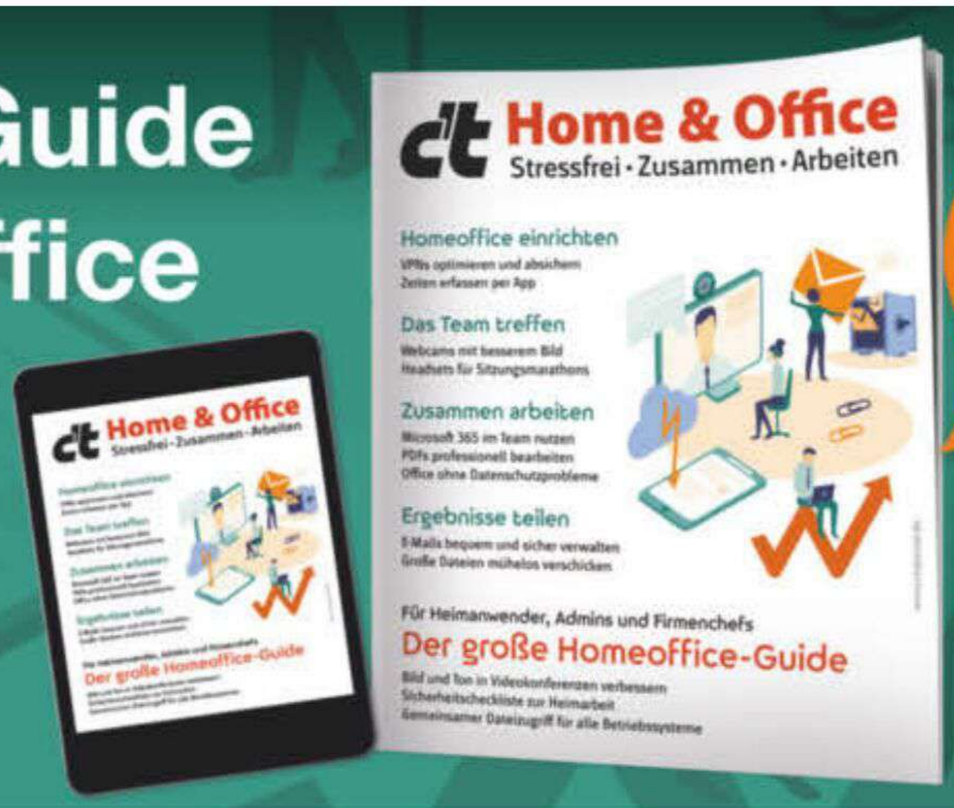
Grundsätzlich schreitet die Entwicklung bei der Vermeidung von Metadaten rasch voran. Messenger wie Briar nutzen dezentrale Verbindungen über das Tor-Netzwerk, um Metadaten zu verschleiern; Signal hat „Sealed Sender“ erfunden, damit der Signal-Server Absender und Empfänger nicht zuordnen kann; XMPP oder Matrix föderieren ihre Server, damit zumindest keine einzelne zentrale Instanz existiert, bei der alle Metadaten anfallen (siehe S. 30).

Viel Bewegung gibt es auch bei Gruppenchats. Auf der einen Seite des Spektrums an Kompromissen steht Telegram, dessen Gruppen lediglich transportverschlüsselt sind. Der Server kennt Metadaten und Inhalte, aber dafür unterstützen Telegram-Gruppen bis zu 200.000 Mitglieder. Das andere Extrem ist Signal, das Gruppen über den Double-Ratchet-Algorithmus abwickelt und den Server nicht mal wissen lässt, wer in welcher Gruppe ist. Signal-Gruppen skalieren aber nur schlecht und sind daher auf 1000 Mitglieder beschränkt. Dazwischen liegt zum Beispiel WhatsApp, das Gruppenzugehörigkeiten vom Server verwalten lässt und in ihnen nur die symmetrischen Ratschen nutzt. Das skaliert besser, kostet aber die Selbstheilung und erzeugt Metadaten auf dem Server. (syt) c't

Weitere Infos

ct.de/wa6f

Der Praxis-Guide fürs Homeoffice



NEU

Als Heft + PDF mit 29 % Rabatt

heise Shop

shop.heise.de/ct-ho21

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

Privacy statt Buzzwords

Die DSGVO setzt auf den mündigen, informierten Bürger. Da freut sich die Werbeindustrie und erfindet zu jedem verbraucherfreundlichen Gesetz gefühlt zehn neue Buzzwords, die kein Mensch versteht. Ganz klar: Wer seine Daten schützen will, muss Marketing studieren – oder unser Glossar lesen.

Von **Andrea Trinkwalder**



Bild: Sven Hauth

Kleingedrucktes verstehen

Privatsphäre: Verstehen statt wegklicken	138
Datenschutz-ABC	142
Onlinewerbung und Datenschutz	148
Zwischen Datenschutz und -nutz	156
Datenschutz-Fragezeichen bei Apps	164

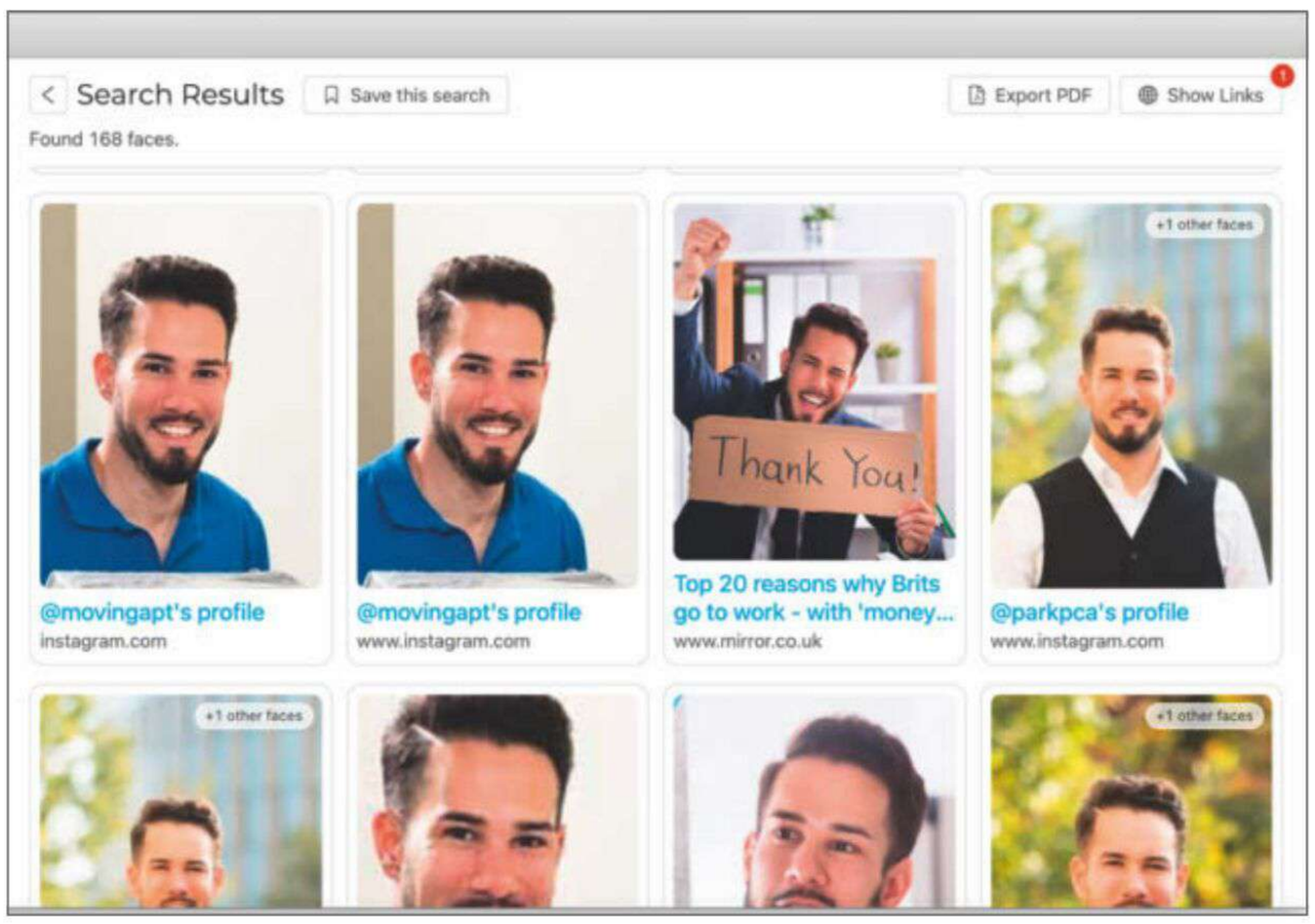
Es war einmal ein sicherer Hafen für Daten von EU-Bürgern in den USA. Der war zwar kein Hafen, sondern ein Abkommen, und auch nicht sicher, weil Geheimdienstler trotzdem auf die Verbraucherdaten zugreifen durften. Deshalb wurde der Hafen trockengelegt und durch einen Privatsphäre-Schild ersetzt. Bis herauskam, dass der bloß ein umetikettierter sicherer Hafen ist – also auch nicht sicher. Der Europäische Gerichtshof erklärte den Schild für unwirksam, weshalb die Daten in den USA jetzt ohne Hafen und ohne Schutzschild herumliegen beziehungsweise dort nicht mehr einfach herumliegen dürfen – und die Welt um zwei schöne Buzzwords ärmer ist. Das fällt aber kaum ins Gewicht: Es bleiben noch genügend andere, die Verwirrung stiften und Privatsphäre draufschreiben, wo Überwachung drinsteckt.

Die zentralen Begriffe rund um Datenschutz, -sammeln und -verwertung zu verstehen, ist wichtig, denn täglich verlangen zig Cookie-Banner eine informierte Einwilligung und es vergeht kaum eine Woche ohne Privacy-Grundsatzdiskussionen in den Medien oder vor Gericht. Meist wird dabei auch um die Auslegung der in der DSGVO verwendeten Begriffe gestritten, die Datenschützer naturgemäß sehr eng und Verwerter recht großzügig interpretieren. Das Feilschen und Tricksen beginnt schon bei den zentralen Definitionen der DSGVO, die wir ab Seite 142 erklären (Was sind überhaupt personenbezogene Daten und ab wann kann man von informierter Einwilligung sprechen?), und endet bei Implementierungsdetails wie etwa der Werbe-ID für Mobilgeräte.

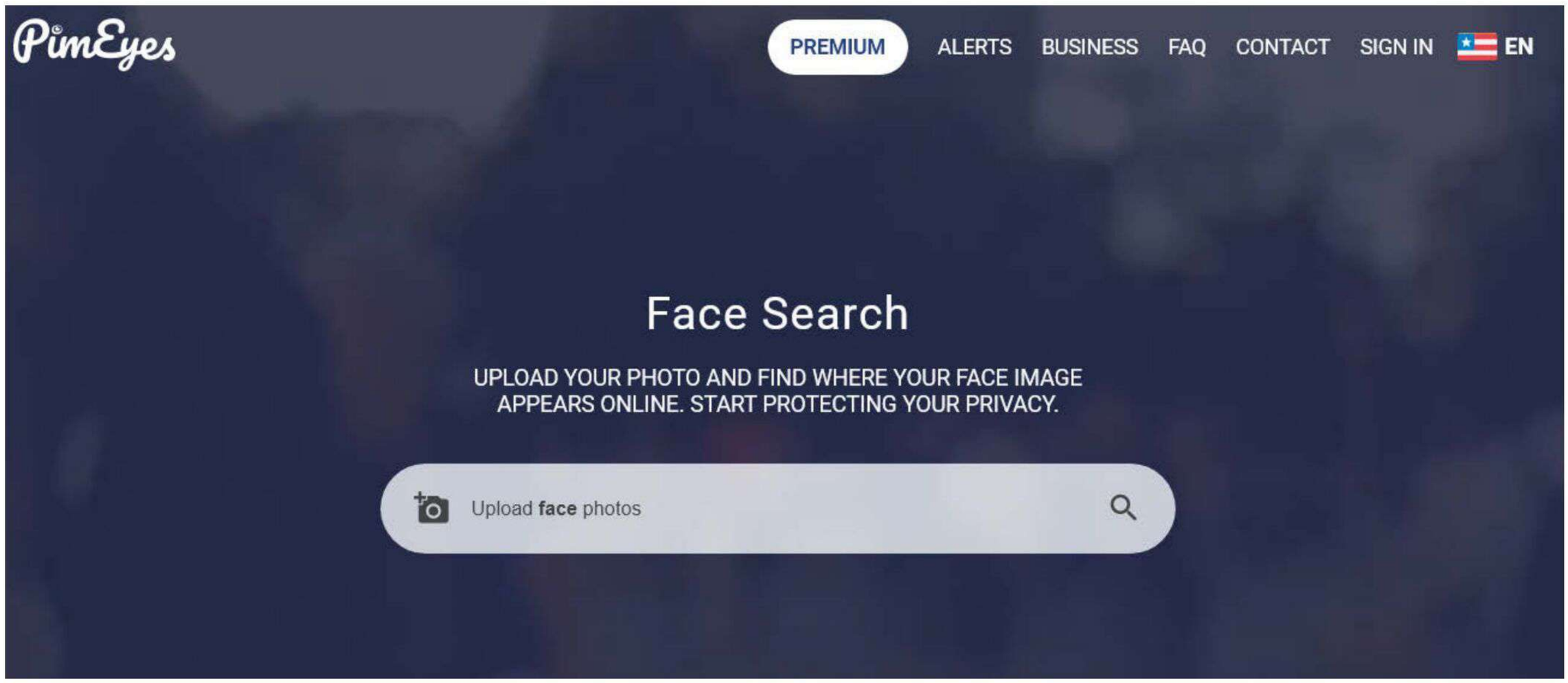
Die lässt sich unter iOS durch Überschreiben mit Nullen praktisch deaktivieren, unter Android aber nur zurücksetzen, woraufhin das System eine neue Identifikationsnummer generiert. Unter Googles Mobilsystem lässt sich die ID also faktisch nicht stilllegen und App-Hersteller könnten theoretisch die alte mit der neuen ID verknüpfen – also den Nutzer weiterhin über Apps und Geräte hinweg tracken. Unterm Strich hat die Werbebranche wohl die höchste Perfektion entwickelt, wenn es darum geht, sich hart an der Grenze des Erlaubten zu bewegen und diese Grenzen permanent auszuloten. Das Glossar ab Seite 148 erklärt den Fachjargon und die Tricks der Marketing-Branche – auch für aufmerksame Zeitgenossen lesenswert, die bei einem Cookie-Banner noch nie versehentlich auf „Alle akzeptieren“ geklickt haben.

Selbstbedienung

Enormen Klärungsbedarf schaffen KI-basierende Verfahren. Beispiele sind die Personensuchmaschinen Clearview (USA) und PimEyes (mittlerweile auf den Seychellen, ursprünglich in Polen beheimatet), die aus öffentlich zugänglichen Personenfotos von Facebook, Instagram und Co. mit einem Scraper kurzerhand riesige biometrische Datenbanken aufgebaut haben – mit mehreren Milliarden Datensätzen bei Clearview und 900 000 bei PimEyes. Diese lassen sich anhand eines Beispielfotos nach weiteren Aufnahmen der abgebildeten Person durchsuchen. Das Scraping verstößt gegen die Nutzungsbedingungen der Social-Media-Plattformen, aber verstoßen Clearview und PimEyes auch gegen die DSGVO? Deren Artikel 9 verbietet in der Regel die Verarbeitung biometrischer Daten zur Identifizierung von Personen. Doch wie das Beispiel Werbe-ID zeigt, entscheidet sich häufig an Details, ob ein Anbieter sich noch im Rahmen des rechtlich Zulässigen bewegt. Der scheidende Hamburgische Datenschutzbeauftragte Johannes Caspar erließ im Januar eine Anordnung zur Löschung von Daten in einem Einzelfall, was Kritikern nicht weit genug geht. Die Bürgerrechtsbewe-



Privater Fahndungsdienstleister: Clearview hat eine Datenbank mit einigen Milliarden Einträgen aus Social-Media-Bildern aufgebaut.



Bitte nur eigene Porträts hochladen: Die Personensuchmaschine PimEyes verkauft sich seit Neuestem als Tool zum Schutz der Privatsphäre.

gungen Privacy International (PI), die vom Datenschutzaktivisten Max Schrems gegründete Organisation Noyb, das Hermes Center for Transparency and Digital Human Rights und Homo Digitalis haben nun zumindest eine Reihe rechtlicher Beschwerden gegen Clearview eingereicht mit dem Ziel, die Firma generell am Abgreifen der Daten europäischer Bürger zu hindern.

Ob und in welchem Maß Daten verarbeitet werden dürfen, hängt auch von deren Gefährdungspotenzial ab. Immer wieder stößt man deshalb auf halbseidene Anonymisierungsversprechen, die entweder bewusst oder unbewusst nicht erfüllt werden. Wie anonym ist k-Anonymität? Und ist Differential Privacy gut (wegen der Privatsphäre) oder schlecht, weil es wie ein astreiner Buzzword-Begriff klingt und an „Alternative Fakten“ erinnert? Wie aufwendig das Verschleiern der Identität angesichts von Big Data und Künstlicher Intelligenz geworden ist und dass auch maschinelles Lernen keine uneingeschränkte Datennutzung rechtfertigt, erfahren Sie ab Seite 156.

Datenoase

Trotz der Urteile des EuGH gibt es ihn noch: Den sicheren Hafen. Er befindet sich in Irland und bewahrt die großen Datenkonzerne, die dort ihre EU-Niederlassung haben, traditionell vor allzu strenger Besteuerung. Ganz nebenbei erweist sich der finanziell vorteilhafte Firmensitz auch angesichts der DSGVO als echter Glücksgriff für die Unternehmen, weil die für sie zuständige irische Datenschutzbehörde wichtige Verfahren gegen die Tech-Riesen systematisch verschleppt, so der Vorwurf des österreichischen Datenschutzaktivisten Max Schrems.

Zwar hat der EuGH im Juni 2021 entschieden, dass auch andere nationale Datenschutzbehörden in Irland ansässige Unternehmen vor den Kadi zerren dürfen. Aber ob und wann dieses Urteil Anwendung findet, ist noch offen. Generell gilt: Bleiben Sie aufmerksam. Dazu gehört auch, das juristische Kauderwelsch in Datenschutzerklärungen zu Websites und Apps verstehen zu können. Eine Anleitung dazu finden Sie ab Seite 164. (atr) c't



Herbstcampus

Wissen, Inspiration und Praxisrelevanz

15. September 2021 – Online

Jetzt Tickets sichern!

Die gewohnt kommunikative Konferenz für Unternehmensentwickler mit:

- mehr als 20 Vorträgen
- Themenclustern aus drei Vorträgen und interaktiven Diskussionen
- Themen: Softwarearchitektur, Containerisierung, Java, APIs, Infrastructure as Code, Teamwork & Weiterentwicklung
- Diskussionsrunden per Chat und Video
- virtuellem Get-together am Abend

www.herbstcampus.de

Silber-Sponsoren

e.solutions

infoteam software

Veranstalter

iX

heise Developer

dpunkt.verlag



Bild: Sven Hauth

Datenschutz-ABC

Was genau sind eigentlich personenbezogene Daten? Was bedeutet in der Praxis die im Datenschutz geforderte Transparenz? Und was bringt mir als Verbraucher das Prinzip der Datensparsamkeit? Im Rahmen unseres Privacy-Ratgebers lüften wir diese Geheimnisse und erklären die wichtigsten Begriffe und Grundlagen der DSGVO.

Von **Joerg Heidrich**

Mit einer Handvoll wichtiger Begriffe steckt die europäische Datenschutzgrundverordnung die Grenze zwischen Privatsphäre und Datensammlern ab. Nur wer deren zentrale Ideen versteht, kann sich gegen Begehrlichkeiten wappnen – und verliert beim Katz-und-Maus-Spiel rund um die europäischen Vorgaben nicht den Faden.

Das Datenschutz-Grundrecht

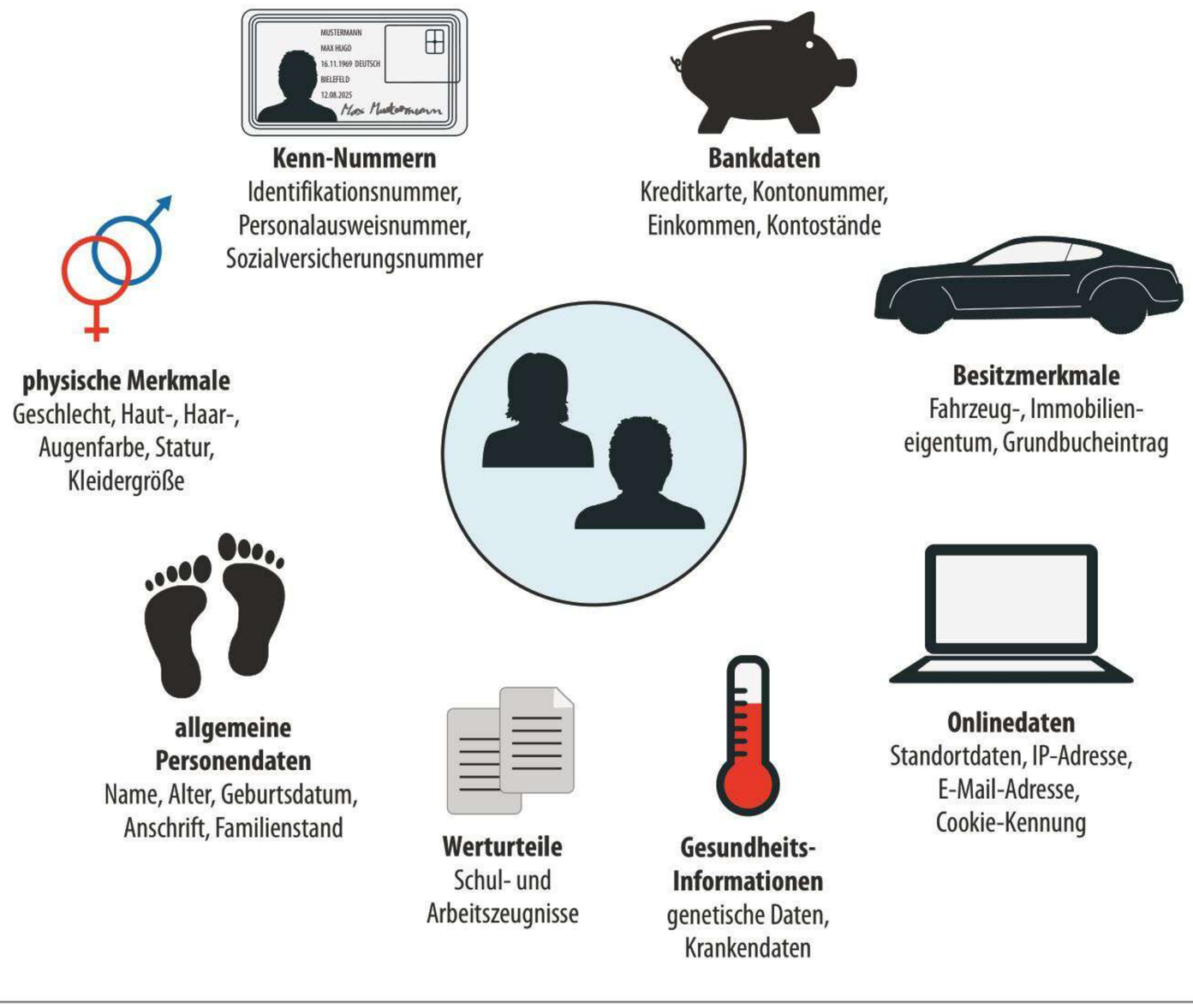
Dass persönliche Daten ein potenziell kritisches Gut sind und sich durchaus gegen ihren „Urheber“ wenden können, hat man schon lange vor Big Data erkannt und deren Schutz vorausschauend im **informationellen Selbstbestimmungsrecht** verankert. Es ist das elementare Grundrecht des Datenschutzes und gesteht dem Einzelnen zu, selbst über die Preisgabe und Verwendung seiner höchstpersönlichen Daten entscheiden zu dürfen. Im Unterschied zu den anderen Grundrechten findet es sich allerdings nicht im Grundgesetz (GG), sondern wurde im Jahr 1983 vom Bundesverfassungsgericht im Rahmen des Volkszählungsurteils geboren: als Weiterentwicklung des **allgemeinen Persönlichkeitsrechts**, siehe ct.de/wrdy.

Die Begründung von damals ist im Jahr 2021 aktueller denn je: Die freie Entfaltung der Persönlichkeit setze „unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus“. Wer sich unsicher sei, ob abweichende Verhaltensweisen jederzeit festgestellt und gespeichert würden, werde versuchen, nicht durch bestimmte Verhaltensweisen aufzufallen. Aufgrund dieses „nachhaltigen Einschüchterungseffektes“ könne der Bürger seine Persönlichkeit nicht mehr frei entfalten – wogegen ihn das Recht auf informationelle Selbstbestimmung schützen soll.

Unter das Grundrecht auf informationelle Selbstbestimmung und in den Anwendungsbereich der DSGVO fallen ausschließlich die sogenannten **personenbezogenen Daten**. Dazu gehören alle Informationen, mit deren Hilfe man eine natürliche Person identifizieren kann oder die sie zumindest identifizierbar machen: ganz naheliegend also alle Angaben, die unmittelbar auf eine bestimmte Person hinweisen wie etwa Name, Adresse oder Fotos. Darüber hinaus umfasst der Begriff aber auch Informationen, bei denen man zusätzliche Kenntnisse braucht, um jemanden zu bestimmen: zum Beispiel Telefonnummer, Autokennzeichen oder Matrikelnummer. Lange gestritten haben die Juristen um die Einordnung von dynamischen IP-Adressen. Inzwischen ist man sich aber einig, dass auch diese Angabe eine Person identifizierbar macht – nämlich mithilfe des Providers, dem die Kontaktdaten des Anschlussinhabers vorliegen. Für nachwachsenden Diskussionsstoff sorgt in der Regel die Werbeindustrie mit ihren immer neuen Ideen, Benutzer zu tracken, angeblich ohne sie zu

Was sind personenbezogene Daten?

Darunter versteht man alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, zum Beispiel:



identifizieren: etwa der fürs Cross-Device-Tracking (S. 150) verwendbaren Werbe-IDs, insbesondere der von Android (S. 153).

Das höchste Schutzniveau genießen die in Artikel 9 der DSGVO genannten **besonderen Kategorien personenbezogener Daten**. Beim Blick auf die Details wird schnell klar, warum: Darunter fallen Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit. Gleiches gilt für genetische und biometrische Daten, Gesundheitsdaten sowie Informationen über das Sexualleben oder die sexuelle Orientierung. Während die DSGVO bereits die Nutzung „normaler" personenbezogener Daten stark reglementiert, liegt die Hürde bei den sensiblen Daten besonders hoch: Diese darf man nur in Ausnahmefällen verarbeiten, etwa zum „Schutz lebenswichtiger Interessen der betroffenen Person" oder wenn die jeweilige Person explizit eingewilligt hat. Außerdem muss man dabei sehr hohe technische und organisatorische Anforderungen erfüllen, um unbefugten Zugriff zu verhindern (Anonymisierung, Pseudonymisierung, siehe S. 156).

Wider den Datenhunger

Die **Zweckbindung** ist einer von mehreren elementaren Grundsätzen des Datenschutzes, die Unternehmen praktisch bei jedem Verarbeitungsschritt beachten müssen. Sie dürfen personenbezogene Daten nur für den Zweck verwenden, zu dem sie ursprünglich erhoben wurden. Und: Diesen Anlass müssen sie vorab festlegen und mitteilen. In der Praxis darf also eine Firma, die aus Sicherheitsgründen IP-Adressen speichert, diese nicht einfach so der Marketingabteilung für ihre Kampagnen überlassen. Unter Umständen sitzt ein Unternehmen also auf einem wahren Datenschatz an Kundeninformationen, darf diesen aber nur eingeschränkt auswerten – weshalb die Zweckbindung auch als „Big-Data-Killer" gilt. Denn gerade das Zusammenkippen von diversen Informationen aus unterschiedlichsten Töpfen und deren Verarbeitung läuft dem Grundsatz der Zweckbindung fundamental entgegen.

Zu den wichtigen Grundsätzen zählen außerdem die **Erforderlichkeit** und die **Datensparsamkeit**. Sie sollen sicherstellen, dass nur solche Daten erfasst und genutzt werden, die der Dienstleister für die jeweilige Aufgabe tatsächlich benötigt. Ausgeschlossen ist das Sammeln von „nice-to-have-Daten". So muss für den Versand eines E-Mail-Newsletters die E-Mail-Adresse genügen, eventuell ergänzt um den Namen. Postanschrift, Telefonnummer oder Geburtsdatum darf der Anbieter daher allenfalls freiwillig abfragen, nicht jedoch als Pflichtfelder.

Die Datensparsamkeit ist eng mit dem Recht auf Vergessen verbunden. Geprägt hat diesen Begriff ursprünglich der Europäische Gerichtshof (EuGH). Dieser hatte im Jahr 2014 entschieden, dass natürliche Personen unter bestimmten Voraussetzungen die Tilgung von Suchmaschinenergebnissen zu ihrer Person verlangen können [1]. Die DSGVO spricht in Artikel 17 von einem **Recht auf Vergessenwerden**, meint damit aber viel weitergehende Rechte als das Suchmaschinenurteil: Demnach dürfen Personen von jeder Stelle, die Informationen über sie speichert, die unverzügliche Löschung ihrer Daten verlangen. Dieser Anspruch besteht allerdings nur dann, wenn der Anbieter keine Rechtsgrundlage zum Vorhalten der betreffenden Daten hat oder diese nach der Erhebung weggefallen ist.

Das Wegfallen der Rechtsgrundlage wiederum kann der Betroffene selbst forcieren, indem er von seinem **Widerrufsrecht** Gebrauch macht und eine früher gegebene Einwilligung zurückzieht. Vor allem für KI-Algorithmen, also mithilfe von Beispieldaten trainierte Systeme, kann solch ein nachträglicher Datenentzug recht unangenehme Folgen haben.

Unternehmen und andere Speicherstellen benötigen also ausgefeilte **Löschkonzepte**, um regelmäßig und automatisiert Daten aus ihren Systemen zu tilgen, bei denen die Erlaubnis zur Speicherung weggefallen ist. So müssen Firmen zwar aus steuerlichen Gründen die Daten aus geschlossenen Verträgen zehn Jahre lang aufbewahren, nach Ablauf dieser Frist aber unverzüglich löschen. Solche Daten länger zu speichern oder auch Informationen aufzubewahren, für die keine Einwilligung oder gesetzliche Erlaubnis besteht, stellt einen Rechtsverstoß dar, der durchaus teuer werden kann. Für eine solche Verhaltensweise wurde Ende 2019 gegen eine große Immobilienfirma ein Bußgeld von über 14 Millionen Euro verhängt. Das Unternehmen hatte unter anderem Daten zu lange aufbewahrt und zudem auch Informationen wie etwa Gehaltsbescheinigungen oder Kontoauszüge unberechtigterweise vorgehalten.

Schutz durch Wissen

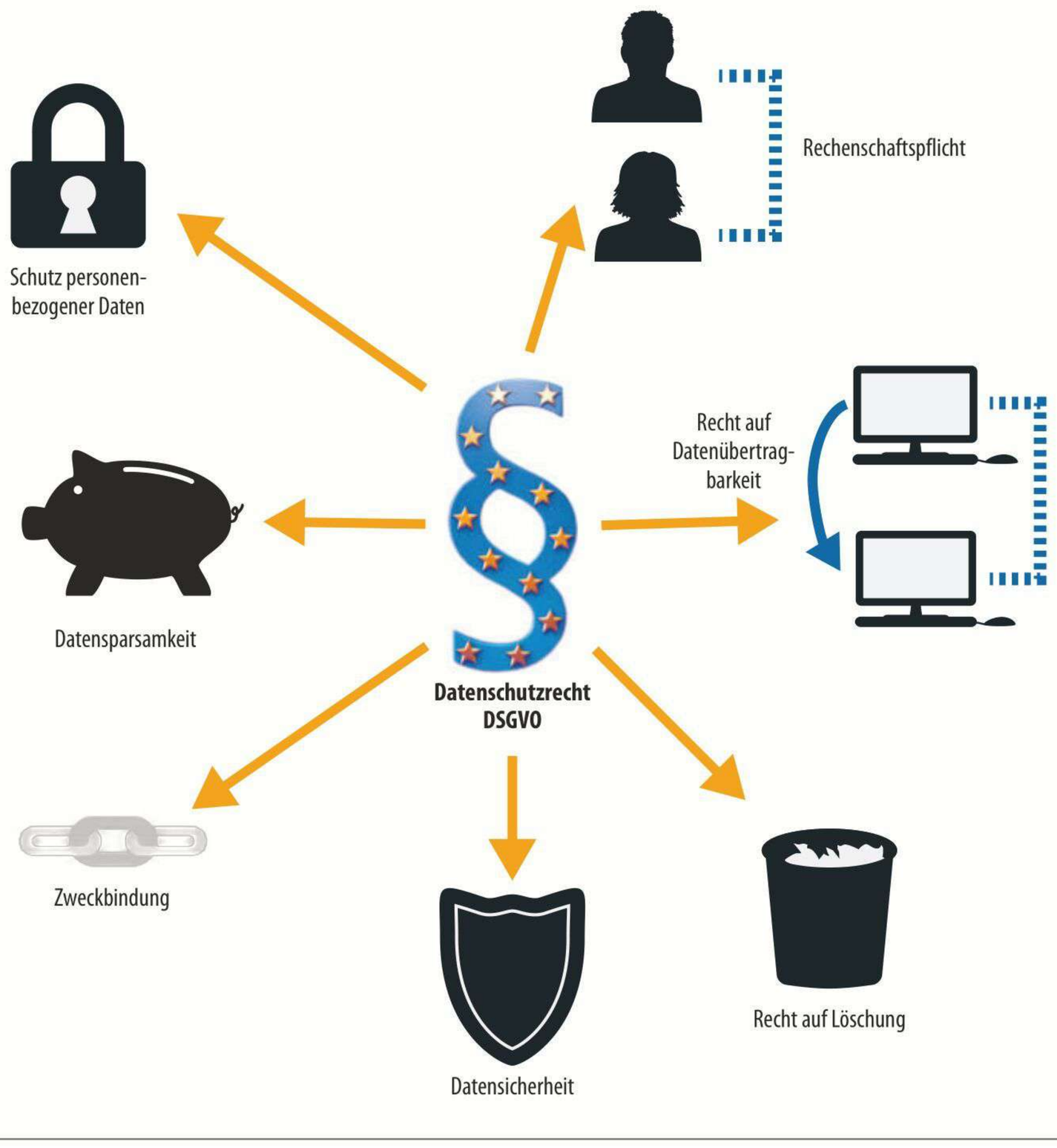
Was genau Datenkonzerne oder der Supermarkt von nebenan so im Laufe der Zeit gesammelt haben, erfahren Betroffene dank **Auskunftsrecht**,

das jeder gegenüber dem Verarbeiter seiner Daten geltend machen kann. Dieses ist auch Teil der Anforderungen an die **Transparenz** der Datenhaltung. Konkret kann der Bürger nicht nur Auskunft über die von ihm gespeicherten Informationen verlangen, sondern auch über deren Weitergabe oder geplante Löschung. Jedes Unternehmen ist verpflichtet, eine Auskunft innerhalb einer Frist von einem Monat zu erteilen – auch wenn keine Daten gespeichert sind. Antragsvorlagen können Sie unter ct.de/wrdy herunterladen.

Die **Einwilligung** in die Verarbeitung der eigenen Daten ist neben der Zweckbindung eine der tragenden Säulen der DSGVO. Der Bürger soll selbst entscheiden, ob er mit der Nutzung seiner Informationen einverstanden ist. Wichtig: Die Einwilligung muss freiwillig erfolgen, also ohne Zwang oder Druck. Ein solcher Zwang kann sich nach Ansicht des

Grundprinzipien der DSGVO

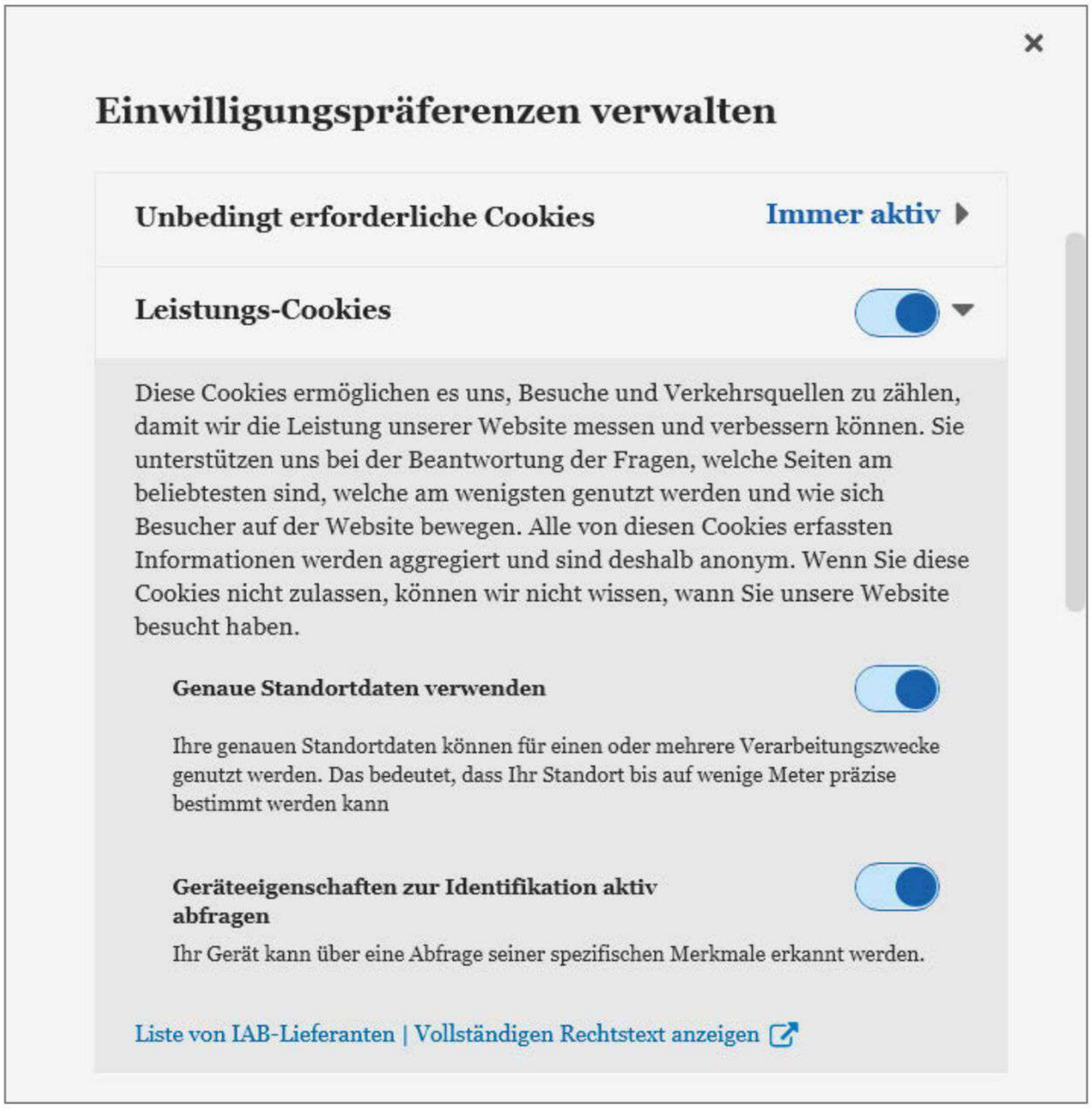
Datenschutz ist ein Grundrecht. Die DSGVO schafft mit ihren zentralen Prinzipien wie Zweckbindung und Datensparsamkeit den Rahmen dafür, wie dieser Schutz in der Praxis umgesetzt werden soll.



Bundeskartellamts in Sachen Facebook auch aus der marktbeherrschenden Stellung des Anbieters ergeben (Az.: B6-22/16).

Sehr praxisrelevant ist die zusätzliche Verpflichtung, den Betroffenen vor der Einwilligung über die geplante Nutzung seiner Daten aufzuklären. Er muss wissen, was ihn erwartet, und auf dieser Basis seine Entscheidung treffen können. Daher muss der Text zur Einwilligung in klarer Sprache aufzeigen, was mit den Informationen wie und wo geschehen soll, es braucht also einen **Informed Consent**. Erst dann kann die Zustimmung erteilt werden – in der Offline-Welt meist durch eine Unterschrift, online reicht das Aktivieren eines **nicht vorangekreuzten** Kästchens (Consent Banner, siehe S. 154). Dieses Verfahren bezeichnet man als **Opt-in**.

Im Gegensatz dazu steht das im US-amerikanischen Raum verbreitete und nicht mehr zulässige **Opt-out-Verfahren**, das den Unternehmen einen fast uneingeschränkten Zugriff auf Daten aller Art bescherte. Es setzt voraus, dass ein Nutzer mit einer Handlung einverstanden ist. Möchte er dies nicht, muss er aktiv widersprechen. Im Falle der E-Mail-Werbung würde er also einfach angeschrieben und müsste von sich aus erklären, dass er damit nicht einverstanden ist. Ein solches Vorgehen wäre in Deutschland aber in den meisten Fällen unwirksam. Wichtige Ausnahme: Für bestehende Geschäftsverbindungen gilt ausnahmsweise eine Opt-out-Regel.



Cookie-Banner mit vorangekreuzten Kästchen sind noch nicht ausgestorben, obwohl die DSGVO das Opt-out-Verfahren für „Nice-to-have-Daten" verbietet.

Vorteil durch Technik

Eine ganz neue und angesichts des hohen technischen Entwicklungstempos wichtige Sichtweise auf den Datenschutz hat die DSGVO etabliert, indem sie die IT-Sicherheit zum elementaren Bestandteil der rechtlichen Vorgaben macht. Unter anderem müssen Unternehmen ihre Daten bei der Verarbeitung vor fremdem Zugriff schützen – und zwar nicht nach Gusto, sondern nach **Stand der Technik**. Darunter versteht man technische Maßnahmen, die dem Markt zur Verfügung stehen und die sich in der Praxis als geeignet und effektiv bewährt haben – also solide, aktuelle Sicherheitssysteme.

Der Stand der Technik muss immer wieder auf neue Entwicklungen geprüft werden, um die Datensicherheit gewährleisten zu können. Auch dieses Thema hat schon die Gerichte beschäftigt. So hat das Landgericht Würzburg in einer der ersten Entscheidungen zur DSGVO (Az.: 11 O 1741/18) vom September 2018 ausgeführt, dass beim Erheben von Daten über ein Kontaktformular „zwingend auch eine Verschlüsselung der Homepage erforderlich" sei. Gemeint ist hier offenbar die SSL/TLS-Verschlüsselung für Websites und insbesondere für Formulare, die laut Gericht stets vorliegen muss.

Ebenfalls zu den technischen Anforderungen der DSGVO gehören die in Artikel 25 neu geschaffenen Vorgaben, Datenschutz bereits bei der Entwicklung von Hard- und Software mitzudenken und Produkte möglichst in einer datenschutzfreundlichen Version an den Mann und die Frau zu bringen. **Privacy by Design**, also „Datenschutz durch Technikgestaltung" bedeutet, dass Produkte von vornherein DSGVO-konform konzipiert sein müssen. Um dieses Ziel zu erreichen, fordert Erwägungsgrund 78 der DSGVO ausdrücklich, personenbezogene Daten zu minimieren sowie möglichst schnell zu pseudonymisieren. Produktentwickler sollten daher immer prüfen, ob sie

die darin ausgeführten Maßnahmen entsprechend umgesetzt haben, wie zum Beispiel die Anonymisierung oder Pseudonymisierung von IP-Adressen (siehe S. 156) oder das automatisierte Löschen von Logfiles.

Diese Regelung wird flankiert vom Gebot der **Privacy by Default**, also dem Schutz der Betroffenen durch datenschutzfreundliche Voreinstellungen. Demnach muss der Hersteller die Default-Parameter und -Optionen in Hard- und Software so setzen, dass sie nur die zwingend notwendigen Daten erheben. Diese Verpflichtung bezieht sich auf die Menge der erhobenen Informationen, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. So sollte zum Beispiel ein Social-Media-Anbieter seinen Dienst so konfigurieren, dass zunächst einmal möglichst wenige Informationen nach außen ersichtlich sind und an Dritte weitergegeben werden.

Privatsphäre-Schild?

Moderne IT kommt nicht ohne Arbeitsteilung aus, weshalb personenbezogene Daten in der Regel an eine Vielzahl von Dienstleistern weitergeleitet werden. Verarbeiten diese Informationen im Auftrag, unter Kontrolle und nach Anweisungen des Auftraggebers, so liegt eine **Auftragsverarbeitung** nach Artikel 28 DSGVO vor. Die Liste solcher Verarbeitungsvorgänge ist lang und umfasst die Verlagerung von Daten in die Cloud ebenso wie die Beauftragung eines Callcenters oder Mailversenders für Marketingaktionen, die Papier-, Akten- und Datenträgervernichtung sowie auch die Nutzung externer Analyse-Tools wie Google Analytics (siehe S. 153).

Bei einer solchen Weitergabe von Daten an Dritte ist neben dem eigentlichen Vertrag eine gesonderte Vereinbarung zur Auftragsverarbeitung (AVV) zu schließen. Sinn und Zweck ist es, zu gewährleisten, dass die dem Dritten anvertrauten Informationen nur zu den vereinbarten Zwecken und auf die vereinbarte Art und Weise verwendet werden. Insbesondere muss die AVV detailliert festlegen, welche **technischen und organisatorischen Maßnahmen (TOM)** zum Schutz der Daten ergriffen werden; entsprechende Vorlagen stellen Datenschutzbehörden sowie der Bitkom zum Download (siehe ct.de/wrdy).

In einer digitalisierten Welt machen Daten schon lange keinen Halt mehr an Landesgrenzen. Dennoch verstößt ein allzu freizügiger Umgang mit sensiblen Informationen klar gegen die DSGVO. Transfers innerhalb des europäischen Binnenmarktes unterliegen denselben Voraussetzungen wie im Inland. Ähnlich unproblematisch gelingt der Austausch mit einer Handvoll Länder, denen die EU ein vergleichbares Datenschutzniveau zubilligt. Zu diesen sogenannten **sicheren Drittstaaten** gehören Israel, Kanada, Neuseeland, Japan und neuerdings auch Großbritannien. Fließen Informationen jedoch über Cloud- oder andere Dienste beispielsweise in die USA, müssen einige Vorgaben beachtet werden. Denn die USA zählen – ebenso wie etwa Indien oder China – nicht zu den sicheren Drittstaaten.

Bislang konnten sich Unternehmen recht mühelos auf die **Privacy-Shield**-Vorgaben berufen, die einen Transfer in die USA erlaubt haben, wenn der Empfänger sich in ein Register eingetragen hat. Seit dem 16. Juli 2020 ist diese Regelung jedoch Geschichte und durch den Europäischen Gerichtshof für ungültig erklärt worden [2]. Damit ist über Nacht die zentrale Rechtsgrundlage des transatlantischen Datenverkehrs weggefallen. Wer trotzdem Daten in die USA exportieren will, kann dies derzeit nur innerhalb eines Konzerns tun oder verwendet die von der Europäischen Kommission genehmigten und im Juni aktualisierten **Standarddatenschutzklauseln**. Dabei handelt es sich um eine Vertragsvorlage, in deren Rahmen sich der US-amerikanische Anbieter verpflichtet, europäischem Datenschutz zu genügen. Allerdings sind auch diese Regeln nach dem EuGH-Urteil angezählt: Es steht noch nicht fest, ob diese Klauseln weiter uneingeschränkt gültig sind.

Ein besonders unangenehmes Kapitel der DSGVO stellen für Unternehmen die **Meldepflichten** der Artikel 33 und 34 dar. Kommt es bei der Verarbeitung zu einer **Verletzung des Schutzes personenbezogener Daten**, so muss der Verantwortliche sich innerhalb von 72 Stunden ab Kenntnis gegenüber der zuständigen Datenschutzbehörde seines Bundeslands erklären (**Databreach Notification**). Eine solche Meldepflicht gilt für Vorfälle, die ein „Risiko für die Rechte und Freiheiten natürlicher Personen“ darstellen. Praktisch ist dies bei nahezu jedem Datenverlust der Fall, sei es online, in einer falsch verschickten E-Mail oder durch einen verlorenen Laptop – und natürlich durch große Datenlecks wie etwa Anfang 2020 beim Autovermieter Buchbinder.

Entsteht gar ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen (in der Regel die Kunden des Unternehmens), müssen auch diese unverzüglich informiert werden. Aus PR-Sicht ist das die Höchststrafe – flankiert von einem saftigen Bußgeld, das die Aufsichtsbehörden der Bundesländer in solchen Fällen verhängen werden.

(atr) c't

Literatur

[1] Joerg Heidrich, **Das Recht auf Vergessenwerden**, c't DSGVO 2021, S. 32

[2] Joerg Heidrich, **Das Ende des Privacy Shields**, c't DSGVO 2021, S. 112

Weitere Infos und Antragsvorlagen

ct.de/wrdy



Bild: Sven Hauth

Onlinewerbung und Datenschutz

Werbung gehört zum heutigen Internet wie Tankstellen zum Autoverkehr. Werbetreibende sind gierig auf Nutzerdaten. Deshalb sollte man zumindest das Grundvokabular dieser Branche verstehen, die gerne mit Buzzwords kommuniziert.

Von **Torsten Kleinz**

Onlinewerbung ist ein Riesengeschäft: Im Jahr 2020 hat die deutsche Werbebranche knapp vier Milliarden Euro nur mit sogenannter Displaywerbung (S. 149) umgesetzt. Das schätzt der Online-Vermarkterkreis im Bundesverband Digitale Wirtschaft. Kaum eine kommerzielle Website kommt ohne Werbung aus.

Ein wesentlicher Treiber der Onlinewerbung sind benutzerbezogene Daten: Je mehr ein Werbeunternehmen über einen Surfer weiß, desto zielgerichteter

kann es Werbung auf ihn zuschneiden und desto höhere Werbeerlöse erzielt es. Jeder, der sich im Internet bewegt, ist daher in ein System eingebunden, das seine Daten vermarktet.

Es kann durchaus rechtmäßig sein, personenbezogene Daten zu erheben, denn Werbung finanziert viele Websites (mit). Entscheidend sind die Transparenz der Anbieter und der Wille des Verbrauchers (Informed Consent, S. 146): Website-Betreiber müssen klarmachen, welche personenbezogenen Daten sie erheben und mit welchen Unternehmen sie sie teilen – und der Surfer muss dem zustimmen.

Die DSGVO schreibt außerdem vor, dass Unternehmen Kunden „in einer klaren und einfachen Sprache“ informieren müssen. Liest man sich die Datenschutzerklärungen von Websites sowie die Consent Banner (S. 154) zur Datenweitergabe durch, die vielen Websites vorgeschaltet sind, ist da allerdings oft noch viel Luft nach oben. Da finden sich dann schon mal Begriffe wie Browser Fingerprinting (S. 69) oder Supply-Side Platform (siehe Grafik auf S. 151) ohne große Erklärung.

Dieses Glossar soll Ihnen helfen, das schon recht spezielle Kauderwelsch der Online-Werbeindustrie zu entschlüsseln – und zu verstehen, was die Fachbegriffe mit Ihnen und Ihren Daten zu tun haben.

Werbeformen

Displaywerbung ist nach wie vor eine der wichtigsten Umsatzquellen beim Online-Marketing. Der Begriff bezeichnet ganz generell die Einblendung von Inhalten auf den Webseiten Dritter, seien es Texte, Bilder oder Videos.

Das **Suchmaschinenmarketing** – kurz: **SEM** für **Search Engine Marketing** – ist hingegen ein eigenständiger Markt. Das bekannteste Beispiel ist der Dienst Google Adwords, der Anzeigen passend zur Suchanfrage über oder neben den organischen Suchergebnissen bei Google anzeigt. Wer etwa nach einer Automarke sucht, kann hier Anzeigen von lokalen Händlern sehen, Werbung für ein Konkurrenzmodell oder einen Tarif für Autoversicherungen. Auch andere Suchmaschinen haben das Geschäftsmodell übernommen, allgemein heißt es **Search Engine Advertising (SEA)**.

Bei der **Search Engine Optimization (SEO)** hingegen wird der Suchmaschinenanbieter nicht direkt bezahlt. Stattdessen handelt es sich um Maßnahmen auf Webseiten, um die Platzierung bei den organischen Suchergebnissen zu verbessern. So müssen alle Informationen für den Google-Bot gut lesbar gemacht werden, damit Seiten ideal platziert werden.

Das **Affiliate Marketing** ist ein Werbemodell, bei dem Partner (Affiliates) Provisionen für von ihnen generierte Leads (S. 154) oder Verkäufe erhalten. Wenn Sie zum Beispiel einen Preisvergleichsdienst nutzen und dann von dort aus in einen Shop wechseln und ein Produkt kaufen, erhält der Anbieter des Preisvergleichers eine Provision.

Beim **Influencer Marketing** platziert der Werbetreibende eigene Inhalte in bestehenden Kanälen, zum Beispiel in einem beliebten Blog oder Instagram-Account. Der Preis richtet sich nach Reichweite und Verkaufstalent des Influencers.

Das Werbe-Ökosystem

Die technischen Werbedienstleister nennen sich selber gerne **Adtech**-Anbieter. Insbesondere das Feld der Displaywerbung ist heute ein hochgradig ausdifferenziertes und vernetztes Geschäftsfeld mit vielen spezialisierten Akteuren und mit besonders weit gehenden Auswirkungen auf den Datenschutz. Sofern nicht anders vermerkt, geht es im Folgenden daher um Online-Displaywerbung.

Website-Betreiber vermarkten die Werbeplätze auf ihren Sites nicht selber, sondern arbeiten mit Dienstleistern zusammen, die diese Aufgabe für sie übernehmen – und oft wiederum viele weitere Partner einspannen. Wer letztlich ein Werbemittel für einen bestimmten Werbeplatz ausliefert, handeln verschiedene Marktteilnehmer mitunter automatisch innerhalb von wenigen Millisekunden aus.

Damit so etwas funktioniert, sind **Displayformate** standardisiert. Zudem können Werbeunternehmen damit eine einmal entworfene Kampagne auf den verschiedensten Websites schalten.

Die Branche ist sehr kreativ, was neue Formate und ihre Bezeichnungen betrifft. Sollten Ihnen im Kontext von Werbung die Begriffe **Skyscraper** oder **Preroll** unterkommen: Das sind solche Standardformate für Bildwerbung. Ersteres bezeichnet ein besonders hochformatiges Bildformat, das meist rechts neben dem Inhalt der Website angezeigt wird.

Prerolls sind Videos, die vor dem eigentlichen Inhalt der Website oder eines anderen Videos angezeigt werden. Wenn Sie sich im Detail für Werbemittel interessieren: Das Interactive Advertising Bureau (IAB) ist für die Standards zuständig; auf der Homepage der Organisation finden Sie weitere Informationen (ct.de/wths).

So harmlos eine Display-Werbung auf den ersten Blick erscheinen mag, etwa ein Banner: Solche Werbemittel werden in der Regel von einem **Ad-Server** des Werbetreibenden geladen, der damit auf jeden Fall Ihre IP-Adresse erfährt. Oft liefert der Ad-Server das Werbemittel außerdem huckepack mit weiteren Inhalten aus, etwa Cookies (S. 152) oder anderen Mitteln für das Targeting (nächster Absatz).

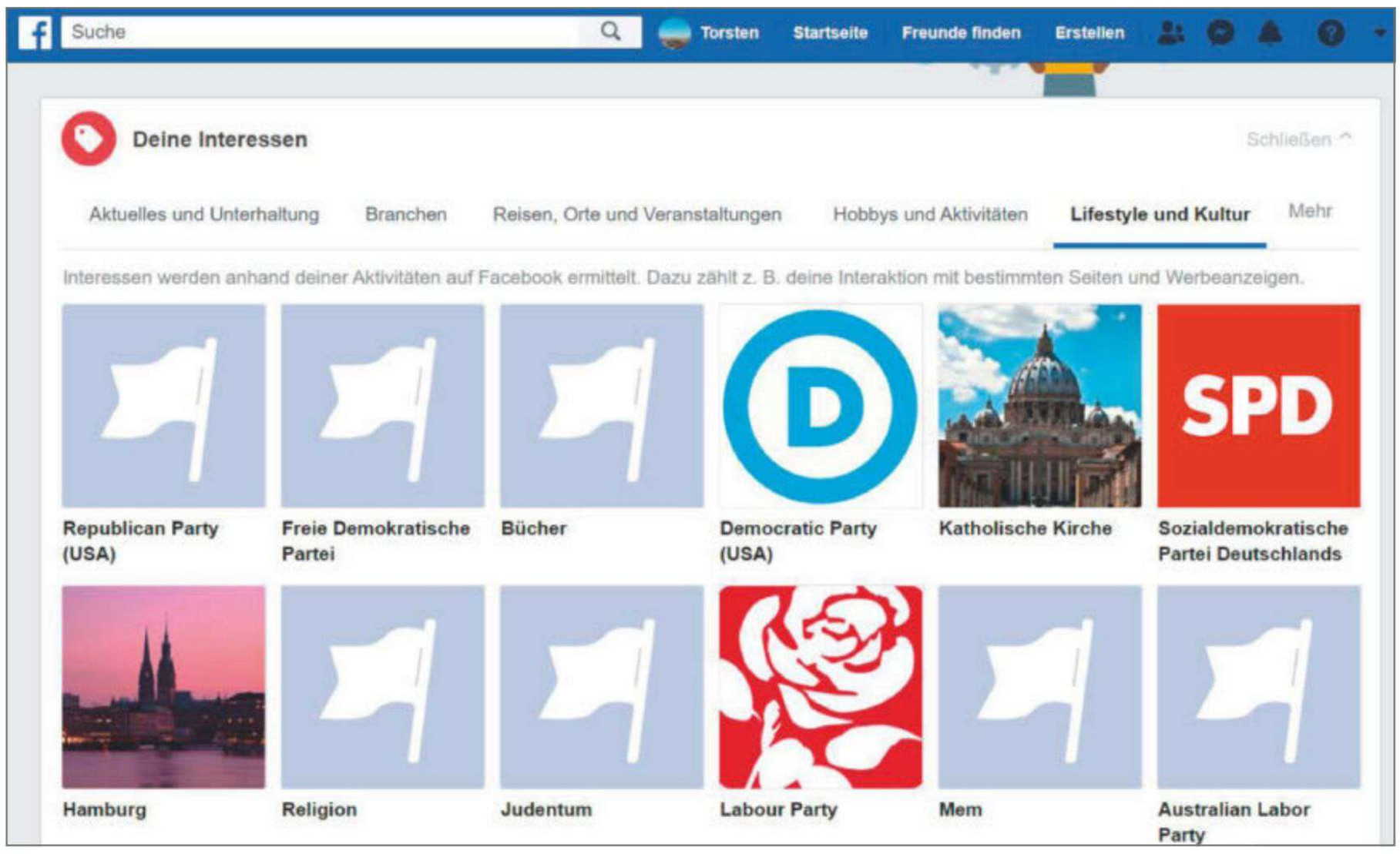
Zielgenau

Beim **Targeting** können Werbekunden nach verschiedensten Kriterien bestimmen, wo sie ihre Werbung ausspielen wollen – etwa nur zu bestimmten Uhrzeiten oder wenn der Wetterbericht Regen ankündigt. Möglich wird das über **Werbenetzwerke** wie das Google Display Network. Diese bündeln Anzeigenaufträge und verfügbare Werbeplätze. So müssen deren Kunden nicht bei jeder Website einzeln anfragen, ob die Platzierung funktionieren kann. Die Netze verteilen die Werbung quer über alle teilnehmende Betreiber.

Vordergründig nutzt Targeting allen: dem Website-Betreiber, dem Werbeunternehmen und dem Surfer: Erstere können mit Targeting mehr Geld für die Werbung auf ihren Seiten einnehmen. Werber wiederum können ihre Budgets zielgenauer und kostengünstiger verteilen. Und Endnutzer erhalten relevantere Werbung: So bekommt der Bastler einfacher mit, wenn es etwa einen Sonderverkauf von Lötkolben gibt, während überzeugte Radfahrer weniger Werbung für neue Automodelle sehen.

Damit Targeting funktionieren kann, benötigen die Werbedienstleister allerdings Daten über die Nutzer. Dafür zeichnen Werbenetze und andere Dienstleister auf, welche Websites Surfer aufsuchen und für welche Inhalte sie sich dort interessieren. Daneben landen noch viele weitere Informationen in ihren Datenbanken: der Standort des Nutzers, sein Browser, der Gerätetyp, manchmal sogar der Akkuladestand eines Gerätes und noch viel mehr. Dank dieses **Trackings** können die Werbenetze Rückschlüsse auf die Kaufinteressen der Nutzer ziehen.

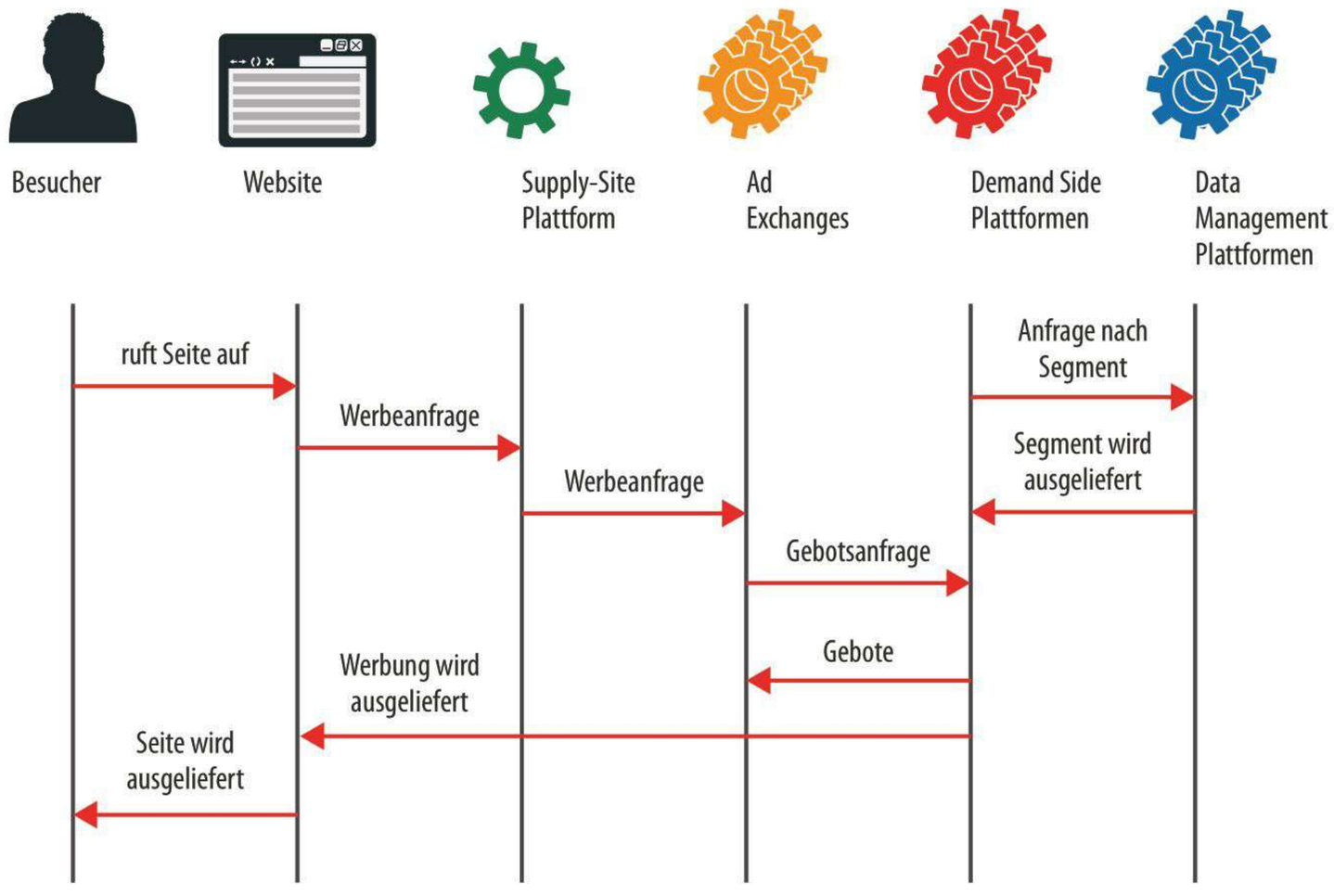
Mit **Predictive Behavioural Targeting** kann die Werbeindustrie sogar auf Daten schließen, die sie gar nicht explizit erfasst hat. So liegt die Vermutung nahe, dass sich ein Leser von Heise Online für Technik interessiert. Wenn ein Nutzer die Fan-Foren von koreanischen Boy-Bands und Hausaufgabenhilfen aufsucht, hat man es vermutlich mit einem jüngeren



Grundlage für das Targeting: Daten über die Nutzer. Facebook zeigt hier, welche Interessen es einem Nutzer zuordnet.

Real Time Bidding

Ein Werbetreibender stellt seine Anfrage auf einer Demand Side Plattform (DSP) ein, zum Beispiel ein Banner, das gezielt über 40-jährigen, an BMWs interessierten Männern angezeigt werden soll. Ruft ein Besucher eine Webseite auf, stellt der Website-Betreiber den darin enthaltenen Werbeplatz auf einer Supply Side Platform ein, die das Angebot über eine Ad Exchange an eine oder mehrere DSPs weiterleitet. Die Daten zur Zielgruppe erhält eine DSP aus Data-Management-Plattformen. Hat eine DSP eine Kampagne, die zum Benutzer passt, bietet sie auf den Werbeplatz. Gewinnt sie die Auktion, liefert sie die Werbung aus.



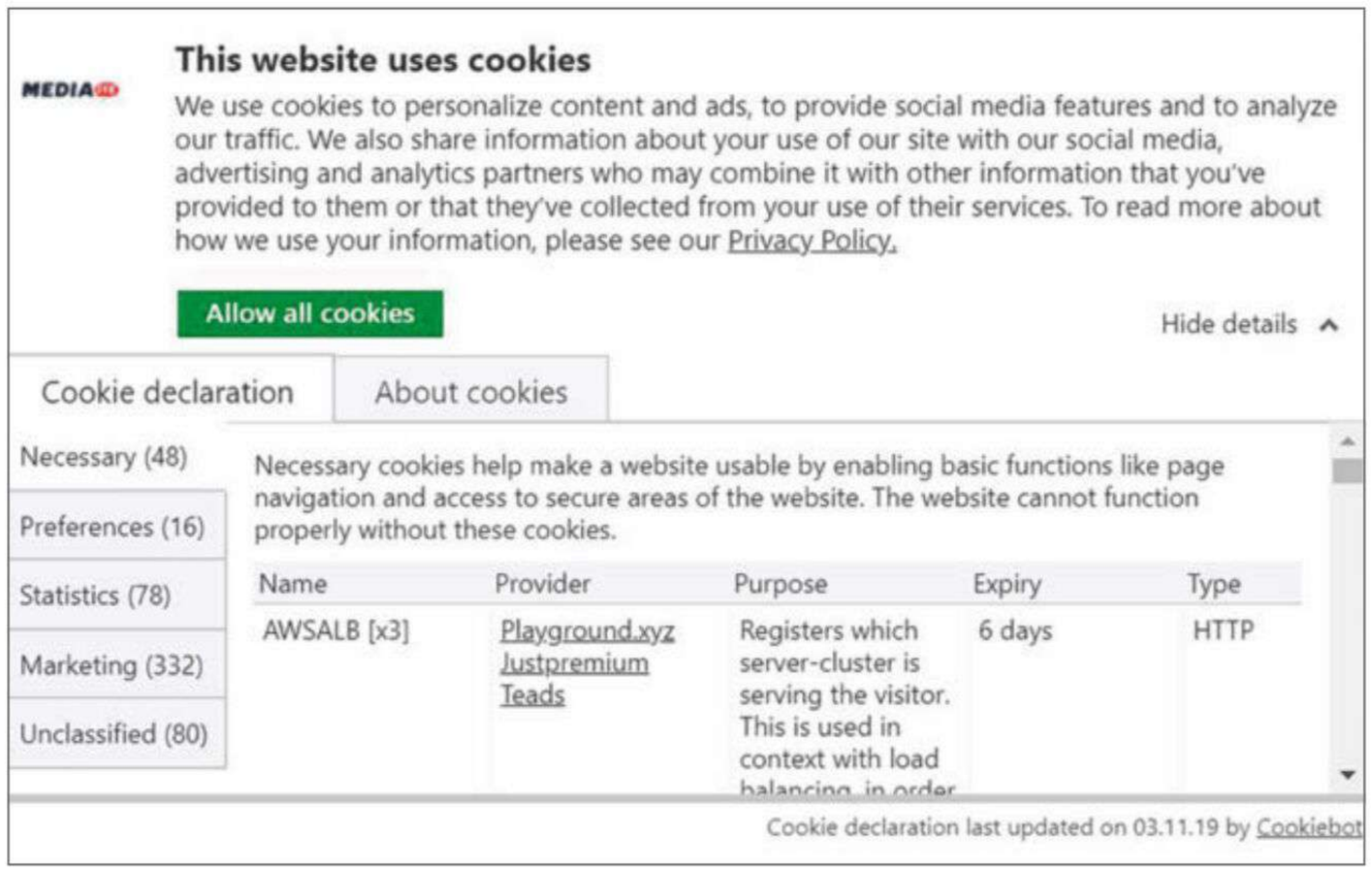
Semester zu tun. Aus tausenden solcher Annahmen und Nutzerstatistiken stellen die Werbenetzwerke ausgiebige **Werbeprofile** zusammen.

Nicht alle dieser Schlussfolgerungen sind korrekt. Wenn Sie mögen, können Sie die Probe aufs Exempel machen: Schalten Sie bei Google die personalisierte Werbung erst ab und dann wieder an. Danach können Sie in der Übersicht Ihres Google-Werbe-Accounts zusehen, wie Ihr Werbeprofil anwächst. Alter, Hobbys, Familienstand – sogar darüber, ob Sie in einer Mietwohnung oder in einer eigenen Immobilie wohnen, stellt Google hier Vermutungen an. Je mehr Daten zusammenkommen, umso umfassender wird das Profil.

Retargeting haben Sie wahrscheinlich schon selbst einmal erlebt, etwa wenn Sie sich in einem Onlineshop für ein bestimmtes Produkt interessiert, es aber dann doch nicht gekauft haben (und manchmal auch, wenn Sie es gekauft haben). Das hat zur Folge, dass Werber das Interesse an diesem Produkt prominent in Ihrem Werbeprofil ablegen – und Sie in der Folge plötzlich Werbung für exakt diesen Artikel zu sehen bekommen.

Lukrative Versteigerungen

Programmatische Werbung treibt das Targeting auf die Spitze. Insbesondere Google hat ein weltweites Auktionssystem etabliert, bei dem Werbekunden auf die Einblendung ihrer Anzeigen auf einem bestimmten Werbeplatz bieten können. Das heißt: Noch während eine Webseite lädt, laufen im Hintergrund



Websites setzen schon mal mehrere hundert Cookies.

automatisierte Hochgeschwindigkeits-Auktionen, bei denen ausgehandelt wird, welche Firma welchen Werbeplatz beliefern darf. Die Auktionsplattformen nennen sich **Supply-Side Plattformen (SSP)**. Wie eine solche Versteigerung abläuft, skizziert die Infografik „Real Time Bidding".

Bei der programmatischen Werbung ist der Privatsphäreverlust für Website-Besucher maximal: Ihre Werbeprofile werden kreuz und quer durch das Netz und die Verwertungsketten geschickt. Wie umfangreich die Datenprofile sind, demonstrierte etwa ein Datenleck bei der Oracle-Tochter Bluekai. Darin fanden sich neben der Web-Historie und einzelnen Transaktionen der Nutzer sogar E-Mail- und Hausadressen (siehe ct.de/wths).

Cookies und andere Tracker

Die für lange Zeit wichtigste technische Grundlage beim Nutzer-Tracking sind **Cookies**, genauer gesagt: Third Party-Cookies. Wenn sie keine Cookies setzen können, weichen einige Anbieter auf Techniken aus, die der Oberbegriff **Browser Fingerprinting** zusammenfasst. Die Begriffe Cookies und Browser Fingerprinting erklärt der Artikel auf Seite 72 ausführlich.

Auch **Social-Media-Plug-ins** wie Like- und andere Buttons von Facebook, Twitter und Co. oder Inhalte-**Widgets** wie YouTube-Player haben eine ähnliche Wirkung wie Cookies: Bettet ein Website-Betreiber sie in seine Seiten ein, können die Plattformen mitverfolgen, wer die jeweiligen Seiten aufgerufen hat.

Recht verbreitet ist zudem auch das für Website-Besucher unsichtbare **Facebook-Pixel**. Bettet ein Website-Betreiber dieses in seine Seiten ein, erfasst Facebook alle Seitenaufrufe. Das wiederum können die Website-Betreiber nutzen, um in Facebook Besucher gezielt wieder anzusprechen. Oder der Website-Betreiber kann gezielt Facebook-Nutzer adressieren, die ähnliche Interessen haben wie die Besucher seiner Site, die diese aber noch nicht kennen.

Website-Betreiber arbeiten nicht selten mit Dutzenden Dienstleistern zusammen, die eigene Skripte auf den Seiten einbetten, sodass eine eigene Management-Lösung für die Skripte notwendig wird: ein sogenanntes **Tag Management** – auch so ein Begriff, der in Datenschutzerklärungen auftauchen kann. Damit können Webmaster Skripte je nach Bedarf schnell automatisiert austauschen, ohne bei jeder Änderung den Quellcode einer Website bearbeiten zu müssen.

Analytics

Die Auslieferung von Werbung geht in vielen Fällen mit Analysemaßnahmen einher. Damit überprüfen Website-Betreiber, welche ihrer Inhalte besonders beliebt sind, wo Besucher ihre Seiten verlassen – wo

man also etwa etwas nachbessern muss – und wo mitunter Seiten sogar kaputt sind. Vielleicht können sie ja auch die **Conversion Rate** der Werbemittel erhöhen, um mehr Provision zu kassieren – indem sie mehr Besucher, die ein Werbebanner präsentiert bekommen, dazu bewegen, es anzuklicken.

Die einfachste Möglichkeit, solche **Analytics**-Aufgaben anzugehen, besteht darin, die **Log-Dateien** des eigenen Webservers auszuwerten. Dort fallen schon viele interessante Informationen an, etwa die IP-Adressen der Besucher und die Abrufzeitpunkte der Seiten.

Für viele Zwecke reichen die Daten des Website-Betreibers aber nicht aus. Um gegenüber Partnern, also zum Beispiel Werbekunden, ausweisen zu können, wie viele Besucher und Seitenabrufe seine Website hat, muss er vertrauenswürdige Zahlen eines darauf spezialisierten Dritten aufbieten. Dazu bettet dieser zum Beispiel **Zählpixel** ein, die von seinem externen Server geladen werden. Damit können sie verlässlich ermitteln, wie oft welche Seiten aufgerufen wurden.

In Deutschland ist das zum Beispiel die **Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern**, **IVW**. Um die Besucher von Websites zu zählen, bettet sie Zählpixel in Webseiten der angeschlossenen Sites ein. Auch die **Verwertungsgesellschaft Wort**, **VG Wort**, die die Tantiemen aus Zweitverwertungsrechten von Textautoren verwaltet, bettet Zählpixel in Webseiten ein, um zu messen, wie häufig Onlinetexte gelesen wurden. Im Vergleich zu anderen Tracking- und Analyseverfahren sind die Zählpixel der IVW und der VG Wort aber harmlos.

Das unter Webmastern mit Abstand beliebteste Analyse-Tool ist **Google Analytics**. Mit diesem Onlinewerkzeug können sie zum Beispiel überprüfen, ob ihre Seiten gut in der Google-Suche ranken, wie lange Besucher auf den Seiten verweilen und wo sie herstammen. Damit lässt sich der Erfolg von Werbekampagnen detailliert kontrollieren. Der Preis: Jeder Seitenabruf jedes Nutzers landet in Googles Online-Tool.

Mobiles und Geomarketing

Auf Mobilgeräten ist die Wiedererkennbarkeit für das Tracking bereits eingebaut: Sowohl Apple als auch Google vergeben bei Smartphones und Tablets eine zentrale Geräte-Identifikationskennung, auf die Apps zugreifen können, um einen Nutzer wiederzuerkennen: Die **Werbe-ID** ist also ein Super-Cookie für Mobilgeräte. Loggt sich ein Nutzer in Apps ein, kann die Werbe-ID zudem einem Werbeprofil zugeordnet werden, das auch die Aktivität auf anderen Geräten einbezieht.

Viele Apps binden Software von Google, Facebook oder anderen Werbeanbietern direkt ein und liefern so ausreichend Informationen, um Nutzer wieder einem Werbeprofil zuzuordnen. Parallel versuchen App-Entwickler immer wieder auch zu erfassen, welche anderen Apps ein Nutzer installiert hat, um so Verknüpfungen herzustellen.

Eine der spannendsten Informationen für viele Vermarkter ist: Wo befindet sich ein Nutzer? So können Ladenketten nur in Städten werben, wo sie eigene Filialen haben. Oder Nutzer können gezielt beworben werden, bevor sie auf ihrer Joggingrunde an einem neuen Eiscafé vorbeikommen.

Die Vermarkter können hier auf verschiedene Methoden zugreifen. Zum einen liefert die IP-Adresse des Nutzers zumindest eine grobe Orientierung, von wo aus er zugreift. Ist ein Nutzer mit seinem Smartphone unterwegs, kann der Standort auch per GPS erfasst werden oder über die etwas ungenauere Ortung via Mobilfunkmasten. Wenn der Nutzer zustimmt, kann dies etwa über den Browser geschehen. Viele Werbenetzwerke versuchen, den Standort auch möglichst permanent über im Hintergrund laufende Apps zu erfassen. Das **Geomarketing** erklärt auch, warum Nutzer auf internationalen Websites wie etwa der New York Times deutsche Werbung wiederfinden.

Proximity Marketing geht eine Stufe weiter: Sogenannte **Beacons** senden ständig ein Bluetooth-Signal aus, das von Smartphones in der Nähe empfangen wird. Hat der Nutzer eine entsprechende App installiert, wird auf diese Weise erfasst, wo er sich ganz genau befindet – etwa im Eingangsbereich eines Geschäfts oder vor einem Weinregal. Dementsprechend können dann Werbungen auf das Handy geschickt werden.

Nicht zu Verwechseln ist das Werbe-Tracking mit dem **Tracing** der deutschen Corona-Warn-App. Die App speichert ausdrücklich keine Bewegungsprofile und verhindert durch einen ständigen Austausch der Kennung, dass Bewegungsprofile angelegt werden können.

Abrechnungsdetails

Ähnlich standardisiert wie die Werbeformate sind die Zahlungsmodelle für die Abrechnung. Bei **Cost per Mille (CPM)** – auch bekannt als **Tausenderkontakt-**

preis TKP – wird das Geld ausbezahlt, wenn die Werbung nur angesehen wurde.

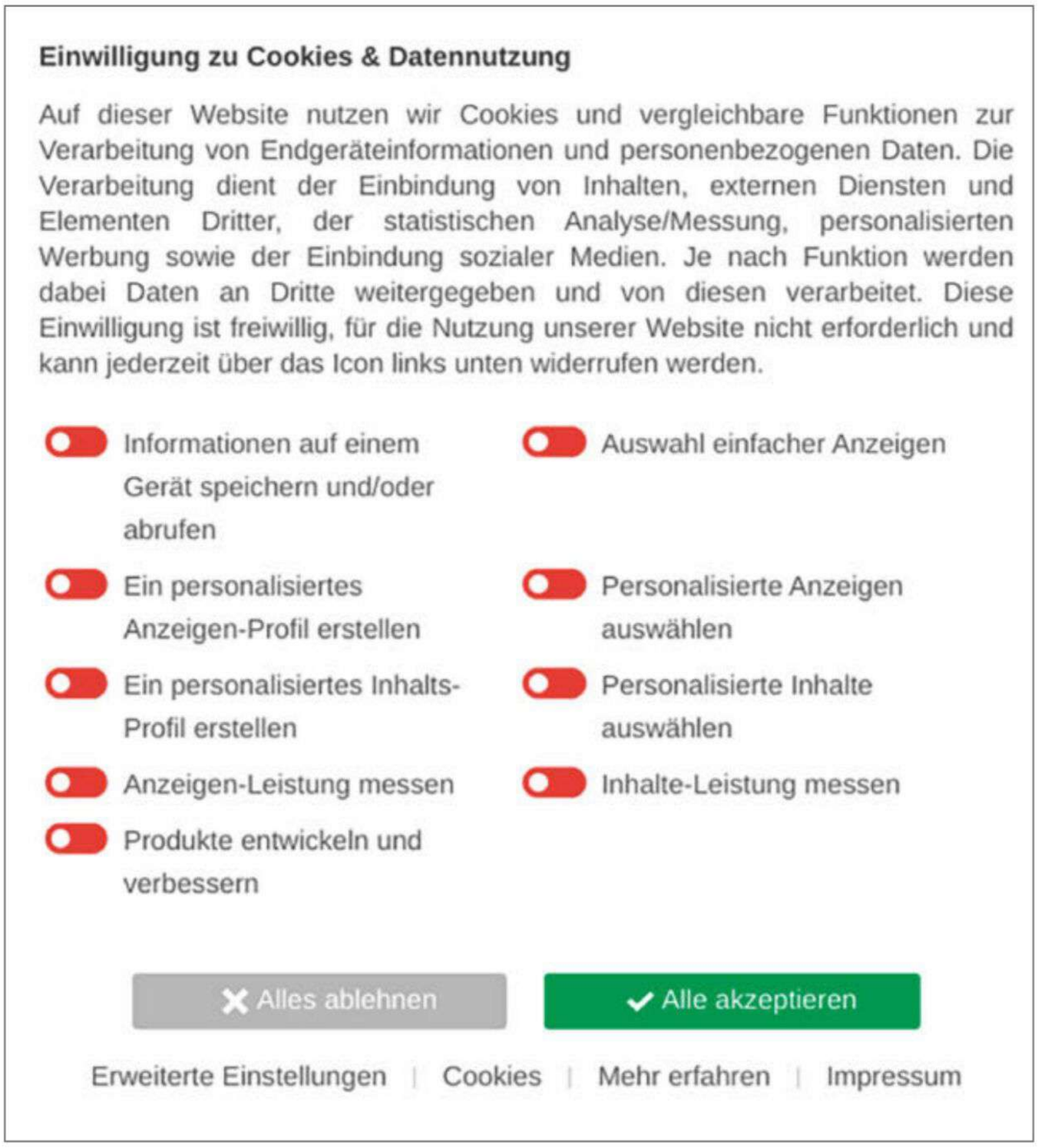
Andere Abrechnungsformen setzen **Leads** voraus, bestimmte Aktionen potenzieller Kunden (**Cost per Lead, CPL**). Im einfachsten Fall ist das ein Klick auf ein Werbemittel, der den Surfer dann zur Website des Werbekunden führt (**Cost per Click, CPC**). Ein Lead kann auch die Installation einer Software oder – bei Affiliate-Werbung – der Kauf eines Produkts sein (**Cost per Order, CPO**).

Dunkle Muster

Webmaster dürfen personalisierbare Daten zu Werbezwecken nur an andere Firmen weitergeben, wenn die Nutzer dieser Datenweitergabe zugestimmt haben. Daher finden sich auf vielen Websites inzwischen **Consent Banner** oder sogar Popups, die die Nutzer über den Datenschutz aufklären und das Einverständnis abfragen sollen. Oft können sie in einem **Consent Management** System detailliert einstellen, welche Cookies gesetzt werden dürfen und zu welchen Werbepartnern der Website-Betreiber welche Daten übertragen darf.

Hierbei kommen allerdings oft **Dark Pattern**s zum Einsatz, üble Tricks im Nutzerinterface-Design. Statt Informationen übersichtlich und einfach erfassbar zu gestalten, geht es bei Dark Patterns darum, den Nutzer zu einer Entscheidung zu bewegen, die nicht in seinem Interesse ist.

Ein beliebter Trick: Den Nutzern wird eine Vorauswahl präsentiert, die absolut akzeptabel erscheint: Die „essenziellen“ Cookies, die zum Funktionieren einer Webseite benötigt werden, sind freigeschaltet, Tracking- und Werbe-Cookies hingegen deaktiviert. Doch wenn der Nutzer dorthin klickt, wo man üblicherweise den OK-Button vermuten würde, gibt er die komplette Datenverwendung frei.



Dark Pattern: Wer nur schnell die Vorauswahl bestätigen will und auf den grünen Knopf drückt, wurde reingelegt.

Werbeblocker und Gegenmaßnahmen

Viele Nutzer versuchen sich komplett von Werbung und Werbe-Tracking zu befreien. Mittel der Wahl ist ein **Adblocker** oder **Tracker-Blocker**. Wichtig: Nicht jeder Adblocker unterbindet automatisch auch das Werbe-Tracking. Und Tracking-Blocker verhindern nicht automatisch die Auslieferung der Werbung.

Firefox, der neue Edge-Browser von Microsoft, Safari und einige weitere Browser haben bereits wirksame Tracker-Blocker eingebaut (siehe S. 72). Der meistverbreitete Browser Chrome vom Werberiesen Google soll solche Funktionen auch erhalten. Google lässt sich dafür aber noch Zeit. Immerhin kann man Chrome mit Add-ons wie uMatrix so aufrüsten, dass auch dieser Browser Werbung effektiv blockiert.

Einige Website-Betreiber mögen es nicht, dass Besucher ihre Werbung und Tracker ausblenden – und sperren solche Besucher aus. Andere wiederum sehen im Wunsch nach mehr Privatsphäre eine Geschäftschance. Für ein paar Euro im Monat erhält man zum Beispiel bei der Zeit und beim Spiegel Zugriff auf die Inhalte ohne eingebundenes Tracking und mit sehr viel weniger oder komplett ohne Werbung. (jo) c't

Literatur

[1] Torsten Kleinz, **Siegeszug der Daten**, Programmatic Advertising: Versteigerte Werbeplätze, c't 21/18, S. 40

Quellen und Tools

ct.de/wths

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.ct-special.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 Redakteurskürzel 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), Sylvester Tremmel (syt)

Koordination: Ann-Sophie Eikermann (ase), Angela Meyer (anm)

Redaktion: Jo Bager (jo), Holger Bleich (hob), Wilhelm Drehling (wid), Ronald Eikenberg (rei), Arne Grävemeyer (agr), Joerg Heidrich (joh), Jan-Keno Janssen (jkj), Michael Koch (miko), Jan Mahn (jam), Angela Meyer (anm), Peter Schmitz (psz), Hans-Peter Schüler (hps), Jan Schüßler (jss), Sylvester Tremmel (syt), Sebastian Trepesch (tre), Andrea Trinkwalder (atr), Marvin Strathmann (str), Axel Vahldiek (axv), Stefan Wischner (swi)

Mitarbeiter: Verena Ehrl, Torsten Kleinz, Jan Kopia, Miriam Legien

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

DTP-Produktion: Lara Bögner, Beatrix Dedek, Madlen Grunert, Lisa Hemmerling, Sarah Hiller, Natalie Hollstein, Kirsten Last, Martina Lübke, Steffi Martens, Sandeep Preinfalk, Marei Stade, Matthias Timm, Ricardo Ulbricht, Ninett Wagner

Fotografie: Andreas Wodrich, Melissa Ramson

Produktion: Christine Kreye (Ltg.), Melanie Becker, Anna Hager, Kevin Harte, Martin Kreft, Pascal Wissner

Illustration: Sven Hauth, Schülp; Thorsten Hübner, Berlin; Albert Hulm, Berlin; Andreas Martini, Wettin

Titel: Steffi Martens, www.flaticon.com, www.freepik.com, www.stock.adobe.com

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Dr. Alfons Schräder

Mitglieder der Geschäftsleitung: Beate Gerold, Jörg Mühle

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

Leiter Vertrieb und Marketing: André Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3–11, 86650 Wemding

Vertrieb Einzelverkauf:
VU Verlagsunion KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1800
E-Mail: info@verlagsunion.de

Einzelpreis: € 14,90; Schweiz CHF 27.90;
Österreich € 16,40; Luxemburg € 17,10

Erstverkaufstag: 24.08.2021

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, vervielfaltigt 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 in c't 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 2021 by
Heise Medien GmbH & Co. KG



Bild: Sven Hauth

Zwischen Datenschutz und -nutz

Gefahr für die Privatsphäre droht häufig dadurch, dass die Informationen von heute mit der Technik von gestern geschützt werden. Deshalb fordert die DSGVO Datenschutz durch Technikgestaltung – veraltete Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren akzeptiert sie nicht mehr.

Von **Michael Koch und Andrea Trinkwalder**

Datenschutz ist ein hohes Gut, Datenanalyse aber auch: Ohne sie gäbe es weder wissenschaftliche Erkenntnisse noch medizinischen, technischen oder wirtschaftlichen Fortschritt. Daten können zwar zum Überwachen und Manipulieren dienen, schaffen aber auch Transparenz und stärken die Demokratie, weshalb Open-Government-Initiativen das Veröffentlichen der von Behörden und anderen Institutionen gesammelten Informationen vorantreiben.

Um Datenschutz und -auswertung in Einklang zu bringen, sollten personenbezogene Informationen in einem möglichst frühen Stadium der Verarbeitungskette verfremdet oder ganz unkenntlich gemacht werden. Wie stark diese Verfremdung ausfallen muss, hängt von mehreren Faktoren ab – etwa der Sensitivität sowie dem Verarbeitungszweck.

Informationen ohne Personenbezug fallen nicht in den Geltungsbereich der DSGVO, dürfen also uneingeschränkt verarbeitet und sogar veröffentlicht oder verkauft werden – Stichwort **Datenhandel**. Auf der Suche nach der Vereinbarkeit von Privatsphäre, Wissensdurst und kommerziellen Interessen entwickeln sich deshalb clevere Techniken, um sämtliche Verbindung zwischen Informationen und Personen zu kappen – aber auch Strategien, die Anonymisierung nur vorgaukeln, um Nutzer auf Schritt und Tritt verfolgen zu können. Dabei kommt es auch häufig zu Missverständnissen und Verwechslungen rund um die Begriffe.

Identifizierbar oder nicht?

Anonymisierung im Sinne der DSGVO ist ein ziemlich eng gefasster Begriff. Er lässt nur Verfahren gelten, die jeglichen Personenbezug unwiderruflich aus den Daten tilgen – also eine **Re-Identifikation** des Einzelnen nahezu ausschließen: Die betreffende Person darf nicht mehr mit „vertretbarem Aufwand“ identifizierbar sein. In grauer Vor-IT-Zeit hat man einfach **direkte Identifikatoren** wie Name und Adresse entfernt – fertig war der Datensatz, der keinerlei Rückschlüsse mehr auf Personen erlaubte.

Doch in einer datengetriebenen, vernetzten Welt genügt das nicht. Heute finden schlaue Algorithmen selbst in vermeintlich nichtssagenden Aufzeichnungen Spuren, die das Individuum enttarnen. Fast jede Datenspur, die ein Mensch hinterlässt, kann verräterische individuelle Merkmale enthalten oder ein unverwechselbares Muster bilden: Von den täglich zurückgelegten Wegen über das Surfverhalten bis hin zu den auf Amazon oder Netflix vergebenen einfachen Sterne-Bewertungen. KI-Verfahren entlarven die Urheber von Produktrezensionen sogar allein anhand ihres Schreibstils.

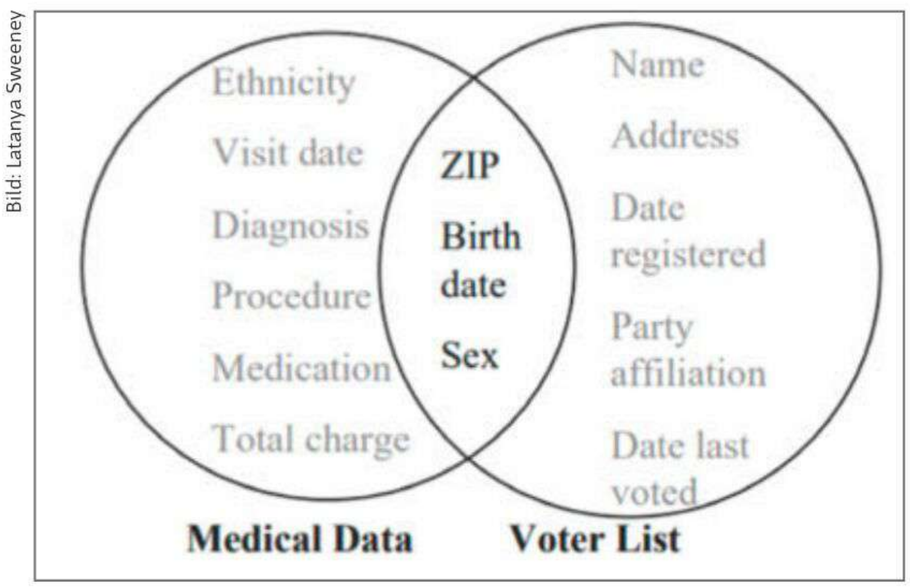
Unzureichend verschleierte Datensätze lassen sich in der Regel leicht mit zusätzlichen Datenquellen kombinieren (**Matching**), die einen eindeutigen Identifikator wie etwa den Namen oder die Telefonnummer enthalten. Auch Kombinationen weniger Merkmale können genügen, um eine Person zuzuordnen, weshalb diese auch als **Quasi-Identifikatoren** bezeichnet werden. So lassen sich 87 Prozent der US-Amerikaner allein anhand der Angabe von Postleitzahl, Geburtsdatum und Geschlecht identifizieren, was sich rechnerisch aus der Alterspyramide sowie der Anzahl der Postleitzahlen ergibt.

Die US-Wissenschaftlerin Latanya Sweeney demonstrierte die Gefahr, indem sie den Gouverneur von Massachusetts in einer vermeintlich anonymisierten Datenbank idenitifizierte. Dafür kombinierte sie einfach die von einer Krankenversicherung „anonymisiert“ veröffentlichten Patientendaten mit einem für 20 US-Dollar hinzugekauften Wählerverzeichnis, das die Klarnamen enthielt, siehe ct.de/wfy7

Aus Sicht der DSGVO gelten Daten, die sich durch zusätzliches Wissen wieder mit einer Person in Verbindung bringen lassen, als **pseudonymisiert** und damit als personenbezogen. Solche Daten dürfen nur im Einklang mit den DSGVO-Grundsätzen verarbeitet werden – zweckgebunden, datensparsam und meist nur mit expliziter Erlaubnis des Nutzers (informierte Einwilligung, S. 145). Auch durch zusätzliche Verschlüsselung verliert ein solcher Datensatz seinen Personenbezug übrigens nicht.

In der Pseudonymisierung sieht die DSGVO das Mittel der Wahl, um den Spagat zwischen möglichst hohem Datenschutz und möglichst guter Verwert-

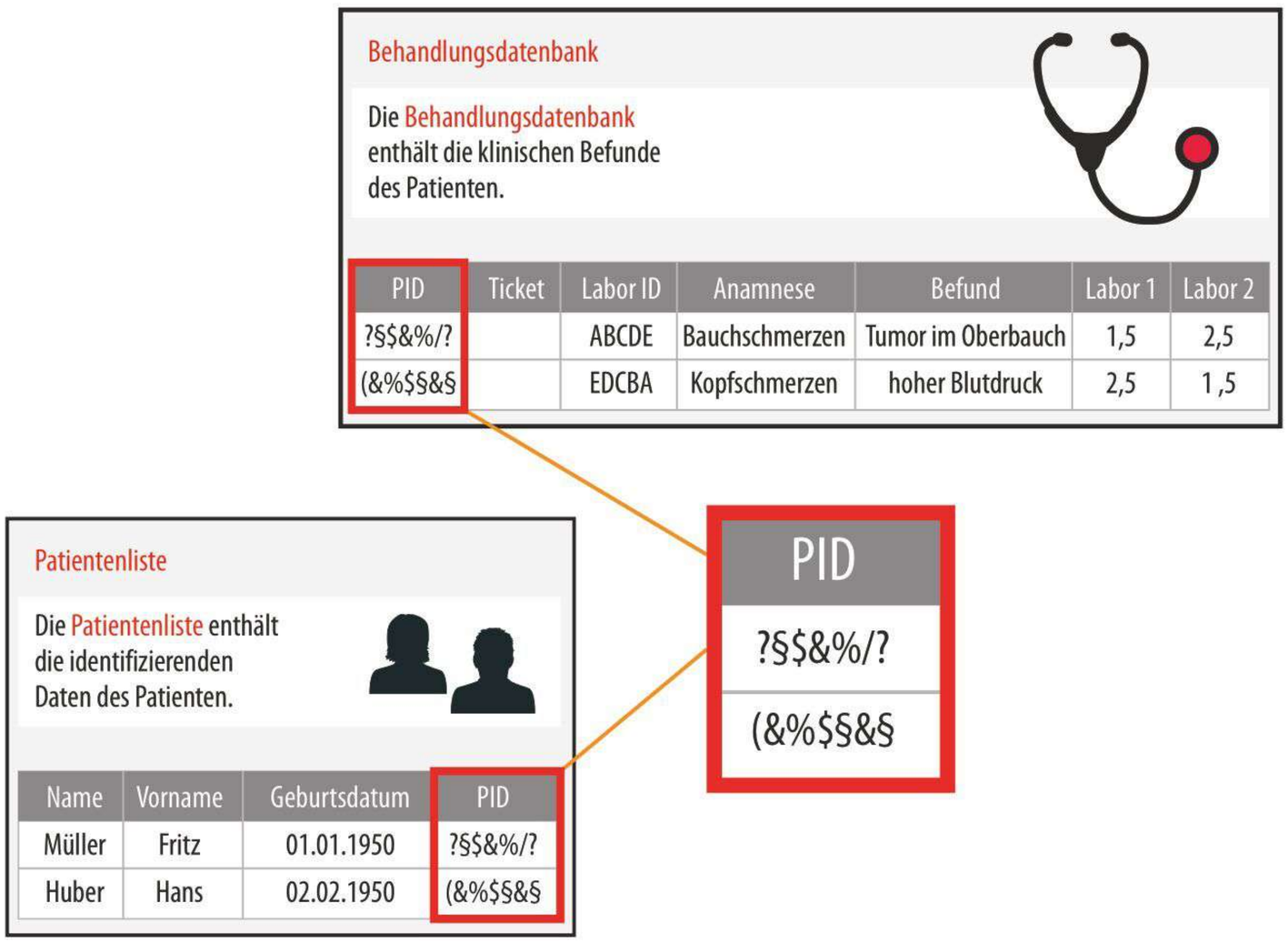
Bild: Latanya Sweeney



Um zu demonstrieren, wie leicht sich Anonymisierung durch geschickte Kombination mehrerer Quellen aufheben lässt, identifizierte die Forscherin Latanya Sweeney den Gouverneur von Massachusetts in einer unzureichend anonymisierten Datenbank mit Gesundheitsdaten – anhand eines Wählerverzeichnisses, das die Klarnamen enthielt.

Referenzierung über Pseudonym

Um Patientendaten zu pseudonymisieren, speichert man alle (Quasi-)Identifikatoren getrennt von den medizinischen Daten – verknüpft über geheime Identifikationsnummern.



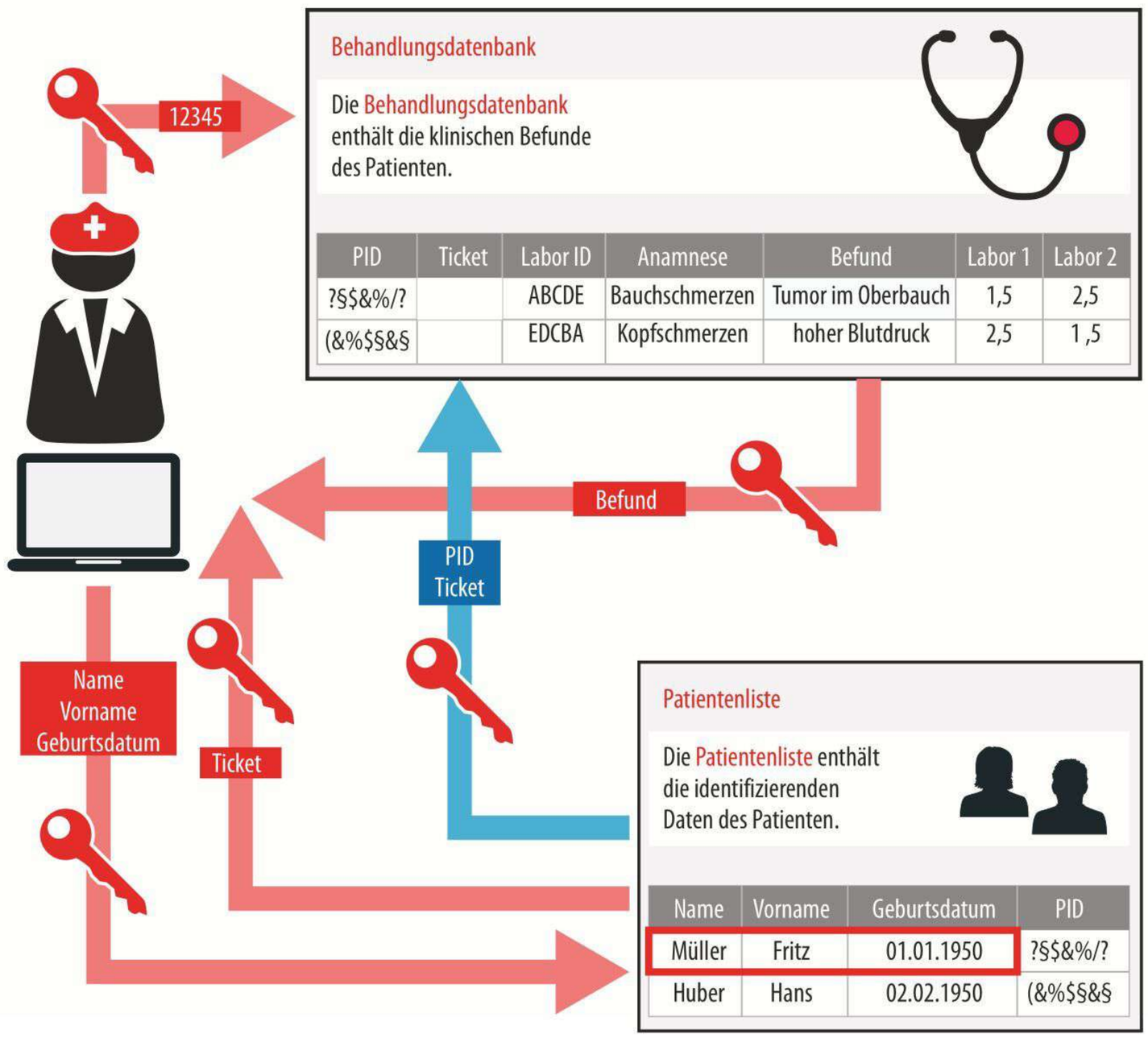
barkeit zu vollbringen. Diese technisch-organisatorische Maßnahme (TOM, siehe S. 147) erlaubt und verlangt die DSGVO deshalb für viele notwendige Verarbeitungsschritte – und zwar gemäß Privacy by Design (siehe S. 146) in einem möglichst frühen Stadium der Verwertungskette. Ähnlich wie bei den Verschlüsselungsverfahren fordert sie auch hier einen modernen technischen Standard ein (Stand der Technik, S. 146), um zu gewährleisten, dass nur befugte Personen die gekappte Verknüpfung wiederherstellen können.

Starke Pseudonymisierung

Zum Beispiel soll in einem Krankenhaus nicht jede Abteilung und jeder Mitarbeiter auf die kompletten Krankenakten der Patienten zugreifen können, schließlich fallen diese unter die besonderen Kategorien personenbezogener Daten (S. 143). Um die sensiblen Aufzeichnungen zu schützen, muss die Verwaltung also sämtliche direkte und indirekte Identifikatoren getrennt von den medizinischen Details speichern und diese bei Bedarf über Identifikationsnummern

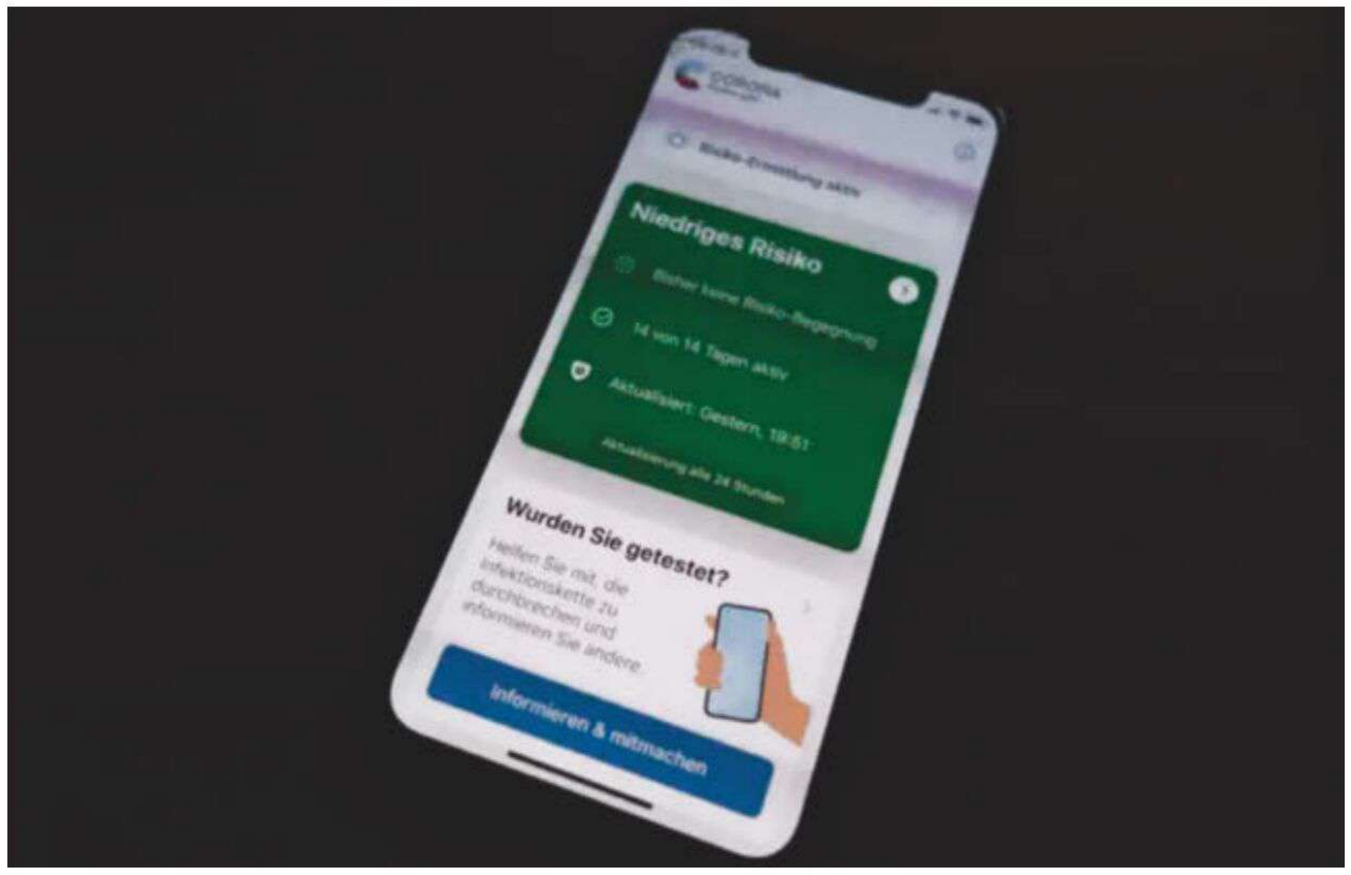
Zugriff des Arztes auf alle Daten

Bei einer Datenbankabfrage – etwa durch einen Arzt – generiert das System ein dynamisches Ticket, das die Informationen aus den getrennten Systemen temporär verknüpft. Die PID bleibt geheim.



verknüpfen. Solche **Token** lassen sich prinzipiell auf unterschiedliche Arten generieren. Stand der Technik sind dynamische, etwa über **Listen** oder **Berechnungsverfahren** generierte IDs. Die **statische Tokenisierung**, also einfaches Ersetzen von Name-Vorname durch eine laufende Nummer oder feste Zeichenkombination, dürfte nach DSGVO-Gesichtspunkten wohl nicht mehr akzeptiert werden, weil auch Unbefugte die Zuordnung leicht nachvollziehen können. Ein sehr informatives Whitepaper mit Leitlinien zur Pseudonymisierung hat die Fokusgruppe Datenschutz im Rahmen des Digitalgipfels 2017 verfasst, siehe ct.de/wfy7.

Ein Beispiel für konsequentes Privacy by Design und einen sehr starken Schutz durch Pseudonymisierung ist die **Corona-Warn-App (CWA)** der Bundesregierung. Sie betreibt einigen technischen Aufwand wie etwa im Zehnminutentakt wechselnde Bluetooth-IDs, lokales Speichern von Begegnungen auf dem Smartphone und Verzicht auf das Erfassen von Standortdaten, um die Identifizierung von Personen hinter den gespeicherten Kontaktereignissen



heise online

Die Corona-App tut, was sie soll, verrät aber nicht viel darüber. Kann sie auch nicht, weil sie der Datensparsamkeit verpflichtet ist.

zu erschweren. Dennoch handelt es sich nicht um Anonymisierung – sonst wäre eine Rückverfolgung und Benachrichtigung ja gar nicht möglich.

Das hohe Schutzniveau der Corona-App geht übrigens zulasten des analytischen Potenzials: Die App erfüllt ihren eigentlichen Zweck, potenziell risikoreiche Begegnungen zu registrieren und bei hohem Risiko Benachrichtigungen zu verschicken (Zweckbindung, S. 144), aber nicht viel mehr: Wer im Nachhinein untersuchen möchte, wie gut etwa die Abstandsmessung funktioniert, besitzt keine zentrale Datenbank zum Auswerten. Unterm Strich lassen sich der wahre Nutzen der App oder deren Schwächen aus ihr selbst heraus nur schwer evaluieren.

Deshalb ist der Betreiber, das Robert-Koch-Institut (RKI) auf freiwillige Datenspenden und auf zusätzliche Befragungen angewiesen, um den Nutzen der CWA abschätzen zu können. Diese Methoden hat das RKI im Frühjahr 2021 angewandt, und im Herbst 2021 soll ein wissenschaftlich fundierter Evaluationsbericht erscheinen.

Verrauscht oder synthetisch

Vor allem wenn sensible Daten veröffentlicht oder geteilt werden sollen, besteht ein sehr hohes Risiko für den Einzelnen. Man denke an eine medizinische Studie, deren Ergebnisse mitsamt den Daten publiziert werden sollen – inklusive Diagnose. Bestimmte Arten von medizinischen Daten lassen sich gar nicht wirksam anonymisieren oder werden dadurch unbenutzbar – etwa eine Computertomografie des Schädels, aus der sich das Gesicht rekonstruieren lässt.

Für andere entwickeln sich zunehmend raffinierte Verschleierungstechniken, dank derer vor allem die Wissenschaft Zugang zu wertvollen Datensammlungen bekommen soll, ohne den gläsernen Bürger zu riskieren. Zentrale Idee hinter den meisten Verfahren ist, die Datenmenge zu reduzieren oder verräterische Merkmale (beziehungsweise Merkmalskombinationen) so zu verändern, dass Individuen in größeren Personenclustern „untertauchen“. Dabei müssen die Werte allerdings so geschickt variiert werden, dass wichtige statistische Größen wie Mittelwert, Standardabweichung, Maxima und Minima erhalten bleiben oder nur leicht schwanken.

Beim **Sampling** wird nicht der komplette Datenstrom gespeichert, sondern nur eine Art Stichprobe davon. Google Maps etwa würde kein Bewegungsprofil über den kompletten Tagesablauf aufzeichnen, sondern nur ein paar Aufenthaltsorte zu zufällig ausgewählten Zeitpunkten. Das allein genügt aber leider nicht: Für Bewegungsdaten haben Forscher herausgefunden, dass nur vier Punkte ausreichen, um 95 Prozent der Nutzer eindeutig zu identifizieren. Und: Dass Sampling in Kombination mit Pseudonymisierung generell kein ausreichend hohes Schutz-

niveau bietet, um gemäß DSGVO als Anonymisierung durchzugehen, haben französische Forscher um Luc Rocher sogar allgemein bewiesen.

Aggregation ist die Kunst, den Einzelnen in der Masse verschwinden zu lassen. Dabei werden mehrere Datenpunkte bereichsweise zusammengefasst, Bewegungsdaten zum Beispiel nach Postleitzahlenbereichen: Anstatt nachverfolgbarer einzelner Linien zeigt die Karte dann nur noch dickere und dünnere Verkehrsströme durch die Stadt. Das ist zum Beispiel ganz nützlich, wenn man jeden Abend beim Lieblingsitaliener im Rotlichtviertel essen geht und nicht möchte, dass öffentlich publizierte Mobilitätsanalysen einen eindeutigen Track vom Eigenheim dorthin zeigen. Um Individuen in dünn besiedelten Gebieten zu schützen, muss die Gesamtzahl der Datenpunkte über einer bestimmten Schwelle (k) liegen, um in die Auswertung einzufließen. Deshalb heißt das Verfahren auch **k-Anonymität**. Solche Aggregationsverfahren wenden zum Beispiel die Telekom und andere Dienstleister an, bevor sie ihre Mobilitätsdaten verkaufen.

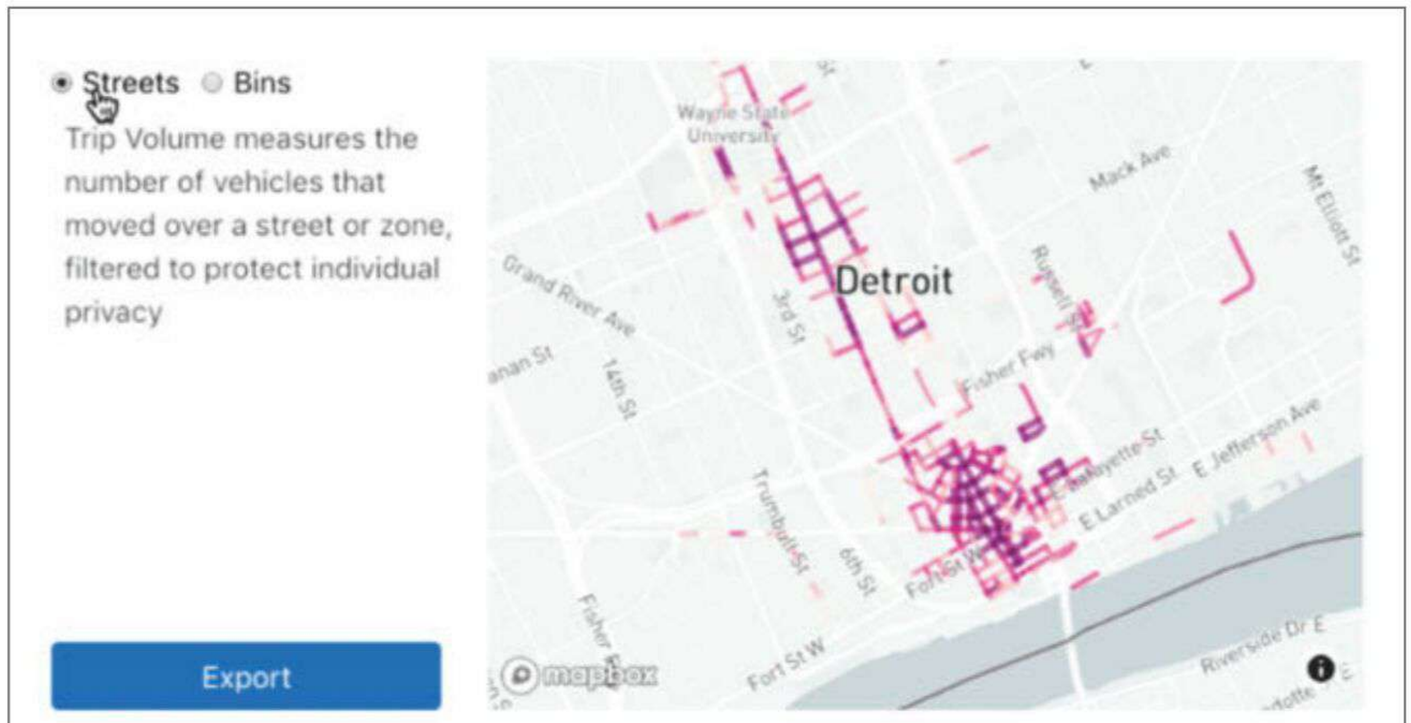
Ein relativ neues Konzept der Datenaufbereitung heißt **Differential Privacy (Differenzielle Privatheit)**. Differential-Privacy-Verfahren versuchen, Rohdaten oder daraus berechnete Statistiken (Mittelwert, Standardabweichung et cetera) so geschickt zu **verrauschen**, dass sie eine möglichst hohe Aussagekraft behalten und dennoch keine Rückschlüsse auf die zugrunde liegenden wahren Werte zulassen [1].

Differential-Privacy-Verfahren haben den Charme, dass man sogar mathematisch exakt festlegen kann, wie hoch der Schutz beziehungsweise der Verlust der Privatsphäre ausfallen darf. Die Umsetzung ist jedoch nicht trivial und mit jeder zusätzlichen Abfrage an die Datenbank sinkt das Schutzniveau – die Anzahl möglicher Berechnungen ist also begrenzt.

Keines dieser Verfahren kann für sich genommen und für jeden Eintrag Anonymität garantieren, denn jedes ist auf eine andere Art angreifbar – etwa durch geschickte Abfragen, Ausschlussverfahren und Hintergrundwissen. In der Praxis werden deshalb oft Kombinationen dieser Methoden eingesetzt.

Wenn alle Methoden zu riskant erscheinen, bleibt nur noch die **Datensynthetisierung**, also mithilfe eines Modells eine künstliche Repräsentation der Originaldatenbank herzustellen: Die einzelnen Einträge sind dann keine echten Messwerte und haben somit ihren Bezug zu den realen Personen verloren, aber die relevanten Eigenschaften wie Cluster oder charakteristische Muster der ursprünglichen Datensammlung bleiben erhalten. Zu den Anwendern ge-





Quelle: sharedstreets.io

Bewegungsdaten enthalten allerlei sensible Informationen, etwa über Arzt- und Krankenhausbesuche. Deshalb werden sie vor der Veröffentlichung aggregiert.

hören das deutsche Institut für Arbeitsmarktforschung sowie das U.S. Census Bureau, das Mobilitätsströme von Berufspendlern synthetisiert hat. Praktischerweise lassen sich quasi alle Datenarten synthetisieren – auch Bild- und Textdateien oder soziale Graphen. Dennoch entledigt man sich damit nicht aller rechtlicher und ethischer Probleme: Solche Sammlungen könnten etwa missbraucht werden, um wichtige Datenschutzprinzipien zu unterlaufen oder kritische Systeme wie die biometrische Gesichtserkennung anzugreifen.

Herausforderung Künstliche Intelligenz

Auch die Entwicklung des **Maschinellen Lernens** und **Künstlicher Intelligenz** dürfte hierzulande von modernen Verschleierungstechniken profitieren. KI lebt von Daten, und zwar von enormen Datenmengen (**Big Data**), die für das Training der Algorithmen benötigt werden. Wer wie die US-Konzerne Google, Amazon und Facebook bereits viel Material angehäuft hat, gehört auch zu den weltweit führenden KI-Entwicklern. Doch dürfen sie die ihnen anvertrauten Fotos, Videos und Sprachaufzeichnungen beliebig verwenden?

Vollständig anonyme Daten oder wirksam anonymisierte Statistiken von EU-Bürgern dürfen uneingeschränkt ins Training von KI-Algorithmen einfließen, da diese nicht in den Anwendungsbereich der DSGVO fallen. Generell sind alle Informationen ohne Personenbezug wie Wetter-, Börsen- oder Logistikdaten unproblematisch – sofern deren Nutzung nicht gegen andere Regelungen wie etwa das Urheberrecht verstößt. Dieses hat bereits das Schicksal einiger öffentlicher Mega-Fotosammlungen besiegelt, da die ursprünglich nur für Forschungszwecke freigegebenen Trainingsbilder auch in kommerzielle KI-Entwicklung einflossen.

Der rechtskonforme Umgang mit personenbezogenen Daten gestaltet sich allerdings noch ein Stück weit komplizierter. Wer personenbezogene Daten fürs maschinelle Training benötigt, muss die Vorgaben der DSGVO befolgen. Eine Rechtsgrundlage, nach der etwa Facebook die auf seiner eigenen Plattform veröffentlichten Porträts beim KI-Training einsetzen dürfte, wäre die Einwilligung der betroffenen Person. Einerseits können sich Unternehmen per Einwilligung sehr weitreichende Nutzungsrechte sichern – sogar für besonders sensible Informationen wie die ethnische Herkunft, politische Meinungen oder Gesundheitsdaten. Andererseits lassen sich im Falle des Widerrufs einzelne personenbezogene Daten vor allem beim unüberwachten Lernen nicht mehr aus dem trainierten Algorithmus entfernen. Daher ist die Einwilligung für KI-Betreiber letztlich ungeeignet. Zudem bleibt aufgrund der Blackbox-Eigenschaften von Algorithmen fraglich, ob der Einzelne eine informierte Einwilligung (S. 145) überhaupt rechtskonform abgeben kann.

Literatur

[1] Sylvester Tremmel, **Berechenbar privat**, Wie Differential Privacy funktioniert, c't Daten schützen 2020, S. 80

[2] Sylvester Tremmel, **Die K-Frage**, Wie man Daten richtig anonymisiert, c't Daten schützen 2020, S. 76

Weitere Infos

ct.de/wfy7

Zweckbindungsproblem

Als Rechtsgrundlage können auch die **berechtigten Interessen der Verantwortlichen** gelten. Diese sind wiederum gegen die Interessen der betroffenen Person, deren Daten verarbeitet werden sollen, im Rahmen einer **Risikobewertung** abzuwägen. Einzelne Daten wie Vorname, Stadtname oder Geburtsjahr, über die sich Personen nur indirekt identifizieren lassen, könnten zwar als wenig riskante Trainingsdaten eingestuft werden. Problematisch bleibt aber, dass die Daten meist zu anderen Zwecken als dem maschinellen Lernen erhoben wurden.

Nicht-sensible Daten dürfen in einigen Fällen für maschinelles Lernen genutzt werden, wenn der Weitergabe ein Rechtsgeschäft mit der betroffenen Person zugrunde liegt, beispielsweise bei der Verwendung von Spracherkennungssoftware. Hierbei sind, wie auch bei allen anderen Datenverarbeitungen, personenbezogene Daten zu pseudonymisieren, wo dies möglich ist.

Mögliche Lösungen dies- und jenseits der DSGVO

Eine mögliche Lösung versprechen Techniken wie das **Federated Machine Learning**, bei dem ein vortrainiertes Modell aufs Endgerät heruntergeladen und mit den personenbezogenen Daten lokal verbessert wird. Das Ergebnis ist ein optimiertes Modell ohne Personenbezug, das dann wieder auf den zentralen Server des KI-Betreibers hochgeladen wird. Auch **vortrainierte neuronale** Netze wie Apples Face ID oder die Bildersuche Excire arbeiten ausschließlich lokal. Weil synthetische Daten nicht in den Anwendungsbereich der DSGVO fallen, bieten auch solche sich als Alternative fürs maschinelle Lernen an – etwa wenn Gesichtserkennungssoftware wiederum mit KI-generierten Gesichtern trainiert wird. Allerdings kommt es auch hier aufs Verfahren an: Manche Bildgeneratoren kupfern noch zu viele – möglicherweise sensible – Informationen aus den Trainingsdaten ab. (atr) ct

MIT Technology Review
Das Magazin für Innovation von Heise

Die Welt verstehen, wie sie morgen sein wird.

2 Ausgaben inklusive Prämie nach Wahl:

40 % Rabatt

mit-tr.de/testen



leserservice@heise.de +49 541/80 009 120 trvorteil.de/testen

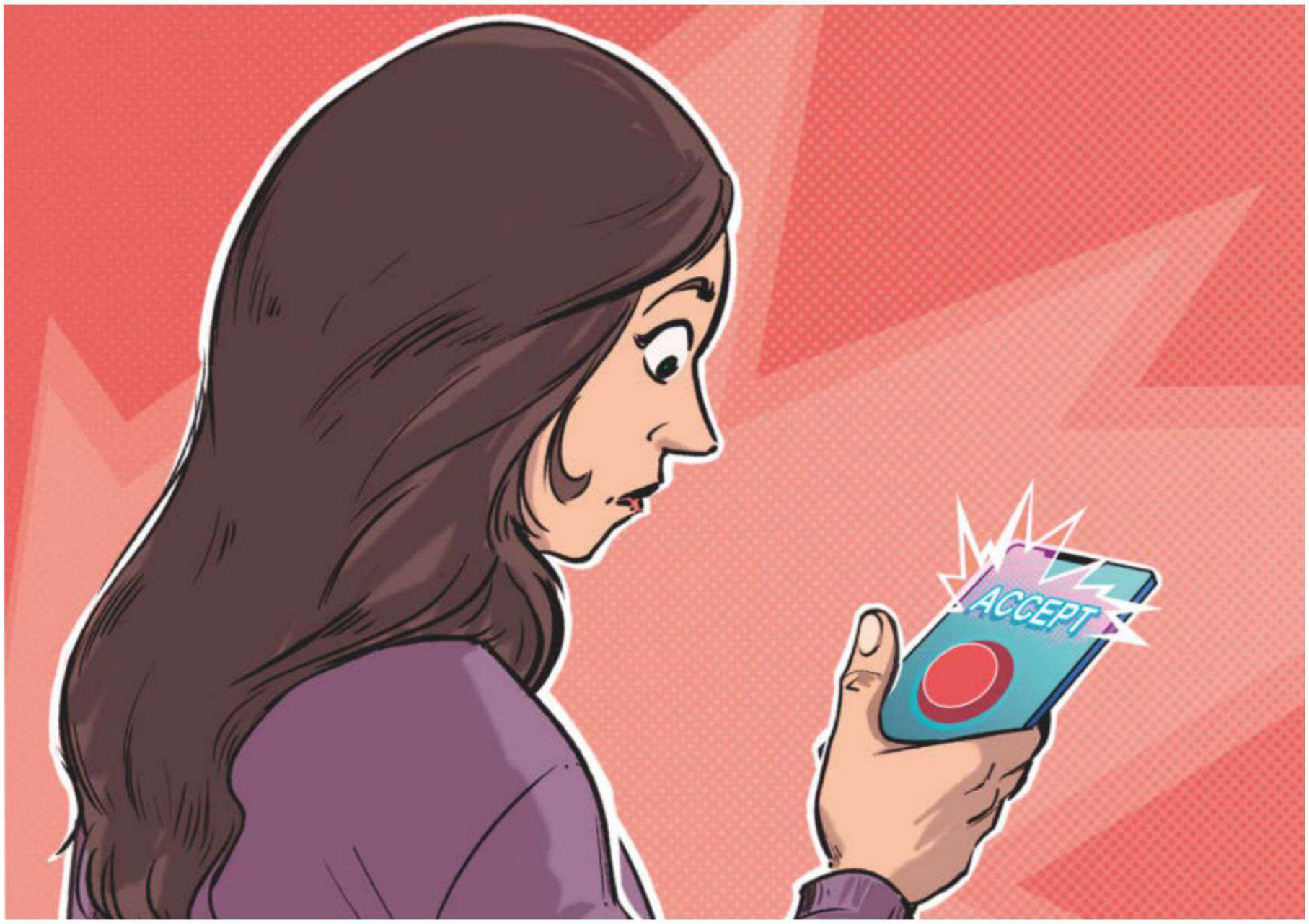


Bild: Albert Hulm

Datenschutz-Fragezeichen bei Apps

Beim flinken Tippen auf Smartphone und Tablet nicken viele User die Datenschutzbedingungen der Apps allzu schnell ab. In den seitenlangen Dokumenten verstecken sich allerdings oft Klauseln, die rechtlich fragwürdig sind.

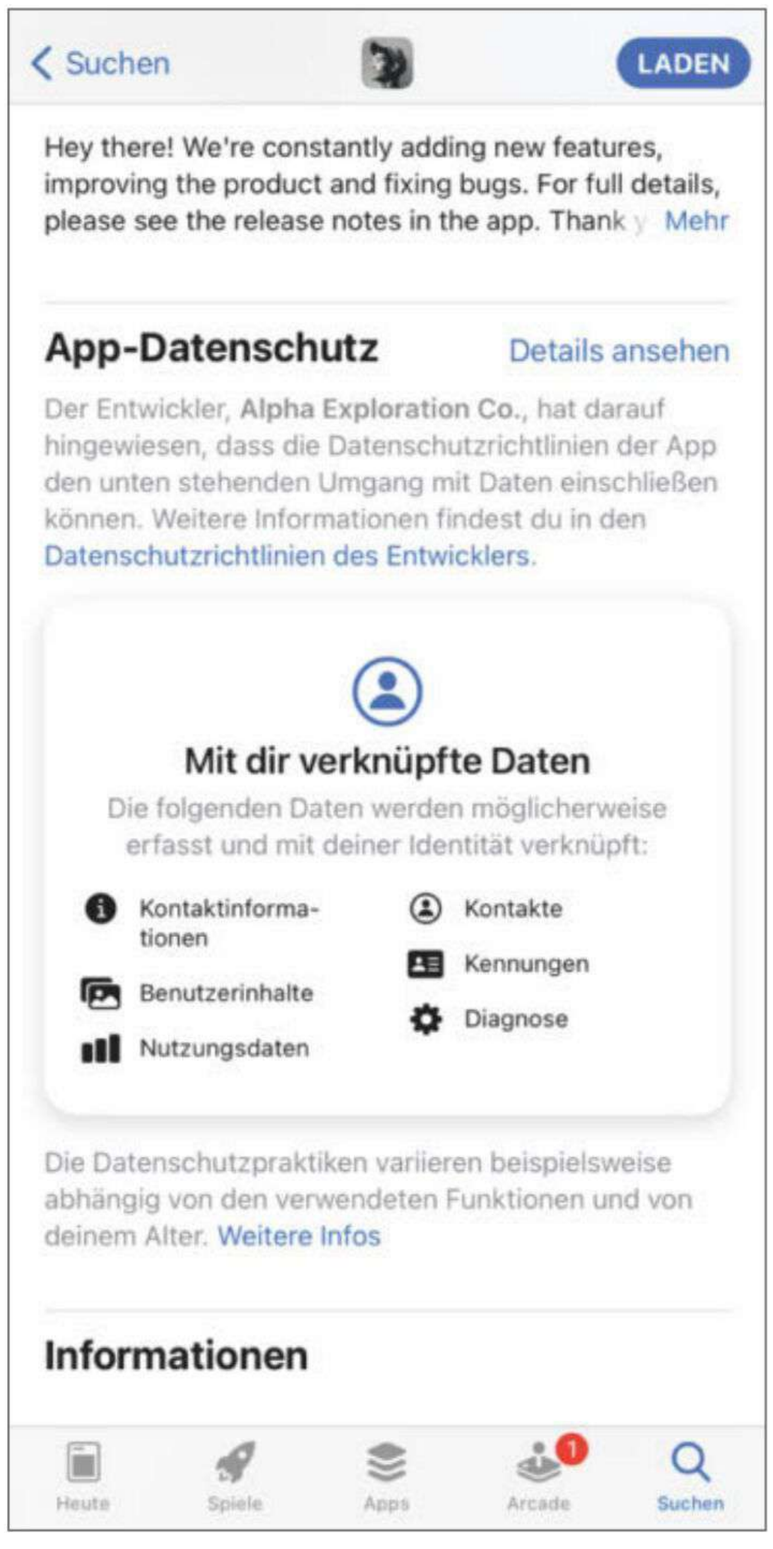
Von **Miriam Legien**

Die europäische Datenschutz-Grundverordnung (DSGVO) verlangt, dass „betroffene Personen“ vor Speicherung und Verarbeitung ihrer personenbezogenen Daten hinreichend informiert werden. Anbieter von Mobil-Apps tun das normalerweise durch Datenschutzerklärungen, in die man spätestens dann einwilligt, wenn man die betreffende Anwendung nutzt. Mancher eilige Smartphone-Jongleur tut sich die Lektüre solcher nicht gerade lesefreundlicher Dokumente gar nicht erst an – er vertraut vielmehr darauf, dass damit schon alles seine Richtigkeit haben wird.

Dieses Vertrauen ist nicht immer gerechtfertigt. Obgleich die verbindliche Einführung von Datenschutzerklärungen bereits im Mai 2018 erfolgt ist und damit nun schon fast drei Jahre zurückliegt, weist die Umsetzung der Vorschriften bei vielen Apps noch erhebliche Mängel auf.

Schon vor der Installation einer App erfasst die als Verteiler auftretende Plattform eine Vielzahl personenbezogener Daten. Wenn der Nutzer einen Download auslöst, erfährt auch der Anbieter der App, wer zu seinem Produkt greift. Für Nutzer besteht dabei das Risiko, die Kontrolle über ihre Daten zu verlieren – das betrifft vom Store-Account über die IP-Adresse bis hin zu Zahlungsinformationen allerlei, was personenbezogen ist oder zumindest im Zusammenspiel mit anderen Daten Rückschlüsse auf die Identität des Nutzers zulässt.

Dessen Zustimmung zu den Datenschutzbedingungen des Anbieters muss nicht unbedingt ausdrücklich erfolgen. Auch eine „konkludente" Zustimmung reicht – der Nutzer zeigt sie stillschweigend, indem er etwa die App herunterlädt.



In kompakter, übersichtlicher Form erscheinen Datenschutzhinweise in Apples App-Store – etwa zur Clubhouse-App.

Gib mir was zu lesen!

Apple hat in seinem App-Store für viele Anwendungen Informationen über den Datenschutz integriert. Diese Hinweise sind zwar nicht optimal auffindefreundlich – aber das Scrollen nach unten lohnt sich. Dort erfahren Nutzer beispielsweise, wer für die Datenverarbeitung verantwortlich ist und für Betroffene als Ansprechpartner fungiert. Für detaillierte Informationen werden die eigentlichen Datenschutzbedingungen des Verantwortlichen verlinkt.

Im Google Play Store muss man demgegenüber genauer hinschauen. Hier verstecken sich die Links zu den Datenschutzerklärungen oft weit unten im Beschreibungstext zur jeweiligen App. Kurzinformationen zu den Datenverarbeitungen bietet das Standard-Portal für Android-Apps normalerweise nicht.

Es lohnt sich, die im Store aufgeführten oder per Link angebundenen Informationen auf bestimmte Fragen hin abzuklopfen. Das Ergebnis zeigt schon ziemlich deutlich, wie ernst der jeweilige Verantwortliche die europäischen Datenschutzbestimmungen nimmt. Die DSGVO räumt in ihrem dritten Kapitel den von Datenerhebung und -verarbeitung Betroffenen umfangreiche Rechte ein. Deren Spektrum reicht von transparenter Information (Artikel 12) bis zur Ablehnung automatisierter Einzelfallentscheidungen (Artikel 22). Die nationalen Gesetzgeber können diese Rechte etwa zugunsten der Strafverfolgung oder anderer übergeordneter Zwecke einschränken (Artikel 23).

Elementar ist insbesondere das Auskunftsrecht (Artikel 15): Es ermöglicht dem Betroffenen meistens erst, andere Rechte wie die auf Berichtigung und Löschung seiner Daten geltend zu machen. Wenn ein Nutzer vom Verantwortlichen Auskunft über seine Daten verlangt, muss dieser innerhalb eines Monats die geforderten Informationen bereitstellen. Das kann die Art der Daten betreffen, die Verarbeitungszwecke und die Frage, an wen welche Informationen weitergegeben worden sind.

Für die App-Nutzung spielt das Recht auf Widerruf (Art. 7 Abs. 3) eine wichtige Rolle: Eine vom Betroffenen

abgegebene Einwilligung muss jederzeit widerrufbar sein – und zwar so einfach, wie sie erteilt worden ist. Ein solcher Widerruf gilt dann aber nur für zukünftige Datenerhebungen oder für die Weiterverarbeitung bereits erhobener Daten.

Datenschutzinformationen der App-Anbieter sind nicht nur vor dem Download vom Store aus zugänglich. Eine Datenschutzerklärung muss auch innerhalb der installierten App über wenige Klicks auffindbar und auf die jeweilige Anwendung zugeschnitten sein. Diese Dokumente sind meistens nach einem bestimmten Muster aufgebaut. Im besten Fall beginnen sie mit einem Inhaltsverzeichnis, das dabei hilft, gewünschte Informationen aufzufinden. Wichtig ist unter anderem, dass sie die Kontaktdaten des Verantwortlichen nennen. Vorsicht ist geboten, wenn schon diese Angabe fehlt. Dasselbe gilt, wenn die Informationen insgesamt unverständlich beziehungsweise ungeordnet scheinen oder wenn nur pauschale Angaben zu Datenverarbeitungszwecken und Rechtsgrundlagen zu finden sind. Die DSGVO geht davon aus, dass personenbezogene Daten überhaupt nur dann erfasst, gespeichert, verarbeitet oder weitergegeben werden dürfen, wenn es eine Rechtsgrundlage dafür gibt – also einen der rechtfertigenden Gründe, die in Artikel 6 und 9 der Verordnung aufgeführt sind.

Deutsch, bitte!

Auch ein außerhalb der EU ansässiger Verantwortlicher, der Waren oder Dienstleistungen in Deutschland anbietet, muss die DSGVO beachten. Er ist verpflichtet, eine Datenschutzerklärung in „transparenter und verständlicher Form“ zur Verfügung zu stellen. Viele Anbieter kollidieren schon dadurch mit dieser Bestimmung, dass sie ihre Dokumente hierzulande nicht in deutscher Sprache darbieten. So sind etwa innerhalb der Apps für die Diskussions-Audioplattform Clubhouse und den Messenger Signal nur die englischen Datenschutzerklärungen enthalten beziehungsweise verlinkt. Dem steht als positives Beispiel die PayPal-App gegenüber, die eine deutsche Datenschutzerklärung verfügbar macht.

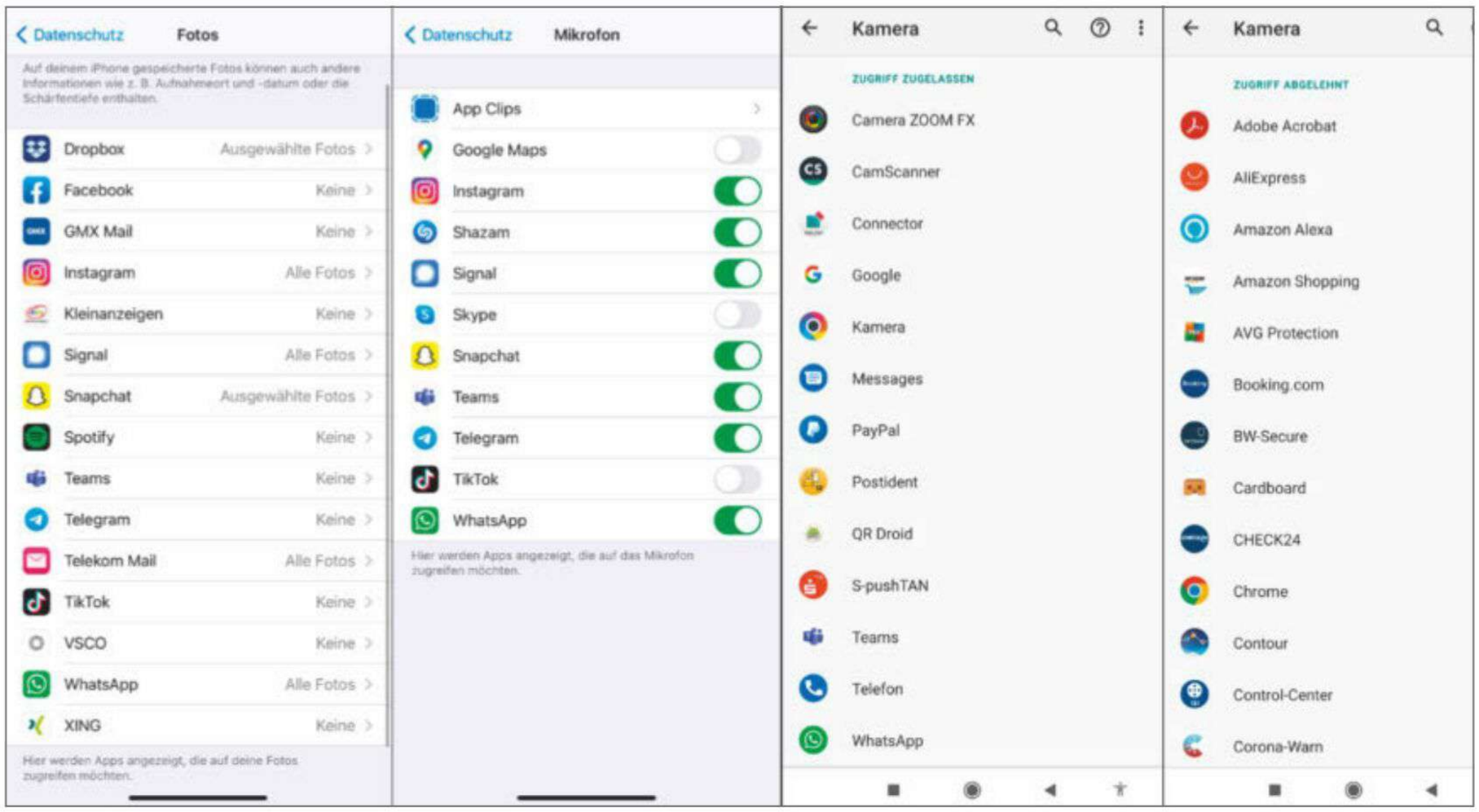
Was willst du wissen und warum?

Zu den Informationspflichten des Verantwortlichen gehört es aufzuschlüsseln, welche personenbezogenen Daten er erhebt und verarbeitet. Misstrauen ist etwa angebracht, wenn er hierzu keine oder nur sehr pauschale Angaben macht wie „Die App verarbeitet personenbezogene Daten im Sinne der DSGVO“.

Der Nutzer muss zudem wissen, auf welche Rechtsgrundlage sich die Verarbeitung seiner Daten stützt. Nach Artikel 6 Abs. 1 der DSGVO müssen die Verantwortlichen nämlich einen guten Grund dafür haben. Vorbildlich sieht es diesbezüglich bei der ntv-App aus: Unter „Einzelne Verarbeitungszwecke“ listet die Datenschutzerklärung hier jede einzelne Verarbeitung mit der dazugehörigen Rechtsgrundlage auf. Auch für die Xing-App gibt es eine verständliche und ausführliche Darstellung.



Nicht ganz so komfortabel lassen sich Datenschutzinformationen im Google Play Store abrufen – zur Datenschutzerklärung für die eBay-Kleinanzeigen-App führt dort ein leicht zu übersehender Link.



Die DSGVO gewährt unter anderem das Recht, die Einwilligung in die Datenverarbeitung zu widerrufen. Eine App-bezogene Funktion dafür bieten die Datenschutzeinstellungen des Betriebssystems (links iOS, rechts Android).

Wenn keine Rechtsgrundlage genannt wird, will sich der Anbieter möglicherweise ungerechtfertigte Datenverarbeitung offenhalten. Unzureichend ist es auch, wenn sich die gesamte Datenverarbeitung nur auf eine gemeinsame Rechtsgrundlage stützt, etwa ein „berechtigtes Interesse“ des anbietenden Unternehmens. Wenn es etwa heißt „Die App verarbeitet Ihre personenbezogenen Daten zu Werbe- und Analysezwecken auf Grundlage unseres berechtigten Interesses“, sollten bei datenschutzbewussten Nutzern innere Alarmlämpchen zu blinken beginnen.

Sag mir, wohin

Da nicht überall auf der Welt das gleiche Datenschutzniveau besteht, ist es wichtig, wo der Verantwortliche die personenbezogenen Daten des Nutzers speichert. Eine Speicherung auf deutschen Servern, wie beispielsweise bei der Instant-Messaging-App Ginlo, ist normalerweise unproblematisch: Die dafür Verantwortlichen sind dabei automatisch an die in Deutschland und der EU geltenden strengen Datenschutzbestimmungen gebunden, die eine unberechtigte Weitergabe – etwa an fremde Behörden – unter Strafe stellen. Eine Speicherung im außereuropäischen Ausland, wie sie zum Beispiel bei TikTok und Facebook geschieht, ist riskant. Sie wäre datenschutzrechtlich nur zu vertreten, wenn der App-Anbieter eine zusätzliche Garantie abgibt.

Bevor der Europäische Gerichtshof (EuGH) 2020 das Privacy-Shield-Abkommen zwischen den USA und der EU für unwirksam erklärt hat, konnten Unternehmen es als Datenschutzgarantie für den Datenexport verwenden. Seit der EuGH-Entscheidung ist das nicht mehr möglich. Die dadurch notwendige Umstellung für den Nachweis eines aus europäischer Sicht akzeptablen Datenschutzniveaus betrifft nicht zuletzt auch App-Anbieter. Es lohnt sich also, bei der Lektüre von Datenschutzerklärungen darauf zu achten, ob der Verantwortliche versichert, europäisches Datenschutzniveau zu gewährleisten – und auf welche Rechtsgrundlage er sich dabei stützt. Das Privacy-Shield-Abkommen sollte in keiner aktuellen Datenschutzerklärung mehr zu finden sein.

Nicht nur der Speicherort, sondern auch die Angabe der potenziellen Empfänger für die Nutzerdaten ist wichtig. Geht es um Werbenetzwerke – und wenn ja, um welche?

Formulierungen wie „Ihre Daten können von uns an Dritte weitergegeben werden“ reichen nicht aus. Die möglichen Empfänger müssen näher beschrieben werden; außerdem muss der App-Anbieter dabei die Zwecke und Rechtsgrundlagen der Datenweitergabe nennen. Falls sich der Verantwortliche eine

Datenweitergabe an ausländische Partner vorbehält, besteht für den Nutzer ein ebensolches Datenschutzrisiko wie bei der Datenspeicherung auf ausländischen Servern. Facebook und Instagram stützen ihren Datentransfer in Drittländer nun beispielsweise auf europäische Standardvertragsklauseln.

Zugriffsrechte im Blick behalten!

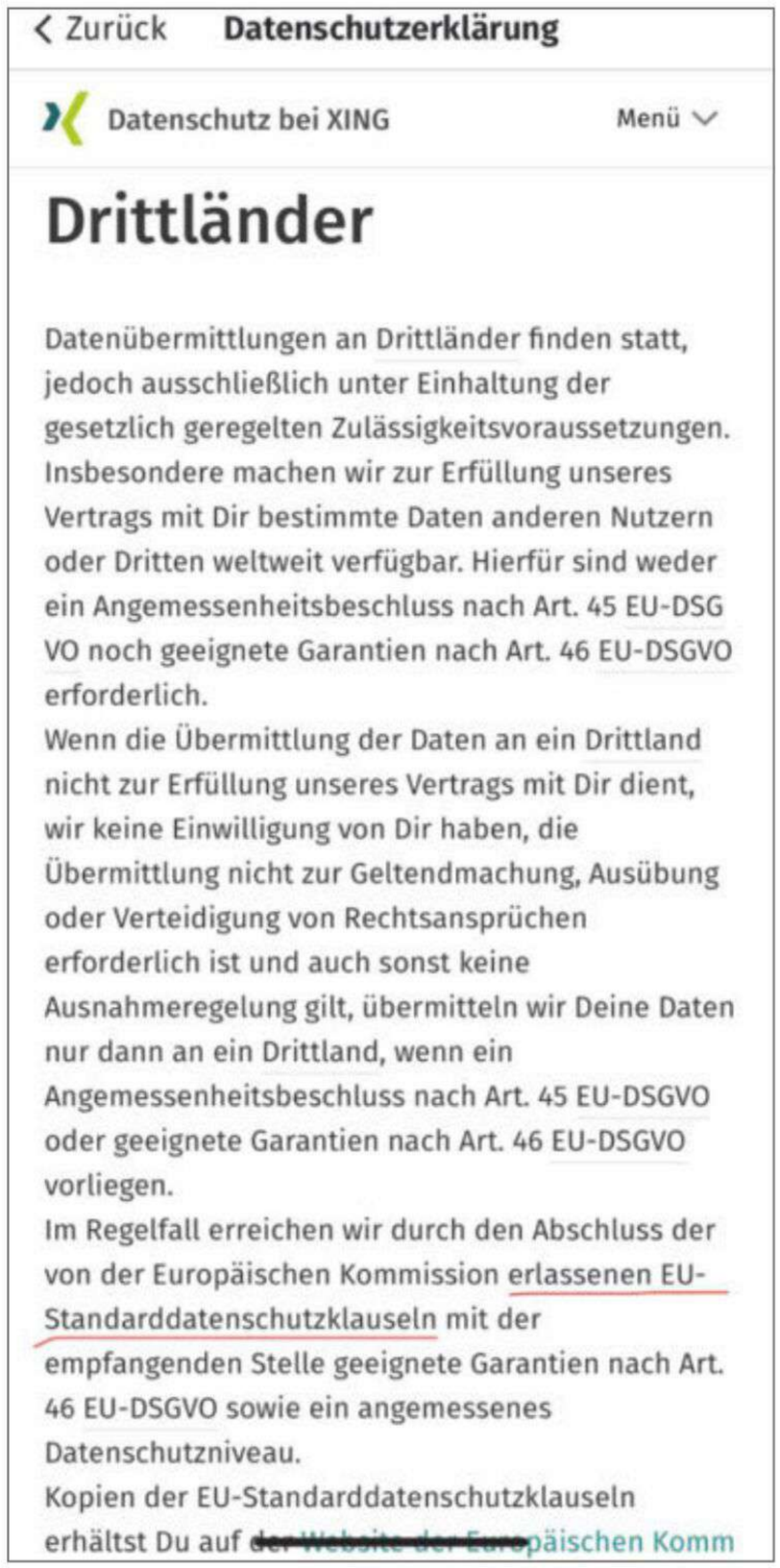
Nachdem sich eine neue App auf dem Mobilgerät angesiedelt hat, ist es wichtig, ihren Zugriff auf Daten und Funktionen zu regeln. Das gilt insbesondere für Android-Apps: Dort herrscht erfahrungsgemäß in dieser Hinsicht ein ziemlicher Wildwuchs.

Viele Anwendungen möchten auf Kamera, Mikrofon, Bilder, Kontakte und andere sensible Bereiche zugreifen. Für eine Navigations-App ist beispielsweise der Zugriff auf die Standortdaten unumgänglich. Aber wozu braucht etwa die Amazon-Shopping-App Zugriff auf die Smartphonekamera?

Die Grundsätze „Privacy by Design“ und „Privacy by Default“ verpflichten App-Verantwortliche dazu, die technischen Rahmenbedingungen und Voreinstellungen ihrer Anwendungen so datensparsam wie möglich zu gestalten. Nicht selten erlauben sich Anbieter eine Datenverwendung, die nicht erforderlich und damit auch nicht rechtmäßig ist.

Schlagzeilen machte etwa 2018 die App „La Liga“ von den Ausrichtern der beiden spanischen Profifußball-Ligen: Sie hörte Nutzer übers Smartphonemikrofon ab, um angebliche Pay-TV-Betrügereien aufzuklären. Wer die App verwenden wollte, musste ihr Zugriff aufs Mikrofon gewähren. Dadurch konnte der Anbieter Umgebungsgeräusche aufzeichnen und mit Standortdaten verknüpfen, um nicht genehmigte Spielübertragungen aufzuspüren. Die Nutzer wussten nichts von dieser Verarbeitung ihrer Daten und von deren Zweck. Die spanische Datenschutzbehörde AEPD verhängte 2019 in dieser Sache unter anderem wegen des Verstoßes gegen das Transparenzgebot ein Bußgeld von 250 000 Euro.

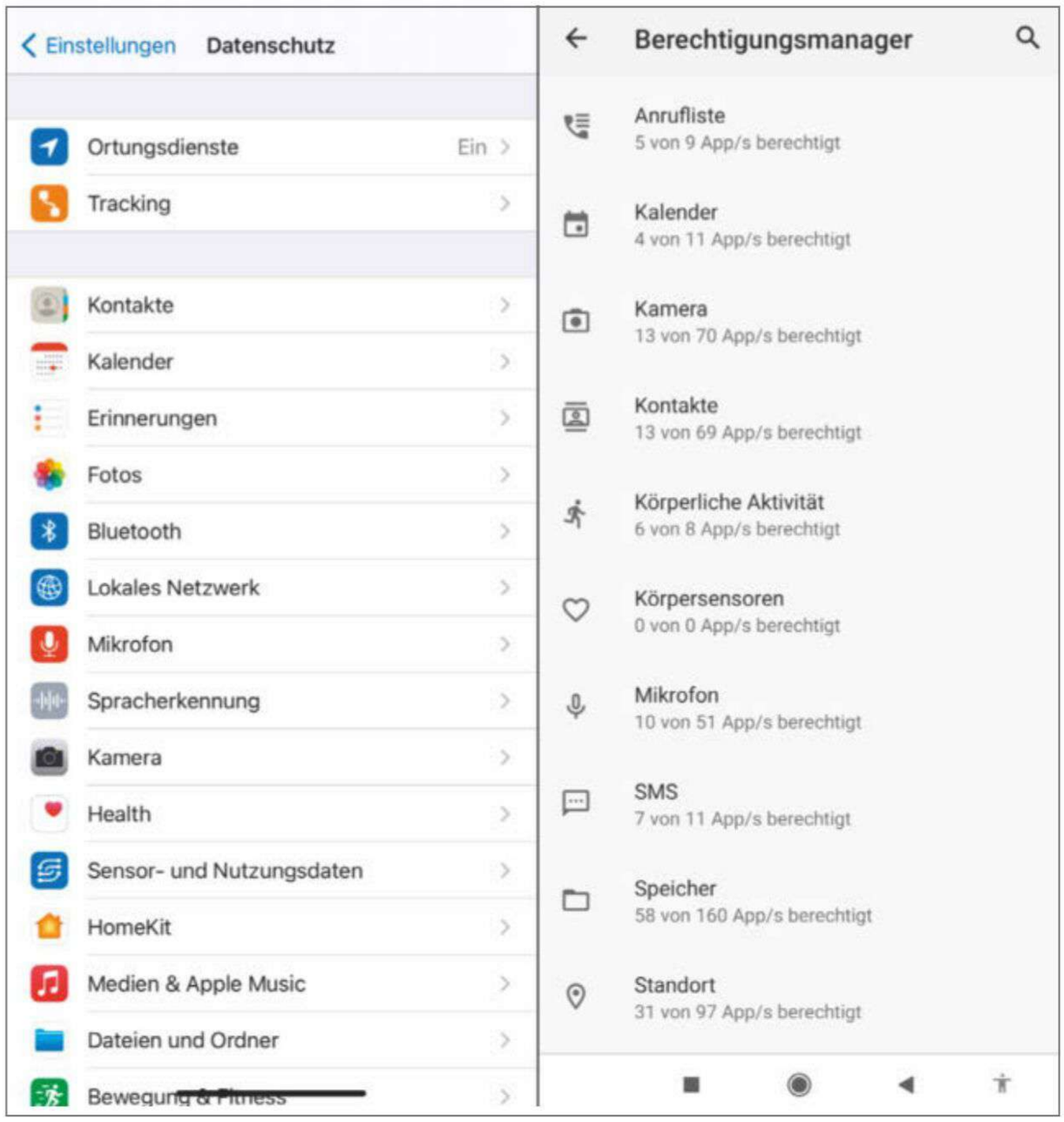
Aktuell stehen unter anderem die Datenschutzbedingungen der Clubhouse-App in der Diskussion: Wenn ein Nutzer jemand anderen zur Clubhouse-Teilnahme einladen will, sendet die App die freigegebenen Kontaktdaten aus dem persönlichen Telefonbuch des Mobilgeräts an ihren Betreiber Alpha Exploration in den USA. Der speichert personenbezogene Daten der Eingeladenen und verschafft sich damit die Möglichkeit anzuzeigen, wie viele „Freunde“ einer Telefonnummer bereits auf seiner Plattform angemeldet sind. Die Personen hinter den gespeicherten Telefonnummern werden allerdings nicht nach ihrer Zustimmung zu den Datenschutzbedingungen von Alpha Exploration gefragt – ganz abgesehen davon, dass auch die Datenspeicherung in den USA ohne Erlaubnis der Betroffenen gegen die DSGVO verstößt. Damit hat dann nicht nur der App-Anbieter, sondern möglicherweise auch jeder Einladende datenschutzwidrig gehandelt.



Obacht: Der Anbieter gibt Daten ins Ausland weiter. Das kann auch bei deutschen Dienstbetreibern geschehen – etwa bei Xing.

Riegel vorschieben

Die App-bezogenen Datenschutzeinstellungen von iOS und Android geben Anwendern Gelegenheit, Zugriffsrechte für einzelne Apps zu überprüfen und nicht



Die Datenschutzeinstellungen im Betriebssystem (links iOS, rechts Android) geben Auskunft darüber, welchen Apps der Zugriff auf welche Art von Daten des Mobilgeräts erlaubt worden ist.

plausible Zugriffe gar nicht erst zu erlauben. Wenn eine App beispielsweise Zugriff auf Bilder oder auf die Kamerafunktion verlangt, obwohl das ihrem Anwendungszweck fernliegt, ist Misstrauen angebracht.

Anwendungen sehen für sich bisweilen per Default weitaus mehr Zugriffsrechte vor, als sie sinnvollerweise brauchen und haben dürften. Es empfiehlt sich aber stets, Apps nur Zugriff auf diejenigen Daten und Funktionen zu gewähren, die für ihre Nutzung wirklich notwendig sind.

Besonders kritisch ist der Zugriff auf die Kontakte, also das im Mobilgerät gespeicherte persönliche Telefonbuch. Diesen beanspruchen beispielsweise viele Messenger-Apps, um sich mit der Kontaktliste des Nutzers zu synchronisieren. Ob man das in vollem Umfang erlaubt, will gut überlegt sein: Die Verarbeitung der personenbezogenen Daten aus der Kontaktliste erfolgt grundsätzlich ohne Einwilligung der Betroffenen und verstößt damit gegen die DSGVO – siehe Clubhouse.

Wo es möglich und sinnvoll ist, empfiehlt es sich, den Zugriff auf sensible Datenbereiche zeitlich zu beschränken. So kann man bei Apps, die einen Standortzugriff beanspruchen, diesen möglicherweise auf die Dauer der direkten Nutzung dieser App beschränken. Ein zeitlich unbeschränktes Zugriffsrecht aufs Mikrofon birgt im schlimmsten Fall das Risiko, dass der Nutzer abgehört und die Aufnahmen verwendet und weitergegeben werden – siehe „La Liga“.

Achtung, Profilsammler!

Wer der Weitergabe von App-übergreifenden Daten und dem Zugriff auf Smartphone-Funktionen wie Kamera, Mikrofon und Standortermittlung zustimmt, macht es Anbietern leicht, Nutzer- oder Bewegungsprofile zu erstellen. „Profiling“ ist laut Artikel 4 Nr. 4 der DSGVO „jede Art der automatisierten Verarbeitung personenbezogener Daten, die dazu führen soll, persönliche Eigenschaften der betroffenen Person zu bewerten“.

Manche Anbieter haben ein starkes Interesse daran, persönliche Vorlieben, Gesundheitszustand und Interessen, Verhalten und Aufenthaltsorte von Nutzern zu erfassen. Sie verwenden die gewonnenen Informationen nicht nur für eigene Zwecke; die Ergebnisse können auch ein durchaus lukratives Handelsgut darstellen. Eine Zustimmung zum Datenzugriff kann weitreichende Folgen haben, die auf den ersten Blick nicht zu überschauen sind. In der Praxis ist es allemal besser, sich dergleichen vorher gut zu überlegen, als die erfolgte Entscheidung im Nachhinein rückgängig machen zu wollen. Die DSGVO verschafft Betroffenen zwar Auskunfts- und Löschungsansprüche, aber oft muss man dennoch mit Konsequenzen leichtfertig erlaubter Datennutzung leben.

Der bestehende Zwiespalt zwischen schnellem, bequemem Gebrauch von Anwendungen beziehungsweise Diensten auf Mobilgeräten und dem Schutz der persönlichen Daten lässt sich nicht wegdiskutieren. Wer aber die Datenschutzerklärungen zumindest auf die genannten neuralgischen Punkte abklopft und Zugriffsrechte bewusst einstellt, tut damit schon einiges, um die Kontrolle über die eigenen Daten zu behalten. (psz) c't

AKTION
MIT LESERRABATT

Reiner SCT Authenticator

Mit dem Reiner SCT Authenticator schützen Sie Ihren Online-Account effektiv und komfortabel vor Hackern. Und mit unserem Leserrabatt können Sie dabei auch noch richtig Geld sparen.

Um Passwörter besser abzusichern, nutzt man häufig einen zweiten Faktor. Das bedeutet, dass Sie beim Einloggen nicht nur nach dem Passwort gefragt werden, sondern zum Beispiel auch nach einem kurzzeitig gültigen Zahlencode, den nur Sie kennen.

Einige Dienste schicken Ihnen den Code per SMS zu, was jedoch nicht absolut sicher ist. Am besten generieren Sie den Code bei Bedarf einfach selbst. Mit einer Zwei-Faktor-App, wie dem Google Authenticator auf dem Smartphone, ist dies sicherer, jedoch nicht besonders komfortabel: Wenn Sie gerade am Rechner surfen, müssen Sie das Handy entsperren und den Code-Generator suchen. Smartphone-Surfer müssen die App wechseln und den Code über die Zwischenablage von A nach B kopieren.

Viel komfortabler und noch sicherer klappt das mit dem Reiner SCT Authenticator. Er arbeitet im Prinzip wie der Google Authenticator, nur als eigenständiges Gerät, das ohne Schnittstellen zur Außenwelt garantiert virenfrei bleibt (siehe Seite 60). Wählen Sie auf dem knallgelben Gerät einfach einen der gespeicherten Dienste wie Facebook, Google oder Paypal und der Authenticator zeigt Ihnen sofort einen gültigen Zwei-Faktor-Code für Ihren Account an.

Mit der aktuellen Firmware können Sie bis zu 60 Accounts speichern. Wer möchte, kann den Zugriff durch eine PIN schützen.

Die Verknüpfung mit Ihren Online-Accounts ist denkbar unkompliziert: Scannen Sie einfach den QR-Code, die Ihnen der jeweilige Dienst bei der Einrichtung der Zwei-Faktor-Authentifizierung (Online Time Password, OTP) anzeigt. Übrigens ist das kompakte Gerät auch ein ideales Geschenk für Freunde und Familie: Die simple Bedienung erinnert an einen TAN-Generator, wie ihn viele vom Online-Banking kennen. Damit ist die supersichere Zwei-Faktor-Authentifizierung auch für Menschen zugänglich, denen die Nutzung einer Smartphone-App zu umständlich oder kompliziert wäre. Auch Personen ohne Smartphone können mit dem Reiner SCT Authenticator von dem Sicherheitsgewinn profitieren.



Klein, gelb und sicher: Mit dem Reiner SCT Authenticator schützen Sie Ihre Online-Accounts effektiv vor Hackern.

Liste kompatibler Dienste
ct.de/w1h7

Die Leser dieses Heftes erhalten im heise shop 5,- Euro Rabatt* auf den Authenticator nach Eingabe des Rabattcodes

DATENSCHUTZ2021

auf shop.heise.de/daten21

*Nur solange der Vorrat reicht. Preis- und andere Irrtürmer vorbehalten. Das Angebot ist gültig bis zum 31.12.2021 (Stand: August 2021).

Sind Sie sicher?

NEU im heise shop

Auch als PDF zum Download!





iX KOMPAKT IT-Sicherheit

Datenschutz umfasst mittlerweile so viel mehr als den Schutz vor Cyberattacken. Nach DSGVO und Ende des Privacy Shield sind auch rechtliche Maßnahmen zu ergreifen. Die neuesten Aspekte rund um den Datenschutz finden Sie zusammengefasst hier im iX Kompakt IT-Sicherheit.

shop.heise.de/ix-sicherheit20

14,90 € ›

› 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

shop.heise.de/ix-sicherheit20 ›

shop.heise.de/ct-fritzbox21

Router sicher im Griff!

Heft + PDF
mit 29 % Rabatt





shop.heise.de/ct-fritzbox21

Wappnen Sie Ihre Fritzbox gegen Angriffe von Außen und machen Sie Ihr Smart Home fit mit dem neuen **Sonderheft von c't:**

- ► Ihre Fritzbox absichern, erweitern, tunen
- ► Auch im Set mit Fachbuch erhältlich
- ► Über 170 Seiten konzentrierte c't-Expertise
- ► Für Abonnenten portofrei

Heft für 14,90 € • PDF für 12,99 € • im Set 29 % günstiger!

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