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.

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.

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.

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.

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.

ZUM HEFT

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

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

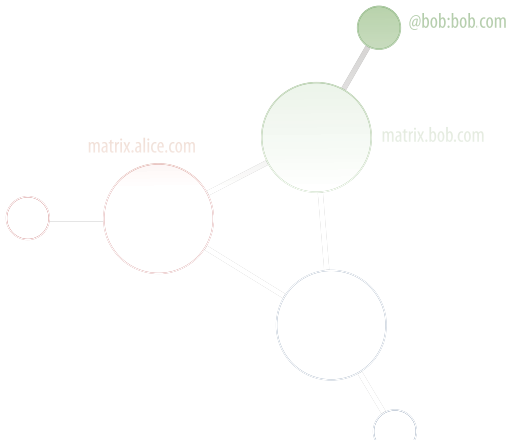
Tagesabläufe und Abweichungen davon rekonstruieren sowie herausfinden, wer mit wem sprach [1].

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.

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.



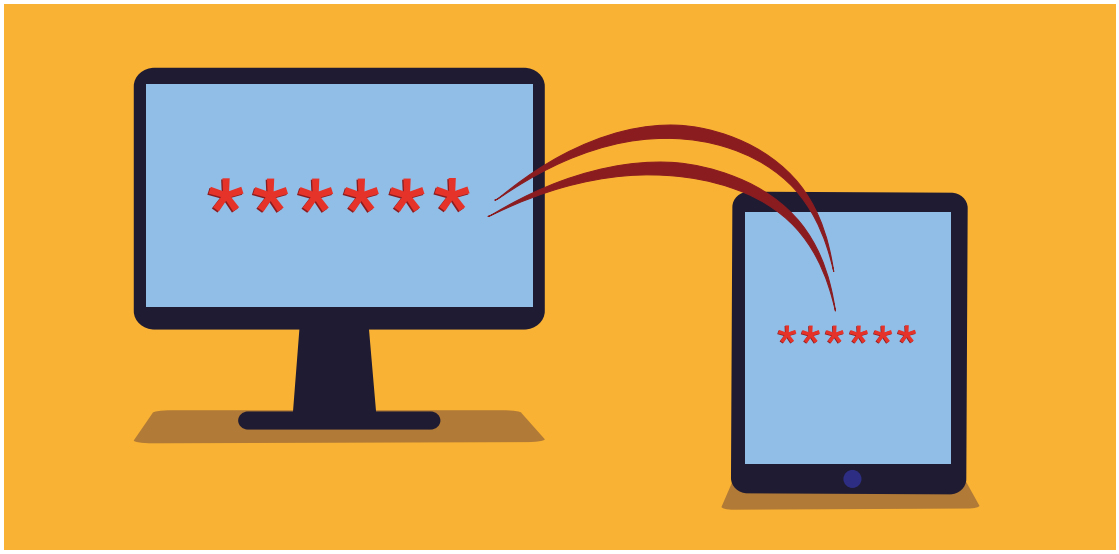
Beide Protokolle „föderieren“, man kann also auch mit Leuten chatten, die sich bei anderen Servern angemeldet haben – dann muss man sich aber wieder um Metadaten sorgen und den Betreibern dieser Server vertrauen.

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



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 Komfort-

flächen 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.

Lesen Sie mehr in c’t Daten schützen 2021

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.

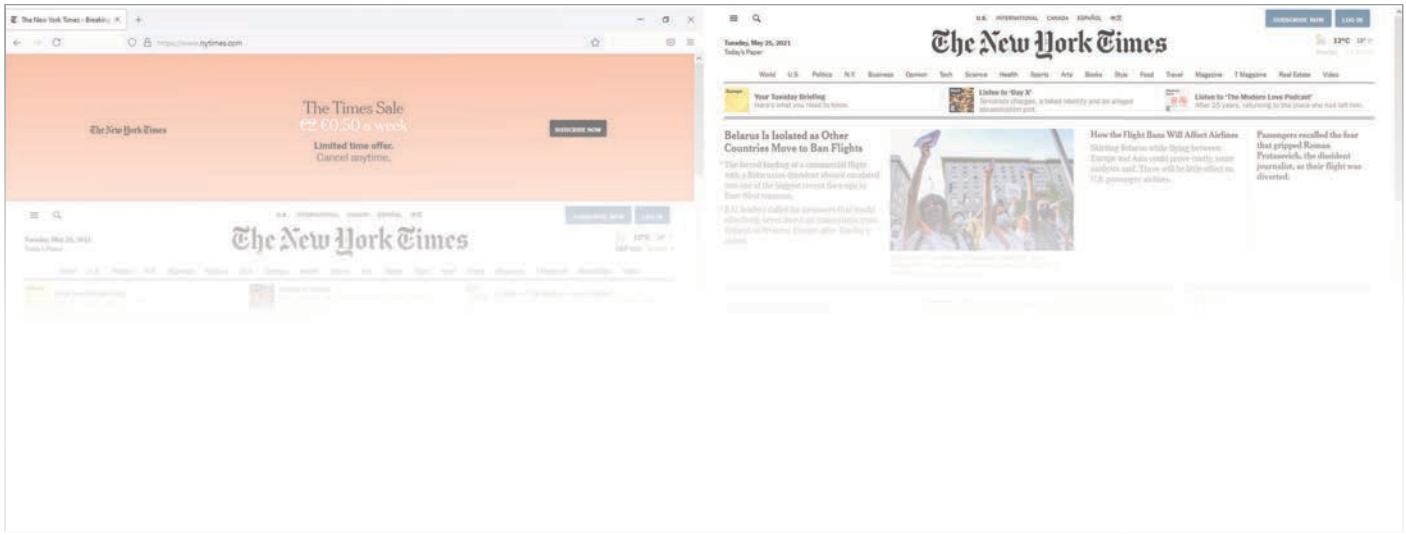
Unsere Beispielkonfiguration für PCs und Macs ist bestmöglich auf Komfort und Datenschutz ausgerichtet, was durchaus einen Kompromiss bedeutet: Denn viel Komfort bedeutet oft wenig Datenschutz und umgekehrt. Uns war wichtig, dass der Browser komfortabel bedienbar bleibt und Websites weitgehend wie gewohnt 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



Lesen Sie mehr in c’t Daten schützen 2021

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

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

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