Zehn Regeln für Ihre digitale Sicherheit

Selbst, wer sich selbst für vollkommen uninteressant hält, besitzt Daten, die er schützen sollte. Wie das am besten gelingt.

Simon Hurtz

Nur ein paar Tipps reichen, um sicher unterwegs zu sein: Ein Mann am Handy. Foto: Getty Images

Die geleakten Daten von Politikern, Prominenten und Journalisten in Deutschland, die ein bislang unbekannter Hacker in Form eines perfiden Adventskalenders veröffentlicht hat, machen deutlich: Privatsphäre ist ein Grundrecht, und es ist in Gefahr.

Hinter dem Angriff stecken wohl keine mächtigen ausländischen Dienste. Vieles deutet daraufhin, dass es sich um einen Einzeltäter handelt, den das Verlangen nach Aufmerksamkeit antrieb. Vermutlich wurden nur relativ wenige Personen gehackt, aber das reichte, um an die Daten von Hunderten Unbeteiligten zu gelangen.

«Ich habe doch nichts zu verbergen»: Wie gefährlich und falsch diese Aussage ist, zeigen die Datensätze. Selbst, wer sich selbst für vollkommen uninteressant hält, besitzt Daten, die weder Kriminelle noch staatliche Geheimdienste etwas angehen: Informationen über Dritte. Adressbücher mit Telefonnummern, E-Mailkonten mit Nachrichten, Messaging-Apps mit Fotos und Chatverläufen, all das kann Angreifern wie diesem in die Hände fallen.

Zu viele Menschen gehen fahrlässig mit diesen Daten um. Nicht einmal jeder zehnte Gmail-Nutzer sichert sein Konto mit der sogenannten Zwei-Faktor-Authentifizierung. Der Anteil der Menschen, die Passwort-Manager einsetzen, ist nur unwesentlich grösser. 86 Prozent der Befragten geben an, sich ihre Kennwörter zu merken. Für Gedächtniskünstler mag das eine akzeptable Vorgehensweise sein. Wenn Normalsterbliche ihre Zugangsdaten auswendig kennen, bedeutet das meist, dass sie zu einfach und damit unsicher sind.

Wenn es eine Lehre gibt, die Politiker, Journalisten, die jeder Internetnutzer aus dem aktuellen Fall ziehen können, dann diese: Die zentralen Regeln der IT-Sicherheit sind 2019 wichtiger denn je. Jeder einzelne sollte sie kennen und befolgen und sein Umfeld dafür sensibilisieren.

1. Verwenden Sie lange, zufällige und einzigartige Passwörter

Über sichere Passwörter kursieren viele Mythen: Weder sind Sonderzeichen nötig, noch müssen Sie Ihre Kennwörter regelmässig wechseln. Entscheidender ist die Länge: Acht Zeichen sind das absolute Minimum, zwölf erhöhen die Sicherheit signifikant, für wichtige Konten sollten Sie 16 Buchstaben und Ziffern verwenden.

Vermeiden Sie dabei Phrasen wie «DuKommstNichtVorbei» oder den Klassiker «Passwort», der auch mit Sonderzeichen («Pa$$w0rt1!!») nur unwesentlich besser schützt. Kriminelle setzen Software ein, die solche Abwandlungen leicht errät. Genauso fahrlässig ist es, Nutzernamen, Telefonnummern oder andere persönliche Daten als Zugangsdaten zu verwenden

Der schlechteste Platz für Passwörter

Niemand käme auf die Idee, nur einen Schlüssel für Haustür, Wohnungstür, Tresor und Fahrradschloss zu verwenden. Diese analoge Vorsicht scheint im digitalen Leben ausser Kraft gesetzt zu sein: Viele Menschen nutzen dieselben Passwörter für mehrere Konten. Das ist fatal: Wenn Hacker Zugangsdaten erbeuten, versuchen sie fast immer, sich damit auch bei anderen Seiten einzuloggen.

Am sichersten sind komplett zufällige Kennwörter, die Sie sich nicht selbst ausdenken, sondern generieren lassen. Diese Funktion bringen die meisten Browser mit. Auf den Seiten von Passwortmanagern wie Lastpass, Dashlane, 1Password und Roboform können Sie Passwörter generieren lassen. Das ist sinnvoll, denn einen Passwort-Manager sollten Sie ohnehin verwenden.

2. Nutzen Sie einen Passwort-Manager

Ihr Gedächtnis ist der schlechteste Platz für Passwörter. Stift und Papier sind nur geringfügig besser – wenn Sie den Zettel verlieren oder unterwegs nicht dabeihaben, sperren Sie sich aus. Vertrauen Sie Ihre Login-Daten stattdessen einem Passwort-Manager an. Damit verwalten sie

alle Anmeldeinformationen und synchronisieren diese über mehrere Geräte hinweg. Ein zentrales Master-Kennwort gibt Ihnen Zugriff auf alle anderen Zugänge – dass dieses Passwort besonders lang und sicher sein sollte, versteht sich von selbst.

Zwar können auch die Anbieter von Passwortmanagern gehackt werden, doch die meisten Dienste verschlüsseln die Daten der Nutzer mit sicheren kryptografischen Verfahren. Angreifer erhalten dann nur Zeichensalat, mit dem sie wenig anfangen können. Die deutsche Stiftung Warentest hat neun Passwort-Manager getestet und vier davon als «empfehlenswert» eingestuft. Die «Süddeutsche»-Redaktion hat mit Lastpass und Keepass gute Erfahrungen gemacht. Beide Dienste sind kostenlos.

3. Vermeiden Sie Single Sign-on

Single-Sign-on (SSO) beschreibt ein Verfahren, bei dem ein einzelnes Konto genutzt wird, um sich bei unterschiedlichen Diensten anzumelden. Google, Facebook und Twitter bieten etwa an, sich mit dem jeweiligen Account bei anderen Webseiten anzumelden. Sie müssen dann kein Passwort vergeben und keine zusätzliche Login-Daten speichern.

Das ist komfortabler und sicherer, als doppelte oder einfach zu erratende Kennwörter zu verwenden. Aber die Methode birgt eigene Risiken. Einerseits gibt es Bedenken, was den Datenschutz angeht, insbesondere beim Login mittels Facebook. Andererseits können sich Kriminelle, die Zugriff auf einen Ihrer Hauptaccounts erlangen, damit bei weitere Diensten anmelden. Setzen Sie deshalb besser auf getrennte Zugangsdaten, die Sie über einen Passwort-Manager verwalten.

4. Misstrauen Sie Sicherheitsfragen

«Wie lautet der Vorname Ihrer Grossmutter mütterlicherseits?» Oder: «Wie hiess Ihr erstes Haustier?» Manche Anbieter setzen solche Fragen als zusätzliche Absicherung ein, wenn Nutzer ihr Passwort vergessen haben oder zurücksetzen wollen. Grundsätzlich ist ein zweiter Faktor eine gute Idee, aber die Sicherheitsfragen bergen ein Risiko: Oft lassen sich die Antworten erraten oder aus öffentlich einsehbaren Informationen, zum Beispiel aus Profilen in sozialen Netzwerken, rekonstruieren.

Eine simple, aber effektive Strategie ist es, bewusst falsche Antworten zu geben. Eine Grossmutter mit dem Vornamen «Wackelpudding» wird vermutlich kein Angreifer erraten, zumal die Zahl der Versuche begrenzt ist. Wenn Sie ganz sicher gehen wollen, generieren Sie als Antwort auf die Sicherheitsfrage ein zweites, zufälliges Kennwort, das Sie ebenfalls in Ihrem Passwort-Manager speichern.

5. Sichern Sie wichtige Konten mit einem zweiten Faktor

Die gute Nachricht: Immer mehr Dienste bieten mittlerweile Zwei-Faktor-Authentifizierung (2FA) an. Die schlechte: Viele Menschen sind zu bequem oder zu leichtfertig, um ihr Konto damit zu schützen. Sie verzichten ohne Not auf einen zweiten Faktor, der Angreifer auch dann aussperrt, wenn diese das Passwort erbeuten. Oft handelt es sich um einen Code, den Sie in einer separaten App empfangen oder per SMS zugeschickt bekommen. Manchmal kommen auch biometrische Merkmale oder zusätzliche Hardware wie der Yubikey zum Einsatz.

Alle Methoden haben eines gemeinsam: Das Passwort allein reicht nicht, in den meisten Fällen benötigen Hacker physischen Zugriff auf Ihr Smartphone. Das senkt das Risiko für einen erfolgreichen Angriff

signifikant. 2FA können Sie bei mehreren Dutzend grösserer Anbieter aktivieren, darunter Facebook, Google, Apple und Amazon. Das Anmelden dauert eine Minute länger, aber die Sicherheit sollten Ihnen den Aufwand Wert sein. Vor allem beim E-Mail-konto (das Hackern oft Zugriff auf weitere Accounts ermöglicht, da sie darüber Passwörter zurücksetzen können) und Diensten wie Ebay, Paypal oder Ihrem Bankzugang sollte 2FA Pflicht sein.

6. Nutzen Sie Messenger mit Ende-zu-Ende-Verschlüsselung

Ende-zu-Ende-Verschlüsselung (E2E) klingt nach einer komplizierten Angelegenheit. Das Gegenteil ist der Fall. Sie müssen sich keinen PGP-Key zulegen und Ihre E-Mails chiffrieren, um sicher zu kommunizieren. Viele Messenger verschlüsseln Ihre Nachrichten, sodass weder Geheimdienste noch Kriminelle mitlesen können. E2E bedeutet, dass Text, Bilder und Videos lokal auf dem Gerät des Absenders in Zeichensalat verwandelt und erst mit dem einzigartigen Schlüssel des Empfängers – und nur von diesem – in den Ursprungszustand gebracht werden können. Das unterscheidet sie von der sogenannten Transportverschlüsselung.

Phishing ist schwer zu erkennen

Sogar Whatsapp, das die meisten Menschen eher mit miesem Datenschutz als mit vorbildlicher Sicherheit verbinden, setzt auf E2E. Mehr als anderthalb Milliarden Nutzer chatten also bereits verschlüsselt. Die Inhalte ihrer Nachrichten sind sicher. Ihre Metadaten und Adressbücher sind es aber nicht: Der Mutterkonzern Facebook greift auf Telefonnummern zu, und Whatsapp speichert, wann sie mit wem schreiben. Besser machen es Apps wie Signal, Wire und Threema. Hier finden Sie eine Übersicht empfehlenswerter Messenger.

7. Prüfen Sie Links und Anhänge vor dem Öffnen

Nigerianische Prinzen landen bei Ihnen zuverlässig im Spam-Ordner, und das angebliche Millionenerbe eines verschollenen Onkels macht Sie nicht neugierig, sondern misstrauisch? Herzlichen Glückwunsch, Sie haben den ersten Test bestanden. Diese banalen Betrugsversuche waren aber ohnehin nur für die treudoofsten Nutzer bestimmt.

Für Sie haben Kriminelle raffiniertere Methoden entwickelt. Moderne Phishing-Nachrichten sind auf den ersten Blick kaum noch von echten Nachrichten zu unterscheiden. Scammer fälschen E-Mails und ganze Webseiten, die sich nur durch Kleinigkeiten vom Original unterscheiden. Meist versuchen die Betrüger, ihren Opfern mit Schadprogrammen verseuchte Anhänge unterzujubeln oder sie auf Webseiten zu lotsen, wo sie angeblich ihr Passwort zurücksetzen oder ihre Zugangsdaten eingeben sollen.

Die wirksamsten Gegenmittel sind Vorsicht und gesunder Menschenverstand. Versichern Sie sich besser dreimal, ob Sie dem Absender vertrauen (und achten Sie dabei auf jedes Zeichen der E-Mailadresse), bevor Sie einen Anhang öffnen oder auf einen Link klicken. Geben Sie Passwörter nur auf Seiten ein, deren URL Sie sorgfältig geprüft haben. Lassen Sie sich dabei nicht von dem Schlosssymbol in die Irre führen, das viele Browser in der Adresszeile anzeigen, um eine HTTPS-Verbindung zu markieren. Das bedeutet nur, dass die Verbindung verschlüsselt ist, sagt aber nichts darüber aus, ob auf der anderen Seite Kriminelle sitzen, die Ihre Daten abgreifen.

8. Halten Sie Ihr System aktuell

Fast jedes Programm und jedes Betriebssystem enthält Sicherheitslücken. Die Frage ist nur, wann sie entdeckt und ausgenutzt werden. Die meisten Hersteller veröffentlichen deshalb regelmässig Patches, um Schwachstellen zu schliessen. Viele Apps und Systeme aktualisieren sich von selbst oder weisen auf Sicherheitsupdates hin. Nehmen Sie diese Warnungen ernst und verzögern Sie die Installation nicht.

Das trifft vor allem auf Adobe-Produkte wie Flash und den Acrobat-Reader zu, für die immer wieder Notfall-Patches erscheinen. Auch iOS, MacOS, Android, Windows und Linux sollten Sie aktuell halten. Dabei ist zwischen dringenden Sicherheitsupdates und Aktualisierungen mit neuen Funktionen zu unterscheiden. Nötig sind nur Patches, die akute Schwachstellen beheben. Insbesondere Microsoft macht Nutzer bei Funktionsupdates oft zu Testkaninchen, die teils unfertige Software testen.

9. Entknüpfen Sie alte E-Mailadressen

In Ihrem Facebook-Konto ist eine E-Mailadresse hinterlegt, die Sie seit Jahren nicht mehr genutzt haben? Das öffnet ein Einfallstor für Kriminelle. Wenn diese den E-Mailaccount übernehmen, können sie das Facebook-Passwort zurücksetzen und selbst ein neues vergeben. Ein Youtuber, dessen Daten beim aktuellen Hack erbeutet wurden, sagte der «Süddeutschen Zeitung», dass der Täter bei ihm diese Methode verwendet habe.

Die Vorsichtsmassnahme ist natürlich nicht nur bei Facebook wichtig, sondern bei allen Konten, die private oder sensible Daten enthalten: Hinterlegen Sie dort aktuelle Kontaktinformationen und achten Sie insbesondere darauf, dass E-Mailadresse und Handynummer stimmen.

10. Nutzen Sie offene Wlans mit VPN

Ein Virtuelles Privates Netzwerk (VPN) baut eine separate Verbindung zwischen Geräten auf. Meist verbindet es den Rechner oder das Smartphone eines Nutzers mit dem Server des VPN-Anbieters. Es kann als zusätzliche Sicherheit dienen, wenn Sie Ihre Aktivitäten vor Ihrem Internetanbieter oder dem Wlan-Betreiber verbergen wollen.

Das gilt insbesondere für offene Hotspots, falls Sie dem Betreiber nicht hundertprozentig vertrauen oder unsicher sind, ob Dritte versuchen, das Netzwerk zu überwachen. Solche Wlans finden Sie oft an Flughäfen und Bahnhöfen oder in Cafés. Das VPN verschleiert Ihre Identität und leitet die Daten durch einen virtuellen Tunnel.

Doch Vorsicht: Falls Sie ein VPN nutzen wollen, müssen Sie den Anbieter sorgfältig auswählen. Ein privates Netzwerk nützt nichts, wenn Ihre Aktivitäten bei einem zwielichtigen Unternehmen landen. Seien Sie vor allem bei kostenlosen VPNs vorsichtig, die mit unbegrenztem Datenvolumen und hohen Geschwindigkeiten werben: Viele Dienstleister sammeln und vermarkten Ihre Daten. Hier erfahren Sie mehr darüber, nach welchen Kriterien Sie den Anbieter auswählen sollten.

Süddeutsche Zeitung