Georg Stadler

DIGITALE SICHERHEIT

Die praktische Toolbox zum Schut
von E-Mails, Smartphone, PC & Co

FBV

VORWORT

»Die größte existierende Sicherheitslücke ist unsere Bequemlichkeit.«

Liebe Leserinnen und Leser,

der Beginn des Jahres 2019 wurde überschattet von einem großen Daten-Leak, das in Deutschland tagelang für Aufregung sorgte. Sensible Daten und Dokumente von Politikern und Prominenten waren plötzlich für jeden im Netz verfügbar. Und sind es, etwas Recherchewillen vorausgesetzt, noch immer. Zu den veröffentlichten Daten gehörten die Mobilnummern von Politikern wie Martin Schulz, zahlreiche Privatadressen, persönliche Chats, interne Parteidokumente, aber auch Kreditkartendaten, Impfpässe sowie Einzugsermächtigungen für Lastschriftverfahren.

Ging man anfangs im Zusammenhang mit dem Leak noch von einem gezielten Hackerangriff aus, stellte sich schnell heraus, dass die Daten nicht etwa von einem mit

allen Wassern gewaschenen Cyberkriminellen oder gar von einem ausländischen Geheimdienst mit unheimlichem Know-how und Spezialwissen beschafft worden waren. Nein, beim mutmaßlichen Täter handelt es sich wohl um einen 20-jährigen Schüler, der mit viel Fleiß und Akribie die wohl größte Sicherheitslücke ausgenutzt hat, die in jedem erdenklichen Fachbereich weltweit existiert: die Bequemlichkeit von uns Menschen.

Der Angreifer hatte sich den Zugang zu Rechnern, Servern, Mail-Postfächern und persönlichen Social-Media-Profilen vor allem durch schlecht gesicherte Passwörter besorgt. Mit Sicherheit wäre die Datensammlung des Täters etwas weniger umfangreich ausgefallen, wenn seine Opfer ein paar einfache Grundregeln beim Schutz ihrer Daten und Nachrichten beachtet hätten. Doch genau das haben sie nicht getan!

Wenig später zeigte die Veröffentlichung der sogenannten »Collections 1–5« – eine Sammlung von mehr als 2 Milliarden (!) Mail-Adressen, dazugehörigen Passwörtern und weiteren Daten –, dass auch Millionen Bürger privat Opfer von Internet-Hacks sind. Auch sie dürften sich zu wenig abgesichert oder sich fahrlässig im Netz bewegt haben.

Dabei gibt es eine ganze Reihe einfacher Regeln und Kniffe, die jeder auf seinem Smartphone und auf seinem PC schnell und unkompliziert umsetzen kann, um die Grundsicherheit seiner Daten deutlich zu erhöhen. Um diese Maßnahmen geht es in diesem kleinen Leitfaden. Sie können sogar gleich während des Lesens damit

beginnen, die meisten der von mir vorgeschlagenen Sicherheitsmaßnahmen umzusetzen. Sie werden sehen, so schwer ist es nicht.

Unter *www.hackerimpfung.de* finden Sie weiterführende Informationen und Anleitungen rund um das Thema Datensicherheit.

Viel Erfolg!

München, Januar 2019
Georg Stadler

So funktioniert der Klau von Daten

Nicht nur Bequemlichkeit führt dazu, dass viele von uns ihre Daten nur mangelhaft schützen. Es gibt noch zwei weitere Faktoren: Unwissenheit und Resignation.

Das Thema Datensicherheit ist für sich genommen extrem unsexy. Es erscheint vielen als zu kompliziert und schwer zu verstehen. Also machen sie sich gar nicht erst die Mühe, sich damit zu beschäftigen. Die Folge sind ganz konkrete Wissenslücken in Sachen Sicherheit, dank derer Angreifer ein leichtes Spiel haben.

Außerdem glauben viele, Datenschutz sei ohnehin zwecklos, weil in diesem Bereich eine hundertprozentige Sicherheit nicht möglich sei: Wer immer es wolle, könne auf alle erhobenen Daten zugreifen. Aussichtslos, sich dagegen zu wehren.

Ein solches Denken ist gefährlich. Ja, Daten sind immer hackbar. So wie in jedes Haus eingebrochen werden kann. Doch es macht einen großen Unterschied, ob die Tür des Hauses offen steht oder abgeschlossen ist, ob das Haus eine Alarmanlage hat und ob der wertvolle Schmuck in einem Safe und nicht nur lose in einer Schublade liegt.

Ich bin sicher, dass jeder von Ihnen, bevor Sie aus dem Haus gehen, zumindest die Tür ins Schloss fallen lässt, wenn nicht sogar abschließt. Obwohl Sie wissen, dass ein Einbrecher diese Sicherheitsvorkehrung locker mit einem Stemmeisen bezwingen kann. Doch die geschlossene Tür macht es einem potentiellen Dieb ein bisschen schwerer. Vielleicht sogar so schwer, dass er sich lieber eine leichtere Beute, wie zum Beispiel ein Haus mit einem geöffneten Fenster, sucht.

Jede Sicherheitsmaßnahme, die Sie an Ihrem Smartphone oder an Ihrem PC aktiv umsetzen, erschwert es einem Dieb, an Ihre Daten zu gelangen. Doch wie gehen diese Diebe eigentlich vor?

In der Regel nutzen Datendiebe Schwachstellen in der IT von Telekommunikations-, Software- oder Handels- und Finanzunternehmen aus, um sensible Kundendaten auszuspähen. Diese Daten werden dann entweder an Dritte verkauft oder aber – zum Beispiel im Fall von Kreditkartendaten – von den Dieben selbst missbraucht. Betroffen von solchen Attacken waren bereits namhafte Unternehmen wie Vodafone, Twitter, Adobe oder internationale Banken in der Schweiz, Chile oder den USA.

Damit Sie ein Gefühl dafür bekommen, dass diese Angriffe Sie persönlich betreffen, bitte ich Sie, jetzt sofort jede Ihrer aktuell genutzten Mail-Adressen auf den folgenden Webseiten checken zu lassen:

https://haveibeenpwned.com

Die deutsche Alternative des Hasso-Plattner-Instituts:

https://sec.hpi.de/ilc

Diese Webseiten zeigen an, ob Ihre Mail-Adresse in der Vergangenheit Teil eines entdeckten Hacks war. In der Regel ist es nicht Ihr Mail-Account, der gehackt wurde, sondern ein wenig abgesicherter Online-Account, bei dem Sie Ihre Mail-Adresse eingerichtet haben. Gehören Sie zu den Menschen, die für sämtliche Accounts ein und dasselbe Passwort verwenden, sollten Sie sofort das Passwort für diesen Mail-Account ändern. Tun Sie dies nicht, besteht die Gefahr, dass Hacker einen vollständigen Zugriff auf Ihren E-Mail-Account haben. Selbst, wenn Sie glauben, dass Ihre privaten Mail-Nachrichten keine wertvollen Informationen beinhalten, weil sie nur privater Natur sind, kann Sie der Datenklau teuer zu stehen kommen.

Ihr Mail-Account dient ja nicht nur als Messenger, sondern sehr wahrscheinlich auch als Zugang zu weiteren Accounts wie Zahlungsdienstleistern und Online-Shops. Nutzen Sie auch dort dasselbe Passwort – wie es aus Bequemlichkeit oft der Fall ist –, können sich die Datendiebe dort ohne Problem einloggen. Sind in diesem Online-Shop zusätzlich auch noch Ihre Kreditkarten-Daten oder andere Zahlungsmöglichkeiten automatisch hinterlegt – so eine One-Click-Bestellung ist ja schon sehr praktisch! –, haben die Hacker gefunden, worauf sie von Anfang an aus waren. Richtig, Ihre privaten Gespräche mit Freunden und Familie sind in der Regel für Hacker nicht sehr inte-

ressant. Ihre Konto- und Kreditkarten-Nummer dagegen schon.

In welchen Online-Shops sie suchen müssen, erfahren die Hacker übrigens durch Newsletter oder Bestellbestätigungen in Ihrem Postfach. Ich bin mir sicher, dass die wenigsten den Newsletter eines Online-Shops als sensibles Datenmaterial ansehen. Missachtet ein Online-Shopper jedoch einfachste Sicherheitsmaßnahmen und verwendet zum Beispiel immer wieder ein und dasselbe Passwort gepaart mit derselben Mail-Adresse, werden selbst alltägliche Newsletter zur Gefahr.

Ich bitte Sie daher nochmal: Checken Sie all Ihre genutzten Mail-Adressen unter *https://haveibeenpwned.com* oder *https://sec.hpi.de/ilc* und ändern Sie im Falle eines Hacks umgehend Ihr Passwort, sowohl in Ihrem Mail-Account, als auch überall dort, wo Sie möglicherweise Kontoinformationen hinterlegt haben.

• • • • • • •

TIPP: Abonnieren Sie die Nachrichten auf der Seite *https://haveibeenpwned.com*. Dann werden Sie im Fall eines neu entdeckten Hacks sofort informiert und können kontrollieren, ob Sie davon betroffen sind.

• • • • • • •

1.

E-MAIL-SICHERHEIT

Wie zuvor beschrieben, ist Ihr Mail-Account der Schlüssel zu fast allen Internet-Accounts. Sichern Sie ihn richtig ab. Ändern Sie JETZT das Passwort für Ihren Mail-Account und verwenden Sie ein neues sicheres Passwort. Welche Eigenschaften ein sicheres Passwort hat, wie Sie mit Sicherheitsfragen umgehen sollten und welche Möglichkeiten es gibt, Ihre Passwörter professionell zu verwalten, erfahren Sie im Kapitel 2: *Passwort-Sicherheit*. Doch es gibt neben einem starken und möglichst langen Passwort noch andere Sicherheitsmaßnahmen, mit denen Sie Ihren Mail-Account schützen können.

Step 1:
Verwenden Sie einen Mail-Account mit einer Zwei-Faktor-Authentifizierung.

Eine Zwei-Faktor-Authentifizierung stellt sicher, dass der erstmalige Zugriff auf Ihren Mail-Account nicht nur mittels Passwort möglich ist, sondern zusätzlich über eine zweite Maßnahme der Authentifizierung erfolgt. Diese Identifizierung kann beispielsweise über SMS, eine App oder spezielle kleine Geräte, auch »Token« genannt, erfolgen. Sollten Sie das Online-Banking Ihrer Bank nutzen, ist Ihnen das Prinzip bestimmt schon vertraut. Um eine Überweisung zu tätigen, müssen Sie sich nicht nur mit Ihrem Passwort auf der Webseite der Bank anmelden, sondern die Überweisung zusätzlich mit einer TAN-Num-

mer oder mit einer App freigeben. Besonders sicher wird dieses Verfahren dann, wenn die zwei Authentifizierungsmöglichkeiten (Passwort + TAN) an zwei verschiedenen Orten gespeichert und aufbewahrt werden. Sie sollten daher bei der Zwei-Faktor-Authentifizierung möglichst darauf achten, dass beide Authentifizierungsmethoden physisch voneinander getrennt sind. Beispielsweise, indem die 1. Authentifizierung auf Ihrem PC erfolgt, die 2. Authentifizierung jedoch auf Ihrem Smartphone. In der Praxis nutzen die meisten fast nur ein Smartphone, um online zu gehen. In diesem Fall ist die Zwei-Faktor-Authentifizierung meist auf dem Smartphone vereint. Doch selbst wenn die physische Trennung nicht möglich ist, erhöht die Zwei-Faktor-Authentifizierung die Sicherheit und sie ist immer besser als die alleinige Absicherung mit einem Passwort.

Übertragen auf Ihren Mail-Account entsteht nun folgendes Szenario: Hat jemand Ihr Passwort erbeutet und will sich damit von einem anderen PC oder einem anderen Smartphone in ihren Mail-Account einloggen, ist dies nur dann möglich, wenn diese Person auch die zweite Authentifizierung kennt. Sprich: Hat der Datendieb nicht auch Ihr Smartphone gestohlen, mit dem Sie jeden neuen Zugriff zum Mail-Account bestätigen müssen, ist der Zugriff auf Ihren Mail-Account für ihn deutlich erschwert.

In der Regel erfolgt die Aktivierung der Zwei-Faktor-Authentifizierung beim Einrichten Ihres E-Mail-Kontos. Sie müssen dafür meist ihre Mobilfunknummer oder eine alternative Mail-Adresse hinterlegen. Aus eigener Erfah-

rung weiß ich, dass viele Nutzer sich in diesem Fall lieber für die alternative E-Mail entscheiden. Sie wollen nicht, dass die datenhungrigen Internetkonzerne auch noch ihre Mobilfunknummer kennen. In diesem Fall ist die Angabe der Mobilfunknummer jedoch die bessere Entscheidung, da Sie von einem unerlaubten Login-Versuch unmittelbar erfahren und mit Hilfe Ihres E-Mail-Providers Gegenmaßnahmen einleiten können.

Beispiel für eine Zwei-Faktor-Code-Abfrage

Eine dritte Möglichkeit ist die Nutzung sogenannter Authenticator Apps oder Tokens, wie zum Beispiel dem »Google Authenticator«. Diese Programme werden meist per QR-Code mit dem Account verknüpft und generieren bei Bedarf den zusätzlichen Sicherheitscode.

Ist die Zwei-Faktor-Authentifizierung nicht aktiviert, kann es immerhin noch sein, dass Sie eine Nachricht bekommen, in der nachgefragt wird, ob wirklich Sie hinter

dem Login von einem fremden Gerät stecken. Allerdings kann es in so einem Fall bereits zu spät sein, wenn der Angreifer die schwache Sicherung ausgenutzt und das Passwort Ihres Accounts geändert hat.

• • • • • • •

TIPP: Sie müssen diese Zwei-Faktor-Authentifizierung nicht bei jedem Einloggen verwenden, oft lässt sich ein Browser als »vertrauenswürdig« markieren. Hier wird dann nicht mehr nach dem Zwei-Faktor-Code gefragt. Vertrauenswürdig sind aber nur Computer, auf die *ausschließlich Sie* Zugriff haben. Wenn Sie im Urlaub Ihre Mails in einem Internetcafé checken, oder aber bei einem Freund oder im Büro erstmals auf Ihre Mails zugreifen, sollten sie das Gerät nicht als vertrauenswürdig einstufen. Immer wenn Ihr PC mehreren Personen frei zugänglich ist, sollten sie Vorsicht walten lassen.

• • • • • • •

Überprüfen Sie daher jetzt sofort, ob Ihr E-Mail-Provider eine Zwei-Faktor-Authentifizierung anbietet. Tut er das, aktivieren Sie die Funktion wie in der Anleitung Ihres E-Mail-Providers beschrieben. Arbeitet er dagegen ohne Zwei-Faktor-Authentifizierung, sollten Sie über einen Wechsel Ihres E-Mail-Providers nachdenken (siehe Seite 21: *Woran Sie einen guten E-Mail-Provider erkennen*).

In der Regel bieten sämtliche relevanten E-Mail-Provider eine Zwei-Faktor-Authentifizierung an, etwa Microsoft, Apple oder Google. Zwei der großen deutschen

Mailanbieter fehlen allerdings in der Liste: »GMX« und »Web.de«. Leider bieten beide keine Zwei-Faktor-Authentifizierung an (Stand Februar 2019). Aber auch der eigene Facebook- oder Amazon-Account lassen sich mit einer Zwei-Faktor Authentifizierung schützen. Zu finden ist die Zwei-Faktor-Authentifizierung meist in den *Erweiterten Sicherheitseinstellungen*.

Die Aktivierung für alle Ihre wichtigen Konten ist zwar mühsam, erhöht jedoch Ihre Sicherheit signifikant.

Woran Sie einen guten E-Mail-Provider erkennen

Sollten Sie festgestellt haben, dass Ihre alte Mail-Adresse kompromittiert ist, können Sie nicht nur das Passwort oder die Mail-Adresse wechseln, sondern mit einem neuen E-Mail-Provider gleich klar Schiff machen. Mittlerweile gibt es neben den klassischen großen Mail-Anbietern auch kleinere Mitbewerber auf dem Markt, die die Sicherheit Ihrer Kunden besonders ernst nehmen. Allerdings sind diese Dienste meist kostenpflichtig (ab 1 Euro im Monat). Da jedoch auch große Mail-Anbieter Ihre Kunden mittlerweile oft vor die Entscheidung stellen, sich entweder Werbung anzusehen oder für eine werbefreien Mail-Zugang zu bezahlen, ist dies eine Investition, über die Sie nachdenken sollten.

Einen sicheren E-Mail-Provider erkennen Sie zum Beispiel daran, dass er möglichst wenig von Ihnen wissen will. Bei einem Anbieter wie Posteo ist es zum Beispiel möglich, anonym zu bezahlen. Außerdem werden bei der

Anmeldung keine unnötigen persönlichen Daten von Ihnen abgefragt.

Ein sicherer E-Mail-Provider arbeitet zudem mit einer verschlüsselten Mailbox, auf die er selbst keinen Zugriff hat. Vorbildlich ist auch die Veröffentlichung von Transparenzberichten, in denen zum Beispiel Rechenschaft über staatliche Kontrollanfragen abgelegt wird. Eine Zwei-Faktor-Authentifizierung ist bei an Sicherheit interessierten Anbietern eine Selbstverständlichkeit.

Empfehlenswerte E-Mail-Provider mit guten Sicherheitskonzepten sind:

- Posteo.de (kostenpflichtig – Berlin)
- Mailbox.org (kostenpflichtig – Berlin)
- protonmail (kostenpflichtig – Schweiz)
- tutanota (Basisversion kostenlos – Hannover)

Step 2:
Achten Sie beim Einrichten Ihres Mail-Programms auf eine verschlüsselte Verbindung zum Provider.

In der Regel ist eine verschlüsselte Verbindung zum Provider Standard und erfolgt automatisch. Sollten Sie nicht sicher sein, ob Ihr Mail-Programm mit einer solchen verschlüsselten Verbindung arbeitet oder ob Sie die verschlüsselte Verbindung ausgeschaltet haben, prüfen Sie