MENSCHEN IM GESPRÄCH

"Nur ein Passwort zu verwenden ist riskant"

29. Oktober 2019, 14:36 Uhr ▪ 100× gelesen ▪ 0 ▪ 0 ▪

hochgeladen von Silvia Gschwandtner

Autor: Silvia Gschwandtner aus Linz

Wie man sich am besten vor Datenklau im Internet schützt haben wir Datensicherheits-Experten Rene Mayrhofer von der Johannes Kepler Universität gefragt.

LINZ. Rene Mayrhofer ist Leiter des Instituts für Netzwerke und Sicherheit, sowie im Leitungsteam des neu eröffneten LIT Secure and Correct Systems Lab an der Johannes Kepler Universität. Davor war er als Experte für die Sicherheit der Android Plattform bei Google zuständig. Mit der StadtRundschau hat er über Passwörter, Cookies und Alexa gesprochen.

Wo lauern die größten Sicherheitslücken im privaten Bereich?
Rene Mayrhofer: Es gibt mehrere Bereiche, die Privatpersonen direkt betreffen. Einerseits gibt es immer mehr "Internet of Things" (IoT) Geräte im Hauhalt wie zum Beispiel Staubsaugerroboter, Kameras oder verschiedene Sensoren. Diese sind oft mit dem Internet verbunden, werden aber weder automatisch mit der neuesten Software aktualisiert noch mit guten Passwörtern geschützt und können so Fremdzugriffe erlauben. Andererseits ist es leicht, den Überblick über die verschiedensten digitalen Dienste wie Web-Logins, Streaming-Services oder diverse Messenger zu behalten. Jeder Dienst braucht oft einen eigenen Account und damit kommen schnell viele Passwörter zusammen.

Wie kann man diese absichern und was muss man dabei beachten?
Ich empfehle drei Grundregeln: Alle Sicherheitsupdates einspielen, wenn diese verfügbar werden, vom persönlichen Smartphone bis hin zu den IoT-Geräten im Haushalt. Am besten sollten Geräte diese automatisch einspielen können.

Passwortmanager verwenden, um für alle Dienste verschiedene, lange Passwörter zu verwenden, ohne sich diese merken zu müssen. Gute Passwortmanager integrieren direkt mit dem Browser und synchronisieren zwischen verschiedenen Geräten. Noch besser sind sogenannte Tokens für Zweifaktor-Authentifizierung wie die verschiedenen USB-Sticks nach dem FIDO2/WebAuthn Standard, die es ab ca. 20€ gibt. Dabei wird für jeden Login ein eigener digitaler Schlüssel verwendet und Passwort-Phishing-Angriffe (welche auch noch mit einem Passwortmanager funktionieren können) laufen ins Leere.

Nur solche Dienste konfigurieren und aktivieren, die man auch nutzt. Wenn man z.B. eine Kamera vor der Haustür nur von zu Hause aus verwendet, braucht diese auch keinen Internet-Zugriff.

Ist es riskant, das gleiche Passwort für alles zu verwenden?
Ja, das ist riskant. Dasselbe, einfach zu erratende Passwort für viele Dienste zu verwenden ist zwar einfach, aber unsicher. Wenn nur einer der Dienste einen Fehler hat, können die Zugangsdaten dann für die anderen Dienste verwendet werden. Am besten verwendet man verschiedene, komplexe Passwörter für verschiedenen Dienste.

Wie soll man sich die ganzen Passwörter merken?
Diese sollte man sich nicht merken, sondern aufschreiben. Wer keinen Passwortmanager verwenden möchte, der die Passwörter im Browser automatisch ausfüllen kann, kann sie einfach auf einer Papierliste notieren, die daheim bleibt - sofern man die Dienste primär von dort verwendet. Eine Passwortliste in der Geldtasche mitzutragen wäre allerdings kontraproduktiv.

Kann man Alexa, Siri und Co. trauen?
Die Frage ist, wofür und wo man solchen Sprachassistenten vertrauen möchte. Sie ermöglichen oft eine leichtere Benutzung mancher Dienste, sollten aber in sensiblen Umgebungen mit vertraulicher Kommunikation mit Bedacht eingesetzt werden.

Haben Sie persönlich so ein Gerät?
Ich baue mir solche Assistenten selbst, die ohne Abhängigkeiten zu externen Servern auskommen. Diese haben eine schlechtere Erkennungsqualität der Spracheingabe und viel weniger Funktionen, aber ich kann damit experimentieren, was lokal im Gerät funktioniert und was nicht.

Soll man Cookies einfach akzeptieren?
Diese Diskussion läuft gerade sehr aktiv. Es ist klar, dass man nicht bei jeder aufgerufenen Seite die oft lange Liste der verwendeten Cookies genau durchgehen wird, weil dies zu viel Aufwand kosten würde. Manche aktuellen Browser experimentieren bereits damit, Cookies von externen Servern automatisch zu limitieren. Eine einfache Methode, die bei allen weit verbreiteten Browsern hilft, ist der Privatsphäre- oder Inkognito-Modus. Dabei sehen die Webserver zwar immer noch, von wo die Dienste abgerufen werden, aber hinterlegte Cookies werden nach dem Schließen des Fensters nicht gespeichert.

Welche Browser, Mailprogramme etc. soll man benutzen?
Das hängt viel vom persönlichen Einsatzgebiet und Geschmack ab. Manche sind auf einfache Bedienung oder Geschwindigkeit auch auf langsameren Geräten optimiert, andere speziell auf Sicherheit und Privatsphäre. Es sollten auf jeden Fall nur solche sein, die auch schnell Sicherheitsupdates bekommen. Ich persönlich verwende auf meinem Laptop und Desktop nur Browser und Mailprogramme, die im Kern Open Source sind.

Warum haben Ihrer Meinung nach viele Menschen im Internet so wenig Sicherheitsbewusstsein?
Ich verstehe das sehr gut. Das Thema ist komplex und man muss sich damit auseinandersetzen, weil Manches nicht unbedingt der üblichen Erwartung entspricht. Außerdem stehen Sicherheitsmechanismen oft mit der einfachen Benutzbarkeit in Konflikt. Die Wahl zwischen einfach und sicher sollte aber nicht auf Endbenutzer abgeladen werden, sondern die Entwickler von Systemen haben die Aufgabe, einen guten Kompromiss zu schaffen. Wenn ein System unsicher verwendet wird, sollte man nicht Benutzern die Schuld daran geben, sondern nach besseren Möglichkeiten suchen.

Autor:
Silvia Gschwandtner aus Linz

Folgen ℹ **9** folgen diesem Profil

KOMMENTARE