IT-SICHERHEIT

Das Passwort ist ein Auslaufmodell

Von Uwe Sievers | 16. Mai 2019 | Ausgabe 20

Ein Kennwort gilt als der Standard für Zugriff auf Daten und Dienste. Dessen Sicherheit gilt jedoch als überholt. Alternativen sind gefragt.

Foto: Foto [M]: panthermedia.net/designer491/VDIn

So kryptisch wie möglich sollten Passwörter sein. Doch sie sind schwer zu behalten und können Hackern in die Hände fallen. Weltweit suchen Forscher nach Alternativen.

Anfang Mai ist jedes Jahr Weltpassworttag und jedes Jahr wird die Sicherheit von Passwörtern kritisch diskutiert. Jedoch halten zahlreiche Tipps zur Mindestlänge und Verwendung von Sonderzeichen viele nicht davon ab, schlicht die Ziffernfolge 123456 als Passwort zu wählen. Sicherheitsexperten sind immer wieder fassungslos, Forscher suchen nach sicheren Alternativen.

Einfach ist das nicht, weiß Norbert Pohlmann, Professor für Informationssicherheit an der Westfälischen Hochschule und Leiter des dortigen Instituts für Internet-Sicherheit: „Jeder Anbieter im Internet, der Passwörter für die Zugangskontrolle verwendet, hat ein dazu passendes Authentifikationssystem aufgebaut, das zum Beispiel eine Nutzerdatenbank beinhaltet."

Passwörter überprüfen: Doch selbst sichere Passwörter werden zum Risiko, wenn Anbieter im Internet sie unverschlüsselt ablegen. Dadurch werden sie bei einem digitalen Systemeinbruch zur leichten Beute – für Hacker ein Glücksfall. Erst recht, wenn das gleiche Passwort auf verschiedenen Plattformen verwendet wird.

Es empfiehlt sich daher, in gewissen Abständen zu überprüfen, ob die eigenen Zugangsdaten in falsche Hände geraten sind. Dazu existieren im Internet Angebote, wie der Identity Leak Checker des Hasso-Plattner-Instituts oder der Webdienst „Have I Been Pwned". Wer dort seine E-Mail-Adresse eingibt, erfährt ganz schnell, ob sich ein dazugehöriges Passwort im Umlauf befindet. Solche Passwörter dürfen als verbrannt gelten, denn gewöhnlich werden sie im Cyberuntergrund für wenig Geld angeboten.

Auch Google oder Facebook kennen die Probleme und bieten an, die eigenen Nutzer gegenüber anderen Plattformen zu authentifizieren. Anbieter zeigen das zumeist deutlich, etwa in der Form: Log-in mit Facebook-Konto. Die Sicherheit erhöht das aber nur geringfügig: Der Anbieter erhält zwar keine Zugangsdaten, aber dafür erfahren Google oder Facebook von jedem Zugriff. Außerdem können Anbieter weitere Nutzerdaten von den Internetkonzern anfordern, etwa Geburtsdatum oder Geschlecht. Letztlich basiert der Zugang auch weiterhin auf einem Passwort, das liegt jedoch bei Google oder Facebook.

Passwörter nicht mehr zeitgemäß: Generell gelten Passwörter nicht mehr als zeitgemäßer Sicherheitsstandard. Experten empfehlen deshalb Alternativen wie die Zwei-Faktor-Authentifizierung. Hierbei wird ergänzend zum Faktor Passwort noch ein weiteres Merkmal verlangt, dass über einen anderen Kanal läuft, etwa über das Smartphone, an das ein einzugebender Code gesendet wird.

Dem liegt das Prinzip zugrunde, etwas, das man kennen muss, mit etwas, das man besitzen muss, zu koppeln. Vielen Anwendern ist das jedoch zu kompliziert. Außerdem liefern gestohlene Smartphones eventuell Kriminellen neue Möglichkeiten, auf fremde Rechnung Waren zu bestellen.

Einfacher geht es mit biometrischen Daten: Das Smartphone kann mit Fingerabdruck oder Iris-Scan entsperrt und Autotüren mit einem Handvenen-Scanner geöffnet werden. Allerdings ist die Sicherheit dieser Methoden mangelhaft. Der Hacker Jan Krissler vom Chaos Computer Club, eher bekannt als Starbug, hat mehrfach Sicherheitsdefizite biometrischer Verfahren demonstriert, angefangen mit nachgemachten Fingerabdrücken über Kontaktlinsen als Irisimitate bis hin zu gefälschten Handvenenverläufen, die er jüngst in einem Vortrag auf der Security-Tagung IT-Defense zeigte.

Geklaute Fingerabdrücke: Werden diese Daten gestohlen, entstehen besondere Probleme. Während Nutzer bei Passwortdiebstählen das Passwort ändern können, ist derartiges etwa bei entwendeten Irisdaten unmöglich. „Wer biometrische Daten verwendet, sollte darauf achten, dass diese Daten immer nur auf dem eigenen Gerät, beispielsweise dem Smartphone, gespeichert werden“, rät deshalb Pohlmann.

Das ist aber nicht immer die Regel: Eine Recherche des Bayrischen Rundfunks ergab, dass etliche Millionen Biometriedaten im Darknet angeboten werden. Sie stammen demnach oft aus großen Datensammlungen von Behörden, die diese häufig für Ausweisdokumente erfassen. IS-Terroristen haben sich darüber bereits gefälschte Identitäten verschafft.

Wissenschaftler arbeiten deshalb intensiv an besseren Verfahren, auch Pohlmann. Einst hat er an seinem Institut die Spezifikation für den sicheren Personalausweis miterarbeitet. „Jetzt haben wir alle positiven Eigenschaften davon auf das Smartphone gebracht“, berichtet er.

Gemeinsam mit dem Start-up Xignsys entwickelte er XignQR, ein sogenanntes Challenge-Response- oder Frage-Antwort-Verfahren, das im automatisierten Dialog zwischen Server und Endgerät des Nutzers diesen legitimiert. „Der Nutzer leitet die Authentifizierung ein, in dem er einen QR-Code einscannt, der jedoch nur die URL zu einem Authentifikationsdienst darstellt“, erklärt Pohlmann. Vereinfacht dargestellt, „läuft auf Basis starker Kryptografie im Hintergrund ein Dialog zwischen den Geräten ab, bei dem der Server am Ende die persönlichen Daten zur Person anzeigt, die diese dann bestätigen muss“, beschreibt er das Vorgehen.

Durch eine Kombination mit weiteren Faktoren wie PIN, Biometrie oder USB-Token könne die Methode auch in Bereichen mit hohen Sicherheitsanforderungen eingesetzt werden. „Bei solchen Anwendungen steht der Server direkt beim Kunden, wie es etwa bei VW der Fall ist“, berichtet Pohlmann. Zu den Kunden zählt auch die Stadt Gelsenkirchen: „Dort kann man damit Parkausweise beantragen und bezahlen“, weitere Dienste sollen folgen.

Ein anderes vielversprechendes Verfahren setzt auf Stimmerkennung. Das in den USA ansässige Unternehmen Pindrop hat einen „digitalen Stimmabdruck“ entwickelt, wie das Europachef Jürgen Vollmer nennt. Das Verfahren basiert darauf, dass sich Nutzer vorab authentifizieren und eine Stimmprobe hinterlassen. „Wir können jedoch nicht nur Nutzer eindeutig erkennen, wir können sogar feststellen, ob Sie ein iPhone 7 oder Samsung 8 verwenden“, erläutert er.

Naheliegende Betrugsversuche, wie aufgezeichnete Stimmen, werden ebenso erkannt. „Wir hören auch am Ton, über welchen Carrier jemand anruft“, womit sich etwa der Mobilfunkanbieter des Kunden feststellen lässt. Großes Interesse an dieser Technologie besteht laut Vollmer beim Onlinebanking von Finanzinstituten, bei Callcentern sowie bei Mobilfunkanbietern.

Hierzulande bietet die Deutsche Telekom seit letztem Sommer die Identifikation per Stimme bei ihren Hotlines an. Sie basiert auf der Technologie des Unternehmens Nuance. Jeder, der möchte, kann sich über sein einzigartiges Stimmmuster identifizieren lassen. Er oder sie muss dazu nur einen Stimmabdruck hinterlegen. Beim nächsten Anruf wird dann die Stimme erkannt. Sicherheitsbedenken will die Telekom mit einer Zertifizierung durch den TÜV begegnen, die derzeit noch läuft.

https://sec.hpi.de/ilc/ https://haveibeenpwned.com/