PASSKEYS – DIE ALTERNATIVE ZUM PASSWORT

Passwörter sind eine Schwachstelle für Ihre Online-Konten. Wer sicher vor Hackern sein will, steigt jetzt auf Passkeys um.

Hacker können Passwörter stehlen oder knacken und gelangen so immer häufiger in fremde Online-Konten. Mit Passkeys gibt es zum Glück eine Alternative. Das sind nahezu unknackbare Schlüssel, die auf Ihrem Smartphone gespeichert und für das Anmelden genutzt werden.

Passwörter sind international als Standard zum Anmelden auf Internetseiten, in Apps und für vieles mehr verbreitet. Nur wer Benutzername und Passwort kennt, bekommt Zugriff. Doch um für jede Seite ein eigenes, sicheres Passwort zu haben, benötigen Nutzer und Nutzerinnen Passwort-Manager auf allen ihren Geräten. Das ist vielen zu aufwendig, sodass sie meist dieselben, oft unsicheren Passwörter auf allen Seiten verwenden. Cyberkriminelle haben damit leichtes Spiel. Und selbst sichere, individuelle Kennwörter sind kein perfekter Schutz, da Hacker sie stehlen oder mit Brute-Force-Angriffen knacken. Bisher gab es allerdings keine einfache Alternative. Das ändern Google, Microsoft, Apple und viele weitere Unternehmen jetzt: FIDO-Passkeys sollen Anmeldungen einfacher und sicherer machen!

Mittlerweile haben fast alle großen Internetseiten die Anmeldung per Passkeys im Angebot. Neben Google, Apple und Microsoft bieten auch viele andere Internetdienste das Anmelden mit der Passwort-Alternative an. Die FIDO-Allianz erwartet für 2025, dass jede vierte der 1.000 meistgenutzten Seiten im Internet Passkey-Anmeldungen ermöglicht. Schon jetzt sind die wichtigsten Seiten dabei, etwa Amazon, PayPal, Ebay, TikTok, Uber und viele andere. Der Einzelhandel und die Reisebranche haben bereits angekündigt, dass sie großflächig nachziehen wollen, um die persönlichen Daten Ihrer Kunden besser zu schützen. Damit wirken Sie der steigenden Bedrohung entgegen, dass Hacker über Social Engineering Zugriff auf die Konten erhalten. Zudem erwarten die Passkeys-Macher, dass auch mehr Banken und Finanzdienstleister auf Passkeys umsteigen, um mehr Sicherheit zu bieten.

Nicht nur das Anmelden auf Internetseiten wird durch Passkeys sicherer, auch für den Zahlungsverkehr stellen sie eine Alternative zum Authentifizieren dar. Denn jede Zahlung benötigt eine Bestätigung der Identität. Das ging früher über SMS, die sich mittlerweile einfach abfangen lassen. Viele Banken haben heute eine eigene App zur Bestätigung. Passkeys kommen aber ohne App aus und benötigen auch keine Einmalcodes oder ähnliches, die sich ebenfalls abfangen ließen.

FIDO ist eine Allianz von Hunderten Unternehmen weltweit, die ein sichereres Anmeldeverfahren entwickelt hat und dieses als Alternative zu Passwörtern verbreiten möchte. Bekannte Mitglieder sind neben Google, Apple und Microsoft zum

Beispiel PayPal, Visa, Mastercard, Amazon, Samsung und viele mehr. Das FIDO-Anmeldeverfahren nutzt Standardverschlüsselungsverfahren in einer nutzerfreundlichen Art und Weise, um sichere Anmeldungen zu ermöglichen. Der Nutzer teilt einer Website oder einer App nur noch mit, dass er sich anmelden möchte, und bestätigt das auf seinem Smartphone. Ein Passwort ist dafür nicht nötig.

Um FIDO nutzen zu können, muss der Service, bei dem man sich anmelden möchte, das unterstützen. Ähnliche Verfahren gab es bereits von anderen Anbietern, aber dazu wurde in der Regel eine Authenticator-App benötigt. Das fällt jetzt weg, da Google, Microsoft und Apple in ihren Betriebssystemen die Voraussetzungen für die Nutzung von FIDO schaffen. Der Nutzer oder die Nutzerin registriert sich wie bisher bei einem Service und trägt alle nötigen Daten ein. Statt eines Passworts erzeugt die Seite ein Schlüsselpaar für die Public-Key-Authentifizierung. Der öffentliche Schlüssel wird auf dem Server gespeichert, der private Schlüssel nur beim Benutzer – entweder in einer entsprechenden App oder direkt vom Betriebssystem. Möchte der User sich später anmelden, schickt die Website oder die App eine entsprechende Anfrage nach dem privaten Schlüssel los. Der Nutzer sieht das nur durch eine Bestätigungsabfrage auf seinem Smartphone. Die bestätigt er mit Fingerabdruck, PIN oder Face ID, alles Weitere regelt das Betriebssystem im Hintergrund.

- Der Nutzer oder die Nutzerin braucht sich keine Passwörter mehr auszudenken und zu merken.
- Passwörter können nicht mehr gestohlen werden – weder beim User noch beim Anbieter, da immer beide Schlüssel für eine Anmeldung benötigt werden. Stiehlt ein Hacker den öffentlichen Schlüssel auf einer Website, fehlt ihm das private Gegenstück. Das lässt sich auch nicht aus dem öffentlichen erzeugen. Gelingt es Kriminellen, die privaten Schlüssel eines Nutzers zu stehlen, muss er diese erst einmal als solche erkennen – die Schlüssel sind kryptische Zeichenketten – und weiß dann trotzdem nicht, für welche Internetseiten sie sind. Zudem fehlt ihm das zugehörige Smartphone.
- Die Schlüssel sind automatisch sicher und können nicht erraten werden.
- Anmelden wird einfacher: kurz auf dem Smartphone bestätigen und fertig, kein Suchen nach dem Passwort, keine Passwort-vergessen-Funktion, keine Bestätigung per E-Mail.

Wer sich auf dem Arbeits-Mac auf einer Seite angemeldet hat, möchte das natürlich auch weiterhin auf dem privaten Android-Smartphone tun können. Die FIDO-Schlüssel werden daher in Ihrem Google-, Microsoft- oder Apple-Konto gespeichert und bei Bedarf erstellt das Betriebssystem eine Kopie des Schlüssels, um diesen zu den anderen Betriebssystem-Welten zu übertragen. Beim Wechsel zwischen den Welten kann daher eine zusätzliche Bestätigung nötig sein. Der Rest funktioniert aber wieder automatisch. Es soll sogar möglich sein, dass Sie sich auf dem PC eines Freundes auf einer Seite anmelden, Ihr Smartphone wird automatisch per Bluetooth erkannt und Sie müssen nur noch bestätigen.

Werden bestehende Registrierungen übernommen?

Anbieter, die FIDO unterstützen, werden Möglichkeiten schaffen, bestehende Konten auf FIDO umzustellen. Wie genau das funktioniert und ob dadurch auch das unsichere Passwort ersetzt wird, hängt vom Anbieter ab.

Was passiert, wenn das Smartphone verloren geht?

Da die Passkeys in den Nutzerkonten von Apple, Microsoft und Google gespeichert werden, lassen Sie sich wiederherstellen, wenn das Smartphone gestohlen oder beschädigt wird. Sie brauchen also nicht zu fürchten, dass Sie irgendwann von Ihren Konten ausgesperrt sind.

Passkeys in Passwort-Managern

Viele Passwort bieten mittlerweile auch an, zusätzlich zu Passwörtern Ihre Passkeys zu speichern. So haben Sie einen zusätzlichen Schutz, falls Ihr Smartphone einmal verloren geht.