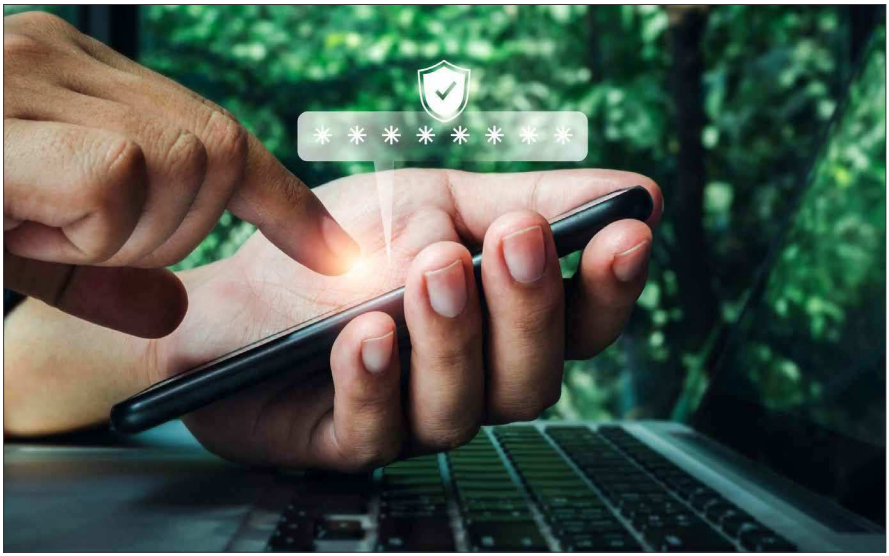
Apple, Google und Microsoft unterstützen FIDO2

Eine Zukunft ohne Passwörter rückt näher

Passwörter sind die Achillesferse des Netzes. Schon seit vielen Jahren arbeiten die Anbieter an sicheren Alternativen. Neue Fortschritte der FIDO-Allianz lassen hoffen.



› Sichere Authentifizierungsverfahren, die Fingerscans oder Gesichtserkennung nutzen, können Passwörter in Zukunft obsolet machen. (Foto: tete_escape – shutterstock.com)

Das Ende des Passworts ist nah – zumindest wenn man den Ankündigungen von Apple, Google und Microsoft glauben darf. Die drei Internet-Giganten wollen ein standardisiertes, passwortloses Authentifizierungsverfahren in ihre Plattformen integrieren. Basis dafür ist die Arbeit der FIDO-Allianz (Fast Identity Online), die seit 2013 an offenen und sicheren Standards für die Identifizierung von Nutzern beim Zugang zu Anwendungen und Services im Web entwickelt.

Gemeinsam mit dem World Wide Web Consortium (W3C) haben die FIDO-Mitglieder schon 2019 mit FIDO2 ein Verfahren vorgestellt, das Passwörter überflüssig machen soll. Das funktioniert folgendermaßen: Will sich eine Person per FIDO für einen Dienst registrieren, wird auf dem Gerät des Benutzers ein Schlüsselpaar

generiert. Der öffentliche Schlüssel wird an den Server gesendet und der private Schlüssel auf dem Endgerät sicher in einem sogenannten FIDO-Authenticator gespeichert. Der Zugriff auf diesen Authenticator lässt sich durch biometrische Verfahren wie Iris- und Fingerabdruck-Scan oder Gesichtserkennung absichern. Hierzu könnten alternativ auch Hardware-Tokens dienen, die sich via USB, NFC oder Bluetooth mit dem Rechner oder Smartphone verbinden.

Bei der Anmeldung an besagtem Dienst muss der Endgerätebesitzer den Besitz seines privaten Schlüssels nachweisen. Erst wenn das erfolgreich geschehen ist, wird der öffentliche Schlüssel zwischen Nutzer und Webdienst ausgetauscht. Der abfragende Dienst bekommt über den öffentlichen Schlüssel lediglich mitgeteilt, dass die sich einloggende Person auch wirklich im Besitz des privaten Schlüssels ist. Als sichere Authenticators für die privaten Schlüssel fungieren Hardware-Tokens wie Funk- oder USB-Sticks sowie PCs und Smartphones mit integrierten Kryptochips, die Betriebssysteme wie Windows 10 oder Android ab Release 7 nutzen. Sie können die Schlüssel sicher verwahren.

Neue Funktionen für mehr Komfort

Das Verfahren ist erprobt und funktioniert. Bisherige Implementierungen setzten jedoch voraus, dass sich die Nutzer mit ihren verschiedenen Endgeräten auf jeder Website oder bei jeder App neu anmelden mussten, um die passwortlose Funktionalität nutzen zu können. Zwei neue Funktionen für das sichere passwortlose Anmelden sollen künftig mehr Komfort bieten:

- User sollen auf ihre FIDO-Anmeldedaten – auch als „Passkey" bezeichnet – von all ihren Geräten aus zugreifen können, ohne sich für jedes Konto neu anmelden zu müssen. Das gilt auch für ganz neue Geräte, die in Betrieb genommen werden.
- Nutzer können künftig die FIDO-Authentifizierung auf ihrem Mobilgerät nutzen, um sich bei einer App oder Website auf einem Gerät in der Nähe anzumelden, unabhängig von Betriebssystemplattform oder Browser.

Apple, Google und Microsoft haben angekündigt diese Funktionen innerhalb eines Jahres in ihre Plattformen einzubauen. „Benutzerfreundlichkeit ist entscheidend dafür, dass die Multi-Faktor-Authentifizierung in großem Umfang angenommen wird", sagte Andrew Shikiar, Executive Director und Chief Marketing Officer (CMO) der FIDO Alliance. Man begrüße die Entscheidung der Internet-Größen, diese benutzerfreundliche Innovation in ihren Plattformen und Produkten zu unterstützen. Shikiar rechnet damit, dass andere folgen werden, so dass es zu einer Welle zusätzlicher FIDO-Implementierungen kommen könnte.

„Veraltete passwortbasierte Authentifizierung beseitigen“

„Dieser Meilenstein ist ein Beweis dafür, dass die gesamte Branche zusammenarbeitet, um den Schutz zu erhöhen und die veraltete passwortbasierte Authentifizierung zu beseitigen“, freut sich Mark Risher, Senior Director of Product Management bei Google. Er kündigte an, die FIDO-Technologie in Chrome, ChromeOS, Android und anderen Plattformen verfügbar zu machen. Auch Kurt Knight, Senior Director of Platform Product Marketing bei Apple, beteuerte, wie wichtig die Zusammenarbeit für neue, sicherere Anmeldemethoden sei, „die einen besseren Schutz bieten und die Schwachstellen von Passwörtern beseitigen“.

Für die Verbraucher müsse das Verfahren zu einem selbstverständlichen Teil ihres Lebens werden, sagte Alex Simons, Corporate Vice President Identity Program Management bei Microsoft. „Jede praktikable Lösung muss sicherer, einfacher und schneller sein als die heute verwendeten Passwörter und herkömmlichen Multi-Faktor-Authentifizierungsmethoden.“ Simons blickt optimistisch nach vorne: „Wir sehen eine vielversprechende Zukunft für FIDO-basierte Anmeldeinformationen sowohl in Verbraucher- als auch in Unternehmensszenarien und werden die Unterstützung in allen Microsoft-Anwendungen und -Diensten weiter ausbauen.“

Passwörter – die Kakerlaken des Internets

Experten mahnen seit langem bessere Sicherheitsmechanismen für die Authentifizierung von Nutzerinnen und Nutzern an. „Obwohl wir im Jahr 2022 wissen, dass Passwörter von Natur aus unsicher sind, ist es immer noch eine Herausforderung, die Menschen dazu zu bringen, darauf aufzupassen“, sagte Merritt Maxim, Forschungsdirektor und Sicherheitsspezialist beim Analystenhaus Forrester, dem „Wall Street Journal“. Passwörter seien „die Kakerlaken des Internets“ – lästig, hartnäckig und es lohne sich, sich die Zeit zu nehmen, um sie zu töten.

Passwörter lassen sich abfangen, ausspähen oder durch vielfaches Ausprobieren knacken. Das funktioniert, weil viele Internet-Nutzerinnen und -Nutzer bei der Wahl ihrer Passwörter bequem sind und diese auch für verschiedene Dienste mehrfach verwenden. Ende Februar meldete der deutsche ITK-Branchenverband Bitkom, 29 Prozent der über 1000 befragten Internet-User hierzulande nutzten für verschiedene Online-Dienste dasselbe Passwort, auch wenn das große Sicherheitsrisiken berge.

Dabei seien sich die Menschen der Problematik grundsätzlich bewusst. Immerhin drei Viertel achten dem Bitkom zufolge bei der Erstellung neuer Passwörter auf

einen Mix aus Buchstaben, Zahlen und Sonderzeichen. Allerdings sind sie meist nicht bereit, ihre Passwörter in regelmäßigen Abständen zu ändern. Nur 38 Prozent der User sind dazu bereit, und einen sicheren Passwort-Generator oder einen Passwort-Safe zum Erstellen und Verwalten sicherer Passwörter haben gerade einmal 18 Prozent im Einsatz.

Starke Passwörter sind ein Muss

„Einfache oder immer gleiche Passwörter zu verwenden, ist fahrlässig", warnt Sebastian Artz, Bereichsleiter für Cyber- und Informationssicherheit beim Bitkom. Viele Kriminelle nutzten digitale Wörterbücher und gängige Passwortlisten, sie könnten damit schwache Passwörter über einen automatisierten Abgleich in kurzer Zeit ermitteln. „Starke Passwörter, etwa für besonders schutzbedürftige E-Mail-Accounts, sind deshalb ein absolutes Muss." Gängige Eingabemuster – beginnend mit einem Wort, gefolgt von einer Zahl und einem Sonderzeichen am Ende – seien zwar leichter zu merken, von Kriminellen aber auch leichter vorherzusehen und auszunutzen, warnt der Security-Experte.

Artz empfiehlt die Nutzung der Zwei- oder Multi-Faktor-Authentifizierung, bei der eine Anmeldung mithilfe eines zweiten Faktors, etwa eines SMS-Codes oder eines Anrufs, bestätigt werden muss. Bisher machen allerdings nur 37 Prozent der Nutzerinnen und Nutzer in Deutschland davon Gebrauch.

FIDO-Standard muss noch Kinderkrankheiten überwinden

Der Weg in eine passwortlose Zukunft ist noch weit, sagen Sicherheitsexperten. FIDO2 sei ein relativ neuer Standard mit den entsprechenden Kinderkrankheiten, konstatiert Stephan Schweizer, Chief Executive Officer der Nevis Security AG. Zahlreiche Unternehmen und Organisationen arbeiteten an Komponenten wie Authentifizierungsdiensten, Browsern, Betriebssystemen, Hardware zur Verarbeitung biometrischer Daten oder Security-Tokens. Daraus ergibt sich eine riesige Anzahl möglicher Kombinationen von Software und Hardware. Bis sie alle einwandfrei zusammenspielen, werden noch ein paar Jahre vergehen, und die Anbieter müssen in der Zwischenzeit immer wieder nachjustieren.

Dazu kommt, dass das Verfahren erst einmal das Vertrauen der User gewinnen muss, sagt Forrester-Analyst Maxim. Obwohl das FIDO2-System die biometrischen Daten nicht weitergebe, könnten gerade datenschutzbewusste Nutzer davor zu-

rückschrecken, ihr Gesicht oder ihre Fingerabdrücke zum Entsperren von Geräten und Diensten zu verwenden. Auch Vertrauen in die Cloud-Infrastrukturen von Apple, Google und Microsoft ist gefragt. Gerade wenn das System künftig automatisch und komfortabel funktionieren soll, müssen die FIDO2-Passkeys der Anwender plattformübergreifend über die Clouds der Anbieter auf verschiedenste Geräte verteilt werden können. Hier ist eine starke Verschlüsselung zur Absicherung gefragt. „Aber wir dürfen nicht vergessen, dass die Abschaffung von Passwörtern eine Reise und kein Sprint ist", bittet FIDO-Director Shikiar um Geduld.

Martin Bayer

Spezialgebiet Business-Software: Business Intelligence, Big Data, CRM, ECM und ERP; Betreuung von News und Titel-Strecken in der Print-Ausgabe der COMPUTERWOCHE.