LANline

10,– €
Oktober 2019
27. September

IT ■ Network ■ Datacenter www.lanline.de

# Security

## KI als Angriffswerkzeug

## Software-Defined Perimeter

## Zero-Trust-Modelle

## Mit Marktübersicht Security-as-a-Service-Anbieter

**SDN-Lösungen von VMware und Microsoft**
Netzwerke für dynamische RZs

**Im Praxistest: Anydesk Version 5**
Remote Desktop unter der Lupe

**Schw**
**Sp**

Sonderdruck Nevis
Passwörter als
Sicherheits-
risiko

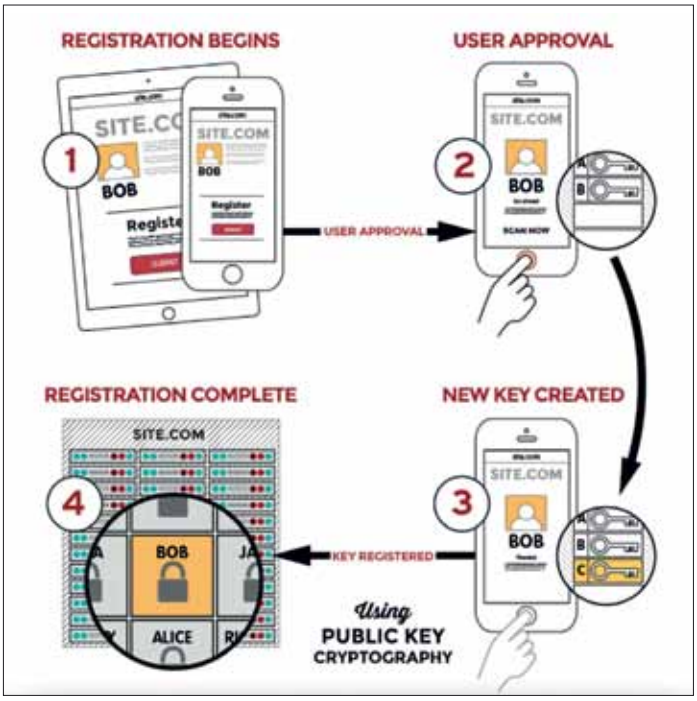
**Passwortfreie Authentisierung mit FIDO**

# Passwörter als Sicherheitsrisiko

Benutzername und Passwort sind als Mittel der Authentisierung von Online-Usern weder zeitgerecht noch sicher. Dies zeigt die steigende Zahl erfolgreicher Angriffe auf Benutzerkonten. Den Wunsch nach benutzerfreundlicher und sicherer Authentisierung erfüllen Ansätze, die ohne Passwörter auskommen. Gegeben ist dies bei Authentisierungsverfahren auf Basis des FIDO-Standards (Fast Identity Online).

Um den Zugriff auf Cloud-Anwendungen und Online-Services zu schützen, melden sich Nutzer meist durch Eingabe eines Benutzernamens, etwa der E-Mail-Adresse, und eines Passworts an. Das BSI empfiehlt in Kapitel M 2.11 der IT-Grundschutz-Kataloge Passwörter, die aus mindestens acht Zeichen bestehen und Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen enthalten. Doch das Verfahren gilt als überholt: Längere und kompliziertere Passwörter sind heute erforderlich. Doch ist es für Nutzer zahlreicher Accounts praktisch unmöglich, sich viele komplexe Passwörter zu merken. IT-Sicherheitsexperten empfehlen, möglichst lange Phrasen zu verwenden, etwa „Sein Hausdrachen fährt ein Elektroauto und trägt lila Kontaktlinsen“, oder raten zum Passwortsafe. Derlei Software bietet häufig die Option einer automatischen Generierung komplexer Login-Zeichenfolgen. Doch zahlreiche Nutzer verwenden nach wie vor einfache Passwörter, wie eine Auswertung des Hasso-Plattner-Instituts ergab. Demnach zählten 2018 Begriffe wie „12345“ oder gar „123“ zu den am häufigsten genutzten Passwörtern.

Der Service-Provider Verizon stellt in seinem „2019 Data Breach Investigations Report“ fest, dass es in rund 30 Prozent der erfolgreichen Angriffe zum Diebstahl von Anmeldedaten kam. Außerdem haben Hacker ihr Arsenal von Angriffsmethoden erweitert. Sie nutzen beispielsweise das Credential Stuffing. Es basiert darauf, dass Nutzer häufig dieselben oder ähnliche Log-in-Daten für mehrere Konten verwenden. Haben die Angreifer die Zugangsdaten eines Benutzerkontos ermittelt, testen sie in großem Stil durch, ob der Anwender dieselben Passwörter oder Variationen davon für Anmeldung bei Online-Diensten, Web-Shops, Banken oder Unternehmensnetzen verwendet.




**Registrierungsvorgang bei FIDO: Der private Schlüssel kann mit Hilfe von biometrischen Verfahren wie einem Fingerabdruck-Scanner erzeugt werden. Er bleibt auf dem Endgerät des Nutzers.** Bild: FIDO Alliance

## Mehrstufiges Sicherheitskonzept

Doch welches Konzept soll an die Stelle von Passwörtern treten? Hardware-Token oder Zugangskarten inklusive Lesegeräte bringen oft keine echte Verbesserung. Denn solche Komponenten sind kostspielig und unhandlich. Umfragen haben ergeben, dass bis zu 40 Prozent der Anmeldeversuche scheitern, weil Nutzer den Token verlegt haben oder das Kartenlesegerät gerade nicht zur Hand ist. Einfacher ist es, für eine mehrstufige Authentisierung Biometrietechnik zu verwenden, die in Smartphones integriert ist: Fingerabdruck- und Iris-Scanner oder Gesichtserkennung. Der Vorteil liegt darin, dass mittlerweile ein Großteil der Smartphones über zumindest eine dieser Funktionen verfügt. Außerdem nutzten 2018 bereits zwei Drittel der Besitzer von Mobilgeräten biometrische Authentisierungsverfahren, so eine Studie des schweizerischen Softwarehauses AdNovum.

Bei der Umsetzung eines solchen Sicherheitskonzepts bietet sich der Einsatz des FIDO-Standards an. Die FIDO Alliance hat eine offene Spezifikation für die Authentisierung von Nutzern von IT- und Online-Services entwickelt. Die Spezifikation standardisiert die Kommunikation zwischen dem Endgerät (etwa dem Smartphone) und dem Backend-Server und definiert zudem die Hardwareschnittstellen für die Einbindung des Fin-

gerabdrucklesers, der Kamera oder der mittlerweile weit verbreiteten „Secure Enclaves“ zur sicheren Ablage von Schlüsselmaterial. Bei der Secure Enclave handelt es sich um einen speziellen Security-Chip, der das Auslesen von Schlüsselmaterial auf Hardwareebene unterbindet.

Die initiale Registrierung ist zudem mittels Offline-Verfahren (Out-of-Band Authentication, OOB) möglich, beispielsweise per QR-Code. Der Nutzer erhält diesen per Briefpost oder im Browser-Fenster eines zweiten Endgeräts. Nach dem Einscannen des QR-Codes ordnet Authentifizierungssoftware das Endgerät dem Nutzerkonto zu und generiert ein Schlüsselpaar aus öffentlichem und privatem Schlüssel. Der private Schlüssel verbleibt immer auf dem Gerät und wird in der Secure Enclave sicher hinterlegt. Der öffentliche Schlüssel erreicht über das standardisierte FIDO-Protokoll den Authentifizierungs-Server. Während der Authentisierung eines Benutzers kommt die Auswertung der biometrischen Merkmale wie Gesichtserkennung oder Fingerabdruck lediglich für die Freischaltung des privaten Schlüssels zum Einsatz. Dies garantiert, dass die biometrischen Daten das Gerät des Benutzers niemals verlassen. Bei älteren Endgeräten ohne Fingerabdruck- oder Gesichtsscanner erfolgt die Freischaltung des privaten Schlüssels mit Hilfe eines PIN-Codes. Auch dieser verbleibt lokal auf dem Gerät und ist daher nicht den gleichen Bedrohungen ausgesetzt wie ein Passwort, das der Browser an einen Web-Server übermittelt.

Die Kombination aus asymmetrischer Verschlüsselung, Benutzeridentifikation auf dem Endgerät sowie sicherer Ablage des Schlüsselmaterials macht es für Angreifer extrem schwierig, das Authentisierungssystem auszuhebeln oder Authentisierungsdaten zu entwenden. Die Ausbreitung der Secure Enclaves auf den Endgeräten ist schon weit fortgeschritten: Apple, Google und Samsung haben dies bei ihren mobilen Geräten bereits umgesetzt.

Wichtig ist, dass Unternehmen eine passwortfreie Authentisierung in ein erweitertes IT-Security-Konzept einbinden können. Eine Möglichkeit besteht darin, zusätzliche Merkmale wie Geolokation, Device-Fingerprint oder Tippverhalten zu nutzen, um die Identität eines Nutzers zweifelsfrei festzustellen. Die zusätzlichen Merkmale bilden einen Risiko-Score, den die Sicherheitssoftware für jeden Login neu berechnet. Sein Wert steigt, falls das beobachtete Verhalten für eine bestimmte Session vom normalen Benutzerverhalten abweicht.


**Eine passwortfreie Authentisierung lässt sich in ein umfassendes IT-Security-Konzept einbinden, das Standortdaten und Nutzerverhalten für einen Risiko-Score heranzieht.** Bild: Nevis

Ein Beispiel: Ein Kunde, der in Berlin ansässig ist, meldet sich plötzlich von einem Endgerät bei seinen Online-Services an, das laut seiner IP-Adresse in Asien steht. Der erhöhte Risiko-Score führt dann beispielsweise dazu, dass die „Auto-Login“ Funktionalität dynamisch deaktiviert wird und sich der Benutzer über eine starke Zwei-Faktor-Authentisierung neu einloggen muss.

Mit der Kombination aus biometrischen Verfahren und zusätzlichen Merkmalen lässt sich ein extrem hohes Sicherheitsniveau erreichen. Ergänzend dazu sollte eine Sicherheitslösung in der Lage sein, auch während der Session umgehend auf verdächtige Vorgänge zu reagieren und die Session im Notfall zu beenden oder ein verdächtiges Endgerät zu sperren. Ein weiteres Sicherheitselement betrifft die App auf dem mobilen Endgerät, die zur Authentisierung dient: Sie sollte gegen Manipulationsversuche und Reverse Engineering gehärtet sein.

Unternehmen, die eine Lösung für die passwortfreie Authentisierung einsetzen wollen, sollten zudem prüfen, welche Implementierungsverfahren der Anbieter bereitstellt. Hierbei stehen verschiedene Ansätze zur Verfügung. Einerseits kann man das Verfahren mittels Software Development Kit (SDK) in eine existierende Applikation integrieren. Andererseits kann man auch auf eine Standard-Access-App zurückgreifen, die sich mit geringem Aufwand an das „Look and Feel“ des Unternehmens anpassen lässt.

## Trend: Maschinen und Dinge authentisieren sich

Bereits heute ist absehbar, dass der passwortlosen Authentisierung mittels FIDO die Zukunft gehört. Dazu tragen Faktoren wie die Digitalisierung von Services bei, bis hin zu Online-Konsultationen beim Arzt. Hinzu kommt ein weiterer Faktor: das Internet der Dinge (Internet of Things, IoT). Auch Maschinen, Messgeräte, digitale Stromzähler und Systeme der Gebäudetechnik haben eine „digitale Identität“, die es zu schützen gilt. Daher benötigen auch solche Komponenten Authentisierungsverfahren, die sich einfach handhaben und flexibel einsetzen lassen. Standardisierte Ansätze wie zum Beispiel FIDO sind vor diesem Hintergrund unverzichtbar.

Stephan Schweizer/wg

Stephan Schweizer ist Chief Product Officer bei Nevis, www.nevis-security.ch.