nevis®

Vor diesen Angriffsarten können Sie sich mit MFA schützen

Die Multi-Faktor-Authentifizierung als Sicherheitsmechanismus und entscheidender Faktor in der IT-Sicherheitsstrategie, ist ein Authentifizierungsverfahren, bei dem zwei oder mehr Faktoren (Berechtigungsnachweise) kombiniert und validiert werden.

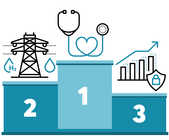
Ziele der MFA

- → Integration einer **zusätzlichen Sicherheitsebene** in den Prozess der Authentifizierung
- → Erfüllung der **Compliance-Anforderungen**
- → **Identifizierung** autorisierter Nutzer und Zugangsgewährung zu gewünschten Ressourcen
- → **Verhinderung von Identitätsdiebstahl** durch das Ausnutzen schwacher Passwörter
- → Frühzeitige **Vereitelung von Angriffsmethoden** der Cyberkriminellen
- → **Schutz sensibler Daten** vor Datenmissbrauch
- → **Optimierung der User Experience** durch ein intuitives und sicheres Login

Kosten für Datenhacks

Die Folgen von Datenhacks sind enorm: So kostet ein Datenverstoss ein Unternehmen durchschnittlich **4,79 Mio. Euro**. Deutschland belegt damit den 3. Platz nach den USA mit 8,21 Mio. Euro und dem Mittleren Osten mit 5,99 Mio. Euro.

Kosten nach Branche



Sortiert nach Branche dominiert der Gesundheitssektor eindeutig das Branchenranking mit den durchschnittlich höchsten Kosten: Allein 2020 sind durch Datenleaks **weltweit 7,15 Mio. Euro Kosten** entstanden, gefolgt von der Energiebranche und dem Finanzbereich auf den Plätzen 2 und 3.

Lieber einmal mehr absichern

x2 **Zwei-Faktor-Authentifizierung = 2FA**
→ zwei Validierungsverfahren

x? **Multifaktor-Authentifizierung = MFA**
→ mehr als zwei Validierungsverfahren

Je mehr Authentifizierungsfaktoren zusammenspielen, desto höher ist der Schutz vor Datenmissbrauch.

Die 4 Faktoren der Authentisierung

Wissen

Ein Faktor, den nur der Nutzer kennt.

Möglichkeiten: Passwort, PIN, Antwort auf eine Sicherheitsfrage, Transaktionsnummer, Einmal-Passwort (OTP)

Haben

Nutzung eines mobilen Zusatzgerätes, das bei der Authentifizierung relevante Informationen abfragt.

Früher: TAN-Generator, Hardware-Token

Heute: Smartphone + Authentifizierungs-App zur Generierung eines Einmal-Passwortes

Sein

Biometrische Faktoren, mit denen der Nutzer identifiziert wird.

Möglichkeiten: Fingerabdruck, Iris, Profil des Gesichts oder Tonlage der Stimme

Standort

Es wird die IP-Adresse des Benutzers abgefragt, die durch den Standort mittels GPS-Daten oder die Nutzungsdauer ergänzt werden kann.

Wovor MFA genau schützt – Die Top 5 Angriffsmethoden

*„Mit **Personalisierung und Glaubwürdigkeit** komme ich zum Ziel"*

Phishing

Ein Hacker gibt sich als eine vertrauenswürdige Quelle seines Opfers aus und sendet ihm eine gefälschte E-Mail. Darin wird das Opfer zu einer Handlung aufgefordert, wie etwa sich über einen Link in das Bankkonto einzuloggen. Der Link ist bösartig, sodass das Opfer beim Auswählen des Links nicht zur gewünschten Website gelangt, sondern auf einer manipulierten Website landet. Diese ist so konzipiert, dass der Hacker im Hintergrund bereits während des Logins die Anmeldedaten abgreifen kann und Zugang zum Konto erhält.

*„Ich bekomme **jedes Wort mit**, das du schreibst."*

Keylogger

Der Keylogger ist ein Überwachungsprogramm und wird meist auf dem Gerät des Opfers über einen Virus installiert. Indem er jeden Tastenanschlag des Nutzers erfasst, werden auch Anmeldedaten, Passwörter und Antworten auf Sicherheitsfragen oder Bankdaten aufgezeichnet. Diese Daten werden dann für böswillige Zwecke verwendet.

*„Ich probiere so lange **jede Kombination** aus, bis ich Erfolg habe."*

Brute-Force-Angriffe

Beim Brute-Force-Angriff nutzen Hacker ein Programm, das jede erdenkliche Anmeldekombinationen aus Passwort und Benutzername generiert, um sich mithilfe der Varianten Zugang zu einem Konto zu verschaffen. Die Folgen sind gravierend: angefangen mit der Kaperung von Unternehmenssystemen über die Verbreitung von Malware und die Platzierung von Spam-Anzeigen bis hin zum Hacken von Nutzerkonten.

*„Ich weiss, dass du deine **Login-Daten auf mehreren Plattformen** nutzt."*

Credential Stuffing

Credential Stuffing ist eine Sonderform der Brute-Force-Angriffe und wird von Hackern derzeit sehr häufig im Internet genutzt. Dabei werden Passwörter verwendet, die durch Datenpannen öffentlich wurden oder zuvor illegal abgegriffen wurden. Cyberkriminelle geben diese anschliessend auf möglichst vielen Webseiten ein in der Hoffnung, dass die gleichen Login-Daten aus Passwort und Benutzername bei mehreren Diensten gleichzeitig verwendet werden.

*„Ich **höre heimlich mit** – nur siehst du mich nicht."*

Man-in-the-Middle-Angriffe

Ein Hacker beobachtet beim Man-in-the-Middle-Angriff (kurz: MITM) mithilfe eines Programms die Interkation eines Opfers mit einer weiteren Anwendung zum Beispiel bei der Nutzung eines öffentlichen WLANs. Im Hintergrund können dabei durch ein Programm des Hackers Anmeldedaten abgegriffen, Daten beschädigt oder sogar eine Kommunikation sabotiert werden. MITM-Angriffe auf öffentliche Hotspots sind durch die Verbreitung von SSL und moderne Browser wie Google Chrome zwar seltener geworden, doch werden sie weiterhin für hochentwickelte Angriffe genutzt.

Bei allen fünf Angriffsmethoden ist das Passwort eine entscheidende Schwachstelle, die sich durch den Einsatz von MFA eliminieren lässt. Denn Hacker können zwar den 1. Authentifizierungsfaktor „Wissen" knacken, doch spätestens, wenn es an die zweite Stufe der MFA geht, enden die Möglichkeiten der Cyberkriminellen.

Folglich schützt die MFA zuverlässig sensible Unternehmensdaten, indem sie eine breite Anzahl von Angriffsmethoden abwehrt und die Zero Trust-Strategie in der modernen Cyberbedrohungslandschaft fördert.

nevis®

Mehr zur Multi-Faktor-Authentifizierung erfahren Sie bei Nevis, dem Schweizer Marktführer für Customer Identity and Access Management:
nevis.net