ASSESSMENT

Risikobewertung: Sicherheit bei der Multi-Faktor-Authentifizierung (MFA)

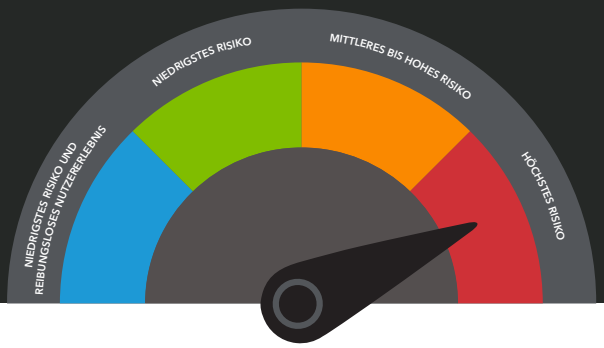
Die Risikoskala aktueller Authentifizierungslösungen im Detail

80 % aller Hacker-Angriffe gehen mit gestohlenen Anmeldedaten oder schlechtem Passwortmanagement einher[1] und mehr als 613 Millionen Passwörter wurden aufgrund von Sicherheitsvorfällen kompromittiert.[2] Eine Multi-Faktor-Authentifizierung (MFA) als zusätzliche Sicherheitsebene bei der Anmeldung senkt dieses Risiko deutlich. Die meisten herkömmlichen MFA-Lösungen weisen jedoch Schwachstellen auf, die leicht ausgenutzt werden können.

Wie hoch ist die Authentifizierungssicherheit Ihres Unternehmens? Wir klären über die Risiken aktueller Authentifizierungsmodelle auf:

Höchstes Risiko

Authentifizierung mit Nutzernamen und Passwort



Unternehmen, die sich einzig und allein auf die Sicherheit von Anmeldedaten zur sicheren Authentifizierung verlassen, sind höchst anfällig für Angriffe, denn Nutzernamen und Passwörter waren noch nie so unsicher. Anmeldedaten werden von hochmotivierten Cyberkriminellen gestohlen, gehackt und gesammelt und anschließend monetarisiert, also eigenständig genutzt oder im Dark Web weiterverkauft.

So umgehen Cyberkriminelle Nutzernamen und Passwörter:

- **Credential Stuffing**
- **Phishing**
- **Password Spraying**
- **Brute-Force-Methode**
- **Vergangene Sicherheitsvorfälle / Wiederverwendung von Passwörtern**
- **Passwortrücksetzung**
- **Keylogging**
- **Direktes Abgreifen von Anmeldedaten vor Ort**

Hinzu kommt, dass Nutzer häufig dieselben Passwörter auf verschiedenen Websites verwenden. Dies ist eine zusätzliche Bedrohung für die Sicherheit Ihres Unternehmens, denn Sie sind nur so sicher wie Ihr unsicherstes Nutzerkonto. MFA ist notwendig, da selbst die komplexesten, von einem Algorithmus generierten Passwörter Schwachstellen aufweisen. Letztendlich ist davon abzuraten, sich nur auf eine Sicherheitsebene, in diesem Fall die einfache Authentifizierung, zu verlassen. Branchenführende Sicherheitslösungen enthalten immer mehrere Sicherheitsebenen.

Mittleres bis hohes Risiko

Standardmäßige Multi-Faktor-Authentifizierung (MFA)

Gemeinsam mit Ihren vorhandenen Sicherheitsmechanismen für die Authentifizierung verbessern zusätzliche MFA-Funktionen Ihre Unternehmenssicherheit sofort. MFA, einschließlich der Zwei-Faktor-Authentifizierung (2FA), besteht aus mindestens zwei separaten Authentifizierungsfaktoren zur Verifizierung von Nutzern. Der erste Faktor ist typischerweise ein Passwort. Der zweite (und potenziell dritte) Faktor kann Folgendes sein: Etwas, das Sie kennen, wie eine PIN oder Antwort auf eine Sicherheitsfrage. Etwas, das Sie haben, wie ein Gerät, ein Einmalcode/-passwort oder Hardware-/Software-Token. Oder etwas, das Sie ausmacht, wie biometrische Merkmale (Fingerabdruck oder Gesichts-ID) oder kontextuelle Signale wie ein Standort.

Herkömmliche MFA reduziert das Risiko zwar deutlich im Vergleich zu einfacher Authentifizierung mit Nutzername und Passwort, ist jedoch trotzdem anfällig für unterschiedliche Methoden, mit denen die Authentifizierung umgangen werden kann, darunter:

- **Phishing**
- **Verwendung transparenter Proxys – MITM-Angriffe (Man-in-the-Middle)**
- **Abfangen von Authentifizierungscodes über E-Mail oder SMS**
- **Credential Stuffing**
- **Replay-Angriffe**
- **SIM-Swapping**
- **Social Engineering**
- **Schwachstellen von Onlineseiten bei MFA-Vorgängen**

Es gibt viele gut dokumentierte Beispiele dafür, wie Cyberkriminelle die Multi-Faktor-Authentifizierung umgehen. Ein aufsehenerregender Angriff im Jahr 2020 wurde mit Hilfe einer Kombination aus Social Engineering und Phishing durchgeführt, um eine MFA-Lösung zu umgehen. Dieser hätte durch die Verwendung physischer Sicherheitsschlüssel verhindert werden können.

Niedrigstes Risiko

FIDO2-MFA über physische Sicherheitsschlüssel

FIDO2 ist die aktuell sicherste standardbasierte Authentifizierungsmethode ohne die Schwachstellen herkömmlicher MFA. So entfällt das Risiko von Phishing-, MITM- und Replay-Angriffen. Der FIDO2-Standard basiert auf den Spezifikationen der Web-Authentifizierung des World Wide Web Consortium und dem entsprechenden Client to Authenticator Protocol der FIDO Alliance. Dieses Authentifizierungsmodell ist die Zukunft der MFA – eine Authentifizierung über verschlüsselte Anmeldedaten, die immer auf dem Gerät des Nutzers bleiben und niemals auf einem Server gespeichert werden. FIDO2 ist der Weg hin zu einer Authentifizierung, die komplett ohne Passwort funktioniert.

Der Nachteil an FIDO2-MFA ist, dass sie sich nur durch den Kauf physischer Sicherheitsschlüssel für jeden Nutzer als Authentifizierungsfaktor implementieren lässt.

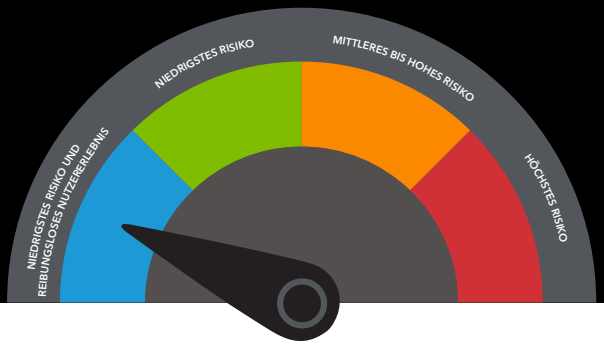
FIDO2 ist zwar der sicherste Standard, jedoch stellt die Implementierung mit Hilfe von Hardware-Sicherheitsschlüsseln viele Herausforderungen dar:

- **Kosten für Einkauf und Verwaltung der Schlüssel für alle Nutzer**
- **Aufwand für die Verteilung und Verwaltung der Schlüssel**
- **Ersetzen verlorener Hardwareschlüssel**
- **Aktualisieren oder Patchen der Hardwareschlüssel nicht möglich**
- **Ungleiche Verteilung – nur bestimmte Mitarbeiter bekommen Schlüssel**

Kauf, Konfiguration, Verteilung und Verwaltung physischer Hardwareschlüssel für alle Mitarbeiter sind eine kostspielige und zeitaufwändige Angelegenheit. Darüber hinaus müssen Nutzer bei jeder Anmeldung einen physischen Schlüssel in ihr Gerät einstecken. Dies ist ein Aufwand für die Nutzer und senkt die Produktivität.

Niedrigstes Risiko und reibungsloses Nutzererlebnis

Die nächste Generation der MFA an der Edge



Akamai MFA ist die FIDO2-Lösung der nächsten Generation und verfügt über einen verschlüsselten und phishing-sicheren Authentifizierungsfaktor. Der Service nutzt eine Smartphone-App anstelle eines physischen Sicherheitsschlüssels und umgeht damit die Schwierigkeiten, die Unternehmen oft davon abhalten, FIDO2-MFA zu implementieren. Die Lösung lässt sich schnell und einfach mit Hilfe eines Smartphones bereitstellen und bietet höchste Authentifizierungssicherheit sowie ein reibungsloses Nutzererlebnis. Akamai MFA beseitigt das Phishing-Risiko und ist der Weg hin zu einer Authentifizierung, die komplett ohne Passwort funktioniert.

Weitere Informationen zu Akamai MFA sowie eine kostenlose 60-tägige Testversion finden Sie auf: **akamai.com/mfa**.

Quellen:

1. https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/
2. https://haveibeenpwned.com/Passwords

Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai bietet Schutz vor Angriffen und Bedrohungen, beschleunigt Entscheidungen und Anwendungen und liefert herausragende Online-Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter www.akamai.com, im Blog blogs.akamai.com oder auf Twitter unter @Akamai. Unsere globalen Standorte finden Sie unter www.akamai.com/locations. Veröffentlicht: März 2021