Multifaktor-Authentifizierung

Passwörter haben ihre Wirkung verfehlt. Welche Lösung bietet sich als Alternative an?

Schutz von Anmeldedaten in kleinen und mittelständischen Betrieben

MFA

Es kommt zu zahlreichen Datensicherheitsverletzungen. Schuld daran sind schwache Passwörter.

Die Passwortsicherheit ist eines der größten aktuellen Probleme beim Schutz von Informationen. Aus dem 2017 Verizon Data Breach Report geht hervor, dass 81 Prozent der Datensicherheitsverletzungen durch schwache oder gestohlene Passwörter verursacht wurden. Um diese Herausforderungen zu meistern, setzen viele Organisationen auf die Multifaktor-Authentifizierung (MFA). Die mehrschichtige Herangehensweise soll dazu beitragen, dass Passwörter bei der Zugriffsgewährung eine weniger wichtige Rolle spielen.

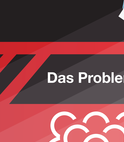
Leider lassen sich herkömmliche MFA-Lösungen in kleinen und mittelständischen Unternehmen häufig nur schwer umsetzen und verwalten. Um sich einen besseren Überblick über den aktuellen Status der Passwortsicherheit und die Nutzung der MFA zu machen, gab WatchGuard eine Umfrage unter den Eigentümern und IT-Entscheidungsträgern in Unternehmen mit 100 bis 1.000 Mitarbeitern in den USA, Großbritannien und Australien in Auftrag.
Daraus ergaben sich die folgenden Erkenntnisse.

Nach Erkenntnissen von WatchGuard ist es bei **25% der KMU** nach deren eigenen Angaben **in den letzten** 18 Monaten **zu einer Datensicherheitsverletzung gekommen**.

Unseren Erkenntnissen zufolge sind Sicherheitsschwachstellen im Wesentlichen auf schwache Passwörter (privat wie geschäftlich) zurückzuführen:

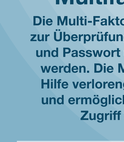
47% der Mitarbeiter nutzen **einfache oder schwache Passwörter**

31% nutzen Netzwerkpasswörter **auch** für **private Anwendungen**



30 % halten ihre **Passwörter nicht geheim**

40 % klicken auf Phishing-E-Mails usw.



36% nutzen ungesichertes WLAN

Das Problem wird NICHT durch die Schulung gelöst

Obwohl **80%** der Unternehmen behaupten, **ihren Mitarbeitern Schulungen** zum Thema Passwortsicherheit anzubieten, **besteht das Problem fort**.

Die Unternehmen sind auf der Suche nach einer besseren Lösung. Dabei würden 84% eine technische Lösung einer Variante mit Passwortrichtlinien vorziehen.

Die Lösung lautet Multifaktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) ist eine Methode zur Überprüfung von Anmeldungen, bei der Benutzername und Passwort um eine zweite Sicherheitsschicht ergänzt werden. Die MFA verhindert den unbefugten Zugriff mit Hilfe verlorengegangener oder gestohlener Passwörter und ermöglicht überprüften Benutzern einen einfachen Zugriff auf ihre Konten und Informationen.

Wie viele KMU nutzen tatsächlich MFA?

67% der Unternehmen nutzen MFA-Lösungen ABER 29% VERZICHTEN AUF MFA!

Es ist eine gute Entwicklung, dass Unternehmen verstärkt MFA-Lösungen einsetzen. Aber nicht alle Methoden sind gleich wirkungsvoll. Wenn Unternehmen keine MFA-Lösungen mit fortschrittlichen Sicherheitsmethoden nutzen, besteht ein zusätzliches Risiko. SMS-Nachrichten gelten beispielsweise als unsicher, da sie von Angreifern imitiert oder abgefangen werden können. Hardware-Token stellen ebenfalls ein Risiko dar, weil sie verlorengehen oder gestohlen werden können und dadurch eine Sicherheitslücke entsteht.

Warum?

Warum entscheiden sich nicht mehr KMU für die neuesten MFA-Technologien?

- 61 % haben den Eindruck, dass sich die meisten Lösungen **an größere Unternehmen richten.**
- 24 % halten die Wartung **und den Support für zu kompliziert**
- 24 % halten die Implementierung **für zu schwierig**
- 24 % halten die Lösungen **für zu kostspielig**
- 22 % rechnen mit **internen Widerständen**
- **17 % sind der Auffassung, SIE BRÄUCHTEN KEINE MFA-LÖSUNG!!**

Wir haben zurzeit keine MFA-Lösung, aber das hört sich großartig an!

Für diejenigen, die ein Kaufinteresse haben:

65% planen die Anschaffung einer Lösung

83% haben Interesse an MFA

Token?
38% würden ein Desktop-Token kaufen
28% ein Token für angeschlossene Hardware
26% ein mobiles Token
25% SMS

54% würden Cloud-basierte Server vorziehen

Passwörter allein reichen nicht mehr aus. Verhindern Sie, dass ein schwaches Passwort eines einzelnen Mitarbeiters die Ressourcen und Informationen Ihres Unternehmens gefährdet – testen Sie noch heute AuthPoint!

WatchGuard AuthPoint

WatchGuard AuthPoint bietet Multi-Faktor-Authentifizierung (MFA) auf einer benutzerfreundlichen Cloud-basierten Plattform. Da sich die Lösung in der Cloud befindet, müssen Sie keine Hardware bereitstellen, und der Zugriff kann von jedem beliebigen Ort aus verwaltet werden. Die mobile App zeigt jeden Anmeldeversuch an und erleichtert es den Benutzern, Anmeldungen zu genehmigen oder zu verweigern. AuthPoint kann außerdem in zahlreiche Drittanbieteranwendungen integriert werden, etwa gängige Cloud-Anwendungen, Webdienste, VPNs und Netzwerke.
Weitere Informationen erhalten Sie unter www.watchguard.com/authpoint-de

WatchGuard