ROI - Multifaktor-Authentifizierung

Von 100 Personen nutzen vier bis sechs durchgehend schwache Passwörter oder geben ihr Passwort weiter ... wie viele davon arbeiten für Ihr Unternehmen?

Angesichts dessen, dass nur ein gestohlenes Passwort Ihr Netzwerk gefährden kann, müssen Sie sich fragen, wie wahrscheinlich es ist, dass einer oder mehrere Ihrer Mitarbeiter nicht sorgfältig mit Passwörtern umgehen. Noch alarmierender ist die Tatsache, dass sich die Kosten in Verbindung mit einer Sicherheitsverletzung – durch direkte Geldbußen, Kosten für Untersuchung und Gefahrenabwehr sowie indirekte Kosten durch verlorene Kunden und geringe Mitarbeiterproduktivität – auf mehrere Millionen Euro belaufen können. Folgende Statistiken können helfen, die Risiken zu beziffern und gegen die erwarteten Kosten für eine MFA-Lösung abzuwägen.

RISIKEN/AUSGABEN IN ZUSAMMENHANG MIT DATENSICHERHEITSVERLETZUNGEN

9.350
Durchschnittliche Anzahl kompromittierter Datensätze

Die Menge der **gestohlenen Daten** bei einer durchschnittlichen Sicherheitsverletzung beträgt **9.350 Datensätze**
2017 Ponemon State of SMB Cybersecurity Report

1,32 Mio. USD
Durchschnittliche Kosten für kompromittierte Datensätze

Durchschnittliche Kosten für eine Datensicherheitsverletzung = **141 USD** pro Datensatz mit vertraulichen Daten
2017 Ponemon Institute Cost of Data Breach Study

81%
Prozentsatz der Sicherheitsverletzungen durch schwache/gestohlene Passwörter

Dies ist die **beliebteste Taktik** bei Hackern
Verizon Data Breach Investigations Report 2017

3
Anzahl der Benutzer (von 100) mit 123456 als Passwort

10% der Menschen haben schon einmal mindestens eines der 25 schlechtesten Passwörter auf der diesjährigen Liste verwendet und fast 3% das schlechteste: **123456**
http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

6
Anzahl der Benutzer (von 100), die dasselbe Passwort für alle Online-Anmeldungen nutzen

6% der US-amerikanischen Internetnutzer verwendeten 2017 **dasselbe Passwort** für alle Konten
(https://www.statista.com/statistics/763091/us-use-of-same-online-passwords/)

1
Anzahl der verlorenen/gestohlenen Passwörter, die für eine Sicherheitsverletzung in einem Netzwerk ohne MFA notwendig sind

Datei mit **1,4 Milliarden** gehackten/ausgelesenen Passwörtern im Darknet gefunden, die von „potenziellen Hackern zur Einspeisung in sogenannte Credential Stuffing-Apps hätten verwendet werden können"
(Forbes, 11. Dezember 2017)

GESCHÄTZTE INVESTITIONEN FÜR EINE CLOUD-BASIERTE MFA-LÖSUNG

0 USD
Zusätzliche Infrastruktur zum Hosten des Authentifizierungsmanagements

Das gesamte Management erfolgt über die Cloud und ist **im Preis enthalten.** Einige Funktionen erfordern Software auf dem Gateway und den Agents

0 USD
Kauf von Hardware-Token

Die kostenlose mobile App dient zur Authentifizierung auf einem **Smartphone** – keine zusätzliche Hardware erforderlich

2.700 USD
Geschätzte jährliche Kosten für MFA pro 100 Mitarbeiter

Dies entspricht **2,25 USD/Benutzer/Monat** – Verwendung nur für Referenzzwecke. Wenden Sie sich an einen WatchGuard-Partner, um Ihren AuthPoint-Preis zu erfragen

Minimale
Ausgaben für IT-Mitarbeiter

Token-Bereitstellung erfolgt **automatisiert,** wiederkehrende Aufgaben für IT-Mitarbeiter sind in erster Linie Wartung und Überwachung

DIE VORTEILE DER CLOUD-BASIERTEN MFA WIEGEN DIE KOSTEN AUF

Mit einer Investition von nur 2,50 USD pro Benutzer und Monat oder weniger reduzieren Sie die Wahrscheinlichkeit einer Sicherheitsverletzung durch ein gestohlenes Passwort. Die Cloud-basierte MFA erfordert keine Ausgaben für zusätzliche Infrastruktur, Hardware-Token, Software-Support und Wartung.

WatchGuard AuthPoint

AuthPoint bietet Multi-Faktor-Authentifizierung (MFA) auf einer benutzerfreundlichen Cloud-Plattform. Die mobile AuthPoint-App macht jeden Anmeldeversuch sichtbar und dank der Ausführung als Cloud-Dienst muss keine Hardware bereitgestellt werden. Sie kann überall verwaltet werden und bietet Integrationen mit Drittanbieteranwendungen, einschließlich gängiger Cloud-Anwendungen, Webdienste, VPNs und Netzwerke. **Weitere Informationen erhalten Sie unter: www.watchguard.com/authpoint**