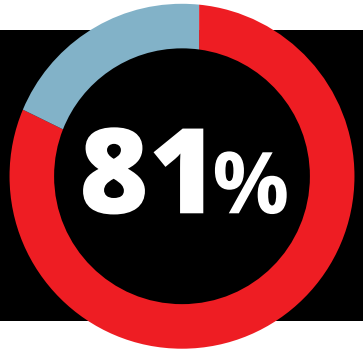
# UMFRAGE: Mittelständische Unternehmen benötigen auch Multifaktor-Authentifizierung!

# EINFÜHRUNG

Die Passwortsicherheit ist eines der größten aktuellen Probleme beim Schutz von Informationen. Aus dem **Verizon Data Breach Report** geht hervor, dass **81 Prozent der Datensicherheitsverletzungen im Zusammenhang mit schwachen oder gestohlenen Passwörtern stehen**. Um diese Herausforderungen zu meistern, setzen viele Organisationen auf die Multifaktor-Authentifizierung (MFA). Die mehrschichtige Herangehensweise soll dazu beitragen, das Risiko der reinen Passwortsicherheit zu reduzieren.

Bei der Multi-Faktor-Authentifizierung muss ein Benutzer zur Bestätigung seiner Identität mindestens zwei identifizierende Faktoren bereitstellen. Bei diesen Faktoren kann es sich um Dinge handeln, die die Benutzer wissen (z. B. Passwort oder PIN), besitzen (z. B. Hardware-Token oder Smartphone) oder aufweisen (z. B. Fingerabdruck). Ein einfaches Beispiel für die Authentifizierung ist ein Geldautomat. Um die Funktionen des Automaten nutzen zu können, müssen die Benutzer ihre Debitkarte einführen (ein Ding, das sie besitzen) und ihre PIN eingeben (ein Ding, das sie wissen).

Leider lassen sich herkömmliche MFA-Lösungen in Unternehmen häufig nur schwer umsetzen und verwalten. Dies gilt insbesondere für Unternehmen mit eingeschränkten IT-Ressourcen. Um sich einen besseren Überblick über den aktuellen Status der Passwortsicherheit und die Nutzung der MFA zu machen, gab WatchGuard Technologies eine Umfrage unter den Eigentümern kleiner und mittelständischer Unternehmen und unter den IT-Entscheidungsträgern in Unternehmen mit weniger als 1.000 Mitarbeitern in den USA, Großbritannien und Australien in Auftrag. Daraus ergaben sich die folgenden Erkenntnisse.



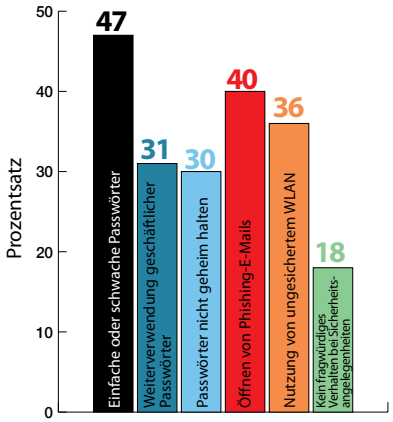

**81 Prozent der Datensicherheitsverletzungen sind auf schwache oder gestohlene Passwörter zurückzuführen.**

# DER AKTUELLE STAND DER PASSWORTSICHERHEIT

Schwache Passwörter sind ein ernstes Problem. Laut Umfrage behaupten 83 Prozent der Eigentümer und IT-Entscheidungsträger, dass ihre Mitarbeiter um die Bedeutung der Best Practices für Passwörter wissen. Obwohl Arbeitgeber also bei ihren Mitarbeitern die Notwendigkeit von Passwortsicherheit erkennen, haben sie erhebliche Bedenken, beim Schutz von Unternehmens-, Personal- und Kundendaten allein auf Passwörter zu setzen. 84 Prozent der Befragten sind der Auffassung, dass schwache Passwörter für bis zu 60 Prozent aller Cyberangriffe verantwortlich sind. Dieser Wert ist im Vergleich zu den oben erwähnten Zahlen aus dem Verizon-Bericht noch niedrig.

Trotz eines allgemeinen Bewusstseins für Best Practices bei Passwörtern und für das Thema Sicherheit werden die Kenntnisse nicht vollständig umgesetzt. Nahezu die Hälfte (46 Prozent) der Befragten ist der Auffassung, dass sie die Mitarbeiter nicht dazu zwingen können, starke Passwörter zu verwenden. Die meisten befragten Unternehmen bieten ihren Mitarbeitern eine Passwortschulung an, oder es gelten Richtlinien, die die Mitarbeiter zur Einhaltung der Best Practices auffordern. In den Richtlinien wird etwa festgelegt, dass lange und komplexe Passwörter verwendet werden müssen, die regelmäßig zu ändern sind. Die Befragten waren dennoch der Meinung, dass ihre Mitarbeiter regelmäßig die folgenden schlechten Praktiken für ihre Passwörter an den Tag legten:

- **47%** der Befragten sind der Auffassung, dass ihre Mitarbeiter **einfache oder schwache Passwörter verwenden**
- **40%** denken, dass ihre Mitarbeiter **auf Phishing-E-Mails klicken**
- **36%** sind der Meinung, dass ihre Mitarbeiter **ungesicherte WLAN-Verbindungen nutzen**
- **31%** glauben, dass die Mitarbeiter **geschäftliche Passwörter auch für private Anwendungen nutzen**
- **30%** sind der Auffassung, dass ihre Mitarbeiter **ihre Passwörter nicht geheim halten**
- **18%** glauben, dass ihre Mitarbeiter **kein fragwürdiges Verhalten in Sicherheitsangelegenheiten zeigen**



**Schlechte Mitarbeiterpraxis beim Umgang mit Passwörtern**

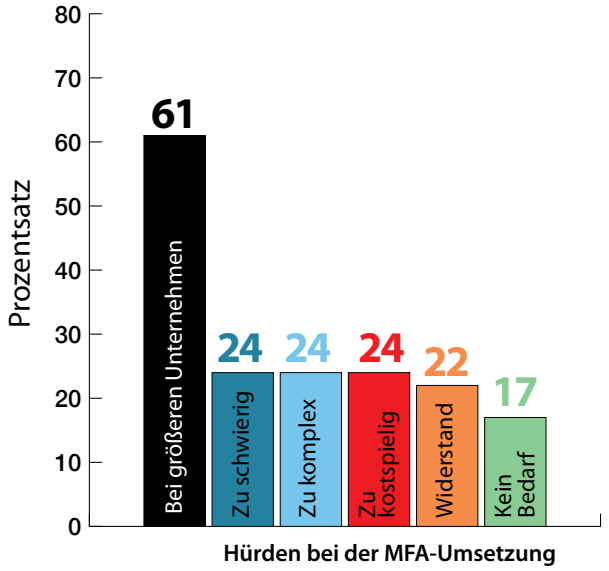
Zur Lösung dieser Probleme sagten **84 Prozent der IT-Entscheidungsträger** in Unternehmen mit unter 1.000 Mitarbeitern, sie würden **sich von einer technischen Lösung mehr versprechen als von Richtlinien zur Erzwingung starker Passwörter**.

# HÜRDEN BEI DER MFA-UMSETZUNG

Wenn also IT-Entscheidungsträger eine technische Lösung bevorzugen und ihren Mitarbeitern bei der Umsetzung bewährter Passwortpraktiken nicht trauen, stellt sich die Frage, warum nicht mehr kleine und mittelständische Unternehmen auf MFA-Lösungen setzen.

Die Meinung der Unternehmen zur MFA ist im Folgenden dargestellt:

- **61%** haben den Eindruck, dass sich MFA-Lösungen an **größere Unternehmen** richten
- **24%** halten die Wartung und den Support von MFA-Lösungen für **zu kompliziert**
- **24%** sind der Ansicht, dass eine MFA-Implementierung **zu komplex** ist
- **24%** halten MFA-Lösungen für **zu teuer**
- **22%** vermuten **innerbetrieblichen Widerstand** gegen die MFA
- **17%** sind der Auffassung, **SIE BRÄUCHTEN KEINE MFA-LÖSUNG**




Dies sind alles berechtigte Einwände (mit Ausnahme des letzten Punkts, denn nach unseren Erkenntnissen ist bei Unternehmen aller Größen ein MFA-Bedarf festzustellen). **Unternehmen mit eingeschränkten IT-Ressourcen benötigen eine MFA-Lösung**, die **ihr Budget nicht überschreitet** und bei der **Bereitstellung keine Support Probleme bereitet**.

# WIE GÄNGIG IST MFA?

Von den Unternehmen, die keine MFA-Lösung implementiert haben, würden 83 Prozent es nutzen wollen. 65 Prozent planen sogar die Anschaffung einer MFA-Lösung. Damit gibt es zurzeit eine deutliche Dynamik zugunsten von MFA-Lösungen, sogar unter den Unternehmen mit weniger als 1.000 Mitarbeitern. 67 Prozent der befragten Unternehmen nutzen zurzeit zumindest für einen Teil ihrer Benutzer eine nicht weiter spezifizierte Form der MFA. 29 Prozent nutzen die MFA überhaupt nicht. 29 Prozent ist ein sehr hoher Anteil an Unternehmen, da in diesem Fall ein Fehler eines einzelnen Mitarbeiters zu einer Datensicherheitsverletzung führt. Außerdem sind die 67 Prozent eine irreführende Zahl. Schauen wir uns die Werte etwas genauer an.

Von den Unternehmen, die bereits eine MFA-Lösung einsetzen…

- nutzen **56 % Desktop-Authentifikatoren**
- nutzen **47 % SMS**
- nutzen **44 % mobile Token**
- wissen **40 % nicht**, um welchen MFA-Typ es sich handelt
- nutzen **61 % Cloud-basierte Authentifizierungsserver**


Es ist eine gute Entwicklung, dass Unternehmen verstärkt MFA-Lösungen einsetzen. Aber nicht alle Methoden sind gleich wirkungsvoll. Wenn Unternehmen MFA-Lösungen ohne fortschrittliche Sicherheitsmethoden nutzen, besteht ein zusätzliches Risiko. SMS-Nachrichten gelten beispielsweise als unsichere Authentifzierungsmethode, da sie von Angreifern imitiert oder abgefangen werden können. Hardware-Token stellen ebenfalls ein Risiko dar, weil sie verloren gehen oder gestohlen werden können und dadurch eine Sicherheitslücke entsteht, die zu einer Sicherheitsverletzung führen könnte.

# FAZIT

MFA-Lösungen sind nicht mehr nur für Großkonzerne zugänglich. Bei dieser Umfrage stellte sich heraus, dass zwar die Mehrheit der IT-Entscheidungsträger in Unternehmen mit weniger als 1.000 Mitarbeitern Passwortrichtlinien eingerichtet hat und Schulungen durchführt, drei Viertel der Befragten jedoch trotzdem davon ausging, dass ihre Mitarbeiter ein schlechtes Verhalten in puncto Sicherheit an den Tag legten. Außerdem sind sich nahezu alle Befragten einig, dass Passwörter mit Hilfe einer technischen Lösung verbessert werden sollen.

Daher müssen wir eine MFA-Lösung anbieten, die kostengünstig und leicht bereitzustellen und zu verwalten ist, damit die vermeintlichen Schwierigkeiten, die Unternehmenseigentümer und IT-Entscheidungsträger von der MFA-Implementierung abhalten, keine Rolle mehr spielen. Eine moderne MFA-Lösung ist keine optionale Vorkehrung, sondern eine unternehmerische Notwendigkeit.


**Einzelheiten zur Umfrage:**
Diese Umfrage wurde von CITE Research für WatchGuard Technologies durchgeführt. Die Umfrage fand unter 650 Eigentümern kleiner und mittelständischer Unternehmen sowie IT-Entscheidungsträgern in Unternehmen mit weniger als 1.000 Mitarbeitern in den USA, Großbritannien und Australien statt. Die Umfrage wurde im April und Mai 2018 durchgeführt.

b.o.c.
IT-SECURITY

BOC IT-Security GmbH

+49 661 9440440 / info@boc.de

www.boc.de

## Unsere Produkte nutzen WatchGuard-Technologie

WatchGuard® gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Es bietet die zentralen Technologien, um sich gegen die heutigen aggressiven Bedrohungen zu wehren.



WatchGuard®