KUPPER Gruppe.

Benötigen **mittelständische Unternehmen Multifaktor-Authentifizierung?**

Multifaktor-Authentifizierung – was ist das

Der Begriff „Zwei-Faktor-Authentifizierung“ oder „starke Authentifizierung“ ist nicht neu. Er wurde bereits in den 90er Jahren verwendet, meist in Bezug auf einen Hardware-Token, der Einmalpasswörter in Zusammenhang mit festgelegten Passwörtern generierte. Eigentlich bezeichnet die Zwei-Faktor-Authentifizierung den Einsatz von zwei der folgenden Faktoren:

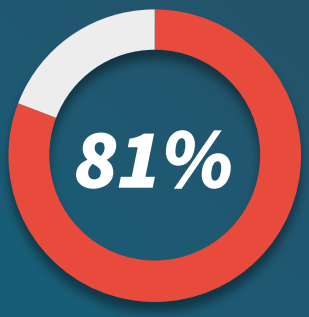
- **Informationen: Passwort, PIN**
- **Ressource: Token, physisches Gerät (Mobiltelefon), Schlüssel**
- **Körperteil: Fingerabdruck, Gesichtserkennung**

Die Technologieentwicklung eröffnete die Möglichkeit, mehrere Faktoren zu kombinieren, ohne die Benutzerfreundlichkeit einzuschränken. Die Verwendung von zwei oder mehr Faktoren wird heute Multifaktor-Authentifizierung (MFA) genannt. WatchGuard AuthPoint ist ein gutes Beispiel für die Anwendung der MFA mit mehr als zwei Faktoren zur Authentifizierung.

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 bereits viele Organisationen auf die Multifaktor-Authentifizierung (MFA). Die mehrschichtige Herangehensweise soll dazu beitragen, das Risiko der reinen Passwortsicherheit zu reduzieren. Teile dieser Technologie hat bereits auch in den privaten Bereich Einzug gehalten. Kleinere und größere Anbieter wie Amazon, Facebook, Google usw. Versenden eine Mail, wenn sich ein Nutzer von einem unbekannten Gerät einloggt. AuthPoint lässt sich so konfigurieren, dass sie etwa alle Authentifizierungsanfrage immer zulassen oder sie bei jedem Authentifizierungsversuch eine Benachrichtigung erhalten.

Bei der sicheren Multifaktor-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 (etwas, das sie besitzen) und ihre PIN eingeben (etwas, das sie wissen).

Die Umsetzung von MFA-Lösungen in Unternehmen ist auch in komplex vernetzten Systemen mit der richtigen Lösung sehr einfach und preiswert geworden, das ist allerdings noch nicht überall bekannt.



81 %
der Datensicherheitsverletzungen sind auf schwache oder gestohlene Passwörter zurückzuführen.

KUPPER
IT. innovativ. effizient. sicher.

Hürden bei der Umsetzung

1. **61% haben den Eindruck, dass sich MFA-Lösungen an größere Unternehmen richten**
2. **24% halten die Wartung und den Support von MFA-Lösungen für zu kompliziert**
3. **24% sind der Ansicht, dass eine MFA-Implementierung zu komplex ist**
4. **24% halten MFA-Lösungen für zu teuer**
5. **22% vermuten innerbetrieblichen Widerstand gegen die MFA**
6. **17% sind der Auffassung, SIE BRÄUCHTEN KEINE MFA-LÖSUNG**

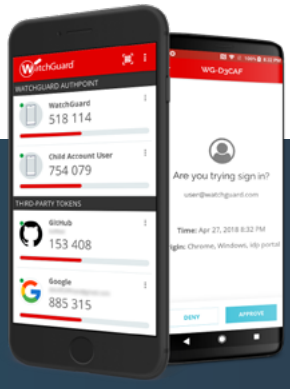
Das ernsthafte Problem von schwachen Passwörtern bleibt unumstritten. Laut der Verizon-Umfrage behaupten 83 Prozent der Eigentümer und IT-Entscheidungsträger mittelständischer Unternehmen, dass ihre Mitarbeiter um die Bedeutung der Best Practices für Passwörter wissen. Obwohl Arbeitgeber also bei ihren Mitarbeitern die Notwendigkeit von Passwortsicherheit erkennen, haben sie erhebliche Bedenken, beim Schutz von Unternehmens-, Personal- und Kundendaten allein auf Passwörter zu setzen. Zur Lösung dieser Probleme sagten 84 % der Befragten, sie würden sich von einer technischen Lösung mehr versprechen als von Richtlinien zur Erzwingung starker Passwörter. Wenn also IT-Entscheidungsträger eine technische Lösung bevorzugen, um ihren Mitarbeitern ein sicheres Anmeldeverfahren zur Verfügung zu stellen, stellt sich eigentlich nur die Frage, wie die oben genannten Punkte adäquat aufgelöst werden können.

1. **61% haben den Eindruck, dass sich MFA-Lösungen an größere Unternehmen richten**
   Das ist aus den Erfahrungen der Vergangenheit heraus nachvollziehbar. Eine MFA musste von IT-Fachpersonal aufgesetzt werden. Notwendige Geräte aufwendig in die Systemlandschaft integriert und Mitarbeiter aufwendig geschult werden. Zwischenzeitlich lösen intelligent konfigurierbare Systeme und neuen Möglichkeiten von Smartphones und Apps diese Aufwände und ermöglichen eine schlanke, leicht integrierbare Lösung.

2. **24% halten die Wartung und den Support von MFA-Lösungen für zu kompliziert**
   Auch dieser Punkt ist nach möglichen Erfahrungen älterer Lösungen nachvollziehbar. Zwischenzeitlich kann das System und die Funktionen über ein zentrales Dashboard verwaltet werden. Auswertungen und Anpassungen bei Veränderungen wie Personal oder bei Auffälligkeiten kann damit schnell und unkompliziert umgesetzt werden.

3. **24% sind der Ansicht, dass eine MFA-Implementierung zu komplex ist**
   Dieser Punkt könnte kurz beantwortet werden mit – Die Einrichtung für alle Mitarbeiter kann in den meisten Fällen, ohne individuelle Unternehmenskomplexität, innerhalb von zwei Tagen erfolgen. Entweder durch die interne IT oder wir als Ihr IT-Dienstleister übernehmen das für sie.

4. **24% halten MFA-Lösungen für zu teuer**
   Solange alles gut geht, ist auch der AirBag im Auto zu teuer. Aber dieser Sicherheitsaspekt ist inzwischen Serienausstattung, da der Preis den Nutzen im Fall des Falles weit überwiegt. Die MFA hat sich preislich inzwischen ebenfalls so entwickelt, dass die Abrechnung über monatliche Beiträge pro Nutzer ungefähr einer Tasse Kaffee entspricht. Wie viel Kaffee monatlich in Ihrem Unternehmen konsumiert wird wissen wir nicht, jedoch glauben wir, dass die Sicherheit ihrer Firma in Kombination mit der einfachen Nutzung der MFA das Ganze wert ist. (Außerdem sparen sie sich bei vielen



Der Einsatz mehrerer Faktoren erhöht die Sicherheit der Lösung insgesamt und bietet zusätzlichen Schutz vor verschiedenen Angriffsarten wie Social Engineering und Remote Access-Trojanern (RATs), die Anwendungen klonen sollen.

Mitarbeitern im Home Office einiges an Kaffeekosten – und Sie bekommen ein besseres Bauchgefühl - nicht durch weniger Kaffee, sondern durch die bessere Absicherung Ihres Unternehmens)

5. **22% vermuten internen Widerstand gegen die MFA**
   Ein älterer Marketing-Ansatz war "keep it simple and stupid" - und genau so muss eine Lösung sein, um den Widerstand der Nutzung gering zu halten. Bei unserer MFA Lösung trifft eben das zu – egal, ob über die Smartphone App oder einen physikalischen Token, je nach Ihrer Konfiguration müssen Ihre Mitarbeiter die Bestätigung nur in Sonderfällen verwenden – beispielsweise bei Nutzung eines neuen Endgerätes. Und selbst dann muss lediglich der Token-Code eingegeben oder auf dem Smartphone innerhalb der App nur der Bestätigungsbutton angeklickt werden. Weitere Zusatzeingaben sind nicht notwendig. Sprechen Sie uns zu den Möglichkeiten gern an.
6. **17% sind der Auffassung, sie bräuchten keine MFA**
   Bei Glaubensfragen halten wir uns lieber zurück.

Wir unterstützen sie!

Als WatchGuard Managed Security Service Provider unterstützen wir Sie bei der Einführung von AuthPoint in Ihrem Unternehmen. Von der Planung über die Umsetzung und dem Rollout der Mobile App bis hin zur Verwaltung der User, übernehmen unsere Security-Experten die gesamte Implementierung Ihrer neuen Multifaktor-Authentifizierung von WatchGuard.

Die Bereitstellung und Verwaltung von AuthPoint erfolgt schnell und einfach über die WatchGuard-Cloud. Dadurch muss keine lokale Software installiert und deren Updates verwaltet werden. Darüber hinaus unterstützt die Cloud die Integration vieler Drittanwendungen und Dienste sodass sich Ihre Benutzer nur einmal anmelden müssen, um alle Anwendungen und Dienste aufrufen zu können.

Wir bieten Ihnen eine MFA-Lösung an, die 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.

SIE SIND INTERESSIERT?
Wir helfen ihnen weiter!

+49 (0) 341 30536-0
it-security@kupper-it.com
www.kupper-it.com/authpoint

WatchGuard™

MULTIFAKTOR-AUHTENTIFIZIERUNG

kostengünstig • leicht bereitzustellen • einfach zu verwalten

KUPPER
IT. innovativ. effizient. sicher.