
Was würden Sie wetten, dass alle Mitarbeiter sichere Passwörter eingerichtet haben?
WatchGuard
Selbst bestätigen, Betrüger verweisen
Be Authentic
with AuthPoint MFA
WatchGuard Technologies

Inhalt

Sie sind nur ein schwaches Passwort von einer Sicherheitsverletzung entfernt …
…. und selbst „komplizierte“ Passwörter können geknackt werden.

Passwörter allein reichen schlicht und ergreifend nicht mehr aus, um Ressourcen, Konten und Informationen zu schützen.
Im Folgenden sind einige Gründe für diese Feststellung aufgeführt:

80 % der Benutzer nutzen DASSELBE Passwort[2] für mehrere Zugänge

6 % der Internet-Benutzer setzen **DASSELBE Passwort für alle Online-Konten ein[2]**

Rund 46 % der Mitarbeiter nutzen **private Passwörter** für Firmenkonten[3]

Die Benutzer wählen zu schwache Passwörter

Die 25 am häufigsten verwendeten schwachen Passwörter des Jahres 2017[1]

1. **123456**
2. **Password**
3. **12345678**
4. **qwerty**
5. **12345**
6. **123456789**
7. **letmein**
8. **1234567**
9. **football**
10. **iloveyou**
11. **admin**
12. **welcome**
13. **monkey**
14. **login**
15. **abc123**
16. **starwars**
17. **123123**
18. **dragon**
19. **passw0rd**
20. **maste**
21. **hello**
22. **freedom**
23. **whatever**
24. **qazwsx**
25. **trustno1**

1. https://www.teamsid.com/worst-passwords-2017-full-list/2. https://www.csoonline.com/article/3244137/password-security/password-managers-grow-up-target-business-users.html3. http://www.statista.com/statistics/763091/us-use-of-same-online-passwords4. https://www.fastcompany.com/40469838/dashlane-reused-password-hygiene

Sind Ihre Passwörter sicher? Das hält Hacker nicht ab.

Hacker kaufen Anmeldedaten einfach im Darknet – ähnlich wie in gewöhnlichen Onlineshops.

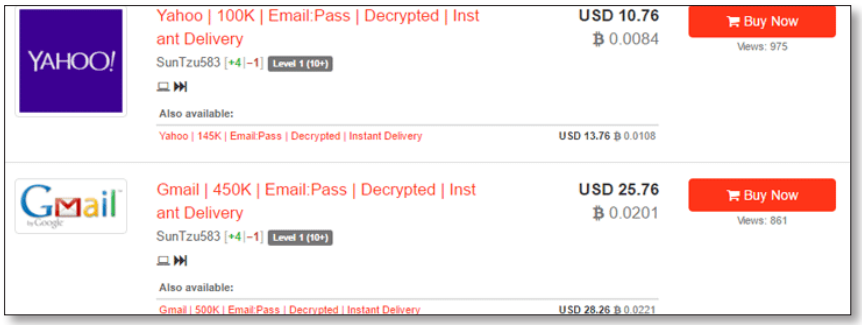
Durchschnittlicher Preis für ein Passwort im Darknet[5]: **160,15 $**
Durchschnittlicher Wert einer Benutzeridentität (kontoübergreifende Anmeldedaten) für einen Hacker: **1.200 $**

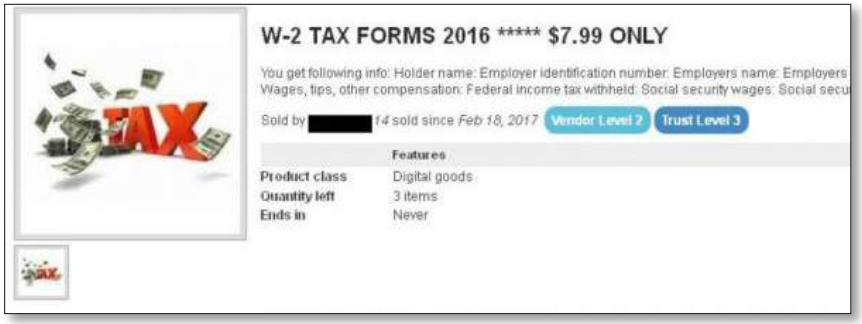
Wenn das geistige Eigentum, die Finanzdaten, Kunden- oder Mitarbeiterdaten oder andere Informationen in Ihrem Netzwerk mehr als 1.200 $ wert sind, lohnt sich für einen Hacker der Kauf der Informationen (d. h. Ihrer Anmeldedaten).

Sind Sie der Auffassung, dass das mit Ihren **Anmeldedaten nicht passieren wird?**
Oder mit denen Ihrer Kollegen?

Im Darknet sind Milliarden Anmeldedaten erhältlich, viele davon von Admin-Benutzern. Allein Ende 2017 wurde eine Datei mit 1,4 Milliarden Klartext-Passwörtern gefunden.[6] Die Wahrscheinlichkeit ist hoch, dass Ihre Anmeldedaten innerhalb weniger Sekunden gekauft werden können.

Für diejenigen, die sich erst einmal im Darknet befinden, ist der Kauf Ihres Kennworts nicht schwieriger als ein Kauf in einem Onlineshop. Rechts sind einige Screenshots von Darknet-Seiten für den Kauf von Passwörtern abgebildet.





5. https://www.nbcnews.com/tech/security/your-identity-sale-dark-web-less-1-200-n855366 6. https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14
7. http://www.cyberinject.com/gmail-yahoo-passwords-on-dark-web/ 8. https://www.theteneogroup.com/2017/06/08/understanding-deep-web-dark-web-guard-network/ 9. https://zerohedge.whotrades.com/blog/43790836676 10. https://zerohedge.whotrades.com/blog/43790836676

Wenn sich ein Hacker dazu entscheidet, Ihr Passwort nicht zu kaufen, sondern zu knacken, **braucht er vermutlich nicht allzu lange dafür.**

Tatsächlich dürfte er in der Lage sein, die Passwörter der meisten Menschen in der Zeit zu knacken, in der Sie diese Tabelle durchlesen[11]

Art	Passwort	Dauer (HSIMP) How Secure Is My Password (wie sicher ist mein Passwort)?	Dauer (PA) Passfault Analyzer-Tool	Sicherheits-ebene
Gängiges Wort mit 8 Zeichen	required	52 Sekunden	<1 Tag	Nutzlos
8 zufällige Zeichen	qkcrmztd	52 Sekunden	<1 Tag	Nutzlos
8 zufällige Zeichen und Ziffern	kqwbv832	11 Minuten	<1 Tag	Nutzlos
8 zufällige Zeichen mit Groß- und Kleinschreibung, Symbolen und Ziffern	J5bZ>9p!	20 Tage	<1 Tag	Riskant

Art	Passwort	Dauer (HSIMP)	Dauer (PA)	Sicherheits-ebene
Passwort mit 2 gängigen Wörtern	orange tea	98 Tage	<1 Tag	Riskant
Passwort mit 3 gängigen Wörtern	this is cool	546 Jahre	<1 Tag	Riskant
Passwort mit 5 gängigen Wörtern	du-bi-du-bi-doo	12 Millionen Jahre	<1 Tag	Riskant

Passwörter lassen sich einfach hacken und bilden nur eine Verteidigungslinie. Wenn Hacker auch nur ein Passwort eines Mitarbeiters stehlen, können sie in der Regel auf das gesamte Netzwerk zugreifen. Sobald sie sich im System befinden, können sie frei schalten und walten. In der Regel verbreiten sie Malware oder stehlen, ändern oder löschen wichtige Informationen.

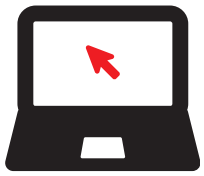
11. https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/

Vereinfachte Übersicht wie ein Hacker ein Passwort stiehlt.

Die Übersicht basiert auf dem Artikel „Hacking the Hacker“ des Computersicherheitsexperten und White-Hat-Hackers Roger Grimes.

Informationen sammeln
(durch Fingerprinting und/ oder Social Engineering)

Auf Konto zugreifen
vermutlich mit verlorengegangenen oder gestohlenen Anmeldedaten



Im System bewegen
und Schwachstellen ermitteln

Administrator-zugriff erlangen
(Erlangung zusätzlicher Berechtigungen)

Angriff ausführen

Grimes betont:

„Falls die Hacker in der Phase des Fingerprintings ihre Hausaufgaben gemacht haben, dann ist diese Phase wirklich nicht besonders schwierig.“

Mit anderen Worten: Hacker haben keine besonderen Schwierigkeiten, auf Ihre Konten zuzugreifen. Manche Hacker verwischen sogar ihre Spuren oder öffnen eine Hintertür für zukünftigen Zugriff. Das ist jedoch nicht immer der Fall.

Es ist leicht, Ihr Passwort zu stehlen

Hacker kommen erschreckend einfach an die Passwörter von Nutzern, und der betriebene Aufwand ist meist äußerst lohnenswert. Die Tools und Technologien der Hacker zur Passwortermittlung sind inzwischen so ausgereift und automatisiert, dass ein „Erraten" des Passworts oft nicht erforderlich ist. Selbst wenn dies doch der Fall ist, helfen Social Engineering (zum Beispiel Pishing-Angriffe oder Trojanische Pferde), Keylogging und andere Methoden dabei, die wahrscheinlichsten Passwörter effizient zu erraten und zu testen. Diese Herangehensweise ist oft sehr erfolgreich.

Zu den gängigsten Methoden zum Hacken von Passwörtern zählen:

Wörterbuchangriff

Hacker versuchen, ein Passwort dadurch zu erraten, dass sie eine Liste gängiger Wörter aus einem Passwort-Wörterbuch ausprobieren. Modernere Passwort-Wörterbücher enthalten Listen mit den am häufigsten in Passwörtern genutzten Wörtern. Dies ist eine relativ einfache Methode, aber eine, die beim Erraten weniger komplexer Passwörter effektiv ist. Wenn Sie in Ihren Passwörtern reale Wörter nutzen, sind Ihre Anmeldedaten gefährdet.

Brute-Force-Angriff

Diese Methode ist nicht so effizient wie ein Wörterbuchangriff, aber effektiver beim letztlichen Erraten des Passworts. Bei dieser Methode setzen Hacker Tools ein, die jede erdenkliche Kombination aus Buchstaben, Ziffern und Symbolen ausprobieren, bis das Passwort erraten wurde. Ähnlich läuft ein umgekehrter Brute-Force-Angriff ab: Hierbei wird ein Passwort für viele Benutzernamen ausprobiert.

Rainbow-Angriff

Bei dieser Methode wird eine sogenannte Rainbow Table zum Knacken von Passwort-Hashwerten (im Wesentlichen in verschlüsselter Form in Systemdatenbanken gespeicherte Passwörter) genutzt. Diese Methode ist deutlich effizienter und effektiver als Brute-Force- oder Wörterbuchangriffe.

Credential-Stuffing-Angriff

Da so viele Personen kontenübergreifend dieselben Passwörter oder Variationen dieser Passwörter verwenden, haben Hacker eine Methode entwickelt, mit der sie automatisch Datenbanklisten mit bei einer Sicherheitsverletzung erlangten Kombinationen aus Benutzername und Passwort auf der Anmeldeseite einer Ziel-Website ausprobieren. Nach Angaben von Shape Security sind 90 % der Anmeldeversuche bei Onlinehändlern auf diese Art von Angriff zurückzuführen. Diese Methode verspricht den Hackern in rund 3 % der Fälle den gewünschten Erfolg.

Social Engineering

Diese Methode ist in verschiedenen Ausprägungen zu beobachten. In allen Fällen geht es darum, dass Personen getäuscht oder manipuliert werden, damit sie ihre Informationen preisgeben oder bestimmte Aktionen ausführen. Gängige Social-Engineering-Methoden zum Stehlen von Passwörtern sind Phishing-Angriffe und Trojanische Pferde. Eine weniger gängige Variante ist das sogenannte Shoulder Surfing. Dabei beobachtet der Hacker einen Benutzer einfach bei der Passworteingabe.

Angesichts der immer ausgereifteren Technologien und Tools, die den Hackern zur Verfügung stehen, ist das Knacken des Passworts häufig die einfachste Komponente eines Hacking-Angriffs. Es ist bisweilen so einfach, dass die Angreifer nicht einmal raten müssen. Das Erschreckendste an dieser Feststellung ist, dass unabhängig davon, wie sicher Ihr Passwort ist, nur ein Kollege ein schwaches Passwort haben muss, und schon ist das gesamte System gefährdet.

Authentifizierung als Schutz:
Die Verhaltensänderung der Mitarbeiter gegenüber Passwörtern funktioniert einfach nicht

Eine Methode zur Senkung des Risikos gestohlener Passwörter besteht darin, die Mitarbeiter in Schulungen dafür zu sensibilisieren, sicherere Passwörter festzulegen und diese häufiger zu ändern. Das Verhalten jedes einzelnen Mitarbeiters zu ändern, ist jedoch nicht nur eine große Herausforderung, sondern auch eine ineffektive Vorgehensweise.

Die Methode funktioniert nach bisherigen Erkenntnissen nicht
Dies wird durch die Millionen von Unternehmen belegt, deren Datenbanken gehackt wurden, und durch die vielen Millionen gestohlenen Passwörter, die online verfügbar sind (im Darknet können viele Anmeldedaten käuflich erworben werden).

Die Nutzung von Tools wird äußerst komplex
Die kontoübergreifende Verwendung eindeutiger, vollständig zufälliger und 16 Zeichen langer Passwörter bringt eine hohe Komplexität mit sich. Die Benutzer entscheiden sich für einfache Passwörter, weil schwierige Passwörter sich nur schwer merken lassen. Viele Benutzer denken sich etwas komplexere Passwörter aus, nutzen diese (oder Variationen davon) aber dann für unterschiedliche Konten ein.

Wenn Passwörter nicht ausreichen, was ist dann notwendig?

Die Multi-Faktor-Authentifizierung (MFA) ist eine Überprüfungsmethode, bei der Anmeldungen mit Benutzername und Passwort um eine zweite Sicherheitsebene ergänzt werden. Sie sorgt dafür, dass Hacker auch dann nicht auf Ihre Systeme zugreifen können, wenn das Passwort eines Mitarbeiters kompromittiert wird.

WatchGuard bietet eine benutzerfreundliche Lösung für die Multifaktor-Authentifizierung, die Unternehmen dabei hilft, ihre Ressourcen, Informationen und Benutzeridentitäten zu schützen: AuthPoint.

AuthPoint ist einfach bereitzustellen, einfach zu verwalten und schon für weniger als die Kosten einer Tasse Kaffee pro Monat und Benutzer erhältlich. Die Lösung ist auch sicherer als eine Zwei-Faktor-Authentifizierung (2FA) und als SMS-basierte Lösungen, kostengünstiger (geringere Gesamtkosten) als Lösungen außerhalb der Cloud und benutzerfreundlicher als Lösungen mit Token.

Wichtiger Hinweis:
Zwischen den einzelnen MFA-Lösungen bestehen deutliche Unterschiede

SMS-basierte Multifaktor-Authentifizierung ist keine vertrauenswürdige und sichere Methode mehr. Benutzer mit SMS-basierter Authentifizierung sollten umgehend zu einer anderen Methode wechseln. Das National Institute of Standards and Technology (NIST) hat 2016 in seinen Leitlinien für digitale Identitäten die Benutzer aufgefordert, die SMS-basierte Authentifizierung nicht mehr zu verwenden:

„Aufgrund des Risikos, dass SMS-Nachrichten möglicherweise abgefangen oder umgeleitet werden könnten, sollten vor der Implementierung neuer Systeme alternative Authentifizierungslösungen in Betracht gezogen werden. Out-of-Band-Authentifizierung [über SMS oder Sprache] ist veraltet. Es wird in Erwägung gezogen, sie in zukünftigen Versionen dieser Richtlinie zu entfernen."

Der Harvard Business Review urteilte sogar: „… die Authentifizierung per SMS kann mit einiger Berechtigung eher als Angriffsvektor denn als Sicherheitsmaßnahme betrachtet werden."

Die SMS-basierte Authentifizierung ist deshalb so riskant, weil Textnachrichten abgefangen werden können. Reddit war eines der bekannteren Opfer dieser Angriffsmethode im Jahr 2018. Reddit kommentierte den Angriff auf der eigenen Website mit Hinweis auf die Schwäche der SMS-basierten Authentifizierung: „Wir haben gelernt, dass eine SMS-basierte Authentifizierung bei weitem nicht so sicher ist, wie wir gehofft hatten. Der Hauptangriff fand über das Abfangen von SMS statt. Wir weisen darauf hin, um jeden dazu zu ermutigen, zu Token-basierter 2FA zu wechseln."

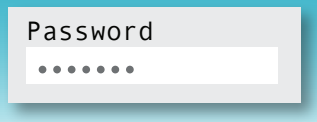
Zwar ist eine SMS-basierte MFA besser als die alleinige Verwendung von Passwörtern und Benutzernamen, aber sie schützt die Benutzer nicht zuverlässig vor Hacking-Angriffen. Um das Risiko abzumildern, benötigen Unternehmen eine MFA, die auf stärkeren Authentifizierungsmethoden basiert.

Wie funktioniert AuthPoint?

AuthPoint ist ein MFA-Service (Multifaktor-Authentifizierung), der Unternehmen dabei hilft, ihre Ressourcen, Informationen und Benutzeridentitäten zu schützen. Benutzer werden bei Verwendung von AuthPoint zu einer Authentifizierung mit mehr als 2 Faktoren statt nur eines Passworts gezwungen.

Diese Faktoren sind eine Kombination von:

- **Informationen** (Passwort, PIN)
- **Gerät** (Token, Smartphone)
- **Körperteil** (Fingerabdruck, Gesicht)



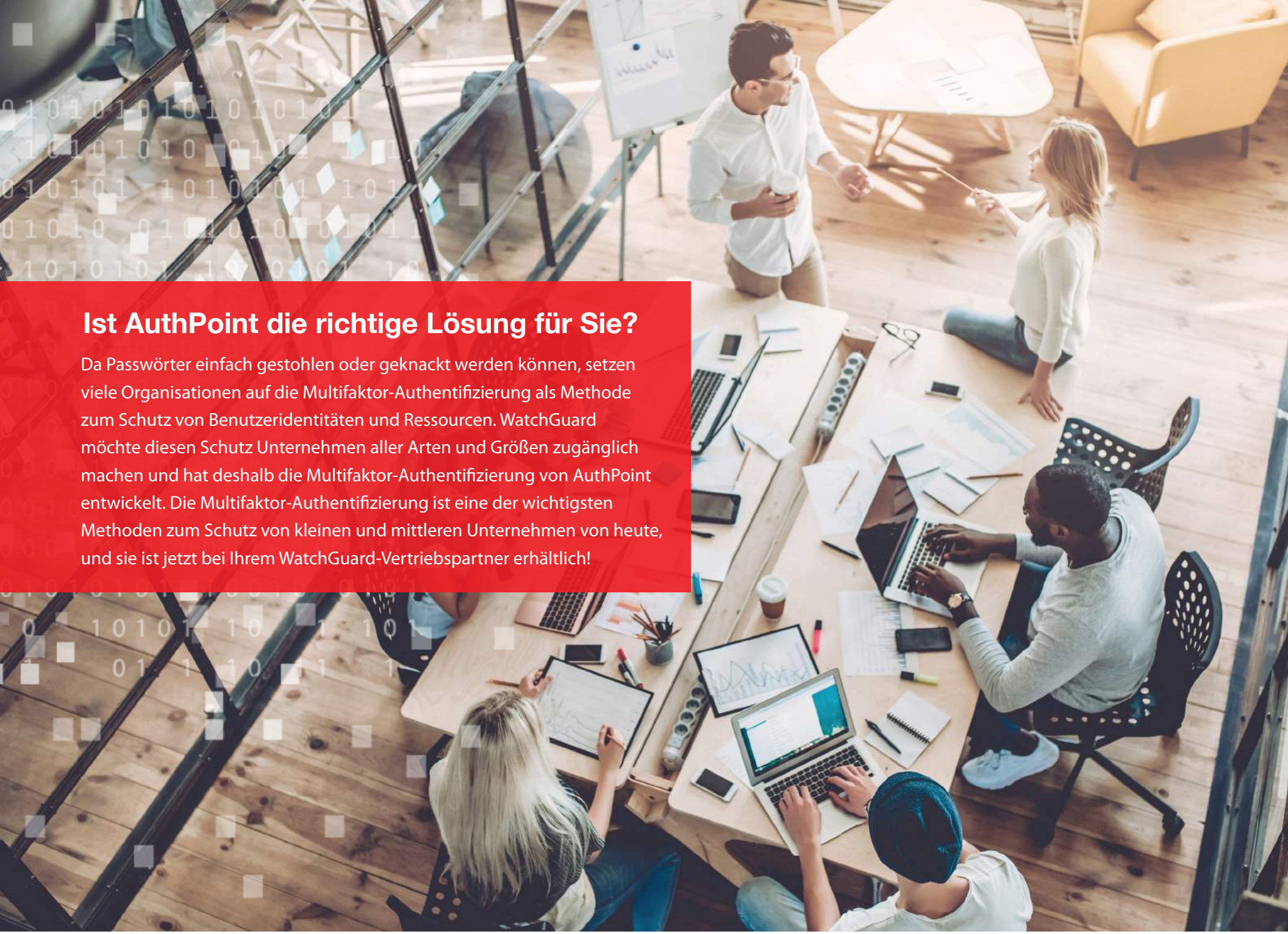
Durch den Einsatz von **mehreren Authentifizierungsebenen** können Unternehmen die Gefahr, dass ihre Konten gehackt werden, erheblich reduzieren. Wenn ein Hacker das Passwort eines Mitarbeiters erlangt, gibt es immer noch eine Sicherheitsebene, die einen Hackingangriff abwehrt.

Mit AuthPoint ist dieser Schutz leicht herzustellen. Mit einer einzigen Berührung in der mobilen AuthPoint-App können die Benutzer Anmeldeversuche genehmigen oder abweisen. Sobald sich die Benutzer angemeldet haben, können sie bei allen wichtigen Konten Single-Sign-On nutzen.

Da die Genehmigungen über die mobile App des Benutzers erfolgen, müssen keine zusätzlichen Token bereitgehalten werden. Einfacher geht's nicht!
AuthPoint befindet sich vollständig in der Cloud. Das bedeutet, dass keine kostspielige Hardware bereitgestellt und keine Software aktualisiert werden muss. Die Lösung kann von jedem beliebigen Ort aus verwaltet werden. Da sie so einfach bereitzustellen und zu verwalten ist, benötigen Sie für den Einstieg keinen eigenen Sicherheitsexperten.

Mobile Mitarbeiter? AuthPoint funktioniert online und offline, d. h., Benutzer können sich auch unterwegs während eines Flugs sicher anmelden und auf ihr Konto zugreifen. Durch den Einsatz von QR-Code-basierter Authentifizierung können Benutzer sich überall und jederzeit anmelden.

Erfahren Sie mehr darüber, wie Sie mit AuthPoint für mehr Sicherheit in Unternehmen sorgen können: **www.watchguard.com/authpoint**



Ist AuthPoint die richtige Lösung für Sie?

Da Passwörter einfach gestohlen oder geknackt werden können, setzen viele Organisationen auf die Multifaktor-Authentifizierung als Methode zum Schutz von Benutzeridentitäten und Ressourcen. WatchGuard möchte diesen Schutz Unternehmen aller Arten und Größen zugänglich machen und hat deshalb die Multifaktor-Authentifizierung von AuthPoint entwickelt. Die Multifaktor-Authentifizierung ist eine der wichtigsten Methoden zum Schutz von kleinen und mittleren Unternehmen von heute, und sie ist jetzt bei Ihrem WatchGuard-Vertriebspartner erhältlich!

Dieser leistungsstarke Schutz steht Ihnen für weniger als den Preis Ihres morgendlichen Cappuccinos zur Verfügung.

Würden Sie also darauf wetten, dass alle Mitarbeiter sichere Passwörter eingerichtet haben? Mit AuthPoint ist das nicht nötig. Die Lösung ist kostengünstig, leistungsstark und benutzerfreundlich.

Wenden Sie sich noch heute an Ihren WatchGuard-Vertriebspartner, und testen Sie AuthPoint einen Monat kostenlos! Weitere Informationen zu AuthPoint finden Sie unter www.watchguard.com/authpoint.

WATCHGUARD-SICHERHEITSPORTFOLIO

Netzwerksicherheit

Unsere Plattform stellt nicht nur Sicherheit auf Enterprise-Niveau bereit, sondern ist von Grund auf so konzipiert, dass der Fokus auf einer einfachen Bereitstellung, Verwendung und fortlaufenden Verwaltung liegt. Dies macht WatchGuard zur idealen Lösung für KMUs, mittelständische Unternehmen und dezentrale Großkonzerne weltweit.

Secure Wi-Fi

Die Secure Wi-Fi Solution von WatchGuard ist eine richtungsweisende Neuerung für den Markt von heute: Sie schafft eine sichere, geschützte WLAN-Umgebung, eliminiert den Verwaltungsaufwand und ermöglicht beträchtliche Kostensenkungen. Die Kombination aus leistungsstarken Verwaltungs- und Analysemöglichkeiten und einer tiefgehenden Visualisierung sichert Unternehmen die entscheidenden Wettbewerbsvorteile für den geschäftlichen Erfolg.

Multifaktor-Authentifizierung

WatchGuard AuthPoint™ ist die ideale Lösung, um die Lücke bei der passwortgestützten Sicherheit zu schließen und so Unternehmen wirkungsvoll vor Sicherheitsverletzungen zu schützen. Die Lösung bietet Multi-Faktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform. Bei der einzigartigen Lösung von WatchGuard wird die „DNA des Smartphones" als Identifizierungsfaktor genutzt. Auf diese Weise erhält nur die richtige Person Zugriff auf vertrauliche Netzwerke und Cloud-Anwendungen.

Mehr erfahren

Weitere Details erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter **https://www.watchguard.com**.

Über WatchGuard

WatchGuard® Technologies, Inc. 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. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für kleine und mittlere sowie dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im Pazifikraum. Weitere Informationen finden Sie unter WatchGuard.de.

WatchGuard

Vertrieb Nordamerika: 1.800.734.9905 • Vertrieb in Deutschland, Österreich und der Schweiz: +49 700 92229333 • Web: www.watchguard.com/authpoint