WARTEN SIE NICHT, BIS ES ZU SPÄT IST.

ERWEITERN SIE DIE SICHERHEIT, UM IDENTITÄTEN ZU WAHREN.

Sie sind nur ein schwaches Passwort entfernt von einer BREACH

… 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:

Im Jahr 2022 spielte bei 74% der Sicherheitsverletzungen der Mensch eine Rolle, hierzu zählen auch gestohlene Anmeldedaten[1]

51 % der Menschen verwenden für berufliche und private Konten dieselben Passwörter[2]

Die Benutzer wählen außerdem **zu schwache Passwörter**

WatchGuard

Hier finden Sie eine Liste der 20 Passwörter, die infolge von Datensicherheitsverletzungen am häufigsten im Darknet auftauchen[3]:

1. 123456
2. 123456789
3. Qwerty
4. Password
5. 12345
6. 12345678
7. 111111
8. 1234567
9. 123123
10. Qwerty123
11. 1q2w3e
12. 1234567890
13. DEFAULT
14. 0
15. Abc123
16. 654321
17. 123321
18. Qwertyuiop
19. Iloveyou
20. 666666

WatchGuard

Passwörter können schnell in die falschen Hände geraten

Im Darknet gibt es ganze Passwortsätze bereits für 8–25 US-Dollar[4] zu kaufen. Damit gelingt das Eindringen in Systeme einfach und kostengünstig. Und wenn das einmal nicht funktioniert, können gewiefte Cyberkriminelle die Passwörter der meisten Menschen in der Zeit knacken, die Sie brauchen, um die Passwortliste auf der vorherigen Seite durchzulesen.[5]

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.

WatchGuard

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 Phishing-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.

WatchGuard

Credential-Stuffing-Angriff

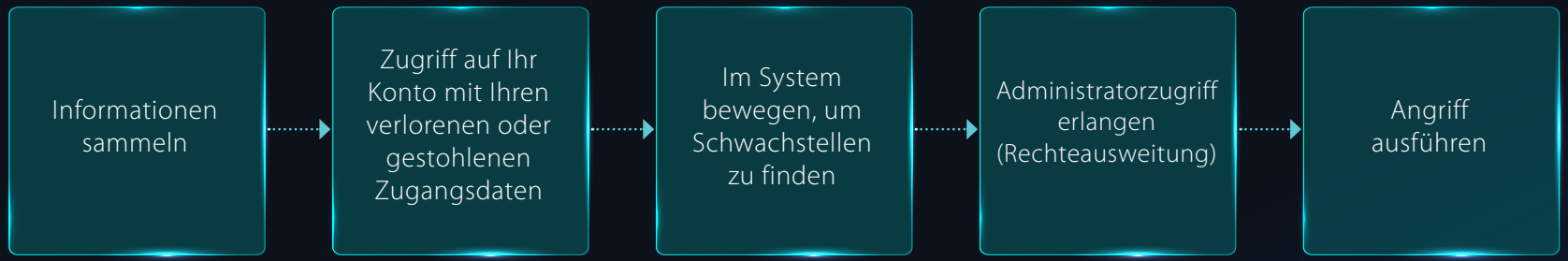
Da so viele Personen kontenübergreifend dieselben Passwörter oder Variationen dieser Passwörter verwenden, haben Hacker eine Methode entwickelt, mit der sie automatisch Datenbanklisten mit bei einer Sicherheitsverletzung erlangten Kombinationen aus Benutzername und Passwort auf der Anmeldeseite einer 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.

Hacker verdienen an verloren gegangenen oder gestohlenen Passwörtern bares Geld, da sie so Datendiebstahl begehen oder auf Ihre Geschäftssysteme zugreifen können, auf denen dann Ransomware oder andere profitable Malware-Angriffe ausgeführt werden. Computersicherheitsexperte und White-Hat-Hacker Roger Grimes beschreibt dieses Verfahren in seinem Buch *Hacking the Hacker*.



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.

Wie soll man überprüfen, ob die Person mit dem Passwort wirklich die Person ist, die sie zu sein vorgibt? Wie kann man die Identität wahren?

Experten in Regierungsbehörden und unabhängigen Agenturen auf der ganzen Welt haben gute Tipps, wie Geschäftssysteme vor Angriffen geschützt werden können. Cybersicherheitsbehörden in den USA, Neuseeland, Kanada, den Niederlanden und Großbritannien haben kürzlich darauf hervorgehoben, dass ein Schutz der Anmeldedaten durch den Einsatz von MFA und Richtlinien für sichere Passwörter bewährte Verfahren im Kampf gegen Cyberangriffe sind.[6] Dabei geht es nicht nur um irgendeine Form der Identitäts- und Anmeldedatensicherheit. Je gewiefter die Kriminellen vorgehen, desto ausgeklügelter werden auch unsere Sicherheitslösungen. Ein Paradebeispiel dafür ist, dass die CISA im August 2021 die Ein-Faktor-Authentifizierung zur ihrer Liste der schlechten Cybersicherheitspraktiken hinzugefügt hat.[7] Dies sendet ein klares Signal an alle Unternehmen, die sich für den Schutz ausschließlich auf Passwörter verlassen.

Viele Unternehmen haben versucht, das Verhalten ihrer Mitarbeiter in Bezug auf Passwörter zu ändern

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 starke Passwörter schwer zu merken sind. Viele Benutzer denken sich etwas komplexere Passwörter aus, nutzen diese (oder Variationen davon) aber dann für unterschiedliche Konten ein.

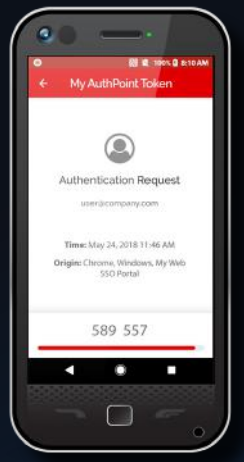
Wenn Passwörter nicht ausreichen, was ist dann notwendig?

Die Multi-Faktor-Authentifizierung (MFA) ergänzt Anmeldungen mit Benutzername und Passwort um eine zweite Sicherheitsebene. Sie sorgt dafür, dass Hacker auch dann nicht auf Ihre Systeme zugreifen können, wenn das Passwort eines Mitarbeiters kompromittiert wird. Die Multi-Faktor-Methode wird gegenüber der Ein-Faktor-Authentifizierung konkret deshalb bevorzugt, weil sie Folgendes abfragt:

Gerät
(Token, Smartphone)

Informationen
(Password, PIN)i

Körperteil
(Fingerabdruck, Gesicht)



WatchGuard

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

Die SMS-basierte Multifaktor-Authentifizierung zählt nicht mehr zu den vertrauenswürdigen und sicheren Methode. 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 anzuhalten, 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.

Der Schutz von Passwörtern ist ebenso wichtig!

Die MFA ist zwar sehr hilfreich, doch noch immer werden Passwörter zur Validierung der Identität genutzt. Deshalb empfehlen Cybersicherheitsexperten zusätzliche Schutz- und Überwachungsmaßnahmen für Anmeldedaten. Insbesondere ein professionelles Passwort-Manager-Produkt ist für viele Unternehmen vielversprechend. Es fördert nicht nur die Verwendung einzigartiger, komplexer Passwörter, sondern stellt Benutzern auch ein Tool zur Verfügung, über das sie ihre Passwörter bei Bedarf einfach und sicher aufrufen und nachschlagen können. Als effiziente Lösung für die Anforderungen des jeweiligen Unternehmens können Passwort-Manager und MFA sogar gemeinsam eingesetzt und verwaltet werden.

Angesichts des florierenden Handels mit verloren gegangenen/gestohlenen Anmeldedaten im Darknet kann ein Überwachungsdienst Unternehmen rechtzeitig warnen, wenn gestohlene Anmeldedaten für ihre Domänen dort auftauchen, bevor diese bei einem Angriff verwendet werden und Schaden anrichten können.

WatchGuard bietet eine benutzerfreundliche Multifaktor-Authentifizierungslösung mit professionellem Passwort-Manager und Darknet-Überwachungsdienst in unserem Produkt AuthPoint Total Identity Security.

WatchGuard®

Wobei hilft AuthPoint Total Identity Security?

AuthPoint ist ein Multifaktor-Authentifizierungsdienst (MFA), 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. Darüber hinaus beinhaltet Total Identity Security unseren Corporate Password Manager- und Dark Web Monitor-Dienst. Ihre Vorteile:

Mehrere Authentifizierungsebenen

Unternehmen können 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 Hacker-Angriffabwehrt.

Verwaltung über WatchGuard Cloud – eine Schnittstelle für die einfache Administration

Die AuthPoint Total Identity Security-Produkte werden vollständig in der Cloud verwaltet. Das bedeutet, dass keine kostspielige Hardware bereitgestellt und keine Software aktualisiert werden muss.

Zufriedene Benutzer und optimierte Übernahme

Mit einer einzigen Berührung in der mobilen AuthPoint-App können die Benutzer Anmeldeversuche genehmigen oder ablehnen. Sobald sich die Benutzer angemeldet haben, können sie bei allen Anwendungen und Umgebungen Single-Sign-On für schnellen Zugriff nutzen. Der Corporate Password Manager steht dabei über dieselbe AuthPoint-App zur Verfügung und kann für geschäftliche und private Passwörter verwendet werden.

Eine Lösung für Unternehmen

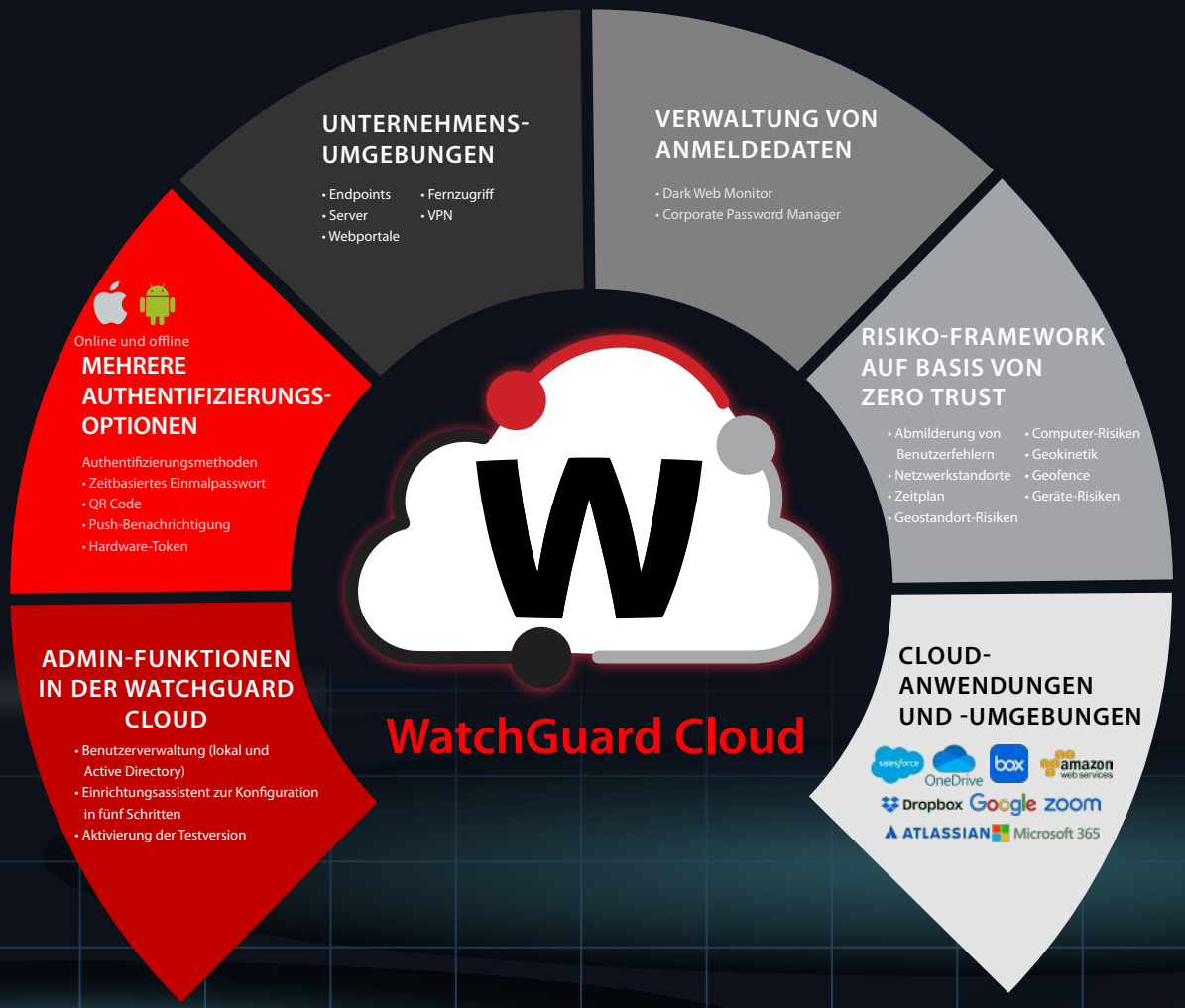
Anders als 2FA und Passwort-Manager, die für die Nutzung durch Endverbraucher entwickelt wurden, wurde AuthPoint speziell für den Einsatz in Unternehmen ausgelegt. Beispielsweise werden Benutzer beim Start von Windows/macOS authentifiziert, online und offline, d. h., Benutzer können sich auch unterwegs während eines Flugs sicher anmelden und auf ihr Konto zugreifen.

Leistungsstarken Schutz erhalten Sie für weniger als den Preis Ihres morgendlichen Cappuccinos.

Würden Sie darauf wetten, dass alle Mitarbeiter sichere Passwörter eingerichtet haben? Schützen Sie Identitäten mit AuthPoint. Die Lösung ist kostengünstig, leistungsstark und benutzerfreundlich.

WatchGuard

Identitäten schützen mit WatchGuard AuthPoint



WatchGuard

Referenzen:

1. https://www.verizon.com/business/resources/reports/dbir/
2. https://www.spiceworks.com/it-security/identity-access-management/news/world-password-day-2022/)
3. https://www.cnbc.com/2022/02/27/most-common-passwords-hackers-leak-on-the-dark-web-lookout-report.html
4. https://www.securitymagazine.com/articles/94405-a-look-into-the-pricing-of-stolen-identities-for-sale-on-dark-web
5. https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity
6. https://www.cisa.gov/uscert/ncas/alerts/aa22-137a
7. https://www.cisa.gov/uscert/ncas/current-activity/2021/08/30/cisa-adds-single-factor-authentication-list-bad-practices

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 **INTERNATIONALER VERTRIEB:** +1 206 613 0895 **WEB** www.watchguard.com/de