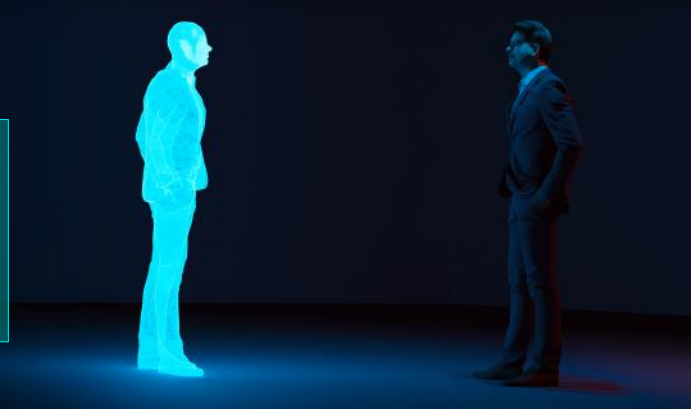
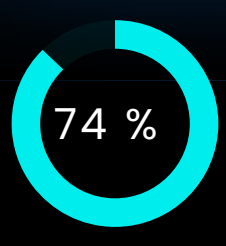
Sind Ihre Maßnahmen zur Identitätssicherung auf dem neuesten Stand?



Die CISA (Cybersecurity and Infrastructure Security Agency) nimmt die Ein-Faktor-Authentifizierung in ihre Liste der schlechten Cyber-Sicherheitsmaßnahmen auf.[1]

WARUM?

Laut dem Verizon Data Breach Investigations Report 2023 spielte im Jahr 2022 bei 74 % der Sicherheitsverletzungen der Mensch eine Rolle, hierzu zählen auch gestohlene Anmeldedaten.[2]



WIE SOLLTEN SIE REAGIEREN?

Cyber-Sicherheitsbehörden aus den USA, Neuseeland, Kanada, den Niederlanden und dem Vereinigten Königreich sagen, dass „die Härtung von Anmeldedaten" mit der Verwendung von MFA und starken Passwortrichtlinien bewährte Maßnahmen gegen das Wachstum von Cyber-Angriffen sind.[3]

★ Bonuspunkt – Die Implementierung einer starken Identitätssicherheit hilft Ihnen, sich für die besten Tarife bei Cyber-Sicherheitsversicherungen zu qualifizieren!

[1] https://www.cisa.gov/BadPractices
[2] https://www.verizon.com/business/resources/reports/dbir/
[3] https://www.cisa.gov/uscert/ncas/alerts/aa22-137a

Fünf Fragen, die Ihnen bei der Auswahl der richtigen Identitätssicherheitslösung helfen

1 Verwendet die MFA-Lösung SMS-basierte Verifizierung als primäre oder standardmäßige Authentifizierungsoption?

Die SMS-basierte Verifizierung ist weniger sicher als andere Methoden, da sie anfällig für Hijacking ist.

2 Unterstützt sie Offline-Authentifizierung?

Mitarbeiter müssen auch ohne Internetverbindung auf ihre Laptops zugreifen können, z. B. im Flugzeug, bei der Nutzung von Hotel- oder öffentlichem Wi-Fi oder wenn die Internetverbindung nur sporadisch funktioniert.

3 Bietet sie sicheres Web Single Sign-On (SSO)?

Web Single Sign-On macht die Lösung nicht nur einfacher, sondern auch sicherer. Web SSO ermöglicht es Ihrem Unternehmen, viele verschiedene Cloud-Anwendungen bereitzustellen, während sich Benutzer nur einmal anmelden müssen, um darauf zuzugreifen – für weniger Passwörter, Zurücksetzungen, Helpdesk-Anrufe sowie glücklichere Mitarbeiter.

4 Enthält sie Tools zur Verwaltung von Anmeldedaten, wie einen Passwortmanager und Dark Web-Überwachung?

Angesichts der breiten Akzeptanz von Passwörtern, die auf mehr als 20 Jahre System- und Anwendungsentwicklung zurückgeht, werden Passwörter auch in Zukunft Bestand haben... und sie sind einer der Faktoren für MFA. Dienste zur Verwaltung von Anmeldedaten verbessern die Sicherheit mit Tools, um den Schutz vor den inhärenten Risiken einer unzureichenden Passwortverwaltung zu verbessern.

5 Wie viel kostet die Lösung?

Kostenlose und kostengünstige Verbraucherprodukte können verlockend sein. Die Preisgestaltung kann bei großen Software-Paketen nicht klar erkennbar sein. Daher ist es wichtig, direkte und indirekte Kosten zu bewerten, um das vollständige Bild zu sehen. Ist der Support im Preis enthalten – sowohl technischer Support als auch Support für die Verwaltung des Abonnements? Muss separate Software lizenziert werden? Verfügen Sie über eine Managementoberfläche, die Unternehmensverwaltung, Reporting und Transparenz ermöglicht? Oder bürden Sie Ihrem IT-Sicherheitsteam zusätzliche Arbeit und Kosten auf? Steigen die Helpdesk-Kosten durch mangelnde Benutzerfreundlichkeit?

Starten Sie noch heute mit AuthPoint Total Identity Security von WatchGuard

- Corporate Password Manager
- Dark Web Monitor
- Multifaktor-Authentifizierung

Eine Antwort, um Identitäten zu schützen
Weitere Informationen erhalten Sie bei Ihrem autorisierten WatchGuard-Händler oder unter https://www.watchguard.com/de/wgrd-products/authpoint.

ÜBER WATCHGUARD

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cyber-Sicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Netzwerksicherheit und -informationen, fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie auf **WatchGuard.de.**