
WatchGuard
RISIKOBASIERTE
AUTHENTIFIZIERUNG
Ein entscheidendes Element für jede
Zero-Trust-Bereitstellung

INHALTSVERZEICHNIS

2010 prägte Forrester Research Inc. erstmals den Begriff „Zero-Trust". Ein Jahrzehnt und eine Pandemie später und angesichts der Tatsache, dass Unternehmen hybride Multi-Cloud-Umgebungen implementieren, kann das Identitäts- und Zugriffsmanagement nicht mehr als optional betrachtet werden. Eine Ausweitung des VPN-Schutzes reicht nicht aus.

Die risikobasierte Authentifizierung verbessert sowohl die Sicherheit als auch die Benutzerfreundlichkeit, da sie eine Einstufung der schutzbedürftigen Ressourcen nach Risikostufe und Benutzertyp ermöglicht. Sie können somit auf die Sicherheitsstruktur in Ihrem Unternehmen abgestimmte Regeln erstellen und flexibel und bedarfsabhängig für höheren Schutz sorgen.

In diesem eBook erörtern wir die starke Verbindung zwischen Zero-Trust-Implementierung und Risikorichtlinien. Wir erläutern, inwiefern diese Ansätze auf der Multifaktor-Authentifizierung mit der heute so dringend benötigten Technologie zum Schutz von Benutzeridentitäten und Cloud-Anwendungen aufbauen.

Warum risikobasierte Authentifizierung?

Anwender-Authentifizierung

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

Die Anwenderauthentifizierung ist eine statische Methode zur Überprüfung der Identität eines Anwenders, wenn dieser versucht, auf eine geschützte Ressource zuzugreifen. Anwender können sich mit einem einzelnen Identitätsnachweis (Faktor) authentifizieren (schwach), oder mit mehreren Identitätsnachweisen (dringend empfohlen).

In einer dynamischen Welt, in der sich die Mobilität der Anwender praktisch immer auf die Sicherheit auswirkt, ist die Multifaktor-Authentifizierung unabdingbar. Sie ist maßgebend für die Bereitstellung eines Zero-Trust-Netzwerks. Warum?

- Anwender verbinden sich von verschiedenen, ungeschützten Netzwerken aus mit Unternehmensressourcen.
- Die Arbeitszeiten sind flexibler geworden, d. h. Anwender arbeiten möglicherweise von früh morgens bis spät abends.
- Geräte könnten mit anderen Familienmitgliedern geteilt worden sein.
- Und all dies bedeutet, dass Angreifer versuchen werden, diese neue Welt der Möglichkeiten auszunutzen.

Anwender-Authentifizierung

Risikofaktoren

- **Mit welchem Netzwerk sind Sie verbunden?**
- **Ist Ihr Computer sicher?**
- **Sind Ihre Mobilgeräte sicher?**
- **Was ist Ihr aktueller Standort?**
- **Befinden sich Ihr Gerät und Ihr Computer am gleichen Ort?**

Die risikobasierte Authentifizierung berücksichtigt bei der Durchführung einer Authentifizierungsentscheidung Risikofaktoren. Sie geht über eine statische Authentifizierung hinaus und erlaubt es Administratoren, Regeln zu erstellen, die das Authentifizierungsverhalten ändern können. Manchmal wird es einfacher, wenn das Risiko gering ist, oder es werden zusätzliche Schritte verlangt, um sicherzustellen, dass es sich um den richtigen Anwender handelt, und der Zugriff wird gesperrt, wenn das Risiko zu hoch ist, selbst wenn der Anwender ein korrektes Einmalkennwort (One-Time Password, OTP) angegeben hat.

Multifaktor-Authentifizierung und Risikobewertung Optimierte Benutzerverwaltung

Die risikobasierte Authentifizierung verbessert sowohl die Sicherheit als auch die Anwenderfreundlichkeit, da sie eine Einstufung der schutzbedürftigen Ressourcen nach Risikostufe und Benutzertyp ermöglicht. Sie können somit auf die Sicherheitsstruktur in Ihrem Unternehmen abgestimmte Regeln erstellen und flexibel und bedarfsabhängig für höheren Schutz sorgen.

Sie könnten zum Beispiel festlegen, dass sich Anwender bei der direkten Verbindung mit einem lokalen Firmennetzwerk nur mit Benutzernamen und Passwort authentifizieren können, aber MFA verwenden, wenn sie von einem separaten Netzwerk aus arbeiten. Und das ist die Definition einer erweiterten Benutzerverwaltung.

Häufige Risikofaktoren, die gegebenenfalls in Authentifizierung-srichtlinien aufgenommen werden könnten

NETZWERKSTANDORT

Ein Unternehmensnetzwerk verfügt möglicherweise über alle Grenzsicherungsmaßnahmen, wie eine Firewall, sicheres WLAN, Bedrohungserkennung usw. Daher würde jemand, der physisch mit diesem Netzwerk verbunden ist, ein geringeres Risiko darstellen als jemand an einem dezentralen Arbeitsplatz mit weniger Sicherheitsmaßnahmen oder jemand, der über das Homeoffice verbunden ist.

RISIKO DURCH MOBILGERÄTE

Das Gerät eines Anwenders, das kompromittiert wurde, stellt ein Sicherheitsrisiko für ein Unternehmen dar. Ein Gerät kann beispielsweise leicht kompromittiert werden, wenn ein Anwender ein iOS-Gerät jailbreakt oder ein Android-Betriebssystem rootet und damit die Sicherheitsmaßnahmen des Betriebssystems umgeht. Ein anfälliges Gerät erhöht das Gesamtrisiko und sollte in der Regel gesperrt werden.

RISIKO DURCH ENDPUNKT/COMPUTER

Wie das Risiko durch Mobilgeräte kann auch das Risiko von Endpunkten oder Computern bei der Bewertung der zu ergreifenden Maßnahmen berücksichtigt werden. Ein Anwender mit seinem eigenen Laptop, mit allen Schutzmaßnahmen, würde ein geringes Risiko darstellen. Wenn derselbe Anwender später am Tag versucht, sich mit einem unbekannten Computer zu verbinden – vielleicht einem Linux-Rechner mit einem Tor-Browser –, würde das Risiko stark ansteigen.

ZEITRICHTLINIEN

Datum und Uhrzeit können für verschiedene Zwecke verwendet werden. Nehmen wir an, eine Unternehmensanwendung wird normalerweise jeden Tag zwischen 1 und 3 Uhr nachts gesichert und gewartet. Mit Hilfe von Zeitrichtlinien könnte der Zugriff auf diese Anwendung während dieser Zeitspanne gesperrt werden. Versucht ein Anwender an einem Wochenende oder vielleicht mitten in der Nacht, auf eine Anwendung zuzugreifen, könnte dies das Risiko drastisch erhöhen. Es könnte sich nämlich um einen Hacker handeln, der einen Angriff durchführt, während das IT-Team ruht, sodass zusätzliche Maßnahmen vorgesehen werden könnten.

Häufige Risikofaktoren, die gegebenenfalls in Authentifizierung-srichtlinien aufgenommen werden könnten

GEOFENCING

Der physische Standort könnte dazu verwendet werden, um den Zugriff aus bestimmten Ländern oder mit bestimmten Standortdaten zu verhindern und so das Risiko eines Angriffs zu minimieren. Ein Unternehmen mit Büros und Aktivitäten nur in den USA könnte eventuell jeden Zugriff außerhalb des Landes blockieren. Der Zugriff auf eine bestimmte Anwendung könnte auch auf einen Bereich rund um ein Firmenbüro beschränkt werden.

GEOGRAFISCHE ZUORDNUNG

Man kann davon ausgehen, dass ein Anwender, der sich mit einem Unternehmensdienst verbindet, ein Mobiltelefon in den Händen hält. Eine Verbindung, die von einem Computer in Sao Paulo, Brasilien, initiiert wird, während das Mobiltelefon seinen aktuellen Standort in Virginia, USA, registriert, könnte zeigen, dass ein Hacker eine Verbindung zu einem Dienst herzustellen versucht und dabei Social Engineering einsetzt, um einen Anwender davon zu überzeugen, die MFA-Authentifizierung zu genehmigen.

Auch wenn einige Geolokalisierungen nicht sehr präzise sind – einige Netzbetreiber leiten die Verbindung an einen anderen Standort um, und bei einigen Android-Geräten kann der GPS-Standort manipuliert werden – kann dies eine weitere Möglichkeit sein, potenzielle Angriffe abzuwehren.

GEO KINETICS

Eine andere Form der Nutzung von GPS- oder Geolokalisierungsfaktoren für eine Risikoentscheidung ist die sogenannte „Geo Kinetics" oder Authentifizierungsgeschwindigkeit. Ein Anwender, der sich um 9.05 Uhr von Seattle aus authentifiziert, kann sich nicht 25 Minuten später von San Diego aus authentifizieren, das 1.300 Meilen entfernt ist. Höchstwahrscheinlich wird beim zweiten Authentifizierungsversuch versucht, die erste Authentifizierung erneut zu verwenden.

Risikorichtlinien verhindern Datensicherheitsverletzungen

Ohne bestehende Risikorichtlinien müsste Ihr Unternehmen jederzeit und für alle Anwender die sicherste Authentifizierungsmethode aktivieren, was in einigen Segmenten zu unnötig hohem Aufwand für die Anwender führen könnte. Mit der Risikoauthentifizierung können Sie Ihre Strategie modernisieren. Sie können damit genau das richtige Maß an Sicherheit mit einem maßgeschneiderten Risikoschutz verwenden und sind eher in der Lage, Bedrohungen zu erkennen und auf diese zu reagieren.

Die folgenden Szenarien zeigen Fälle von möglichen Datenverletzungen, die sich mit aktivierten Risikorichtlinien verhindern lassen.

A

VERWENDUNG GESTOHLENER ANMELDEDATEN

Der Anwender authentifiziert sich regelmäßig mit Benutzernamen, Passwort und einem OTP. Ein Angreifer konnte über das Dark Web oder eine Phishing-Attacke an die Anmeldedaten des Anwenders gelangen, aber das Token konnte nicht gehackt oder geklont werden.

- **Angriff:** Mit Social Engineering ruft der Angreifer den Anwender an und bringt ihn dazu, ein OTP preiszugeben. Der Angreifer gibt die Anmeldedaten und das zeitbasierte OTP ein, um Zugriff auf die geschützte Ressource zu erhalten.

- **Vorbeugung durch Risikorichtlinien:**

  Computerrisikorichtlinien könnten zeigen, dass der verwendete Computer nicht der private Computer des Anwenders ist.

  Geokinetische Richtlinien würden möglicherweise zeigen, dass der Anwender versucht, sich von einem Ort aus zu authentifizieren, an dem der Übergang zwischen zwei Authentifizierungen unmöglich ist.

B

iOS JAILBREAKING (nicht autorisiertes Entfernen von Nutzungsbeschränkungen für iOS)

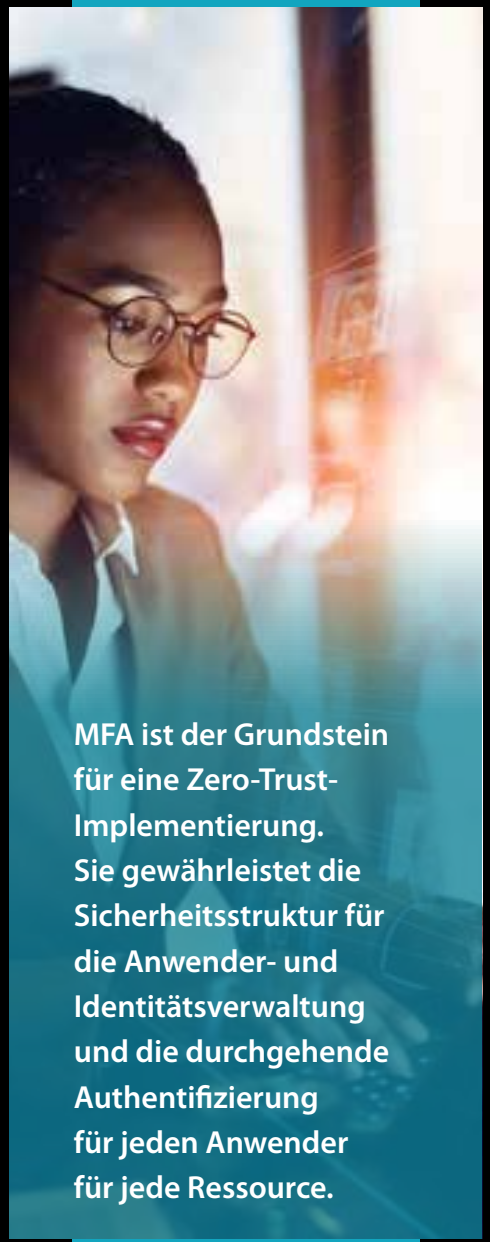
Der Anwender authentifiziert sich mit Benutzernamen, Passwort und Push. Das iPhone wurde vom Benutzer„gejailbreaked" und ein Angreifer hat Malware installiert, die ihm die volle Kontrolle gab. Push ist nicht durch eine PIN oder biometrisch geschützt.

- **Angriff:** Der Angreifer aus einem anderen Land würde sich mit gestohlenen Anmeldedaten authentifizieren und dabei das Telefon des Anwenders überwachen. Bei Eingehen des Push-Signals auf dem Anwendertelefon verwendet der Angreifer das Remote Access Tool (RAT), um den Push zu bestätigen und Zugriff auf die Ressource zu erhalten.

- **Vorbeugung durch Risikorichtlinien:**

  Richtlinien über das Risiko durch Mobilgeräte würden erkennen, dass das Mobilgerät des Anwenders nicht zuverlässig ist und Authentifizierungen von diesem Gerät verweigern.

  Richtlinien zur Geokorrelation würden prüfen, ob sich der Computer an einem anderen Ort als das Mobilgerät befindet und die Verbindung ebenfalls blockieren.



MFA ist der Grundstein für eine Zero-Trust-Implementierung. Sie gewährleistet die Sicherheitsstruktur für die Anwender- und Identitätsverwaltung und die durchgehende Authentifizierung für jeden Anwender für jede Ressource.

Ohne MFA ist Zero-Trust unmöglich.

Identitäts- und Zugriffsmanagement kann nicht länger als optional betrachtet werden. Unternehmen müssen sich auf eine starke Strategie zum Schutz und zur Verwaltung der Anwender konzentrieren, die Kernbereiche, die durch MFA und Risikoauthentifizierung geregelt werden. Dies gibt Ihnen die Möglichkeit, den „trust no one"-Ansatz für Ihr Unternehmensnetzwerk, Ihre Endpunkte und Cloud-Anwendungen voll auszuschöpfen, ohne die Benutzererfahrung zu beeinträchtigen.

Während ein traditionelles Netzwerk auf der Idee des inhärenten Vertrauens aufbaut, geht ein Zero-Trust-Framework davon aus, dass jedes Gerät und jeder Anwender, ob im Netzwerk oder außerhalb, ein Sicherheitsrisiko darstellt. Der Ansatz „never trust, always verify" verwendet mehrere Schutzebenen, um Bedrohungen zu verhindern, laterale Bewegung zu blockieren und detaillierte gezielte Benutzerzugriffskontrollen durchzusetzen.

Unter der Prämisse, dass nichts vollständig vertrauenswürdig ist, konzentriert sich der Zero-Trust-Ansatz auf drei Prinzipien:

Identifizierung von Anwendern und Geräten

Stets wissen, wer und was eine Verbindung zum Unternehmensnetzwerk herstellt Während Unternehmen damit zurechtkommen müssen, dass ihre Belegschaften nun vorwiegend remote arbeiten, ist die Sicherung des Zugangs zu internen Tools eine weitere große Herausforderung. Cloudbasierte Dienste für die Multifaktor-Authentifizierung (MFA) bieten Schutz vor Diebstahl von Anmeldedaten, Betrug und Phishing-Angriffen.

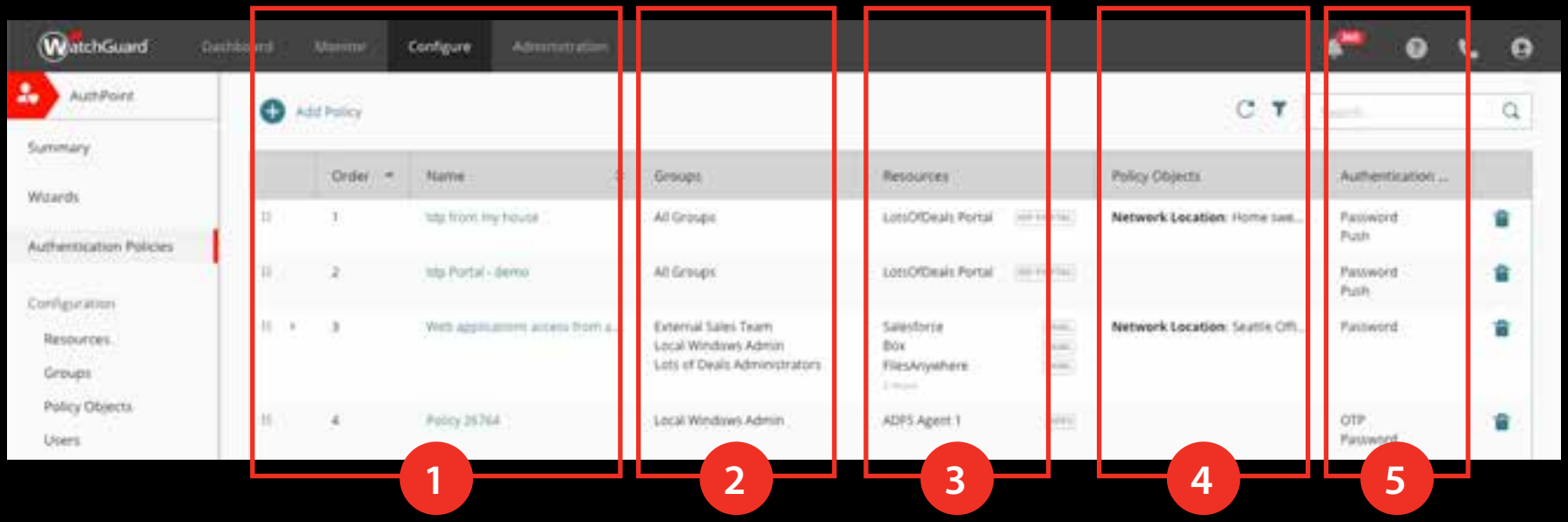
Bereitstellung eines sicheren Zugangs

Beschränken Sie den Zugriff auf geschäftskritische Systeme und Anwendungen auf die Geräte, die über eine ausdrückliche Zugriffsberechtigung verfügen. Im Rahmen des Zero-Trust-Konzepts besteht das Ziel der Zugriffsverwaltung darin, ein Mittel zur zentralen Verwaltung des Zugriffs auf alle gängigen IT-Systeme bereitzustellen und gleichzeitig den Zugriff auf nur bestimmte Anwender, Geräte oder Anwendungen zu beschränken. Single Sign-On (SSO)-Technologien, kombiniert mit MFA, können die Zugriffssicherheit verbessern und Anwender müssen sich weniger Passwörter merken.

Ständige Überwachung

Überwachen Sie den Zustand und die Sicherheitslage des Netzwerks und aller verwalteten Endpunkte. Die Bedrohung durch Malware und Ransomware ist im Zuge des Coronavirus noch größer geworden. Es ist schwieriger, Anwender bei der Internetnutzung zu schützen, wenn sie sich außerhalb Ihres Netzwerks befinden. Um den Bedrohungen die Stirn zu bieten, ist eine beständige, fortschrittliche Sicherheit erforderlich, die über die Antivirenfunktion für Endgeräte hinausgeht.

Beispiel für aktivierte risikobasierte Authentifizierungsrichtlinien, die dem Zero-Trust-Ansatz entsprechen:



1. Der Name der Richtlinie wäre ein Zero-Trust-Mikro-Segment; er kann nach Priorität und/oder Wichtigkeit geordnet werden.

2. Gruppen von Anwendern, mit Active Directory synchronisiert oder nicht, sind diejenigen, denen der Zugriff auf die geschützte Ressource gestattet sein sollte – und zwar nur ihnen.

3. Die Mikro-Segment-Anwendung(en). Dies kann eine einzelne Anwendung oder es können auch mehrere sein, falls die Anwendungen genau die gleiche Richtlinie haben.

4. Richtlinienobjekte oder Risikorichtlinien, die basierend auf Netzwerk, Zeit, Geolocation usw. bestimmte Einschränkungen festlegen können.

5. Bezieht sich auf die Authentifizierungsmethoden, die auf der Grundlage eines Risikofaktors zugelassen werden sollen oder bei denen die Authentifizierung einfach verweigert wird.

Mithilfe von Risikorichtlinien können granulare Regeln auf der Grundlage dynamischer Situationen definiert werden, was besser zu den aktuellen Trends bei Remote-Zugriff und hybriden Arbeitsmodellen in Unternehmen passt.

Verwendung von MFA und Risikorichtlinien für die Zero-Trust-Bereitstellung

Wie wir wissen, ist bei der Zero-Trust-Implementierung davon auszugehen, dass nichts vertrauenswürdig ist. Durch die Definition von Mikro-Segmenten und die Anwendung von Richtlinien, die auf die Sicherheitsanforderungen Ihres Unternehmens zugeschnitten sind, schaffen Sie eine vertrauenswürdige Umgebung. Dies beginnt mit der Identifizierung des Anwenders, der auf diese Anwendungen und Dienste zugreifen wird.

Ein Mikro-Segment könnte eine Cloud-basierte Customer Relationship Management (CRM)-Anwendung sein. Zum Beispiel könnten die Teams des Vertriebs und des technischen Supports Zugriff auf dieses CRM benötigen. Die Konstruktionsabteilung? Vermutlich nicht, also würde diese nicht berücksichtigt. Im Fall des technischen Support-Teams befinden sich alle Mitarbeiter in der gleichen Stadt und arbeiten nur während der Geschäftszeiten, was bedeutet, dass der Zugriff für diese Gruppe vielleicht geografisch und zeitlich begrenzt sein sollte. Und aufgrund der Sensibilität der Daten innerhalb des CRMs sollte immer MFA verwendet werden.

Wenn wir das in Hinblick auf die Authentifizierung und die Risikofaktoren betrachten, gibt es zwei Regeln, die die Risikorichtlinie in Verbindung mit diesem Mikro-Segment definieren werden:

REGEL 1 NAME
CRM FÜR VERTRIEBSTEAM

Wer hat Zugriff: Vertrieb

Anwendung: Cloud CRM

Risikobeschränkungen: Geringes Risiko durch Mobilgeräte, geringes Risiko der geographischen Zuordnung

Authentifizierung: Passwort + Push-basierte Authentifizierung

REGEL 2 NAME
CRM FÜR DAS TEAM DES TECHNISCHEN SUPPORTS

Wer hat Zugriff: Technischer Support

Anwendung: Cloud CRM

Risikobeschränkungen: Geringes Risiko durch Mobilgeräte, Geschäftszeiten, nur USA, geringes Risiko der geographischen Zuordnung

Authentifizierung: Passwort + Push-basierte Authentifizierung

Leitfaden zur Bewertung von Geschäftsrisiken

Die Bewertung des Risikos in Ihrem Unternehmen durch die Betrachtung Ihrer potenziellen Risikoszenarien kann die einzelnen Implementierungen erheblich verbessern, da dynamische Fakten und Analysen in die Entscheidung einfließen.

ERSTELLUNG EINES RISIKO-FRAGEBOGENS

Häufige geschäftliche Anwendungsfälle, die zur Festlegung der für Sie richtigen Risikorichtlinien beitragen können:

- Vor Ort: Greifen Ihre Mitarbeiter vom Büro aus auf Unternehmensdaten und Plattformen zu?
- Dezentrales Homeoffice: Arbeiten viele Ihrer Mitarbeiter von zu Hause aus?
- Externes Café, Gemeinschaftsbüro: Erwarten Sie, dass Ihre Remote-Mitarbeiter von Orten wie Cafés aus auf das Firmennetzwerk zugreifen?
- Mobile Anwender Haben Sie mobile Mitarbeiter, die möglicherweise von unterwegs auf Arbeitsplattformen zugreifen?
- Vertikal: Ist der Service, den Ihr Unternehmen anbietet, an bestimmte Geschäftszeiten gebunden? Beispielsweise Gesundheitsämter
- Drittanbieter: Bieten Sie Auftragnehmern oder Drittanbietern Zugang zum Unternehmen?
- Gerät: Erwarten Sie von Ihren Mitarbeitern, dass sie mit ihren eigenen Geräten auf Arbeitsinformationen zugreifen?

VERSUCHEN SIE ES MIT MIKROSEGMENTIERUNG

Mikrosegmentierung verschafft Ihnen auch einen besseren Überblick über Ihre Ressourcen und Anwender. Nachstehend eine einfache Tabellenvorlage, die für diese Übung verwendet werden könnte – zumindest der erste Teil, der sich mit der Identität beschäftigt.

Zero-Trust-Mikro-Segment

Cloud CRM

Anwendergruppe	Szenario	Netzwerkstandort	Geo-Position	Zeitbeschränkungen	Geräte-Risiko	Computer-Risiko	Authentifizierung
Vertrieb	Arbeit vom Büro aus	Büronetzwerk			Geringes Risiko	Geschäftliches Laptop	Passwort
Technischer Support Finanzabteilung	Mobile Mitarbeiter	Beliebig			Geringes Risiko	Geschäftliches Laptop	MFA mit Push MFA mit QR-Code
Externe Gruppe	Arbeit nur vom Büro aus	Büronetzwerk		Geschäftszeiten	Geringes Risiko	Geschäftlicher Computer	Passwort
	Arbeit über VPN	VPN des Unternehmens		Geschäftszeiten	Geringes Risiko	Geschäftlicher Computer	MFA mit Push
IT - CRM	CRM-Berater	Beliebig	Nur USA	Geschäftszeiten			MFA mit Push
	CRM-Support	Beliebig	Nur USA		Geringes Risiko		MFA mit Push

Mikrosegmentierung Beispiel

Verwenden Sie diese Vorlage als Ausgangspunkt für die Erstellung Ihrer Mikro-Segmente und erweitern Sie sie je nach Ihren eigenen Sicherheitsanforderungen, um spezifischere Zugriffsrichtlinien zu erstellen.

Leitfaden zur Bewertung von Geschäftsrisiken – Fortsetzung

LEITFADEN ZUR BEWERTUNG VON RISIKEN	Risikofaktor		MFA	Risikoattribute		
	Benutzername	Passwort	OTP, QR-Code oder Push	Netzwerk-standort	Authentifizierung-sergebnis	Risikostufe
SZENARIO 1 Firmenmitarbeiter verbindet sich von zu Hause aus mit einer Firmenressource	✓	✓	✓	✗	Zulassen	Bestanden
SZENARIO 2 Firmenmitarbeiter verbindet sich von der Niederlassung in Seattle, Washington, aus mit einer Firmenressource	✓	✓	MFA nicht erforderlich	✓	Zulassen	Bestanden
SZENARIO 3 Anwender versucht, sich von einem unbekannten Ort aus anzumelden, um auf Unternehmensdaten zuzugreifen	✓	✓	✗ MFA nicht möglich	✗	Verweigern	Verweigern

WATCHGUARD UNIFIED SECURITY PLATFORM™

Netzwerksicherheit

Netzwerksicherheitslösungen von WatchGuard sind von Grund auf so konzipiert, dass sie einfach zu implementieren, verwenden und verwalten sind – und darüber hinaus ein Höchstmaß an Sicherheit bieten. Unsere einzigartige Herangehensweise an die Netzwerksicherheit bedeutet, jedem Unternehmen, unabhängig von seiner Größe oder seinem technischen Fachwissen, die bestmögliche Sicherheit auf Enterprise-Niveau zur Verfügung zu stellen.

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

Mit WatchGuard AuthPoint® können Sie die passwortbasierende Sicherheitslücke mithilfe von Multifaktor-Authentifizierung auf einer benutzerfreundlichen Cloud-Plattform ganz einfach schließen. Beim einzigartigen Ansatz 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.

Endpoint-Sicherheit

WatchGuard Endpoint Security ist ein Cloud-natives, fortschrittliches Endpoint-Sicherheitsportfolio, das Unternehmen jeder Art vor gegenwärtigen und zukünftigen Cyberangriffen schützt. Seine auf künstlicher Intelligenz basierende Flagship-Lösung Panda Adaptive Defense 360 verbessert unmittelbar die Sicherheitslage von Unternehmen. Sie kombiniert die Funktionen Endpoint-Schutz (EPP) und Detection and Response (EDR) mit Zero Trust Application und Threat Hunting Services.

Informationen zu AuthPoint

Die AuthPoint Multifaktor-Authentifizierung (MFA) bietet die Sicherheit, die Sie zum Schutz von Anwenderanmeldeinformationen, Vermögenswerten, Konten und Informationen benötigen. Verwalten Sie AuthPoint von überall und jederzeit mit einer benutzerfreundlichen, Cloud-basierten Verwaltungsplattform, die eine risikobasierte Oberfläche für die Richtlinienverwaltung bietet. Auf diese Weise garantieren Sie die bestmögliche Zero-Trust-Umgebung.
Ermöglichen Sie Ihrem Unternehmen mit dem leistungsstarken Schutz von AuthPoint MFA ein souveränes und sorgenfreies Arbeiten. Weitere Informationen

Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Mehr als 18.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 250.000 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 mittelständische und 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 asiatisch-pazifischen Raum.
Weitere Informationen finden Sie unter WatchGuard.de.

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