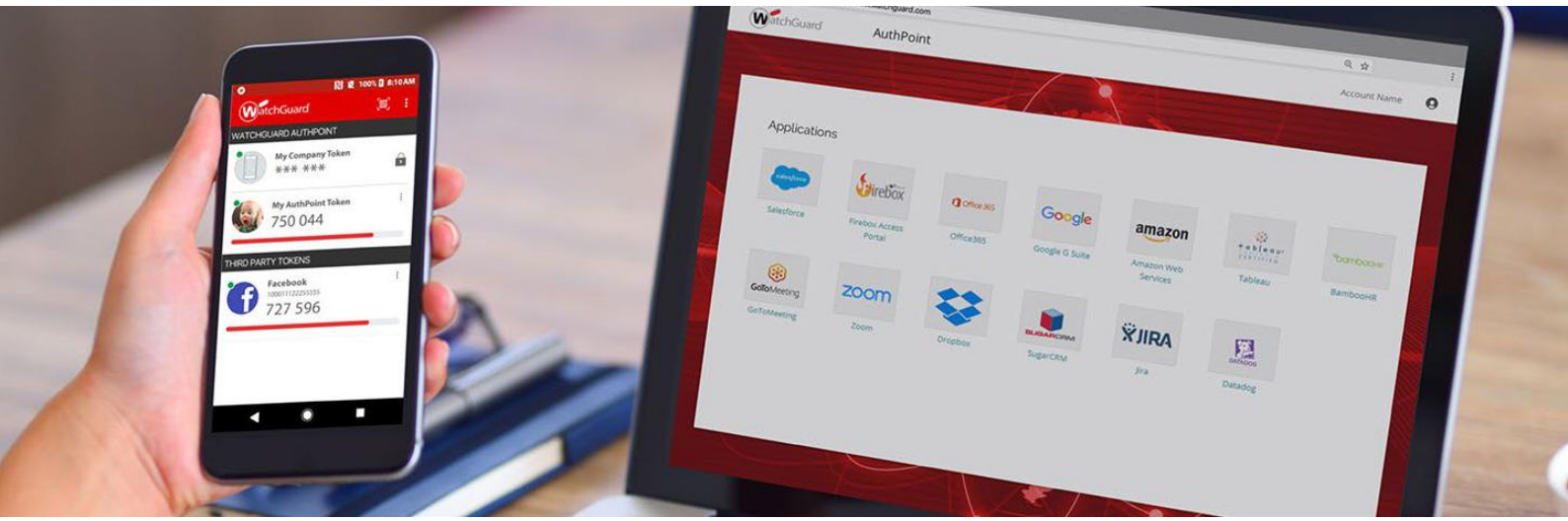
Schutz der Benutzeridentität und Sicherung des Geschäftsvertrauens durch Multifaktor-Authentifizierung

Inhaltsverzeichnis



DIE EVOLUTION DER AUTHENTIFIZIERUNG – UNSER BISHERIGER WEG UND UNSER HEUTIGER STAND

Das Authentifizierungsproblem

Das Internet hat die Art und Weise verändert, wie wir Geschäfte tätigen. Ein schneller Internetzugang zu Hause und an Millionen von WLAN-Hotspots an öffentlichen Orten ermöglicht es Mitarbeitern, überall zu arbeiten – zu Hause ebenso wie in Hotels und Cafés. Unternehmensdaten werden nicht mehr ausschließlich zentral in Serverräumen oder Rechenzentren vor Ort gespeichert, sondern verteilen sich über die Cloud, CMR, E-Mail-Server und Webportale.

Täglich authentifizieren sich Mitarbeiter bei mehreren dieser Dienste. Zuerst an ihrem Computer. Anschließend bei einem E-Mail-Server und vielleicht bei einer Cloud-Anwendung. Wenn sie nicht persönlich im Büro sind, verbinden sie sich häufig über ein VPN mit dem Netzwerk. Und wo befinden sich die Anmeldedaten der Benutzer? Durch den Datenverkehr werden Benutzeranmeldedaten über WLAN-Verbindungen und öffentliche Netzwerke übertragen.

Wenn diese Anmeldedaten an irgendeinem Punkt ausgelesen werden, wie wahrscheinlich ist es, dass dasselbe Passwort auch bei den meisten anderen Diensten verwendet wird? Die Chancen dafür stehen gut. Wer vergibt bei all den Anmeldedaten, die er sich täglich merken muss (für Unternehmenszugriff, Bank, Kreditkarten, Online-Shopping-Websites, soziale Medien, mobile Speicher usw.), freiwillig unterschiedliche Passwörter für all diese Dienste?

Das Passwort, das Sie für den Zugang zur Website Ihres bevorzugten Supermarktes verwenden, ist mit großer Wahrscheinlichkeit dasselbe Passwort, mit dem Sie sich an Ihrem Computer anmelden oder, noch schlimmer, am VPN zur Verbindung mit dem Unternehmensnetzwerk. Das Problem der Passwörter erstreckt sich also nicht nur auf unser Unternehmensnetzwerk. Wir wissen nicht, ob ein Mitarbeiter dasselbe Passwort für jede private Website nutzt oder es sogar irgendwann an eine andere Person weitergegeben hat.

Sie können nicht alleine auf den Schutz durch Passwörter vertrauen. Man kann sie weitergeben. Aufschreiben. Auslesen. Erraten. Knacken. Stehlen.

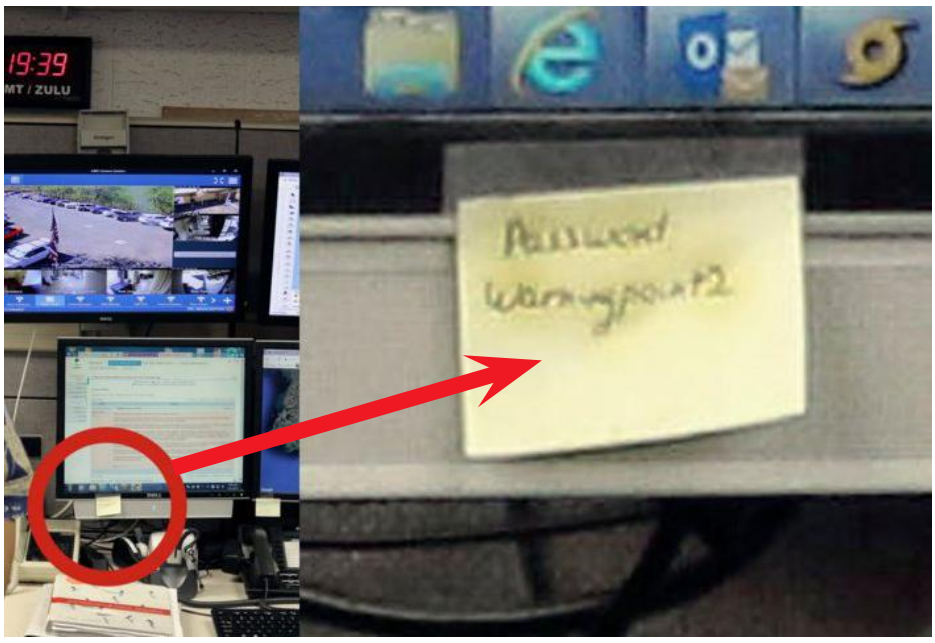
80%

DER DER VERSTÖSSE IM BEREICH HACKING STEHEN IM ZUSAMMENHANG MIT DER VERWENDUNG VERLORENER ODER GESTOHLENER ZUGANGSDATEN.

Verizon Data Breach Investigations Report, 2020

Gestohlene Zugangsdaten und das Dark Web

Das Dark Web ist eine Sammlung anonymer Websites. Diese sind zwar öffentlich zugänglich, verbergen aber die IP-Adressen und machen es so den Anwendern unmöglich, den Host zu identifizieren. Es kommt sehr häufig vor, dass sensible Informationen, die durch Datenschutzverletzungen verfügbar gemacht wurden, schließlich im Dark Web illegal zum Verkauf angeboten werden.



Laut dem Bericht „Global State of Cybersecurity in Small and Medium-Sized Businesses“ von 2019 kam es in 63 Prozent der befragten Unternehmen im vergangenen Jahr zu einem Vorfall, bei dem sensible Kunden- und Mitarbeiterdaten entwendet wurden.

Man denke beispielsweise an die jüngste Datenbank mit Zoom-Anmeldeinformationen, die im April 2020 im Dark Web veröffentlicht wurde. Anzeichen dafür, dass es bei Zoom zu einer Sicherheitsverletzung gekommen ist, gibt es allerdings nicht. Tatsächlich wurde die Datenbank mit Anmeldedaten aufgebaut, die im Dark Web gefunden und gegen Zoom auf ihre Aktualität getestet wurden. Und mehr als 500.000 Anmeldedaten funktionierten für Zoom-Accounts.

Auch wenn Ihr Unternehmen vielleicht nicht gehackt wurde, könnten die Anmeldedaten von Mitarbeitern nach einer Sicherheitsverletzung in einem von ihnen genutzten Dienst, wie LinkedIn oder Facebook, im Dark Web verfügbar sein. Und da Anwender dazu neigen, dieselben Passwörter für mehrere Dienste zu verwenden, ist die Wahrscheinlichkeit groß, dass ein Firmenpasswort dasselbe ist wie das, das durch eine Sicherheitsverletzung bei einem anderen Dienst offengelegt wurde.

Multifaktor-Authentifizierung

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, Schlüssel
- Körperteil: Fingerabdruck, Gesichtserkennung

Die Technologieentwicklung, besonders die zunehmende Smartphone-Nutzung und App-Entwicklung, 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 vier Faktoren zur Authentifizierung.
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.

WARUM MULTIFAKTOR-AUTHENTIFIZIERUNG (MFA)?

Im Folgenden finden Sie Standard-Authentifizierungsfaktoren, die MFA-Lösungen nutzen können:

1. **Informationen**

   (Ihr Passwort)

2. **Ressource**

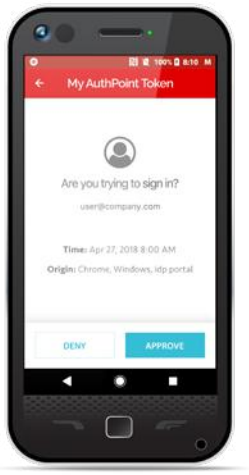
   (Token auf Ihrem Telefon)

3. **Ressource**

   (DNA eines Telefons)

4. **Körperteil**

   (Fingerabdruck für den Zugriff)



Sicherheit und Benutzererfahrung

Die ersten Authentifikatoren bzw. Einmalpasswort-Token wurden üblicherweise als Hardwaregerät ausgegeben und waren kaum größer als ein Schlüsselanhänger (Key Fob). Die Einmalpasswörter änderten sich meist alle 60 Sekunden. Um sich bei einem System zu authentifizieren, musste der Benutzer das Passwort gefolgt von dem im Display angezeigten Einmalpasswort eingeben. Wenn sein Passwort also beispielsweise „meinpasswort" lautete und der aktuell angezeigte Token „122134" war, musste der Benutzer Folgendes eingeben:

```
meinbenutzername
meinpasswort122134
```

Ganz abgesehen davon, dass der Benutzer den Key Fob überallhin mitnehmen musste. Die Tatsache, dass es sich um einen physischen Key Fob handelte, machte die Sache noch schwieriger. Wenn Sie jemals einen Key Fob-Token verwendet haben, haben Sie diesen höchstwahrscheinlich schon einmal zu Hause vergessen und mussten eine andere Person bitten, Ihnen das Einmalpasswort (wiederholt) telefonisch mitzuteilen, oder Sie gingen auf Reisen, während sich der Token am Autoschlüssel befand – und zwar zu Hause.

Sicherheitsexperten bemerkten häufig, dass sich die Benutzerfreundlichkeit umgekehrt proportional zur Sicherheit verhalte. Dies war eine Tatsache und es sollte noch schlimmer kommen. Benutzer mit vernetzten Token oder Smartcards und entsprechenden Lesegeräten mussten Software oder Middleware installieren und digitale Zertifikate verwalten – bei explodierenden Gesamtbetriebskosten. Und wenn sie diese Tools zur Authentifizierung bei mobilen Anwendungen nutzen mussten, wurde es besonders kritisch.

Mit dem Aufkommen von Mobiltelefonen wurden auch SMS immer beliebter und nun konnten SMS zum Versenden von Einmalpasswörtern verwendet werden – solange man guten Empfang hatte. Auf Auslandsreisen war es nicht ungewöhnlich, dass die SMS gar nicht oder erst Stunden später ankam. Und bei der Authentifizierung über einen Smartphone-Browser wurde der Wechsel zwischen Apps zum Albtraum. Nachdem jahrelang nach Möglichkeiten gesucht worden war, die SMS-basierte Authentifizierung zu umgehen, erklärte das National Institute of Standards and Technology (NIST) die SMS im Jahr 2016 schließlich zu einer veralteten Methode der Zwei-Faktor-Authentifizierung.

Bis zum Ende der 2000er Jahre wurden Mobiltelefone immer besser, doch es gab noch immer verschiedene Betriebssysteme und Anbieter, z. B. Symbian, BlackBerry OS, Windows Mobile, BREW usw. Eine App für ein Telefon zu entwickeln war schwierig. Man benötigte die SDKs des Anbieters sowie eine Auswahl verschiedener Telefonmodelle. Das Ausführen einer Java-App involvierte die Installation von J2ME-Software und die Ergebnisse waren optisch nicht ansprechend, bis der Smartphone-Markt zu wachsen begann, was von Android und iOS vorangetrieben wurde. Dies ermöglichte Unternehmen die Entwicklung professioneller Apps unter Berücksichtigung von Richtlinien zur Benutzerfreundlichkeit, sodass Menüs, Schaltflächen usw. dasselbe Format hatten. Ab diesem Zeitpunkt wurden mobile Token immer beliebter.

Das Smartphone wurde Teil unseres Lebens und so selbstverständlich wie das Tragen von Kleidung. Wenn man das Smartphone bei sich trägt, werden Hardware-Token überflüssig.

Und die Push-Technologie veränderte schließlich die traditionelle Abwägung von Benutzerfreundlichkeit und Sicherheit. Sie ermöglichte eine höhere Sicherheit bei verbesserter Benutzererfahrung.

Push-Technologie

BlackBerry stellte diese „Push-Technologie" als Tool vor, das die Produktivität tatsächlich verbessern konnte. Der größte Vorteil bei einem BlackBerry bestand darin, dass man eingehende E-Mails auf dem Telefon beinahe sofort sah. Die rot blinkende Leuchte des BlackBerry wurde Teil unseres Lebens.

Mit der Weiterentwicklung von iPhones und Android-Geräten wurden Push-Dienste für unterschiedliche Anwendungen genutzt: Chat, Nachrichten, E-Mails. Man musste das Telefon nicht mehr aktivieren und sich mit einem Dienst verbinden, denn Benachrichtigungen gingen über dieses neue System ein.

Dies eröffnete auch für die MFA ganz neue Möglichkeiten. Anstatt die App für mobile Token zu öffnen, das Einmalpasswort abzulesen und es einzugeben, konnte man jetzt Authentifizierungsanfragen auf dem Telefon empfangen, die detailliertere Informationen enthielten, beispielsweise wer die Authentifizierung erbat und wo. Dann musste man nur noch eine Schaltfläche drücken, um die Anfrage zu genehmigen oder abzulehnen. Bei korrekter Implementierung wurde dann eine Verbindung zum Dienst hergestellt, der den Zugriff angefordert hatte, und das einzigartige Einmalpasswort wurde zurückgesendet, ohne dass der Benutzer überhaupt erfuhr, wie es lautete.

Inzwischen gibt es eine Methode, die eine höhere Benutzerfreundlichkeit bietet und ebenfalls nur das Drücken einer Schaltfläche erfordert, sodass Sie genau wissen, wo Sie sich sicher authentifizieren – nämlich MFA.

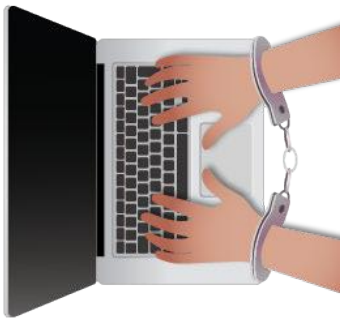
UNSER HEUTIGER STAND

Die COVID-Pandemie hat Millionen von Arbeitnehmern in ihre Wohnungen verlagert. Das Internet wurde dann zu ihrer täglichen Pendelstrecke. Auch Arbeitszeiten gibt es irgendwie nicht mehr. Arbeiten von zu Hause bedeutet, dass das – Heim – Büro immer verfügbar ist.

Worin bestehen einige der erhöhten Risiken, wenn eine große Anzahl von Menschen ihr Leben aus der Entfernung lebt? Seien wir ehrlich: Mitarbeiter, die von zu Hause aus arbeiten, sind ohne die Sicherheit von Firewalls und WLAN-Netzwerken des Unternehmens stärker gefährdet. Leider nutzen Hacker bereits die Gelegenheit für Angriffe auf anfällige Benutzer. Angesichts der beispiellosen Ereignisse, die wir derzeit erleben, ist es unerlässlich, über den Schutz von Mitarbeitern an entfernten Standorten nachzudenken. Wir müssen gewährleisten, dass der Zugriff auf Unternehmensressourcen und -informationen sicher ist, um Datenverluste und wirtschaftliche Einbußen zu verhindern.

Nach dem Ende der Pandemie werden Unternehmen die Möglichkeit der Beibehaltung von Remote-Arbeit oder eines hybriden Modells evaluieren und man wird auf das Arbeiten von Zuhause nicht mehr verzichten wollen. In Bezug auf die Cybersicherheit bedeutet das, dass die Idee eines zentralisierten und gut definierten Netzwerks schlicht nicht mehr ausreicht.

Das Konzept des Zero-Trust-Ansatzes hat daher massiv an Boden gewonnen. Das Netzwerk besteht heute aus Anwendungen, Diensten und Gruppen von Benutzern und Geräten, die Zugriff auf diese benötigen. Benutzer und Geräte sind überall und können daher nicht vertrauenswürdig sein. Die Verwendung von MFA wurde zu einer Voraussetzung, um Vertrauen zu schaffen, besonders jetzt in diesem neuen hybriden Arbeitsmodell.



SCHUTZ IHRER RESSOURCEN MIT MFA

Das neue Unternehmensnetzwerk

Ein Netzwerk besteht nicht nur aus Desktop-Geräten und Servern, die hinter einer Firewall sicher miteinander verbunden sind. Die Unternehmensressourcen verteilen sich über Cloud-Anwendungen, Netzwerkserver und dezentrale Computer. Sie alle haben unterschiedliche Benutzer und Passwörter und manchmal vorübergehenden Zugriff über Drittanbieter. Dies birgt Risiken für die unterschiedlichsten Angriffe. Meist beginnen diese mit einem einfachen Benutzernamen und Passwort, die ausgelesen, geknackt oder durch Social Engineering weitergegeben wurden.

Wir werden Ihnen demonstrieren, wie Sie die WatchGuard AuthPoint-Lösung zum Schutz Ihrer Anwendungen mit MFA nutzen können.

VPNs/Fernzugriff

Fernzugriff auf das Unternehmensnetzwerk ist entscheidend für dezentrale Benutzer und Mitarbeiter auf Dienstreise, um auf Unternehmensserver und interne Informationen zuzugreifen. Doch es reicht bereits

- ein Benutzer mit einem schwachen Passwort, das geknackt wurde
- ein Benutzer mit einem Keylogger-Trojaner auf dem Computer
- ein Benutzer, der sein Passwort oder sogar Einmalpasswort weitergibt

Und schon erhält der Hacker irgendwo auf der Welt Zugriff auf das Netzwerk, meist mit denselben Rechten wie eine Person, die sich am Unternehmensstandort befindet und mit dem Netzwerk verbunden ist.

Bevor Benutzer auf VPNs zugreifen dürfen, ist eine zusätzliche Identitätsprüfung notwendig, die über ein Passwort hinausgeht. Außerdem sollte die MFA-Lösung eine schnelle und einfache Integration mit Firewalls und Fernzugriffs-Gateways über das RADIUS-Protokoll ermöglichen. Beim WatchGuard AuthPoint-MFA-Dienst beispielsweise kann die Einrichtung innerhalb weniger Minuten und auf zwei Arten erfolgen:

1. **Verwendung von Passwort + Einmalpasswort**

   Anders als bei der bloßen Eingabe von Benutzernamen und Passwort in einem VPN-Client oder Browser-basierten VPN ohne Client muss der Benutzer hierbei einfach das Einmalpasswort – üblicherweise sechs Ziffern – an das Passwort anhängen. Die Firewall empfängt die Anfrage und leitet sie an AuthPoint weiter, wo sowohl Passwort als auch Einmalpasswort validiert werden.

2. **Verwendung von Passwort + Push-Technologie**

   Diese Methode bietet die beste Benutzererfahrung, da sich für den Benutzer kaum etwas ändert. Der Benutzer gibt wie zuvor Benutzernamen und Passwort ein. Der Unterschied besteht darin, dass AuthPoint eine Authentifizierungsanfrage als Push-Mitteilung sendet. Der Benutzer empfängt diese Mitteilung in seiner App und sieht genau, wer sich wo authentifizieren möchte. Wenn der Benutzer die identifizierte Person ist, muss er die Anfrage lediglich durch Auswählen einer Schaltfläche bestätigen.

Authentifizierungsmethode	Vorteile	Nachteile
Traditionelles Einmalpasswort	• Typische, bekannte Methode, die seit mehr als 20 Jahren eingesetzt wird	• Anfällig für Social Engineering • Benutzer muss das Einmalpasswort jedes Mal eingeben • Kann für Benutzer verwirrend sein (Passwort + Einmalpasswort oder Einmalpasswort + Passwort?)
Push-Technologie	• Bessere Benutzererfahrung; Benutzer muss Anfrage nur genehmigen oder ablehnen • Mehr Transparenz; Push-Mitteilung zeigt Kontext der Authentifizierung an und reduziert die Wahrscheinlichkeit von Social Engineering • Höhere Sicherheit; in Push-Mitteilung gesendetes Einmalpasswort kann nicht kopiert oder gestohlen werden	• Erfordert eine Datenverbindung über das Mobiltelefon (Online-Authentifizierung)

Cloud-Anwendungen

Mit der Zunahme von Cloud-Anwendungen und -Angeboten wurden immer mehr einfache, aber essentielle Dienste in die Cloud verschoben, beispielsweise E-Mail- und Webserver. Diese Server innerhalb des Netzwerks zu installieren und zu verwalten ist heutzutage undenkbar. Cloud-Dienste bieten nahezu alle Möglichkeiten, darunter CRMs, ERPs, Entwicklungsplattformen usw.
Mit all diesen Diensten treten neue Herausforderungen auf:

- Benutzer müssen sich unterschiedliche Passwörter für die Dienste merken und diese verwalten
- Benutzer müssen URLs mit Lesezeichen versehen und alle Dienste organisieren, auf die sie potenziell Zugriff haben
- Es muss sichergestellt werden, dass kompromittierte Anmeldedaten keinen Zugriff auf andere Dienste ermöglichen, die von überall aus problemlos aufgerufen werden können

Die Entwicklung des SAML (Security Assertion Markup Language)-Protokolls löste die meisten dieser Probleme. Die Implementierung basiert auf zwei wichtigen Einheiten:

- Identity Provider (IdP): Eine Einheit, die für die ordnungsgemäße Authentifizierung und Identifikation von Benutzern verantwortlich ist
- Service Provider (SP): Jede Einheit, die in einem Vertrauensverhältnis zu einem IdP steht und diesen verwendet, um die Identität zu verifizieren

Ganz einfach gesagt: Ein SP steht in einem Vertrauensverhältnis zum IdP, das bedeutet, wenn der IdP einen Benutzer authentifiziert und identifiziert, verlässt sich der SP auf diese Informationen und ermöglicht dem Benutzer Single Sign-On (SSO) beim Dienst – selbst, wenn der Benutzer für den Dienst ein anderes Passwort nutzt. Beispiele für Service Provider sind unter anderem Firebox® Access Portal, Salesforce, Google Apps, BambooHR, Jira und Office365.

Vor diesem Hintergrund leuchtet es ein, dass der IdP der Schlüssel zu allem ist. Sobald der IdP den Benutzer authentifiziert, hat dieser SSO-Zugriff auf alle Cloud-Anwendungen, die diesem Benutzer zur Verfügung gestellt wurden. Die Auswahl des richtigen Identity Provider ist daher entscheidend.

Cloud-basierte MFA-Lösungen können einen IdP-Dienst bereitstellen. Beispielsweise steht einem Abonnenten innerhalb unserer AuthPoint-Lösung ein exklusives Portal zur Authentifizierung von Benutzern zur Verfügung. Sobald der Benutzer authentifiziert wurde, hat er Zugriff auf die Cloud-Anwendungen, die mit seiner Gruppe verknüpft sind.

Dies bietet enorme Vorteile bezüglich Sicherheit und Benutzererfahrung.

- Der Benutzer muss nur die IdP-Portalseite mit Lesezeichen versehen
- Die Haupt-Authentifizierungsmethode kann für erhöhte Sicherheit konfiguriert werden, z. B. Push-basierte Authentifizierung statt traditioneller Einmalpasswörter
- Der Benutzer muss sich nicht alle Passwörter für die Cloud-Anwendungen merken. Sobald das AuthPoint-IdP-Portal den Benutzer authentifiziert, wird ein Vertrauensverhältnis zu den Cloud-Anwendungen hergestellt
- Mit Gruppenrichtlinien können Administratoren genau festlegen, welche Anwendungen jeder Benutzer aufrufen darf
- Wenn Anmeldedaten kompromittiert wurden, erfolgt weiterhin eine MFA, doch der Zugriff durch unbefugte Cyberkriminelle wird blockiert

Anmeldung am Laptop/Computer

Wie bereits erwähnt, können Benutzeranmeldedaten gestohlen, geknackt oder erraten werden. Ein unbeaufsichtigter Computer kann potenziell von einer Person genutzt werden, die im Besitz dieser Anmeldedaten ist. Dies kann auf dem Unternehmensgelände geschehen oder bei dezentralen oder reisenden Mitarbeitern. Die Verwendung von MFA für die Anmeldung am Computer schützt nicht nur den Anmeldevorgang, sondern bietet auch eine bessere Benutzererfahrung.

AuthPoint Logon Agent ist eine Komponente, die auf Windows- und macOS-Computern installiert werden kann und MFA-Funktionen innerhalb des Anmeldevorgangs hinzufügt. Nach Eingabe des Benutzernamens und Passworts erhält der Benutzer eine Push-Mitteilung innerhalb der AuthPoint-App und wird gefragt, ob er die Anmeldung am Computer gestattet.
Die Benutzererfahrung ist sogar noch besser, wenn der Benutzer den Computer sperrt. In diesem Fall müssen Benutzername und Passwort nicht erneut eingegeben werden. Sie müssen lediglich die Anmeldung über die Push-Mitteilung bestätigen.

Dank der Vielseitigkeit der Lösung gibt es auch eine Möglichkeit zur Anmeldung am Computer, wenn keine Internetverbindung verfügbar ist – den Offline-Modus. Dies ist wichtig, wenn der Laptop beispielsweise auf einem Flug genutzt wird. In diesen Fällen kann eine Abfrage/Antwort über einen QR-Code mit verschlüsselten Daten verwendet werden, die nur der AuthPoint-Authentifikator des Benutzers lesen, entschlüsseln und entsprechend beantworten kann.

SCHRITT 1

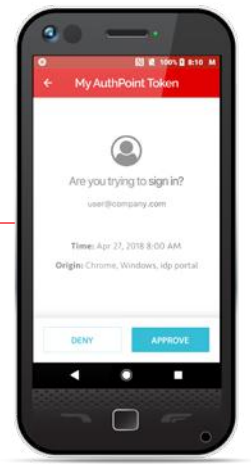
Auf „Push senden“ klicken

SCHRITT 2

Anmeldeanfrage für PC über AuthPoint-App bestätigen

SCHRITT 3

Anmeldung abgeschlossen!



Webportale

Einige Unternehmen stellen Dienste und Lösungen über Webportale bereit. Sie bieten zudem Benutzerkonten an, um eine bessere Benutzererfahrung zu ermöglichen, insbesondere für Unternehmen in Branchen wie Bildung, Gesundheitswesen und Einzelhandel, um nur einige zu nennen. Ein Benutzerkonto kann die Art und Weise verbessern, wie Menschen mit verschiedenen Informationen interagieren, z. B. mit Gesundheitsdaten, eLearning oder anderen Diensten, die eine sichere Identifizierungsmethode erfordern, insbesondere angesichts der zunehmenden Durchsetzung von Datenschutzgesetzen auf der ganzen Welt.

Moderne Geschäftsanwendungen implementieren Standards zur Unterstützung der MFA-Authentifizierung von mehreren Anbietern, einschließlich Web-Single Sign-On (SSO), unter Verwendung von Protokollen wie SAML. Dies ist zwar die am besten geeignete Lösung, doch kann ihre Implementierung schwer und zeitaufwändig sein. Mit APIs für die Authentifizierung lässt sich MFA schnell und kostengünstig zu SSO-Webportalen oder selbstentwickelten Anwendungen hinzuzufügen, ohne dass man ein tiefes Verständnis dafür haben muss, wie Multifaktor-Authentifizierung funktioniert.

Vorteile cloudbasierter MFA-Lösungen

Die cloudbasierte MFA bietet viele Vorteile gegenüber lokalen MFA-Lösungen.

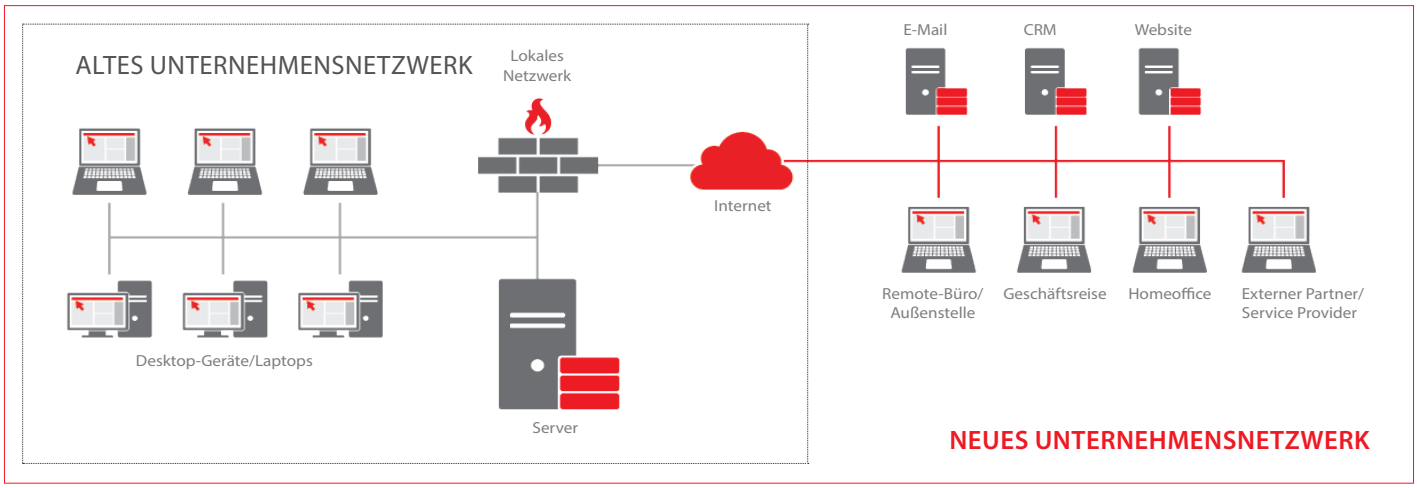
- Keine Installation erforderlich
- Schnelle Bereitstellung
- Keine Investitionen in Hardware oder Betriebssysteme notwendig
- Kein Grund zur Sorge um Patches, Betriebszeit, Leistung oder Hochverfügbarkeit
- Management durch jeden von überall aus möglich

Bei einer lokalen Authentifizierungslösung kann die Einrichtung, Installation und Inbetriebnahme mehr als einen Tag dauern. Mit einer Cloud-basierten MFA wird in weniger als einer Minute eine neue Umgebung für einen Kunden geschaffen und kann sofort konfiguriert werden. Eine Implementierung kann in weniger als einer Stunde abgeschlossen werden.

Remote-Mitarbeiter und verteilte Netze

Wie bereits beschrieben, besteht ein Netzwerk nicht nur aus Desktop-Geräten und Servern, die hinter einer Firewall sicher miteinander verbunden sind. Die Ressourcen eines Unternehmens verteilen sich über Cloud-Anwendungen, Netzwerkserver und dezentrale Computer. Sie alle haben unterschiedliche Benutzer und Passwörter und manchmal vorübergehenden Zugriff über Drittanbieter. Dies birgt Risiken für die unterschiedlichsten Angriffe. Meist beginnen diese mit einem einfachen Benutzernamen und Passwort, die ausgelesen, geknackt oder durch Social Engineering weitergegeben wurden.

Wir demonstrieren Ihnen, wie Sie die WatchGuard AuthPoint-Lösung zum Schutz Ihrer Anwendungen mit MFA nutzen können.



EINEN ZERO-TRUST-ANSATZ OHNE MFA GIBT ES NICHT

Da Angriffe immer ausgeklügelter werden und die Erweiterung des VPN-Schutzes nicht ausreicht, müssen Unternehmen ihr Sicherheits-Framework überdenken, um neue und beschleunigte Bedrohungen zu bekämpfen. 2010 hat Forrester Research Inc. zuerst den Begriff „Zero-Trust" geprägt, der sich auf den Sicherheitsansatz „never trust, always verify" (niemals vertrauen, immer prüfen) bezieht.

Während ein traditionelles Netzwerk auf der Idee des inhärenten Vertrauens aufbaut, geht ein Zero-Trust-Framework davon aus, dass jedes Gerät und jeder Benutzer, 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.

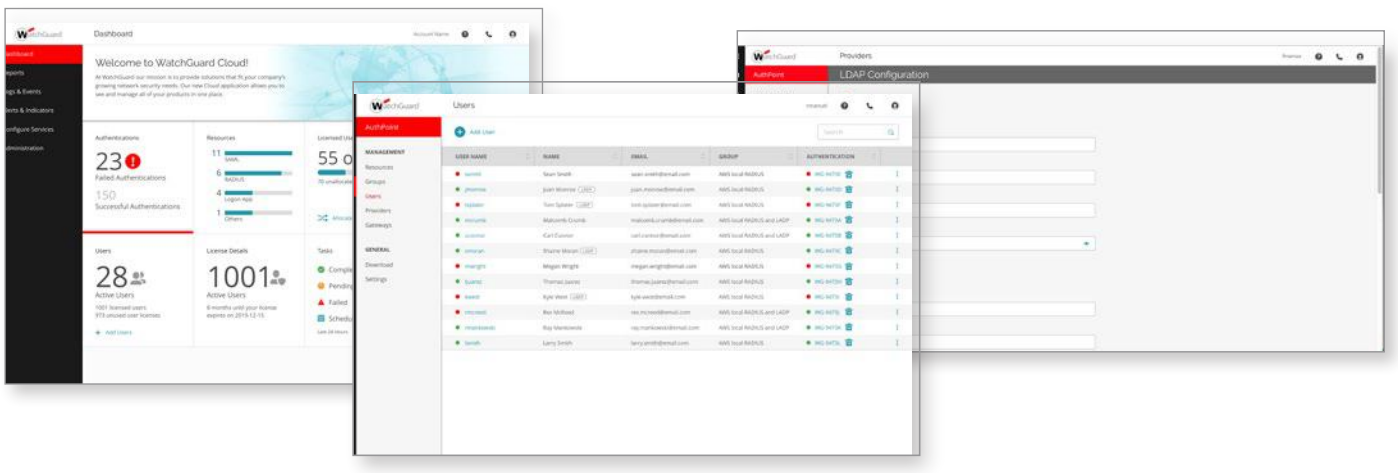
Die Pandemie hat Unternehmen jeder Größe veranlasst, den Zero-Trust-Ansatz zu übernehmen. Benutzer, die sich von überall und zu jeder Zeit mit Diensten verbinden, lokale Anwendungen, die in die Cloud migriert wurden – so sieht das perfekte Szenario für einen Mikrosegmentierungsansatz aus, wie er von der Zero-Trust-Netzwerkspezifikation empfohlen wird.

Die gute Nachricht ist, dass Sie mit der Implementierung von MFA den ersten Schritt in Richtung dieses Ansatzes tun. Die Hauptprinzipien des Zero-Trust-Konzepts konzentrieren sich auf die Überprüfung der Benutzeridentität, der Geräte, des Zugriffs und der Dienste. Das heißt, es werden keine Annahmen über die Sicherheit getroffen und das Risiko für Schwachstellen wird deutlich reduziert. Wenn Sie die Einführung dieses Modells in Betracht ziehen, finden Sie hier drei Schlüsselbereiche für die Implementierung von Zero-Trust-Netzwerken:

1. **Identifizierung von Benutzern und Geräten:** Sie sollten 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.

2. **Bereitstellung eines sicheren Zugangs:** Beschränken Sie den Zugriff auf geschäftskritische Systeme und Anwendungen nur 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 Benutzer, Geräte oder Anwendungen zu beschränken. Single Sign-On (SSO)-Technologien, kombiniert mit MFA, können die Zugriffssicherheit verbessern und Anwender müssen sich weniger Passwörter merken.

3. **Ständige Überwachung:** Überwachen Sie den Zustand und den Sicherheitsstatus 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.



WATCHGUARD AUTHPOINT STEHT FÜR VEREINFACHTE AUTHENTIFIZIERUNG

WatchGuard AuthPoint wurde für eine benutzerfreundliche, kostengünstige und umfassende Multifaktor-Authentifizierung entwickelt. Der Schwerpunkt liegt auf dem wichtigsten Faktor für jedes Unternehmen: Dem Schutz des Zugriffs auf Computer, Anmeldedaten von Benutzern, Netzwerke und Cloud-Anwendungen.

Zu den anerkanntesten Funktionen von AuthPoint gehören die optimale Benutzererfahrung, die schnelle Bereitstellung sowie eine eindeutige Mobilgeräte-DNA. Diese dient zur Abgleichung des Telefons des autorisierten Benutzers bei der Gewährung des Zugriffs auf Systeme und Anwendungen.

Einfach und vor allem nahtlos

Im Vergleich zu anderen MFA-Lösungen machen die folgenden Bereiche AuthPoint überzeugend einfach und absolut sicher:

- Cloudbasiert: Keine Installation von Datenbanken oder Servern.
- Assistenten: In WatchGuard Cloud stehen interaktive Assistenten zur Verfügung, die neue Benutzer bei der Konfiguration von AuthPoint anleiten, einschließlich VPN-Konfiguration, Benutzer-Synchronisation von Active Directory und mehr.
- Mobile AuthPoint-App: intuitives Design, verfügbar in 13 Sprachen und damit weltweit benutzerfreundlich.
- Web-Single Sign-On: Vorkonfiguriertes, cloudbasiertes Portal. Anmeldung mit nur einem Passwort bei allen Cloud-Anwendungen Ihres Unternehmens.
- Dokumentierte Integrationen für Administratoren und Endanwender: Mehr als 120 dokumentierte Integrationen, um Administratoren die Konfiguration und die Durchführung AuthPoint-Upgrades zu erleichtern.

Weitere Informationen zu WatchGuard AuthPoint finden Sie unter **www.watchguard.com/authpoint.**

ÜBER WATCHGUARD

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, Endpoint-Sicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Über 18.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens und sorgen somit für den Schutz von 250.000 Kunden. Die Philosophie von WatchGuard ist es, hochprofessionelle Sicherheitslösungen 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.com/de.

Wenn Sie mehr über WatchGuard, unsere Werbeaktionen und Updates erfahren möchten, folgen Sie uns auf Twitter @WatchGuard, auf Facebook oder auf unserer Seite auf LinkedIn. Lesen Sie auch unseren InfoSec-Blog Secplicity. Darin wird einfach und nachvollziehbar beschrieben, wie Sie den neuesten Bedrohungen am besten begegnen. Hier geht's zum Blog: www.secplicity.org

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.de