Einminütiges Webinar: Zero Trust in Practice

Keine Zeit, das Webinar Zero Trust in Practice anzusehen? Keine Sorge, hier erfahren Sie, worum es geht.

Derzeit herrscht ein regelrechter Hype um das Thema Zero Trust-Sicherheit, aber es steckt mehr dahinter.

Vertrauen war früher eine Ja-oder-Nein-Entscheidung, die auf Netzwerkebene getroffen wurde. Seit Unternehmen zu Mobil- und Cloud-Diensten übergehen, ist eine klare Außengrenze des Netzwerks aber nicht mehr gegeben. Es ist heute nicht mehr möglich, Vertrauen vom Netzwerk abhängig zu machen, und Vertrauen ist keine einfache Ja-oder-Nein-Frage mehr.

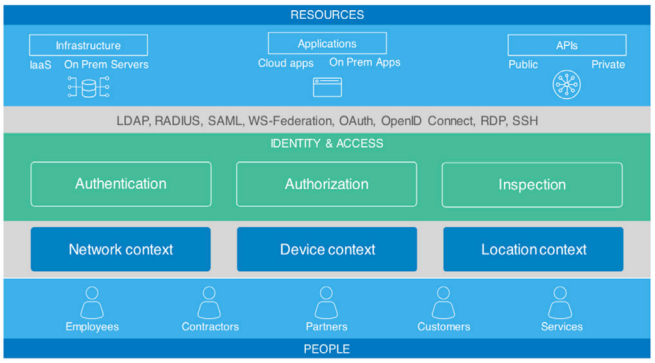
Wer die Überlegungen rund um das **Zero Trust-Modell** kennt, will heute von den praktischen Vorteilen für die Sicherheit profitieren, die das Konzept verspricht. Unabhängig davon, wo Sie auf dem Weg zu Zero Trust-Sicherheit stehen, fragen Sie sich wahrscheinlich, wie Sie diese Konzepte und Architekturen für Ihr Unternehmen nutzbar machen können.

Warum man mit Identität anfangen sollte

Eine einheitliche Identitätsschicht bildet die Grundlage für die Einrichtung flexibler Zugriffskontrollen, die fortlaufende Entwicklung von Richtlinien und zunehmend intelligente Systeme. Zugriff wird anhand von Vertrauen gewährt und dieses Vertrauen hängt vom Kontext ab.

So entsteht kontextabhängiges Vertrauen

Schritt 1: Verschaffen Sie sich einen Überblick über Ihre Ressourcen und die Identitäten Ihrer Benutzer. Gehören sie einer risikoreichen Benutzergruppe an? Auf welche Ressource möchten sie zugreifen? Handelt es sich um ein risikoarmes Tool oder eine risikoreiche Infrastruktur?



Schritt 2: Betrachten Sie den Kontext des Authentifizierungsschritts: Welchen Kontext bilden Netzwerk, Gerät und Standort? Hat sich die IP-Adresse geändert? Melden die Benutzer sich aus einem IP-Bereich des Unternehmens an?

Von einem neuen oder verwalteten Gerät aus? Aus einer neuen Stadt, einem neuen Land oder sogar einer gesperrten Geolocation?

Schritt 3: Kombinieren Sie die Ergebnisse aus Schritt 1 und 2, um kontextabhängig zu reagieren: zur Zwei-Faktor-Authentifizierung wechseln, den Zugriff erlauben/verwehren oder eine Sicherheitswarnung auslösen?

Schritt 4: Lassen Sie getrennte Zugriffsrichtlinien in Bezug auf den Kontext hinter sich, indem Sie laufend das Gesamtrisiko der Anmeldung bewerten.

Richtig umgesetzt, schöpfen Sie so das volle Potenzial von Zero Trust aus: Die richtigen Personen haben die richtigen Zugriffsrechte für die richtigen Ressourcen im richtigen Kontext, und der Zugriff wird laufend geprüft. Dies sollte natürlich mit möglichst geringen Reibungsverlusten erreicht werden. Die Sicherheit sollte die Benutzer unterstützen – und nicht ausbremsen, weil sie zwischen verschiedenen Netzwerken wechseln oder verschiedene Passwörter eingeben müssen.

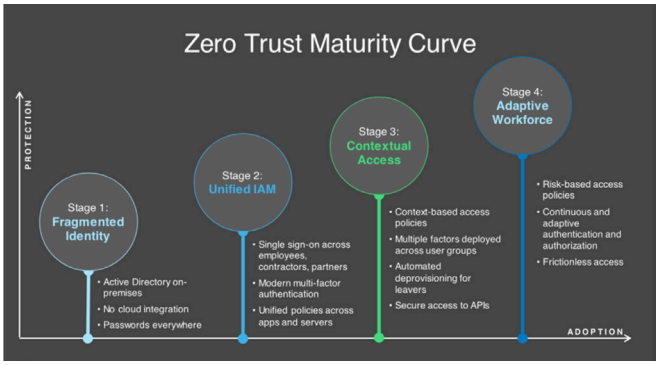
Einminütiges Webinar: Zero Trust in Practice

Problempunkte

Mit Zero Trust lösen wir einige wichtige IT- und Sicherheitsprobleme: mehrere Benutzerspeicher ohne zentrale Informationsquelle („Source of Truth“), immer mehr Passwörter für Unternehmensressourcen, manuelle Verwaltung der PKI und der Schlüssel sowie fehlende Möglichkeit, das Prinzip der geringstmöglichen Zugriffsrechte durchzusetzen. Früher fehlte es an Transparenz des Benutzerverhaltens. Nur der Netzwerkverkehr war sichtbar, sodass Sicherheitsverstöße manchmal erst Wochen, Monate oder sogar Jahre später entdeckt wurden.

Schritte zu Zero Trust

Unabhängig davon, ob es sich bei Zero Trust um eine groß angelegte Unternehmensinitiative oder um ein Einzelprojekt handelt, kann die Reifekurve, die viele unserer Kunden durchlaufen haben, Ihnen als Orientierung dienen.



Fazit

Es gibt keinen Königsweg zu Zero Trust, aber der Weg beginnt mit dem Aspekt Identität: Die Benutzeridentität bildet die Grundlage, fördert die Sicherheit und verbessert die Nutzungserfahrung. Mit einer robusten Identitätsschicht wird Benutzern Vertrauen anhand eines Kontextes zugewiesen, der laufend bewertet wird.

Okta ist die moderne Zero Trust-Plattform und Ihr Sprungbrett: Das Marktforschungsunternehmen Forrester Research hat Okta in einer Marktstudie zum Thema Zero Trust (**The Forrester Wave™: Zero Trust eXtended Ecosystem Providers, Q4 2018**) wie folgt beurteilt:

„Okta ist kompetent darin, Endbenutzer und ihre Zugriffsmöglichkeiten auf ein Netzwerk abzusichern.

Dies ist ein Schlüsselfaktor aller Zero Trust-Strategien und -Organisationen. Das Unternehmen hat viel Zeit und Ressourcen investiert, um Endbenutzern und Unternehmen unkomplizierte Sicherheit zu ermöglichen, und dank seines außergewöhnlichen Wachstums- und Expansionserfolgs verfügt es über eine starke Installationsbasis mit zufriedenen Kunden.“

The Forrester Wave™: Zero Trust eXtended Ecosystem Providers, Q4 2018zufriedenen Kunden.“

Möchten Sie mehr erfahren? **Sehen Sie sich hier das vollständige Webinar an.**

Über Okta

Okta ist der führende Anbieter von Identitätslösungen für Unternehmen. Die Okta Identity Cloud verbindet und schützt Mitarbeiter vieler der weltweit größten Unternehmen. Zudem verbindet sie Unternehmen auf sichere Weise mit ihren Partnern, Lieferanten und Kunden. Durch nahtlose Einbindung in über 5.000 Anwendungen ermöglicht die Okta Identity Cloud den einfachen und sicheren Zugriff von jedem Gerät aus.

Tausende von Kunden, darunter Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks und Adobe, verlassen sich auf Okta, um schneller zu arbeiten, ihren Umsatz zu steigern und ihre Sicherheit zu wahren. Mit Okta kommen Kunden schneller ans Ziel, denn Okta macht den Zugang zu Technologien, die Kunden für ihre Arbeit unbedingt benötigen, sicher und benutzerfreundlich.
www.okta.com