okta

Erste Schritte mit Zero Trust

Vertrauen ist gut, Kontrolle ist besser

Okta Deutschland
Oskar-von-Miller-Ring 20
80333 München

info_germany@okta.com
+49 (89) 26203329

Erste Schritte mit Zero Trust

Kurzfassung

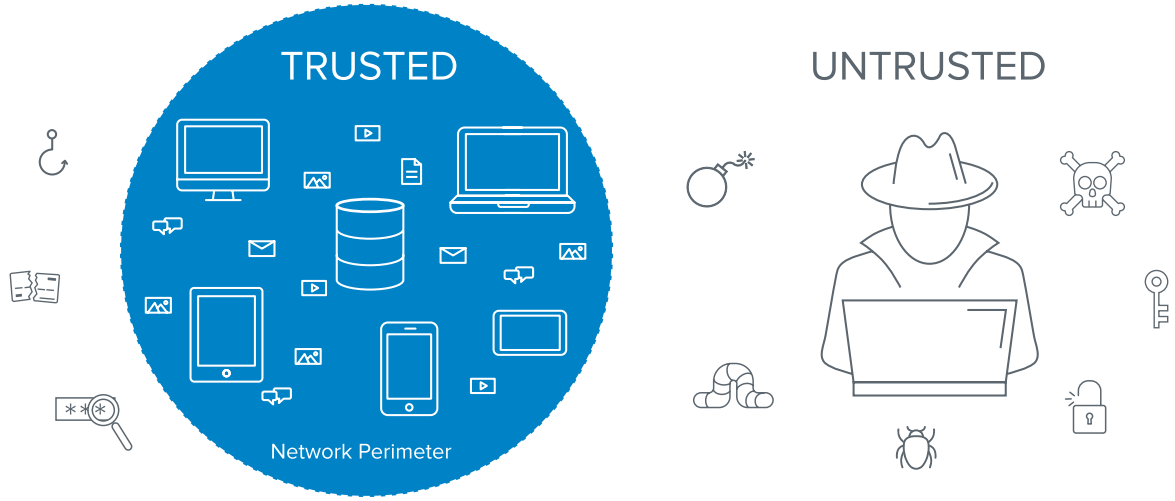
Zero Trust als Sicherheitskonzept verwirft die Vorstellung, es gäbe ein vertrauenswürdiges internes Netzwerk und ein nicht vertrauenswürdiges externes. Seit der Einführung von Mobilgeräten und der Cloud kann man sich bei Sicherheitsfragen nicht mehr auf den Bereich bis zur Netzwerkgrenze beschränken. Die verschiedenen Benutzer (Mitarbeiter, Partner, Auftragnehmer usw.) benötigen einen sicheren Zugriff unabhängig von ihrem Standort, Gerät und Netzwerk. Es gibt keinen Königsweg zu einer Zero Trust-Sicherheitsarchitektur: Die zentrale Technologie für den Einstieg von Unternehmen in Zero Trust ist jedoch das Identitäts- und Zugriffsmanagement.

Wir betrachten nun genauer, welche Veränderungen im Sicherheitsumfeld zur Entwicklung von Zero Trust geführt haben, wie das Framework Zero Trust Extended Ecosystem (ZTX) heute aussieht und wie Unternehmen Okta heute und in Zukunft als Grundlage für ein erfolgreiches Zero-Trust-Programm nutzen können.

Die Herausforderung: Der Schutzwall um Ihre Daten bröckelt

Bei der Schaffung herkömmlicher Sicherheitsarchitekturen ging man von zwei Gruppen aus: den vertrauenswürdigen Personen, die auf alles innerhalb des Unternehmens zugreifen konnten, und den nicht vertrauenswürdigen Personen, die ausgeschlossen wurden. Sicherheits- und IT-Teams investierten in Abwehrsysteme, die die Barriere zwischen diesen beiden Gruppen absicherten, und konzentrierten sich dabei vorrangig auf den Schutz der Netzwerkgrenze, oft mit Firewalls. Es gelang ihnen so, einen Schutzwall zwischen den potenziellen Bedrohungen auf der einen Seite und der Sicherheit innerhalb des Firmennetzwerks auf der anderen zu errichten. Dieses auf Vertrauen basierende Modell ist jedoch problematisch, denn ist die Netzwerkgrenze einmal durchbrochen, hat ein Angreifer relativ einfachen Zugriff auf alles im privilegierten Intranet eines Unternehmens – ganz zu schweigen von dem Chaos, das ein böswilliger Insider anrichten könnte, ohne dafür die Netzwerkgrenze durchbrechen zu müssen.

Sicherung des Unternehmens nach dem Prinzip „Burg mit Burggraben“



Mit der zunehmenden Verbreitung von Mobil- und Cloud-Technologien, aufgrund derer die Arbeit zu einem immer größeren Teil außerhalb eines gesicherten Firmennetzwerks erfolgt, wird es auch zunehmend schwieriger, die Netzwerkgrenze vollständig zu sichern. In dieser Welt gibt es keinen Schutzwall mehr um die sensiblen Unternehmensressourcen: Mitarbeiter, Auftragnehmer, Partner und Lieferanten greifen alle auf Daten innerhalb der traditionellen Netzwerkgrenze zu.

Im Zeitalter von Cloud Computing und Mobilgeräten greifen mehr Menschen denn je von mehr Geräten und Standorten aus auf mehr Ressourcen und Daten zu. Ein einziger böswilliger Akteur reicht aus, um im gesamten IT-Umfeld Schaden anzurichten. Infolgedessen können Unternehmen in keinem Bereich ihrer IT-Infrastruktur mehr von Vertrauen ausgehen.

Die nächste Herausforderung: Die Entwicklung von Zero Trust

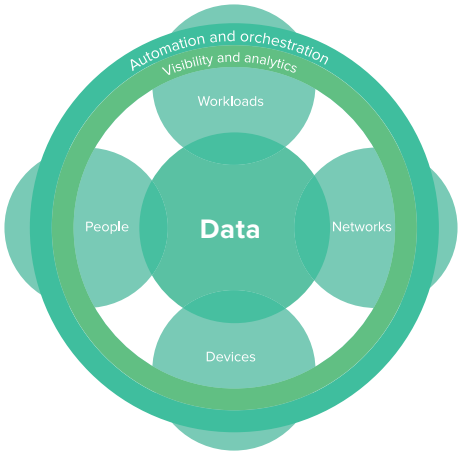
Dieses veränderte Sicherheitsumfeld war der Auslöser für das Entstehen von Zero Trust. Zero Trust ist ein 2009 durch den Analysten Jon Kindervag von Forrester Research entwickeltes Sicherheits-Framework, das sich von der Vorstellung löst, es gäbe ein vertrauenswürdiges internes Netzwerk und ein nicht vertrauenswürdiges externes. Kindervag forderte stattdessen, den gesamten Netzwerkdatenverkehr als nicht vertrauenswürdig zu betrachten. In dem ursprünglichen Rahmenkonzept konzentrierte sich Kindervag auf die Neugestaltung der Netzwerkgrenze und empfahl Unternehmen, den gesamten Datenverkehr im Netzwerk in Echtzeit zu kontrollieren. Dazu benötigt man ein Segmentierungs-Gateway für das Netzwerk. Zero Trust baut dabei auf drei Grundätzen auf: 1. Alle Ressourcen müssen auf sichere Weise zugänglich sein, unabhängig vom Standort. 2. Die Zugriffskontrolle unterliegt dem Need-to-know-Prinzip (Zugriff nur bei Bedarf) und wird strikt durchgesetzt. 3. Unternehmen müssen den gesamten Datenverkehr kontrollieren und protokollieren, um ein korrektes Verhalten aller Benutzer sicherzustellen.

Seit 2009 dient der Erfolg von Cloud und Mobilgeräten wie ein Katalysator auf die Weiterentwicklung des ursprünglichen Zero-Trust-Modells von Kindervag. Das CARTA-Framework[1] von Gartner aus dem Jahr 2017 griff das Zero-Trust-Framework von Kindervag auf. Der Schwerpunkt liegt hier nicht nur auf der Authentifizierung und Autorisierung des Zugriffs im Zugangsbereich, sondern auf einer laufenden adaptiven, risikoabhängigen Bewertung der Nutzung zum Erkennen potenzieller Bedrohungen.

[1] Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats, Gartner, Inc., 22. Mai 2017

Googles BeyondCorp Research wurde 2014[2] veröffentlicht und dient heute als Beispiel für Zero Trust, das erfolgreich im großen Stil praktiziert wird.

Die Weiterentwicklung des Zero-Trust-Frameworks von Forrester – Zero Trust Extended Ecosystem (ZTX), angestoßen vom Analysten Chase Cunningham – unterstreicht ebenfalls diese Verschiebung über die Netzwerksegmentierung hinaus. Die Entwicklung Cunninghams macht Zero Trust von einer „Firewall der nächsten Generation“ zu einem „Zugang der nächsten Generation“ und erhöht die Personenbezogenheit des Modells. Die Steuerung des Zugangs zum Netzwerk und des Zugriffs auf Daten sowie die Kontrolle darüber werden damit zum Schlüssel für den Erfolg. Das Team von Forrester nennt Funktionen wie Single Sign-On (SSO) als unverzichtbares Merkmal und stellt fest, dass die Multi-Faktor-Authentifizierung (MFA) „Zugriffsbedrohungen exponentiell reduziert“.[3]



Auch wenn das Modell sich weiterentwickelte, die zentrale Idee von Zero Trust blieb unverändert. Im heutigen Sicherheitsumfeld geht es nicht mehr um das Netzwerk – es geht um die Personen, die auf Systeme zugreifen, und um die Zugriffskontrollen für diese Personen. Hier kommt die Identität ins Spiel – und damit Okta.

2009 2011 2013 2015 2017 2019

2009: Forrester Zero Trust wird entwickelt

2018: Release des ZTX Framework

2014: BeyondCorp-Forschung von Google veröffentlicht

- Für den Zugriff auf Dienste darf es keine Rolle spielen, vom welchem Netzwerk aus die Verbindung hergestellt wird.
- Der Zugriff auf Dienste wird auf der Basis des Wissens über Person und Gerät erlaubt.
- Jeder Zugriff auf einen Dienst muss authentifiziert, autorisiert und verschlüsselt sein.

2017: Gartner CARTA veröffentlicht

Continuous Adaptive Risk and Trust Assessment

[2] BeyondCorp: A New Approach to Enterprise Security, Google, 2014
[3] The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Inc., 19. Januar 2018

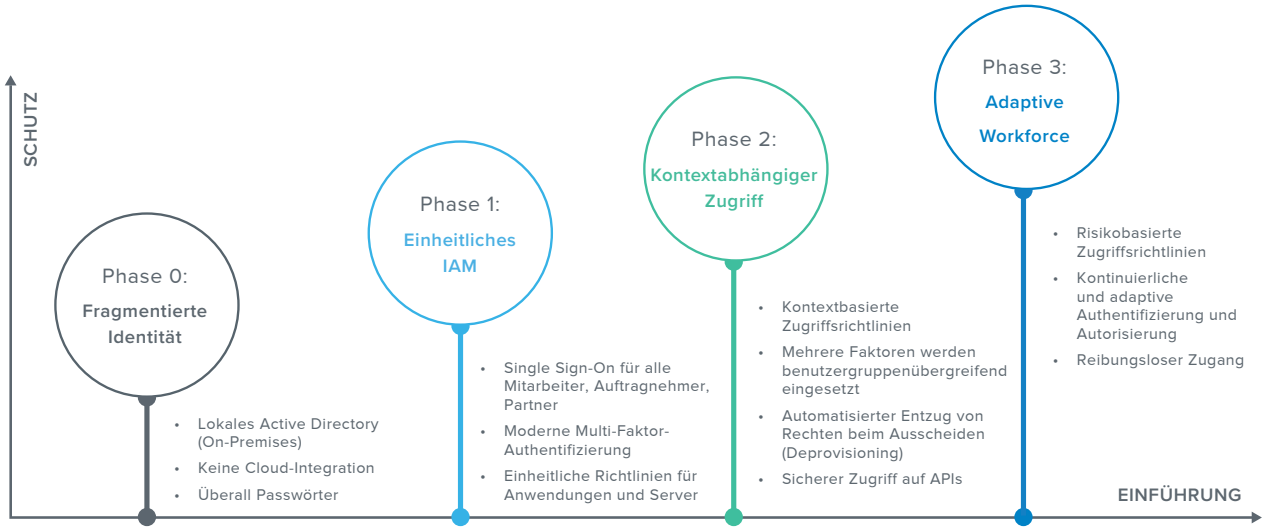
Forrester hat kürzlich auch eine neue Zero-Trust-Studie[4] veröffentlicht, die die Bedeutung des Zugriffs noch stärker betont und Okta als leistungsstarken Akteur auf dem Zero-Trust-Sicherheitsmarkt einstuft. Der Bericht „The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers“ (Q4 2018)[5], befasst sich mit einer Reihe von Anbietern. In den Kategorien „Personal-/Mitarbeitersicherheit“, „ZTX-Vision und -Strategie“ und

„Marktansatz“ erhielt Okta die Höchstwertung. Die Analysten schreiben: „Da die traditionellen Begriffe „Systeme“ und „Infrastruktur“ verschwinden, wird die Identität in all ihren verschiedenen Formen immer wichtiger.“ Da Identität eine wesentliche Rolle spielt, sieht Forrester darin „einen Grundpfeiler von Zero Trust“.

Identität als Grundlage von Zero Trust

Das Grundprinzip von Zero Trust lautet „Never trust, always verify“ – Vertrauen ist gut, Kontrolle ist besser. So wird sichergestellt, dass die richtigen Personen die richtigen Zugriffsrechte für die richtigen Ressourcen im richtigen Kontext haben und der Zugriff laufend bewertet wird – ohne Reibungsverluste für den Benutzer. Da das Ideal von Zero Trust nicht über Nacht erreicht wird, haben wir beim Implementieren von Zero-Trust-Architekturen durch Unternehmen mehrere Phasen der Infrastrukturreife beobachtet:

Reifekurve von Zero Trust



Phase 0: **Fragmentierte Identität**

Viele Unternehmen verfügen zum Beginn der Einführung von Zero Trust noch über eine Vielzahl von lokalen und Cloud-Anwendungen, die weder untereinander noch mit lokalen Verzeichnissen wie Active Directory verknüpft sind. Infolgedessen ist die IT-Abteilung gezwungen, in unterschiedliche Identitäten für eine Reihe von Systemen sowie die vielen Anwendungen und Dienste zu verwalten, die außerhalb der Kontrolle der IT-Abteilung genutzt werden. Für Benutzer bedeutet das auch zahlreiche (und höchstwahrscheinlich unsichere) Passwörter.

[4] Future-Proof Your Digital Business With Zero Trust Security, Forrester Research Inc., 28. März 2018

[5] The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

Ohne Transparenz und Kontrolle über diese fragmentierten Identitäten sind IT- und Sicherheitsteams mit einer Situation konfrontiert, in der Angreifer eine Vielzahl von möglichen Angriffspunkten für den unbefugten Zugriff auf einzelne Systeme finden.

Phase 1: **Vereinheitlichtes Identity and Access Management (IAM)**

Der erste Schritt zur Beseitigung der Sicherheitslücken durch zahlreiche fragmentierte Identitäten ist deren Konsolidierung in einem IAM-System für alle lokalen und Cloud-Ressourcen. Diese Konsolidierung über Single Sign-On (SSO) in Phase 1 ist entscheidend für die Zugriffsverwaltung und sollte sich nicht nur auf Kunden beziehen, sondern auf alle Benutzer, die Zugriff auf einen Dienst benötigen, d. h. das gesamte Unternehmensumfeld mit Mitarbeitern, Auftragnehmern und Partnern. Eine zusätzliche, auf diesem zentralen Identitätszugriffspunkt aufbauende Authentifizierungsstufe durch einen zweiten Faktor trägt außerdem dazu bei, gezielte Angriffe auf Zugangsdaten zu entschärfen. Darüber hinaus ist die Vereinheitlichung von Zugriffsrichtlinien für alle Anwendungen und Server – ein wichtiger Teil der IT-Infrastruktur – der Schlüssel zur Zusammenführung des IAM an einem sicheren Ort, den die IT-Abteilung verwalten kann.

Tausende von Unternehmen verwenden zur Zusammenführung ihrer Benutzeridentitäten Okta SSO. Häufig werden Okta Universal Directory und Okta SSO miteinander kombiniert. Okta Universal Directory ist ein Cloud-Verzeichnisdienst, der als „Single Source of Truth“ für IT-Organisationen dienen kann, also als verbindliche zentrale Datenquelle, die dann als Integrationspunkt für mehrere Anwendungsverzeichnisse und andere lokale Verzeichnisdienste fungiert. Okta SSO vereinfacht die Verwaltung und den Schutz des erweiterten Unternehmens für die IT-Abteilung und beseitigt den für die Benutzer lästigen Wildwuchs der Passwörter. Mit Okta Advanced Server Access kann die IT-Abteilung diese Zugriffskontrolle auch auf die Serverebene ausdehnen und so ein sicheres Zugriffsmanagement für alle von der IT-Abteilung verwalteten lokalen und Cloud-Ressourcen schaffen.

Phase 2: **Kontextabhängiger Zugriff**

Hat die IT-Abteilung das IAM vereinheitlicht, so besteht die nächste Implementierungsphase von Zero-Trust-Sicherheit in der Erstellung kontextbasierter Zugriffsrichtlinien. Dadurch werden aussagekräftige Daten über den Kontext des Benutzers (z. B.: Wer ist er? Gehört er zu einer Risiko-Benutzergruppe?), den Anwendungskontext (d. h.: Auf welche Anwendung versucht der Benutzer zuzugreifen?), den Gerätekontext, den Standort und das Netzwerk erfasst, und die entsprechenden Zugriffsrichtlinien angewendet. So kann beispielsweise mit einer Richtlinie festgelegt werden, dass verwaltete Geräte aus dem Firmennetzwerk nahtlosen Zugriff erhalten, während nicht verwaltete Geräte, die sich von neuen Standorten aus anmelden, zur MFA aufgefordert werden. Unternehmen können auch über Benutzergruppen hinweg mehrere Faktoren einsetzen und so eine Step-up-Authentifizierung auf Basis dieser Authentifizierungsversuche umsetzen. Beispielsweise könnte für risikoarme Benutzer ohne Smartphones eine Einmalkennung ausreichen, während für risikoreiche Ziele eine Authentifizierung mittels Hard-Token und kryptografischem Handshake gefordert wird.

Verlässt ein Benutzer das Unternehmen oder wechselt seine Funktion, so stellt die automatisierte Identitätsvergabe sicher, dass der Benutzer nur Zugriff auf die Tools hat, die er für seine Arbeit benötigt (scheidet der Mitarbeiter aus, wird der Zugriff automatisch gesperrt, was das Risiko von Hintertüren durch verwaiste Konten minimiert). Schließlich sollten diese umfangreichen Zugriffskontrollen auf alle durch das Personal verwendeten Technologien ausgedehnt werden und auch den sicheren Zugriff auf APIs umfassen, die wichtige Bausteine moderner Anwendungen sind, bei mangelnder Sicherheit aber den unbefugten Zugriff auf sensible Daten im Web ermöglichen können.

Viele Unternehmen nutzen mit Okta Adaptive MFA schon heute das kontextabhängige Zugriffsmanagement von Okta. Durch die Verarbeitung einer Vielzahl kontextbezogener Daten über einen Benutzer, ein Gerät, einen Standort, ein Netzwerk und die Anwendung oder den Browser beim Zugriff auf eine Ressource kann das Okta-Richtlinien-Framework kontextabhängig reagieren. Diese Reaktion basiert auf der Risikobereitschaft der Organisation und dient als erste Verteidigungslinie. Das Unternehmen kann etwa für den Fall, dass ein Benutzer versucht, sich von seinem üblichen Firmen-Laptop aus im Firmennetzwerk zu authentifizieren, eine Richtlinie festlegen, die nur die erfolgreiche Eingabe eines Kennworts durch den Benutzer erfordert. Versucht der Benutzer hingegen, sich im Ausland über ein öffentliches WLAN vom Firmen-Laptop aus zu authentifizieren, können die Richtlinien sowohl ein Kennwort als auch einen zweiten Faktor verlangen. Diese Art von kontextabhängigem Zugriff kommt sowohl dem Benutzer als auch der IT-/Sicherheitsabteilung zugute und fordert nicht jedes Mal einen zweiten Faktor, sondern nur bei als risikoreich eingestuften Zugriffsversuchen.

Phase 3: **Adaptives Personal (Adaptive Workforce)**

Die letzte Phase der Implementierung von Zero Trust erweitert den Fokus des Unternehmens auf die Authentifizierung und Autorisierung des Zugriffs. Die Authentifizierung erfolgt also nicht mehr nur am Ort des Zugangs, sondern laufend durch eine adaptive, risikoabhängige Nutzungsbewertung zum Erkennen potenzieller Bedrohungen.

Das sieht zunächst so aus, als würde man den kontextabhängigen Reaktionen aus Phase 2 eine intelligente, risikobezogene Engine hinzufügen, die über die in der vorherigen Phase festgelegten diskreten Richtlinien hinausgeht. Die IT-Abteilung kann nun die Risikobereitschaft festlegen, das Risk-Scoring zur Bestimmung der Risiken eines bestimmten Authentifizierungsvorgangs auf der Grundlage dieser Kontextdaten ermöglichen und in Abhängigkeit davon einen zweiten Authentifizierungsfaktor anfordern. Das Vertrauen ist hier nicht mehr uneingeschränkt: Die adaptive Authentifizierung wird laufend auf eine Änderung eines dieser Anhaltspunkte überwacht und fordert dann zur erneuten Authentifizierung und Autorisierung auf, wenn sich ein Aspekt des Benutzerkontexts ändert. Das bedeutet in der Summe nicht nur mehr Sicherheit dank intelligenter, risikobezogener Zugangskontrollen, sondern auch mehr Benutzerfreundlichkeit, da ein reibungsloser Zugang und sogar eine Authentifizierung ohne Passwort möglich ist, sofern die IT eine entsprechende Richtlinie festgelegt hat.

Mit Okta können Administratoren die Authentifizierung für Endbenutzer durch Richtlinien neu gestalten, was auch Authentifizierungsvorgänge ohne Kennwort beinhalten kann. Durch das Ersetzen von Passwörtern durch einen alternativen Faktor (z. B. Okta Verify oder einen YubiKey) als primären Authentifizierungsfaktor haben IT-Administratoren die Wahl:

Sie können risikobezogene Authentifizierungsrichtlinien festlegen, die anhand der Risikobereitschaft und der verschiedenen Kontextdaten bei Bedarf eine Step-up-Authentifizierung auslösen. Ist das Vertrauen in die Richtigkeit der angegebenen Identität hoch, so wird nur der erste Faktor ohne Passwort vom Benutzer abgefragt.

Okta verfügt einen robusten, richtliniengesteuerten Ansatz mit umfangreichen Kontextdaten, wir entwickeln unsere Richtlinien-Engine allerdings auch dahingehend weiter, dass sie verhaltensbezogene Aspekte deutlich stärker berücksichtigt.

Die meisten Unternehmen stehen beim Thema Zero Trust heute noch ganz am Anfang. Wenn sie jedoch den Grundsatz „Never Trust, always verify“ für ihre IT-Sicherheit weiter umsetzen, unterstützt Okta auch zusätzliche Funktionen, die ein stärkeres und gleichzeitig einfacheres Zugriffsmanagement ermöglichen.

Einbindung von Zero Trust in das erweiterte Sicherheitsumfeld

Okta macht nicht nur Identität zur Grundlage eines Zero-Trust-Systems, sondern bindet auch zahlreiche Sicherheitslösungen ein, um Ihren Zero-Trust-Ansatz zu vereinheitlichen. Über das Okta Integration Network investiert Okta in die nahtlose Einbindung aller Komponenten des erweiterten Zero-Trust-Umfelds und pflegt diese. Das umfasst folgende Bereiche:

netskope	McAfee Together is power.	Datensicherheit
paloalto NETWORKS	CISCO	Netzwerksicherheit
vmware	Carbon Black.	Gerätesicherheit
CYBERARK	BOMGAR	Workload-Sicherheit
splunk>	IBM QRadar	Analytik
servicenow	splunk>	Orchestrierung

Diese umfangreiche Gruppe von Integrationen unterstützt einen herstellerneutralen Best-of-Breed-Ansatz – ein Merkmal der Okta Identity Cloud.

Die intelligente Kontrolle des Zugriffs auf Unternehmensressourcen bildet die Grundlage für verhaltensbezogenes Monitoring, dennoch ist es schwierig, die Ursache für eine Gefährdung zu finden – insbesondere dann, wenn es um die Frage nach dem Täter und nicht nach der Tat geht. Mit Sicherheitsanalysen und SIEM-Integrationen ermöglicht es Okta Unternehmen, den umfangreichen Identitätskontext und die Benutzeraktivitäten von Okta zu nutzen und bei kompromittierten Konten Abhilfemaßnahmen zu erzwingen. Okta lässt sich auch in Cloud Access Security Broker (CASB) wie Netskope und McAfee einbinden und bietet Unternehmen umfassende Transparenz und Warnmeldungen. Das ermöglicht die laufende Überprüfung riskanter Ereignisse während der authentifizierten Sitzungen. Okta kann wie seine SIEM-Partner wertvolle Authentifizierungsdaten zum besseren Erkennen von Anomalien bereitstellen. Das ermöglicht es CASB-Diensten, eine Antwort an Okta zu senden, sodass Okta den Zugriff auf die Identitätsinfrastruktur gegebenenfalls sperren kann. Dies sind nur einige Beispiele dafür, wie Unternehmen mit dem Okta Integration Network das Zero-Trust-Konzept umsetzen können.

Fallstudie: 21st Century Fox

Sicherheit war schon immer ein wichtiges Thema bei 21st Century Fox, einem weltweit führenden Medienunternehmen mit verschiedenen Unternehmensbereichen rund um Film, Fernsehen und Pay-TV. 21st Century Fox erreicht täglich mehr als 1,8 Milliarden Abonnenten in rund 50 Sprachen und verfügt über ein globales Portfolio an Kabel- und Rundfunknetzen sowie eigene Produktionseinrichtungen wie Film- und Fernsehstudios. Vor einigen Jahren wurde ein Hackerangriff auf ein anderes großes Studio zur Initialzündung für die Verschärfung der Sicherheitsziele des Unternehmens.

Phase 1: Erste Schritte mit Zero Trust

21st Century Fox verfügte über alle üblichen perimeterbasierten Sicherheitsvorkehrungen, von Firewalls bis hin zu Virenschutzsoftware. Bei einem der ersten Projekte, mit dem Chief Information Security Officer (CISO) Melody Hildebrandt das IT-Team beauftragte, ging es darum, alle internen Benutzer bei Fox in dieselbe Umgebung zu bringen. Das beinhaltete die Stärkung der Authentifizierung, das leichtere Erfassen der Information, welche Benutzer auf welche Anwendungen zugreifen möchten, sowie die Optimierung der Identitätsmanagementabläufe. Nachdem die Identitäts- und Zugriffsinfrastruktur vereinheitlicht war, versuchte Hildebrandt, eine neue Zero-Trust-Architektur

> „Okta war das Fundament, mit dem wir uns zu einem Zero-Trust-Modell entwickeln konnten. Es war die Identitätsebene, auf der wir die nötige Kontrolle gewinnen konnten, um beurteilen zu können, wer hinter einem Zugriff steht. Es war also auch ein entscheidender Denkanstoß beim Thema Zero Trust.“
>
> **– Melody Hildebrandt, CISO, 21st Century Fox**

aufzubauen. Das sollte Identitätsdiebstahl und Phishing-Angriffe abwehren, die für viele der Datenverstöße verantwortlich sind, die in die Schlagzeilen geraten. Diese Änderungen wurden vorgenommen, ohne die Benutzerfreundlichkeit für Mitarbeiter, Auftragnehmer und unterstützende Partner des Fox-Netzwerks zu beeinträchtigen.

Phase 2: Einführung eines dynamischen, kontextabhängigen Zugriffs auf das erweiterte Unternehmen von 21st Century Fox

21st Century Fox nutzte die Okta Identity Cloud, um diesen Zero-Trust-Ansatz für alle Mitarbeiter umzusetzen: mit Oktas Workforce Identity-Produkten für die Mitarbeiter und API-Produkten von Okta für seine Partner und Auftragnehmer. Das Unternehmen setzte bereits Okta SSO, Universal Directory und Lifecycle Management ein, und beschloss, dies um Adaptive MFA und API-Zugriffsmanagement zu erweitern.

Nach der Einrichtung der zentralen Infrastruktur war der Wechsel zu einem dynamischen Zugriffsmodell für das Team von Hildebrandt unerlässlich. Daher implementierte es Okta Lifecycle Management und Universal Directory. Sobald sich der Status eines Benutzers in Workday, dem HR-System von Fox, ändert, kontrolliert UD dessen Attribute und ordnet den Benutzer in die entsprechende Gruppe ein. Dann stellt Lifecycle Management die Tools und die Zugriffsrechte bereit, die der Benutzer für seine Arbeit benötigt.

Dank dieser Lösung verfügen Benutzer bereits am ersten Tag über alles Benötigte und es besteht kein Risiko mehr, dass Benutzer versehentlich auf Daten zugreifen, für die sie keine Zugriffsbefugnis haben. Zudem ist das Risiko geringer, dass Dritte auf sensible Daten oder Inhalte zugreifen können, wenn Anmeldedaten ausgespäht wurden. Damit werden auch mögliche Probleme unverzüglich beseitigt, wenn ein Mitarbeiter von 21st Century Fox das Unternehmen verlässt oder ein Partner seinen Vertrag beendet: Der Zugriff wird gesperrt, sobald das Konto in Universal Directory gelöscht wurde, sodass keine „Zombie-Konten“ bestehen bleiben. Mit Adaptive MFA ist das Unternehmen auch in der Lage, auf der Grundlage von Faktoren wie der Benutzeridentität, der Art des verwendeten Geräts, des Standorts und der Anwendung, auf die zugegriffen werden soll, intelligente Authentifizierungsentscheidungen zu treffen. Das Unternehmen kann folglich ein hohes Schutzniveau sicherstellen, ohne die Mitarbeiter mit unnötigen Authentifizierungsschritten zu belasten. Als 21st Century Fox Adaptive MFA einführte, hörte es genau auf seine Mitarbeiter und Partner und bot möglichst viele Faktor-Optionen an, darunter Okta Verify, YubiKey, Okta Verify mit Push-, Voice-, SMS- und U2F-USB-Token.

Das Zero-Trust-Ideal von 21st Century Fox: Sicherheit plus Benutzerfreundlichkeit

Der Erfolgsmaßstab für 21st Century Fox ist letztlich die Fähigkeit, Verbrauchern einfach und sicher Inhalte zur Verfügung zu stellen. Ein Beispiel dafür ist Hot Star, eine mobile Anwendung, die das Unternehmen Verbrauchern in Indien anbietet und die kürzlich die Marke von sieben Millionen Live-Zuschauern zum selben Zeitpunkt überschritt. „Es ist eine ziemlich erstaunliche Leistung für eine App, die es seit weniger als zwei Jahren gibt, dass sie nun erstmals mobilen Benutzern in Indien Cricket anbietet und dabei vor DDoS- und potenziellen Credential-Stuffing-Angriffen geschützt ist, die bisher beträchtliche Bedrohungen darstellten“, sagt Hildebrandt.

Mit Okta können sich die Mitarbeiter und Partner von 21st Century Fox auf das konzentrieren, was sie am besten können – unterhaltsame Inhalte für die Kunden des Unternehmens bereitstellen, ohne sich den Kopf über externe Bedrohungen zu zerbrechen. Auf diese Weise ist es gelungen, eine große Sicherheitslücke zu schließen und gleichzeitig die Komplexität für Benutzer und die IT-Abteilung zu reduzieren. Das Fox-Publikum hat guten Grund, begeistert zu sein: Denn von nun an werden die Inhalte noch besser werden.

So geht es mit Okta und Zero Trust weiter

Es gibt keinen Königsweg zu Zero Trust. Auch wenn einige Anbieter Gegenteiliges behaupten, erwarten Unternehmen erstklassige Technologien, die größere Flexibilität und Produktivität ermöglichen. Aus diesem Grund bauen Unternehmen heute bei der Einführung von Zero Trust auf Identität und Okta. Dabei verwenden sie Okta Identity Cloud als Kernstück einer hochmodernen Zugriffsstrategie und stellen so sicher, dass nur die richtigen Personen zur richtigen Zeit Zugriff auf die richtigen Daten haben, ganz nach dem Prinzip: „Never trust, always verify“.

Modernes Zugriffsmanagement

Geringstmögliche Reibungsverluste

Okta investiert weiterhin in die Unterstützung von Unternehmen in allen Implementierungsphasen. Halten Sie sich mit unserem Unternehmens- und unserem Sicherheitsblog (okta.com/blog und www.okta.com/security-blog/) auf dem Laufenden. Sie können weitere Updates auf unserer Plattform erwarten.

Über Okta

Okta ist der führende unabhängige 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 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn und News Corp, 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.

Weitere Informationen finden Sie unter www.okta.com