WHITEPAPER

Zero Trust in der Praxis

Förderung einer vereinheitlichten Identitätssicherheit

Was ist Zero Trust?

Zero Trust ist ein bewährtes Modell zum Implementieren zuverlässiger und gezielter Sicherheit. Es sieht unter anderem vor, dass riskante Berechtigungen, nicht erforderliche Zugriffsrechte und übermäßiger Zugriff beseitigt und durch spezifische Delegierung sowie eine angemessene Provisionierung mit feiner Granularität ersetzt werden.

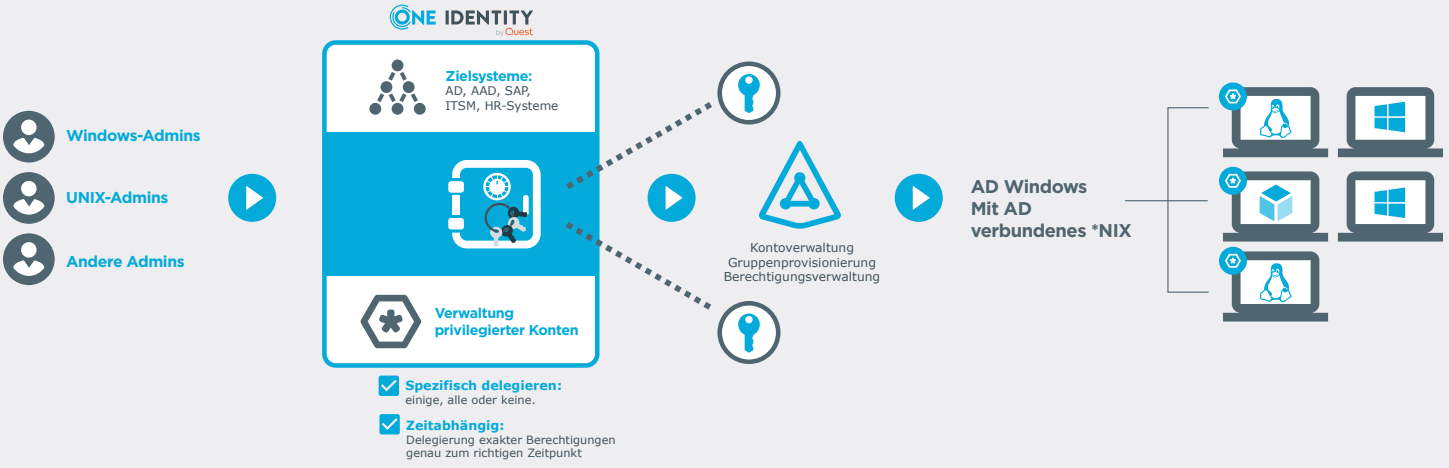
- Mit Zero Trust werden keine Administratorkennwörter mehr geteilt. Zudem wird eine individuelle und dynamische Authentifizierung für jeden administrativen Vorgang ermöglicht.
- Die Umsetzung des Least-Privilege-Prinzips beinhaltet, dass nur die Berechtigungen erteilt werden, die ein Admin für seine Arbeit benötigt – nicht mehr und nicht weniger.

Überblick

Da es sich um einen stichhaltigen und vertrauenswürdigen Ansatz für die Identitätssicherheit handelt, entwickelt sich Zero Trust unter IT-Verantwortlichen schnell zum Sicherheitsmodell erster Wahl. Zero Trust umfasst eine zielgerichtetere Methode für die Sicherheit und Verwaltung des privilegierten Zugriffs und unterscheidet sich mit seinem Mantra „niemals vertrauen, immer überprüfen“ vom Least-Privilege-Modell. In dieser technischen Kurzübersicht werden die Komponenten behandelt, die für eine robuste Sicherheitsaufstellung unerlässlich sind. Wir gehen unter anderem auf folgende Punkte ein:

- Bei Einführung der „Identität als Perimeter“ werden zahlreiche Grundsätze dieses Sicherheitsmodells abgedeckt. Dieser Ansatz erfordert insbesondere eine vereinheitlichte Lösung für die zuverlässige Provisionierung, Verwaltung von Berechtigungen, Verwaltung des privilegierten Zugriffs, starke Authentifizierung sowie für den sicheren Zugriff und die Governance.
- In einem Zero Trust-Modell wird sämtliche Kommunikation abgesichert, aber nicht als vertrauenswürdig erachtet.
- Mit einer „Single Source of Truth“ – bestehend aus zentralisierten und synchronisierten Identitätsdaten – können Organisationen die volle Kontrolle über Identitäten und Ressourcen erhalten. Das ist aber nur dann wirklich erreichbar, wenn das Berechtigungskonzept niet- und nagelfest ist.
- Ein einzelnes Puzzleteil liefert niemals ein umfassendes Sicherheitsmodell – die geschickte Kombination von Lösungen aber schon.

Ermöglichen von Zero Trust mit One Identity



Für viele Organisationen ist Zero Trust greifbar, wenn sie auf modulare und integrierte Lösungen unter anderem für die Verwaltung des privilegierten Zugriffs, das Management von Active Directory (AD)/Azure AD, die Erfassung von Ereignissen sowie die Identity Governance und Identitätsverwaltung setzen. Mit diesem integrierten Ansatz können Sie die zentralen Grundsätze der Zero Trust-Sicherheit bedienen und gleichzeitig für ein optimales Endbenutzererlebnis sorgen.

Der Weg hin zum Zero Trust-Sicherheitsmodell

Durch Modernisierungsbemühungen verändert sich die grundlegende Art und Weise, wie Datenverarbeitungstechnologien angewendet und genutzt werden und auch wie wir darauf zugreifen. In Anbetracht dieser Entwicklung gewinnt die Identitätssicherheit zunehmend an Bedeutung. Initiativen wie die Anwendungsmodernisierung, Cloud-zentrierte Strategien, Netzwerkinnovationen wie softwaredefinierte Netzwerke (SDN) und der geschäftliche Druck durch die Konkurrenz erschweren die Verwaltung und die Absicherung des Zugriffs durch Benutzer und andere nicht menschliche Ressourcen. Wie kann eine Organisation Cloud-basierte Technologien sicher implementieren und gleichzeitig geschäftskritische Ressourcen vor Ort behalten?

Wir alle wünschen uns einwandfreie und geordnete Prozesse, doch in Wirklichkeit arbeiten die meisten Organisationen mit einer bunten Mischung aus lokalen und Cloud-basierten Systemen für die absehbare Zukunft. Das Wahren der Sicherheit, Erfüllen von Compliance-Anforderungen und Ermöglichen einer reibungslosen Benutzererfahrung kann wie eine unmögliche Aufgabe erscheinen.

NIST Zero Trust Architecture

1. Alle **Datenquellen und Datenverarbeitungs-services** werden als Ressourcen erachtet.

2. Sämtliche **Kommunikation wird unabhängig vom Ort im Netzwerk abgesichert**.

3. Der Zugriff auf individuelle Unternehmensres-sourcen wird **auf Sitzungsbasis** gewährt.

6. Die gesamte Ressourcenauthentifizierung und -autorisierung erfolgt dynamisch und wird **streng erzwungen, bevor Zugriff gewährt wird**.

4. Der Zugriff auf Ressourcen wird durch eine **dynamische Richtlinie** bestimmt – mit Angaben zum sichtbaren Status der Client-Identität, zu Anwendung/Service und zum anfordernden Asset – und es können weitere verhaltens- und umgebungsbezogene Attribute berücksichtigt werden.

5. Das Unternehmen **überwacht und analysiert** die Integrität und Sicherheitsaufstellung aller eigenen und zugehörigen Assets.

7. Das Unternehmen erfasst möglichst viele Informationen über den **aktuellen Status von Assets, Netzwerkinfrastruktur und Kommunikation** und nutzt diese, um seine Sicherheitsaufstellung zu verbessern.

Referenz: NIST SP 800-207 „Zero Trust Architecture"

Das muss aber nicht so sein. Sie können all das erreichen, indem Sie im Zuge Ihrer digitalen Transformation dieses Sicherheitsmodell einführen. Nach Implementierung des Modells können Sie die Komplexität reduzieren und grundlegende Metriken definieren, um individuelle Best Practices für die Informations- und Identitätssicherheit zu schaffen.

Identität als neuer Perimeter

Da immer mehr Netzwerkfunktionen Teil einer virtuellen Netzwerkumgebung werden, wurden klassische lokale Firewalls und das statische Routing durch virtuell gekoppelte Ressourcen ersetzt. Die Identitätssicherheit ist der neue Perimeter. Der Schutz von Identitäten erfordert eine starke Authentifizierung, sicheren Zugriff und Governance. In einem Zero Trust-Sicherheitsmodell wird sämtliche Kommunikation abgesichert, aber nicht als vertrauenswürdig erachtet.

Eine zuverlässige Identitätssicherheitsbasis, die sich dynamisch anpasst und vereinheitlichte Richtlinien sowie Zugriffssteuerung für lokale und Cloud-basierte Ressourcen ermöglicht, ist eine kritische Komponente dieses neuen Modells. Mit einer „Single Source of Truth" (zentralisierte und synchronisierte Identitätsdaten) für Rechte, Attribute und Berechtigungen über den gesamten Lebenszyklus der Identität erhalten Organisationen die volle Kontrolle. Zero Trust ist nur dann wirklich erreichbar, wenn das Berechtigungskonzept niet- und nagelfest ist.

Die sieben zentralen Grundsätze

Für das Zero Trust-Modell gibt es gemäß NIST SP800-207 definierte zentrale Grundsätze. Diese Grundsätze helfen Anbietern, Lösungen zu konzipieren, sodass Technologiebenutzer Services zum effizienten und kalkulierbaren Implementieren des Sicherheitsmodells einführen können.

Die NIST-Grundsätze umfassen:

1. **Alle Datenquellen und Datenverarbeitungsservices werden als Ressourcen erachtet.**
2. **Sämtliche Kommunikation wird unabhängig vom Ort im Netzwerk abgesichert.**
3. **Der Zugriff auf individuelle Unternehmensressourcen wird auf Sitzungsbasis gewährt.**

   Bei diesem Schlüsselkonzept der Identitätssicherheit liegt der Fokus speziell auf der Verwaltung erhöhter Berechtigungen. Wenn eine Person oder ein Konto erhöhte Berechtigungen zum Ausführen einer bestimmte Aufgabe benötigt, sind diese Berechtigungen wahrscheinlich nicht immer erforderlich. One Identity Manager, Active Roles und One Identity Safeguard (mit Just-in-Time-Provisionierung) helfen Ihnen beim Umsetzen dieses Konzepts.
4. **Der Zugriff auf Ressourcen wird durch eine dynamische Richtlinie bestimmt – mit Angaben zum sichtbaren Status der Client-Identität, zu Anwendung/Service und zum anfordernden Asset – und es können weitere verhaltens- und umgebungsbezogene Attribute berücksichtigt werden.**

   Das Stichwort ist hier „dynamisch". Durch eine dynamische Richtlinie kann sich der Zugriff in Übereinstimmung mit spezifischen Echtzeitanforderungen des Benutzers ändern. Sowohl Identity Manager als auch Active Roles bieten entsprechende Funktionen sowie einen ausführlichen Audit Trail, mit dem Sie belegen können, wo Zugriff gewährt (oder verweigert) wurde, wer ihn angefordert hat und wann er entzogen wurde.

5. **Das Unternehmen überwacht und analysiert die Integrität und Sicherheitsaufstellung aller eigenen und zugehörigen Assets.**

   Die „Assets“ des Unternehmens umfassen eine Vielzahl von Dingen. Transparenz im Hinblick darauf, wer Zugriff hat, wie der Zugriff gewährt wurde und sogar welche kalkulierten Sicherheitslücken es basierend auf einem Berechtigungsmodell gibt, liefert dem Unternehmen wichtige Informationen für die Entscheidungsfindung. One Identity Manager konzentriert sich auf die Identität sowohl als Asset als auch als zu verwaltendes Objekt, sodass präzise Informationen für Zugriffsentscheidungen und Berichte verwendet werden.

6. **Die gesamte Ressourcenauthentifizierung und -autorisierung erfolgt dynamisch und wird streng erzwungen, bevor Zugriff gewährt wird.**

   Das strenge Erzwingen der Zugriffskontrolle ist ein absolutes Muss für jedes System. Mit den Lösungen von One Identity können Sie die Zugriffssteuerung dynamisch gestalten, um behördliche oder geschäftliche Anforderungen zu erfüllen, indem Sie Identitätsänderungen erkennen und Endsysteme sofort bearbeiten, damit die erforderliche Zugriffsänderung wiedergegeben wird.

7. **Das Unternehmen erfasst möglichst viele Informationen über den aktuellen Status von Assets, Netzwerkinfrastruktur und Kommunikation und nutzt diese, um seine Sicherheitsaufstellung zu verbessern.**

   Transparenz ist für die Sicherheit eines jeden Systems unerlässlich. Ganz gleich, ob es um den aktuellen Stand des Zugriffs oder um durch Änderungen hervorgerufene Ereignisse geht – Lösungen von One Identity decken diesen Grundsatz ab. Während One Identity Manager Transparenz und Governance mit Blick auf Zugriffsstatus und -änderungen ermöglicht, überwacht Active Roles Änderungen an Active Directory Objekten. Gleichzeitig kontrolliert Safeguard den privilegierten Zugriff und One Identity syslog-ng erfasst alle Ereignisdaten, um für ein umfassendes Situationsbewusstsein im Unternehmen zu sorgen.

Es gibt keine Lösung, die die Implementierung eines Zero Trust-Modells auf magische Weise per Tastendruck ermöglicht. Vielmehr sollte Zero Trust zu einer Einstellung bei der Implementierung neuer Systeme, Anwendungen, Netzwerke und sogar physischer Sicherheit werden. Durch die Umsetzung und Kombination dieser Konzepte wird ein Framework geschaffen, mit dem sichergestellt ist, dass Unternehmen alle Möglichkeiten zum Absichern ihrer Infrastruktur nutzen. Die Identitätssicherheit spielt in der modernen Belegschaft eine bedeutende Rolle.

Zero Trust lässt sich mit einem einzelnen Puzzleteil nicht erreichen, dafür aber durch die gekonnte Kombination aller Teile. Mit der vereinheitlichten Plattform für Identitätssicherheit von One Identity, inklusive unserer Funktionen für die Verwaltung des privilegierten Zugriffs, die Verwaltung von Active Directory/ Azure AD, die Erfassung von Ereignissen sowie Identity Governance und die Identitätsverwaltung, können Sie das Sicherheitsmodell implementieren und gleichzeitig für zufriedene Endbenutzer sorgen.

Wie wird Zero Trust in der Praxis erreicht?

Damit Organisationen Zero Trust erreichen können, benötigen sie einen integrierten Ansatz mit einer vereinheitlichten Plattform für Identitätssicherheit. Die Erarbeitung gut durchdachter Praktiken zur Sicherung und Verwaltung von Identitäten kann eine sehr komplexe Aufgabe sein, aber die entscheidende Frage im Hinblick auf die Sicherheit ist, wie sie umgesetzt werden.

One Identity Lösungen ermöglichen Unternehmen mit vielfältigen Umgebungen die Implementierung identitätszentrierter Praktiken, die an der NIST Zero Trust Architecture ausgerichtet sind. NIST liefert solide Technologierichtlinien, die uns auf dem Weg zur Absicherung kritischer Informationen deutlich voranbringen. Diese Richtlinien befassen sich zwar nicht speziell mit der Sicherung vor Ort oder in der Cloud, aber es ist entscheidend, dass wir sie auf die Systeme anwenden, mit denen jeden Tag Zugriffsentscheidungen für sämtliche Organisationen getroffen werden.

One Identity bietet die Lösungen, mit denen Sie die spezifischen NIST-Grundsätze direkt angehen können. Unsere Lösungen umfassen Folgendes:

Zugriffssteuerung mit One Identity Manager, einem Tool, das speziell darauf ausgelegt ist, den Zugriff zu kontrollieren, die Implementierung des Least-Privilege-Prinzips sicherzustellen und den Zugriff dynamisch zu entziehen, wenn er für ein verbundenes System nicht mehr benötigt wird.

Erzwingung des Zugriffs mit minimalen Rechten mit Active Roles, sodass Zero Trust-Konzepte mittels Kontolebenszyklusverwaltung, dynamischer Rollenverwaltung und Zugriffssteuerung und strenger Erzwingung des Least-Privilege-Prinzips für den Zugriff auf Active Directory und alle verbundenen Systeme auch auf Active Directory angewendet werden können.

Verwaltung des privilegierten Zugriffs mit Safeguard, womit die gesamte Palette an Lösungen zur Verwaltung des privilegierten Zugriffs bereitgestellt wird, sodass sichergestellt werden kann, dass die Identitäten und Konten mit umfangreichen Rechten im Unternehmen streng kontrolliert werden und dass dies mit detaillierten Audit Trails und Berichten belegt werden kann.

Protokollerfassung mit syslog-ng für eine flexible und skalierbare Protokollverwaltung im gesamten Unternehmen, sodass SIEM möglichst effizient und kostengünstig genutzt werden kann.

Über One Identity

One Identity von Quest ermöglicht es Unternehmen, lokal, in der Cloud oder in einer Hybrid-Umgebung eine identitätszentrierte Sicherheitsstrategie zu implementieren. Dank unseres einzigartig breit gefächerten und integrierten Portfolios mit Angeboten zum Identitätsmanagement, einschließlich Kontoverwaltung, Identity Governance und Administration sowie Verwaltung des privilegierten Zugriffs, sind Unternehmen in der Lage, ihr volles Potenzial auszuschöpfen und Sicherheit dadurch zu erreichen, dass Identitäten in den Mittelpunkt des Programms gestellt werden und der ordnungsgemäße Zugriff für alle Benutzertypen, Systeme und Daten ermöglicht wird. Weitere Informationen finden Sie unter OneIdentity.com.

© 2021 One Identity LLC ALLE RECHTE VORBEHALTEN. One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC in den USA und anderen Ländern. Eine vollständige Liste der Marken von One Identity finden Sie auf unserer Website unter www.oneidentity.com/legal. Alle übrigen Marken, Dienstleistungsmarken, eingetragenen Marken und eingetragenen Dienstleistungsmarken sind Eigentum der jeweiligen Markeninhaber.
WhitepaperAD-MakingZeroTrustReal-RS-DE-WL-65397