Identity Security:

ein wesentlicher Bestandteil Ihrer „Zero Trust“-Strategie

SailPoint

Perimeterbasierte Sicherheit ist nicht mehr ausreichend

Noch nie war es so schwierig wie heute, Cyber-Risiken zu managen und auf die Herausforderungen einer sich ständig verändernden Geschäftslandschaft zu reagieren. Dies sind einige der Herausforderungen:

- Ein starker Anstieg bei der Anzahl der Remote-Mitarbeiter und der nicht angestellten Mitarbeiter
- Es müssen mehr Arten von Benutzern, nicht-menschlichen Entitäten, Geräten und Datenquellen verwaltet und geschützt werden als je zuvor
- Die stetige Migration von Anwendungen und Workloads in verschiedene Cloud- und Hybrid-Infrastrukturen
- Cloud Services mit unterschiedlichen Identity-Modellen (z. B. mehr vererbte Rollen und Berechtigungen)

Die explosionsartige Zunahme von Cloud Computing, Mobile, IoT, DevOps, Bring-your-own-devices (BYOD) und Heimarbeit-Initiativen hat zu einer Dezentralisierung der IT geführt. Durch die verstärkte Annahme von Mobil- und Cloud-Technologien werden immer mehr Geschäftsvorgänge außerhalb des Unternehmensnetzwerks abgewickelt. Immer mehr Benutzer greifen von einer Vielzahl von Geräten und Standorten aus auf Ressourcen wie Anwendungen und Geschäftssysteme zu. Da Cyberkriminelle unermüdlich versuchen, Benutzerkonten zu kompromittieren, um sich Zutritt zu verschaffen, haben Unternehmen ihre Sicherheitsperimeter verlagert, sodass sie sich nun auf die Arbeitskräfte konzentrieren – darunter Mitarbeiter, externe Dienstleister, Partner, Lieferanten und nichtmenschliche Bots. Die Grundlage von Identity Security ist, den richtigen Zugriff zu ermöglichen und gleichzeitig kontinuierlich das Unternehmen zu schützen. Aus diesem Grund bauen viele Unternehmen auf Identity Security als grundlegende Komponente ihres „Zero Trust"-Sicherheitsprogramms.

„Zero Trust" ist mehr als eine Sicherheitslösung. Es ist eine Strategie.

Zero Trust bietet ein Sicherheitskonzept, das das digitale Geschäft eines Unternehmens ermöglicht und gleichzeitig die Integrität der Datensicherheit gewährleistet, indem es den richtigen Personen mit der richtigen Berechtigung genau den richtigen Zugriff gewährt. Deshalb bildet Identity Security einen wesentlichen Bestandteil einer effektiven Zero Trust-Strategie. Die Vitalität einer Zero Trust-Architektur hängt nämlich von der Integrität der Identitäten, der Wirksamkeit und Stärke der Zugriffskontrollrichtlinien und der Kontinuität der Governance über Identitäten und Zugriff in einer hybriden IT-Umgebung ab.

[1]Zero Trust Adoption Accelerates to Manage work from Home Risks, August 2021

„Zero Trust"-Sicherheit setzt bei Identity Security an

„Zero Trust"-Sicherheit beruht auf dem Prinzip „vertraue nie, überprüfe immer" und „gehe von einem Verstoß aus". In der Praxis bedeutet dies, dass niemand automatisch Zugriff auf Ressourcen haben sollte, weder innerhalb noch außerhalb eines Unternehmens. Grundsätzlich gilt jeder Benutzer als verdächtig, bis er sich als sicher erwiesen hat. Ist der gesamte Netzwerkverkehr per se nicht vertrauenswürdig, so ist die einzige praktikable Sicherheitsstrategie eine Identity-basierte.

Ein erfolgreiches identitätsbasiertes „Zero Trust"-Modell beruht auf dem „Least Privilege"-Prinzip, das sicherstellt, dass alle Benutzer so wenig Zugriffsrechte wie möglich haben, um ihre Arbeit erfolgreich zu erledigen – nicht mehr und nicht weniger. Dazu muss man nicht nur wissen, wer Zugriff auf was hat, sondern vor allem, wer Zugriff haben sollte und unter welchen Umständen.

Laut einem aktuellen IDSA-Bericht sind sich fast alle (97 %) IT-Sicherheitsexperten einig, dass Identity ein grundlegender Bestandteil eines „Zero Trust"-Sicherheitsmodells ist.[2]

Identity Security spielt also eine entscheidende Rolle für den Erfolg eines jeden „Zero Trust"-Programms. Identity Security bedeutet, Technologien einzusetzen, die den Lebenszyklus von Identitäten automatisieren, die Integrität von Identitätsattributen verwalten, durch dynamische Zugriffskontrollen, rollenbasierte Richtlinien und Aufgabentrennung das „Least Privilege"-Prinzip durchsetzen und kontinuierlich eine Vielzahl von Signalen auswerten, um Zugriffsrisiken mithilfe fortschrittlicher Technologien wie KI/ML zu steuern und darauf zu reagieren.

Durch die Implementierung eines starken und umfassenden Identity Security-Programms können Unternehmen den Zugriff auf alle Arten von digitalen Identitäten verwalten und regeln. So können Sie ein „Zero Trust"-Framework einrichten, das sich systematisch an die laufenden Veränderungen im Unternehmen und in der Bedrohungslandschaft anpassen und darauf reagieren kann. Zu den wesentlichen Grundsätzen gehören:

- **Niemals vertrauen, immer überprüfen:** Stellen Sie sicher, dass genaue Zugriffsentscheidungen auf Basis kontextbezogener, aktueller Identitätsdaten getroffen werden.
- **Bereitstellen von ausreichendem, rechtzeitigem Zugriff:** Setzen Sie „Least Privilege" mithilfe von Rollen und komplexer Richtlinienlogik durch.
- **Kontinuierliches Überwachen, Analysieren und Anpassen:** Halten Sie die Sicherheit auf dem neuesten Stand und reagieren Sie dynamisch auf Veränderungen und entdeckte Bedrohungen.

[2] 2021 Trends in Securing Digital Identities.

Zu sagen, „Vertraue niemals", ist die eine Sache. Für das Funktionieren eines Unternehmens ist Vertrauen jedoch keine Option. Indem sie über simple Authentifizierungsentscheidungen hinausgehen und für jeden Benutzer einen vollständigen Identity-Datensatz verwenden – einschließlich Berechtigungen, Befugnissen, Attributen und Rollen – können Unternehmen vertrauensvoll Zugriff gewähren, wenn dieser benötigt wird.

Niemals vertrauen – immer überprüfen

Traditionell mussten Unternehmen nur geschlossene und relativ statische Umgebungen verwalten. Jeder Teilnehmer eines Netzwerks galt als sicher, sobald der Benutzer durch ein ordnungsgemäßes Anmeldeverfahren authentifiziert wurde; dann wurde automatisch Vertrauen gewährt. Doch mit der Auflösung der Netzwerkperimeter und der Einführung von Cloud-Ressourcen gewann eine Vielzahl neuer Identitätsarten (wie externe Dienstleister und Partner) zunehmend an Bedeutung. Das bedeutete, dass IT- und Sicherheitsteams die Art und Weise, wie sie das Unternehmen schützen, grundlegend neu überdenken mussten.

Daher lautet der erste Grundsatz einer „Zero Trust"-Strategie: Niemals vertrauen. Dabei stellt sich die Frage: Wie können Unternehmen operieren, wenn sie ihren Benutzern, die auf Unternehmensressourcen zugreifen, nicht vertrauen? Die Antwort lautet, dass sie verifizieren müssen, dass es sich bei dem Benutzer um denjenigen handelt, der er vorgibt zu sein. Die meisten Unternehmen benötigen dazu eine solide Strategie und Lösung für die Zugriffsverwaltung. Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA) sind entscheidende Sicherheitskomponenten, sie authentifizieren einen Benutzer jedoch nicht vollständig, da sie nicht überprüfen, ob ein Benutzer der ist, der er vorgibt zu sein. Um dies zu erreichen und den Benutzer in Ihren Vertrauenskreis aufzunehmen, müssen Sie alle Attribute berücksichtigen, insbesondere kontextbezogene und aktuelle Identitätsdaten.

Um die für präzise Zugriffsentscheidungen erforderliche Identity-Transparenz zu schaffen, sollten Unternehmen Folgendes gewährleisten:

- **Umfassende Transparenz:** Schaffen Sie eine Rundumansicht aller Benutzertypen und ihres jeweiligen Zugriffs – einschließlich aller Berechtigungen, Ansprüche, Attribute und Rollen.
- **Einzelne Datenquelle:** Erstellen Sie saubere, genaue Identity-Datensätze, auf die sich sämtliche Zugriffsentscheidungen stützen.
- **Datenintegrität:** Halten Sie Ihre Identity-Daten durch die Automatisierung des Identity Lifecycle Management stets auf dem neuesten Stand.

Zu sagen, „Vertraue niemals", ist die eine Sache. Für das Funktionieren eines Unternehmens ist Vertrauen jedoch keine Option. Indem sie über simple Authentifizierungsentscheidungen hinausgehen und für jeden Benutzer einen vollständigen Identity-Datensatz verwenden – einschließlich Berechtigungen, Befugnissen, Attributen und Rollen – können Unternehmen vertrauensvoll Zugriff gewähren, wenn dieser benötigt wird.

Bereitstellung von ausreichendem, rechtzeitigem Zugriff durch das „Least Privilege"-Prinzip

Wenn der erste Grundsatz von „Zero Trust" lautet, niemals automatisch zu vertrauen, ist der zweite, den Zugriff immer auf das niedrigste Maß zu beschränken, auch bekannt als „Least Privilege". Dieses Konzept ist zwar leicht zu verstehen, es jedoch in einem wachsenden und sich ständig verändernden Geschäftsumfeld auf breiter Basis umzusetzen, gestaltet sich äußerst schwierig und ist sehr komplex.

Hier spielen Rollen und rollenbasierte Zugriffskontrollen (Roles and Role-Based Access Controls, RBAC) eine entscheidende Rolle, da sie sicherstellen, dass Benutzer immer über den erforderlichen Zugriff verfügen, ohne dass das Unternehmen übermäßige Risiken eingeht. Unternehmen, die über klar definierte und detaillierte Rollen für den Zugriff verfügen, können den Zugriff leicht zuweisen, anpassen und entfernen, ohne das Risiko einmaliger Zugriffszuweisungen, die oft übersehen und in den meisten Fällen niemals entfernt werden. Zusätzlich zu Rollen ist eine dynamische Logik für Zugriffsrichtlinien erforderlich, damit toxische Zugriffskombinationen vermieden werden, die zu einer Überprovisionierung und sogar Betrug oder Diebstahl führen können. Zum Beispiel, indem sichergestellt wird, dass Benutzer, die Zugriff auf Beschaffungssysteme haben, nicht auch über Berechtigungen in angrenzenden Debitorenbuchhaltungssystemen verfügen, was dazu führen könnte, dass skrupellose Mitarbeiter Unternehmensgelder über betrügerische Bestellungen abzweigen.

Wie können Unternehmen also ausreichenden und rechtzeitigen Zugriff bereitstellen und gleichzeitig das „Least Privilege" wahren?

- **Sichere Zugriffskontrollen:** Gewähren Sie mithilfe von Rollen, fein abgestuften Ansprüchen, Berechtigungen und dynamischen Regeln genau den richtigen Zugriff.
- **Zugriffsautomatisierung:** Werden neue Benutzer angelegt oder Rollen geändert, wird der Zugriff automatisch gewährt und auf der Grundlage der Zugriffsrichtlinie aktualisiert. Um das Risiko zu verringern, werden ungenutzte Zugriffe und ruhende Konten automatisch deaktiviert.
- **Laufende Sicherheitsvorkehrungen & Aufgabentrennung:** Erkennen und verhindern Sie toxische Zugriffskombinationen, um potenziellen Betrug oder Diebstahl zu vermeiden.

Kontinuierliches Überwachen, Analysieren und Anpassen

Viele Unternehmen haben die „Vertraue niemals"- und „Least Privilege"-Prinzipien erfolgreich eingeführt. Die Herausforderung ist jedoch, sicherzustellen, dass ihr „Zero Trust"-Modell relevant bleibt und allen Veränderungen innerhalb und außerhalb des Netzwerks gerecht werden kann. Allzu oft tappen Unternehmen

in die Falle, Zugriffsrichtlinien und -kontrollen festzulegen und zu vergessen, statt sie aktiv zu überwachen, zu steuern und anzupassen. Dies passiert oft, weil Unternehmen mit der Menge der erzeugten Identity-Daten überfordert sind und ihnen das interne Fachwissen fehlt, um ihre „Zero Trust"-Strategie richtig durchzuführen.

Identitätsdaten spielen bei „Zero Trust" eine entscheidende Rolle, da sie wichtige Informationen wie Identitätsattribute, Zugriffsrechte, Zugriffsberechtigungen, Verhaltensdaten sowie Rollen- und Gruppenzugehörigkeiten enthalten. Aufgrund des Umfangs der verfügbaren Identitätsdaten übersteigt es jedoch den Rahmen menschlicher Fähigkeiten, all diese Informationen manuell zu durchforsten. Die Analyse großer Mengen identitätsbezogener Daten zur Anpassung an Veränderungen im Unternehmen und für korrekte Zugriffsentscheidungen erfordert den Einsatz von Tools, die künstliche Intelligenz und maschinelles Lernen einsetzen, sowie Integrationen mit zusätzlichen Sicherheitssystemen, die ihre „Zero Trust"-Strategie stützen.

Durch den Einsatz von Identitätsdaten können Unternehmen dann leistungsfähige Strategien verfolgen, um die Sicherheit auf dem neuesten Stand zu halten und dynamisch auf Veränderungen und entdeckte Bedrohungen zu reagieren:

- **Laufende Zugriffsüberwachung:** Dank KI-gestützter Einblicke erlangen Unternehmen umfassende Transparenz und ein Verständnis für sämtliche Benutzerzugriffe, einschließlich Trends, Rollen, Ausreißern und Beziehungen.
- **Konsequente Governance:** Durch die Messung der Effizienz von Zugriffskontrollen für Anwendungen, Daten und Cloud-Ressourcen wird sichergestellt, dass Berechtigungen richtlinienkonform sind.
- **Koordinierung:** Durch die ständige Überwachung von Risikosignalen aus dem digitalen Ökosystem und die Kommunikation mit dem „Zero Trust"-Gateway wird gewährleistet, dass Sicherheitsrichtlinien in Echtzeit durchgesetzt werden.
- **Erweiterungsfähigkeit:** Indem sie sich benutzerdefinierte Workflows, APIs und Event-Trigger zunutze machen, können Unternehmen ihr Identity Security Programm über andere Cybersicherheits- und Zugriffssysteme hinweg automatisieren.

„Zero Trust" erfordert einen ganzheitlichen Ansatz

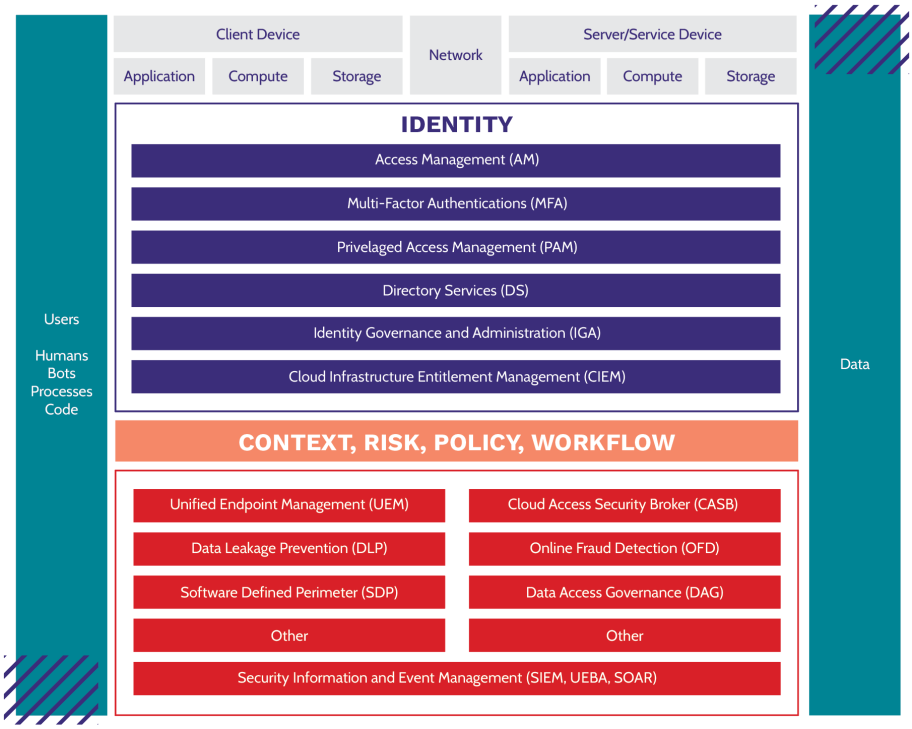
Wir haben bereits dargelegt, inwieweit eine „Zero Trust"-Strategie auf die Zusammenarbeit verschiedener Systeme angewiesen ist. Dieser ganzheitliche Sicherheitsansatz ist für alle „Zero Trust"-Implementierungen entscheidend.

Die Identity Defined Security Alliance (IDSA), ein Konsortium von Identity- und Sicherheitsanbietern, hat eine Referenzarchitektur (Abbildung 1) entwickelt, die ein Framework zum Verständnis der verschiedenen Komponenten für identitätsdefinierte Sicherheit bietet.

[3] IDC Directions 2019

Die verschiedenen Arten von „Benutzern" (links) möchten auf Zielressourcen (Daten, rechts) zugreifen. Verschiedene Identitäts- und Sicherheitskontrollen, die über Identity Management und Governance hinausgehen (dargestellt als einzelne Bausteine, Mitte), spielen alle eine Rolle bei der Sicherung des Zugriffs durch Benutzer auf Geräte, Netzwerke, Infrastruktur, Anwendungen und Daten.

Abbildung 1. Identitätsdefinierte Sicherheitsreferenzarchitektur[1]



Identity Security-Lösungen müssen mit ergänzenden Identity- und Sicherheitstechnologien zusammenarbeiten und diese integrieren, damit eine umfassende „Zero Trust"-Sicherheitslösung entsteht.

Ist Ihre „Zero Trust"-Strategie auf einen Identity Security-Ansatz abgestimmt?

Mit dieser Checkliste können Sie sicherstellen, dass Ihre „Zero Trust"-Strategie auf eine Identity Security-Strategie abgestimmt ist, die mit den sich ändernden Geschäfts- und Sicherheitsanforderungen wachsen und sich anpassen kann.

- **Implementieren Sie ein Identity Warehouse:** Legen Sie ein zentrales Verzeichnis von Identitätsdaten an, das vollständigen Einblick in den Zugriff und das Verständnis für die Identitäten aller Ihrer Benutzer, nichtmenschlichen Einheiten, Geräte und Datenquellen (einschließlich Schatten-IT) bietet.
- **Führen Sie strenge Zugriffskontrollen ein:** Weisen Sie mithilfe von Rollen und der Verwaltung von Zugriffsrichtlinien den Zugriff auf Daten und Anwendungsressourcen nur dort zu, wo er benötigt wird, und legen Sie Richtlinien für die Aufgabentrennung fest, um potenziell toxische Zugriffskombinationen zu vermeiden.

- **Befolgen Sie das „Least Privilege"-Prinzip** Überprüfen Sie kontinuierlich die Identitätsberechtigungen und Rollen Ihrer Benutzer und passen Sie diese an, um sicherzustellen, dass sie im richtigen Umfang und zur richtigen Zeit Zugriff auf die richtigen Ressourcen haben.
- **Überwachen Sie Aktivitätsdaten:** Erfassen Sie, wie Benutzer ihren Zugriff auf die Ressourcen Ihres Unternehmens nutzen, und überwachen Sie diese Protokolle auf verdächtiges Verhalten hin.
- **Warnen Sie bei Aktivitätsdaten:** Kennzeichnen Sie verdächtige Zugriffsaktivitäten oder Änderungen an Berechtigungen und benachrichtigen Sie die zuständigen Administratoren.
- **Entfernen Sie ungenutzten Zugriff:** Deprovisionieren Sie automatisch Zugriffe, die nicht mehr benötigt werden.
- **Automatisieren Sie die Reaktion auf Vorfälle:** Ändern oder unterbinden Sie den Zugriff automatisch, wenn sich die Attribute oder der Standort eines Benutzers ändern.
- **Koordinieren Sie die Reaktion auf Vorfälle:** Integrieren Sie Ihre Sicherheits- und Identitätssysteme, um einen ganzheitlichen Überblick über Sicherheitsereignisse zu erhalten, die eine potenzielle Kompromittierung signalisieren könnten. Führen Sie automatisch Abhilfemaßnahmen durch, wenn riskante Aktivitäten entdeckt werden.

Unternehmen Sie den nächsten Schritt

SailPoint Identity Security bildet den Grundstein für eine effektive „Zero Trust"-Strategie. Die Vitalität einer Zero Trust-Architektur hängt von der Integrität der Identitäten, der Wirksamkeit und Stärke der Zugriffskontrollrichtlinien und der Kontinuität der Governance über Identitäten und Zugriff in Ihrer hybriden IT-Umgebung ab. Als führender Anbieter im Bereich Identity bietet SailPoint Technologien, die den Lebenszyklus von Identitäten automatisieren, die Integrität von Identitätsattributen verwalten, durch dynamische Zugriffskontrollen, rollenbasierte Richtlinien und Aufgabentrennung das „Least Privilege"-Prinzip durchsetzen und kontinuierlich Zugriffsrisiken mithilfe von KI/ML auswerten, steuern und darauf reagieren.

Besuchen Sie **sailpoint.com/solutions/zero-trust**, um mehr zu erfahren.

ÜBER SAILPOINT

SailPoint ist der führende Anbieter von Identity Security für das moderne Unternehmen. Gestützt auf leistungsstarke KI- und ML-Technologien, automatisiert SailPoint die Verwaltung und Kontrolle aller Zugriffe, damit stets nur die richtigen Identitäten zur richtigen Zeit Zugriff auf die benötigten Technologieressourcen erhalten. Unsere hochentwickelte Identity-Plattform integriert sich nahtlos in bestehende Systeme und Arbeitsabläufe und bietet einen einzigartigen Überblick über alle Identitäten und deren Zugriffe. Wir holen unsere Kunden da ab, wo sie stehen: mit einer intelligenten Identity-Lösung, die den Skalierungs- und Geschwindigkeitsanforderungen und den komplexen Umgebungen moderner Unternehmen gerecht wird. SailPoint befähigt die anspruchsvollsten Unternehmen weltweit, ein Sicherheitsfundament zu schaffen, das auf Identity Security basiert.

EB2071-2201