Zero Trust ebnet den Weg

Da Unternehmen immer mehr digitale Projekte verfolgen, sich an eine Belegschaft anpassen müssen, die von überall aus arbeitet, und stets neue Erfahrungen einer Cloud-Nutzung machen, ist Zero Trust heute von zentraler Bedeutung für die IT-Sicherheit.

Seit Forrester den Begriff «Zero Trust» im Jahr 2021 eingeführt hat, ist er in aller Munde – aber nie war der Ansatz so präsent wie heute. Und die Identität – wem man vertrauen kann und womit – ist zentral für Zero Trust. Folgende Grundsätze in der Sicherheitsstrategie des Unternehmens sollten beachtet werden:

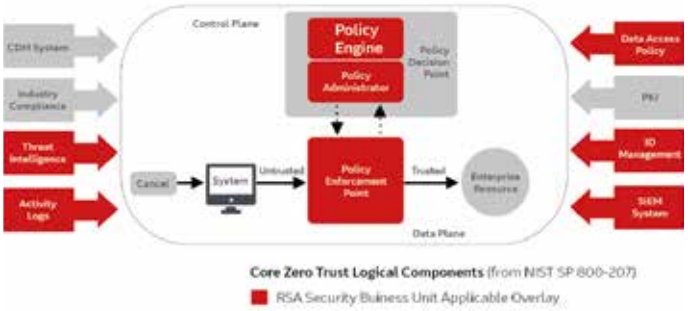
Das richtige Mass an Vertrauen
In diesem Sinne bedeutet «Zero Trust», das richtige Mass an Vertrauen zu schaffen, sei es in einen Benutzer oder ein Gerät, bevor der Zugang zu den Ressourcen der Organisation gewährt wird. Das erforderliche Mass an Vertrauen hängt davon ab, wem oder was und worauf man den Zugang gewähren möchte sowie weiteren Faktoren, die sich alle ändern werden, wenn sich Zugangsumgebung und Kontext ändern.

Ein ständiges Unterfangen
Zero Trust ist weder eine Technologie noch ein Produkt – es ist eine Denkweise. Die Anwendung der Zero-Trust-Prinzipien ist daher ein fortlaufendes Unterfangen und keine einmalige Angelegenheit. Bei Zero Trust geht es darum, Vertrauen als etwas zu betrachten, das kontinuierlich durch einen dynamischen Entscheidungsfindungsprozess aufgebaut werden muss und ständig von sich ändernden Rahmenbedingungen und Risiken beeinflusst wird.

Steckt in den Details
Das NIST (National Institute of Standarts and Technology) hat sieben Grundsätze als Teil seiner Zero-Trust-Architektur definiert. Die Einhaltung erfordert die Beachtung einer Vielzahl detaillierter Aufgaben im Dienste der wichtigsten Ziele: Sicherung der gesamten Kommunikation unabhängig vom Standort, Gewährung des Zugangs auf Sitzungsbasis und Festlegung des Zugangs durch dynamische Richtlinien. Mehrere Komponenten des Identitäts- und Zugriffs-Managements sind für die Verwirklichung dieser Ziele unerlässlich.

SecurID: Zusammenstellung der Schlüsselkomponenten von Zero Trust

Mit den richtigen IAM-Funktionen kommt man von einem abstrakten Konzept zu einer Komponente der Sicherheitsstrategie.
Die Authentifizierung von Zugriffen ist einer der wichtigsten Bausteine von Zero Trust. U.a. stellt die Multi-Faktor-Authentifizierung (MFA) eine zentrale Funktion dar, um das Schutzniveau von Unternehmensressourcen zu erhöhen.
Je nach Rolle eines Nutzers und wie kritisch die Daten sind, mit denen er arbeitet, bieten sich sog. adaptive Faktoren an. Je nach ermitteltem Risiko (Risk-Scoring) werden zusätzliche Authentifizierungsfaktoren für den Zugriff hinzugezogen, z.B. biometrische Merkmale



oder Token. Für die Risikobewertung kommen Parameter wie Standort, Gerät oder Service, von dem aus zugegriffen wird, zum Einsatz.

SecurID bietet eine Reihe von MFA-Methoden sowie Governance- und Lifecycle-Funktionen, die eine Governance-basierte Autorisierung des Zugriffs ermöglichen.
Die umfassenden Funktionen und Möglichkeiten für Sicherheit und Komfort machen die Entscheidung leicht:

- Authentifizierungsmöglichkeiten für unterschiedliche Benutzer und organisatorische Anforderungen
- Einfache Erweiterung on-premise auf die Cloud
- Ständig aktiv mit 99,95-prozentiger Verfügbarkeit und einer einzigartigen «No-Fail»-Funktion für Windows und macOS
- RSA Ready-Technologie-Integrationen für spezifische Zugangsumgebungen

Die Lösung SecurID Governance & Lifecycle (IGL) bietet globalen Unternehmenskunden Identity-Governance- und Verwaltungsfunktionen, die sie benötigen, um Transparenz, Einblick und Kontrolle über den Zugriff auf alle Anwendungen, Systeme und Daten zu erhalten.
SecurID Governance & Lifecycle Cloud erweitert den vollen Funktionsumfang unserer marktführenden Lösung auf die Cloud und sorgt dafür, dass die weltweit sicherheitssensibelsten Unternehmen dynamisch arbeiten, Innovationen beschleunigen und Zero-Trust-Sicherheit mittels Durchsetzung eines Zugriffsmodells mit geringsten Rechten und Unterstützung durch Identifizierung und Beseitigung verwaister Konten und übermässig genutzter Benutzer vorantreiben können. ■

Arrow ECS Internet Security AG
Richtistrasse 11, CH-8304 Wallisellen
✆ +41 (0)43 222 80 00
www.arrow.com