SecurID

Zero Trust: Identitäts- und Zugriffsmanagement ebnet den Weg

Von Zero Trust ist schon immer die Rede **Forrester hat den Begriff im Jahr 2010 eingeführt**, aber die Implementierung von Zero Trust war noch nie so dringend wie jetzt. In dem Maße, in dem Unternehmen mehr digitale Projekte verfolgen, sich an eine Belegschaft anpassen, die von überall aus arbeitet, und neue Möglichkeiten in der Cloud erkunden, wird die Idee von **Zero Trust** heutzutage von zentraler Bedeutung für die IT-Sicherheit. Identität – die Vorstellung, wem und was vertraut werden kann – ist für Zero Trust dabei von zentraler Bedeutung. Wenn Sie über die Rolle von Zero Trust in der Sicherheitsstrategie Ihres Unternehmens nachdenken, sollten Sie die folgenden Grundlagen im Hinterkopf behalten.

Bei Zero Trust geht es um das richtige Maß an Vertrauen

Der Begriff legt keinerlei Vertrauen nahe, aber es geht hauptsächlich darum, Vertrauen nur im Falle einer klaren Vertrauensbasis zu schenken – sogar innerhalb des Netzwerkperimeters eines Unternehmens. In diesem Sinne bedeutet Zero Trust, für Nutzer oder Geräte die richtige Vertrauensstufe einzurichten, bevor der Zugriff auf die Ressourcen des Unternehmens gewährt wird. Das erforderliche Maß an Vertrauen hängt davon ab, wem oder was man Zugang gewähren möchte, worauf man zugreifen möchte und von anderen Faktoren, die sich alle ändern werden, wenn sich die Zugangsumgebung und der Kontext ändern.

Zero Trust ist ein kontinuierliches Bestreben

Zero Trust ist keine Technologie oder ein Produkt; es ist eine Denkweise. Die Anwendung des Zero-Trust-Prinzips ist daher ein dauerhaftes Unterfangen und keine einmalige Bereitstellung. Bei Zero Trust geht es darum, Vertrauen als etwas zu betrachten, das in einem Prozess dynamischer Entscheidungsfindung, der ständig von sich ändernden Kontexten und Risiken beeinflusst wird, kontinuierlich aufgebaut werden muss.

Zero Trust steckt im Detail (definiert von NIST)

NIST hat im Rahmen seiner **Zero-Trust-Architektur** sieben Grundsätze aufgestellt. Um diese Grundsätze zu befolgen, müssen eine Vielzahl von Detailaufgaben im Blick auf die folgenden zentralen Ziele berücksichtigt werden: Sichern der gesamten Kommunikation unabhängig vom Standort, Gewähren des Zugriffs auf Sitzungsbasis und Festlegen des Zugriffs mit dynamischen Richtlinien. Zur Umsetzung dieser Ziele sind diverse Komponenten des Identitäts- und Zugriffsmanagements von Belang, einschließlich einer Policy Engine, eines Richtlinienadministrators und der Richtliniendurchsetzung basierend auf Datenzugriffsrichtlinien.

In dem Maße, in dem Unternehmen mehr digitale Projekte verfolgen, sich an eine Belegschaft anpassen, die von überall aus arbeitet, und neue Möglichkeiten in der Cloud erkunden, wird die Idee von Zero Trust heutzutage von zentraler Bedeutung für die IT-Sicherheit.

SecurID: Zusammenstellung von Kernkomponenten für Zero Trust

SecurID bietet die erforderlichen Identitäts- und Zugriffsmanagementfunktionen, um die Zero-Trust-Grundsätze von NIST zu erfüllen. Verwendet werden dafür:

Rollen- und attributbasierter Zugriff, bedingter Zugriff und risikobasierte Analysen – all dies ist für die Einrichtung der von NIST geforderten Policy Engine und eines Policy Decision Point von grundlegender Bedeutung

Die Fähigkeit, als Richtlinienadministrator zu fungieren, mit **einer Reihe von Authentifizierungsmethoden**, um den Zugriff zu bestimmen, wenn er am Richtliniendurchsetzungspunkt angefordert wird

Governance- und Lebenszyklusfunktionen, die die Grundlage für eine **Governance-fokussierte und sichtbarkeitsgesteuerte Autorisierung** des Zugangs zu Ressourcen schaffen

Integration mit Identitätssystemen wie Microsoft Active Directory (AD), Cloud-basiertes Azure AD und Amazon Web Services (AWS) AD, um Identitäten mit den Richtlinien, der Verwaltung und den Methoden zu integrieren, die für eine Zero-Trust-Architektur erforderlich sind

Erfahren Sie mehr darüber, wie SecurID die Herausforderungen von IAM angeht, die Zero Trust mit sich bringt, mit umfassenden Funktionen von der Authentifizierung bis hin zur Identitäts-Governance und

Informationen über SecurID

SecurID, ein RSA-Unternehmen, ist eine Identitätsplattform, der bereits 13.000 Unternehmen auf der ganzen Welt vertrauen. Sie verwaltet 50 Millionen Identitäten und bietet 30 Millionen Benutzern einen sicheren und bequemen Zugriff. Mit SecurID können Unternehmen in einer digitalen Welt erfolgreich sein und verfügen über umfassende Funktionen für moderne Authentifizierung, Lebenszyklusmanagement und Identity Governance. Ob in der Cloud oder On-Premise – SecurID verbindet Menschen mit den digitalen Ressourcen, von denen sie abhängig sind, wo immer sie leben, arbeiten und spielen. Weitere Informationen finden Sie unter **securid.com**.

SecurID
An RSA Business