PRISMA ACCESS
BY PALO ALTO NETWORKS

Wie Sie das „Zero Trust“-Prinzip auf Cloud-Umgebungen anwenden

Das „Zero Trust“-Prinzip zielt in erster Linie darauf ab, implizites Vertrauen abzubauen und stärkt somit den Sicherheitsstatus und Datenschutz innerhalb eines Unternehmens. Das ist wichtig, denn Vertrauen wird oft ausgenutzt – zum Beispiel der Glauben, dass jeder, dem der physische Zugang zu einem Gebäude gewährt wird, auch Zugriff auf das Netzwerk haben sollte. Mit einem solchen Ansatz erleichtern Unternehmen Hackern die Einschleusung ins Netzwerk und die Ausbreitung darin, denn nach Infiltrierung eines Endpunkts ist es für Angreifer ein Leichtes, durch Command-and-Control-Aktivitäten weiter in das Netzwerk einzudringen und Schaden anzurichten.

Experten arbeiten bereits seit Jahren an Sicherheitsstrategien für Unternehmensnetzwerke, die nicht auf Vertrauen basieren, und haben zu diesem Zweck zum Beispiel verschiedene Punktlösungen eingeführt. So richtige Erfolge wurden bislang jedoch nicht erzielt. Jetzt, wo so viele Unternehmen ihre Anwendungen, Workloads und Ressourcen von internen Rechenzentren in Hybrid- und/oder Public Cloud-Umgebungen und SaaS-Modelle migrieren, haben Sicherheitsteams jedoch die Chance, von vorne zu beginnen und das „Zero Trust“-Prinzip in die gesamte Cloud-Infrastruktur zu integrieren. Doch was bedeutet Zero Trust konkret für Anwendungen in der Cloud?

Wie Sie das „Zero Trust“-Prinzip auf Cloud-Umgebungen anwenden

Einer IDG-Studie zufolge hatten 73 % der befragten Unternehmen 2018 bereits einen Teil ihrer Anwendungen oder Infrastruktur in die Cloud migriert. Bei den übrigen Unternehmen sei eine Migration für 2019 geplant.[1] Dabei sind Anbieter von Cloud-Services wie Google Cloud Platform (GCP™), Amazon Web Services (AWS®) und Microsoft Azure® zwar für die Infrastruktur, aber nicht für den Schutz des Unternehmens vor Cyberrisiken verantwortlich. Im Rahmen des Modells der gemeinsamen Verantwortung liegt es am Kunden, seine Unternehmensdaten und -anwendungen in der Cloud hinreichend zu schützen. Leider stehen Sicherheitsteams hier vor einer Reihe komplexer Herausforderungen, wie nicht autorisiertem Netzwerkzugriff oder der uneinheitlichen Durchsetzung von Sicherheitsrichtlinien für Daten, Benutzer und Geräte auf dem Netzwerk. Daher überrascht es nicht, dass laut Studie „40 % der Datenschutzverletzungen durch unbefugten Zugriff legitimer Benutzer verursacht werden“ und dass „57 % der Unternehmen der nicht autorisierte Fernzugriff auf ihr Netzwerk Sorgen bereitet.“[2]

Der Schutz von Cloud-Umgebungen wird durch den Multi-Cloud-Ansatz vieler Unternehmen zusätzlich erschwert. Public Cloud-Services bieten Unternehmen mehr Flexibilität und meist auch Kosteneinsparungen, wobei oft unterschiedliche Anbieter für verschiedene Geschäftsbereiche oder -anforderungen hinzugezogen werden. Zudem nutzen besonders größere Unternehmen mit mehreren Filialen oder vielen Telearbeitern gerne SaaS-Anwendungen wie Office 365®, Box und G Suite®, um ihre Produktivität und Kollaborationsfähigkeiten zu verbessern. Des Weiteren kommen ständig neue cloudbasierte Apps dazu, deren APIs unbedingt durch fein abgestufte Zugangskontrollen gesichert werden müssen. All diese Umgebungen, Apps, Ressourcen und Cloud-Services gebührend zu schützen und zu kontrollieren ist keine leichte Aufgabe. Genau hier kommt Zero Trust ins Spiel.

1. „2018 Cloud Computing Survey“, IDG, 14. August 2018, https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey.
2. „Remote Access Security: Challenges & Opportunities”, IDC InfoBrief, gesponsert von Akamai, September 2017, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf.

Was steckt hinter der Zero Trust-Strategie?

Die effektivsten Sicherheitsstrategien zielen darauf ab, implizites Vertrauen durch die Erteilung minimaler (d. h. nur unbedingt erforderlicher) Zugriffsrechte zu ersetzen. Eine Zero Trust-Strategie basiert auf dem Grundprinzip „never trust, always verify“ („Glauben Sie nichts ungeprüft!“) und weist verschiedenen Anwendungen und Benutzern standort- und geräteunabhängig unterschiedliche Zugriffsrechte zu. Zero Trust stellt ein Umdenken in der Sicherheitsbranche dar: eine Strategie, die den Zugriff aufs Netzwerk und auf die Cloud ohne angemessene Authentifizierungsverfahren komplett verwehrt.

Ein Grundsatz von Zero Trust ist, dass die Kontrolle nicht nach dem autorisierten Zugriff endet, sondern dass der Netzwerkverkehr durchgehend bis auf Anwendungsebene kontinuierlich geprüft wird. Findet diese laufende Überprüfung nicht statt, wird damit signalisiert, dass der Netzwerkverkehr vertrauenswürdig ist und daher keiner Prüfung bedarf. Das wiederum verstößt gegen das Zero Trust-Prinzip. Zudem werden Hackern dadurch Tür und Tor geöffnet: Wenn sie erst einmal das Gerät eines autorisierten Benutzers infiltriert haben, haben sie Zugang zu allem, was die Berechtigungen dieses Benutzers zulassen.

Leider ist genau das bei vielen erhältlichen Zero Trust-Produkten der Fall: Sie konzentrieren sich ausschließlich auf Zugriffskontrollen und bieten keine nachträglichen Maßnahmen zur Überprüfung und Abwehr von schädlichem Datenverkehr.

Zero Trust in der Cloud: Anforderungen

Forrester Research legt die Grundlagen der Zero Trust-Strategie folgendermaßen dar:

1. Stellt sicher, dass der Zugriff auf alle Ressourcen unabhängig vom Standort auf sichere Weise erfolgt.
2. Ersetzt implizites Vertrauen durch die Erteilung minimaler (d. h. nur unbedingt erforderlicher) Zugriffsrechte.
3. Kontrolliert und protokolliert den gesamten Datenverkehr.

Wenn Sie in Ihrem Unternehmen eine erfolgreiche Zero Trust-Strategie einführen wollen, muss sie all diese Vorgaben erfüllen. Dabei ist ein klarer Überblick über sämtliche cloudbasierte Anwendungen, über die in der Cloud gespeicherten Daten und die Benutzer und Services, die Zugriff darauf haben, unentbehrlich. Ebenso wichtig ist es zu wissen, wie sensibel die jeweiligen Daten sind, damit Zugangskontrollen entsprechend angepasst werden können.

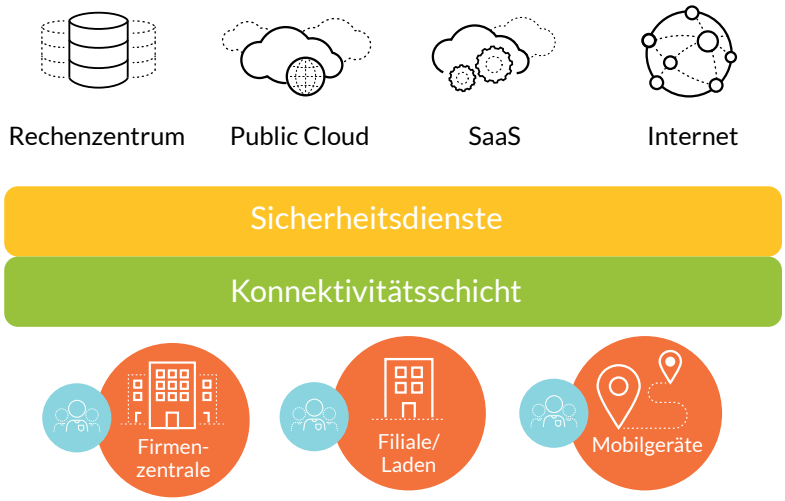

Abbildung 1: Cloud-Service-Architektur für umfassende Sicherheit mit Zero Trust

Außerdem sollte Ihre Zero Trust-Strategie für die Cloud unkompliziert und leicht zu verwalten sein. Denn wenn die Zugriffsrechte für Benutzer nicht standortunabhängig greifen, oder wenn die Authentifizierungsverfahren zu komplex sind, werden Benutzer versuchen, die Zugriffskontrollen zu umgehen und möglicherweise die Netzwerksicherheit gefährden. Benutzer sollten also gemäß ihren Zugangsrechten von verschiedenen Standorten und Geräten aus schnell und einfach auf Anwendungen und Daten zugreifen können.

Für eine auf Zero Trust basierende Sicherheitsstrategie brauchen Sie zunächst einmal cloudbasierte Sicherheitsmaßnahmen wie Sicherheitspunkte, die vorab festgelegte Richtlinien für die Verbindung zwischen Benutzern und Anwendungen durchsetzen. Indem Zugriffe und Datenflüsse bereits in der Cloud geprüft werden, anstatt erst in der Firmenzentrale, werden Ressourcen und Daten vor schädlichem Internetverkehr geschützt. Kurz gesagt: Bei einer Zero Trust-Strategie müssen Sie Ihre Ressourcen nicht einzeln mit Firewalls schützen, sorgen dafür, dass potenzielle Bedrohungen nicht ins Netzwerk dringen können und vereinfachen Ihre Netzwerkarchitektur.

Anwendungsbereich: Zero Trust für private Anwendungen in der Public Cloud

Die Grundsätze des kontextbasierten Zugriffs und der Bedrohungsabwehr sollten immer gemeinsam konsistent im gesamten Unternehmensnetzwerk angewandt werden, vom Rechenzentrum bis zur Cloud. Viele App-Entwickler und Unternehmen haben jedoch unterschiedliche Vorgehensweisen beim Thema Sicherheit, was einer umfassenden, kontextbasierten Sicherheitsstrategie im Wege stehen kann. Nichtsdestotrotz ist es wichtig, dass die Benutzererfahrung während der zunehmenden Verlagerung von Unternehmensanwendungen vom Rechenzentrum in die Cloud nicht beeinträchtigt wird und dass der Zugang zu diesen Anwendungen konsistent sicher bleibt, ganz gleich, von wo aus dieser erfolgt. Bei verwalteten Geräten sollten ausschließlich die dafür autorisierten Benutzer über Geräte, die die einschlägigen Sicherheitsanforderungen erfüllen, auf Anwendungen zugreifen können (ob im Rechenzentrum, in der Cloud oder als SaaS). Bei nicht verwalteten Geräten sollte es möglich sein, auf Anwendungen zuzugreifen, ohne die Geräte erst mit dem Unternehmensnetzwerk zu verbinden. Folglich sollten Benutzern nur die unbedingt erforderlichen Zugriffsrechte erteilt werden.

Anwendungsbereich: Zero Trust für SaaS-Anwendungen

Cloudbasierte Produktivitätsanwendungen sind extrem beliebt. Sie werden typischerweise von vielen verschiedenen Mitarbeitern, Auftragnehmern und Vertragspartnern genutzt, die von überall und diversen Geräten (unternehmenseigen oder BYOD) aus auf sie zugreifen. Aus diesem Grund sollten Unternehmen beim Schutz solcher SaaS-Anwendungen proaktive Maßnahmen und Richtlinien zur Prävention von Angriffen oder Sicherheitsverletzungen einführen.

Zero Trust bietet Ihren Sicherheitsteams einen detaillierten Überblick über sämtliche Anwendungen und deren Nutzung und somit die nötigen Einblicke, um fundiertere Entscheidungen bei der Cloud- und Netzwerksicherheit zu treffen. Durch Authentifizierungsverfahren, die den Zugriff auf unternehmenseigene Anwendungen über die Benutzeridentität regeln, können Sie die Wahrscheinlichkeit eines Angriffs oder Datenlecks erheblich reduzieren. Eine solche Strategie sieht zum Beispiel vor, dass Mitarbeiter mit verwalteten Geräten sofortigen und unbegrenzten Zugang zu den für sie zugelassenen Anwendungen bekommen, während Auftragnehmer und Vertragspartner mit unautorisierten Geräten nur dann Zugriff auf Anwendungen erhalten, wenn sie diese zur Erfüllung ihrer Aufgaben benötigen.

Anwendungsbereich: Zero Trust für DevOps in der Cloud

Wie in den meisten modernen Unternehmen arbeiten Ihre Entwickler wahrscheinlich bereits an neuen cloudbasierten Apps und nutzen dazu viele verschiedene APIs. Damit Ihre Mitarbeiter sicheren Zugang zu den von ihnen verwendeten APIs haben und Ihnen die dafür benötigten Kontextinformationen zur Verfügung stehen, ist ein hohes Maß an Transparenz erforderlich. Diese Kontextinformationen fließen in die Erstellung von Zero Trust-Sicherheitsrichtlinien ein, die Benutzern je nach Gerät und Position im Unternehmen die entsprechenden Zugriffsrechte zuweisen. Mithilfe der bereitgestellten Informationen beschränken Sie den Zugriff auf Ihr Netzwerk auf das absolut Nötigste und bieten Hackern so wenig Handlungsspielraum wie möglich.

In konventionellen Sicherheitsstrategien wird die Identität eines Benutzers erst auf der Konnektivitätsschicht geprüft – also ziemlich nah an den zentralen Unternehmensressourcen. Indem Sie diese Authentifizierungsverfahren auf die Schicht der Sicherheitsdienste verlegen, kommen nicht autorisierte Benutzer gar nicht erst in Kontakt mit den verwendeten APIs. Dies bietet Ihnen eine weitere Verteidigungslinie gegen potenzielle Angreifer, schützt Ihre Anmeldedaten und reduziert die Anzahl von Warnmeldungen, die bei fehlgeschlagenen Authentifizierungsversuchen generiert werden. Außerdem wird Ihren Teams dadurch die Entwicklung von Anwendungen in der Cloud erleichtert, denn Entwickler müssen nur mit der Konnektivitätsschicht der Cloud verbunden werden, und die Sicherheitsdienste sorgen dafür, dass diese Verbindung geschützt wird.

Zusammenfassung

Für Ihre Migration in die Cloud sollten Sie unbedingt in moderne Sicherheitsstrategien investieren, mit denen Sie neuen Bedrohungen einen Schritt voraus bleiben können. Ein Beispiel dafür ist eine Zero Trust-Strategie nach dem Grundsatz „Glauben Sie nichts ungeprüft!“.

Zero Trust baut auf umfassende Transparenz, die konsistente Durchsetzung von Sicherheitsrichtlinien im gesamten Netzwerk (und in der Cloud) und auf fein abgestufte Zugangskontrollen, die direkt auf Geräten oder in der Cloud angewandt werden können, um unautorisierten Zugriff und die oft damit einhergehenden Datenlecks zu verhindern. Anfragen von Benutzern sollten stets geprüft werden, damit ausschließlich autorisierte Benutzer mit den entsprechenden Rechten auf Ihre Anwendungen und Daten zugreifen können und die Verbindung geschützt ist – ganz gleich, wo sich Benutzer, Anwendungen oder Workloads befinden oder welches Gerät verwendet wird.

Doch der Netzwerkzugriff ist nur ein Aspekt von Zero Trust. Zu einer effektiven Zero Trust-Strategie, die die Wahrscheinlichkeit eines Angriffs auf ein Minimum reduzieren kann, gehört auch die Netzwerksegmentierung. Das gilt sowohl für Firewalls zum Schutz von Netzwerkanwendungen als auch für die Cloud. Nur so können Sie dafür sorgen, dass benutzerbasierte Zugriffsrechte umfassend bis auf Anwendungsebene greifen und dass nur bekannter Datenverkehr und legitime Anwendungskommunikation zugelassen werden.

Vor allem ermöglichen eine solch detaillierte Überprüfung und die daraus gewonnenen Informationen eine schnelle Bedrohungserkennung und -abwehr und verdeutlichen, welche geschäftskritischen Daten, Ressourcen, Anwendungen und Services wie zusammenhängen. So können Sicherheitsteams die Zero Trust-Strategie exakt auf die Unternehmensanforderungen und Netzwerkarchitektur abstimmen. Zero Trust bietet Ihnen also effektive präventive Funktionen, um sich gegen Hacker zu wappnen, die versuchen, über Geräte oder Anwendungen in Ihr Unternehmensnetzwerk einzudringen.

Mit Zero Trust können Sie:

- die volle Kontrolle über Daten, Ressourcen und Risiken behalten
- für konsistente und umfassende Sicherheit sorgen
- Ihren Betrieb schnell und flexibel an technische Neuerungen anpassen und diese sogar antizipieren
- Ihre Betriebskosten reduzieren und Komplexität vermeiden

Der Umstieg auf die Cloud muss Ihnen keine Kopfschmerzen bereiten. Mithilfe einer Zero Trust-Strategie behalten Sie während Ihrer digitalen Transformation den Überblick über sämtliche vernetzte Ressourcen und Geräte und sorgen für lückenlose Sicherheit.

Weitere Informationen finden Sie unter paloaltonetworks.com/cloud-security/zero-trust-cloud-security.

PRISMA ACCESS
BY PALO ALTO NETWORKS

Oval Tower, De Entrée 99 -197
1101HE Amsterdam
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de