White Paper

Zero Trust im Rückblick: Meilensteine auf dem Weg zu einem völlig neuen Konzept für die Unternehmenssicherheit

Warum ein Rückblick?

Die Erfindung des Zero-Trust-Konzepts markierte einen absoluten Wendepunkt in der Geschichte der Unternehmenssicherheit. So ist jedenfalls die Überzeugung zahlreicher Cybersicherheitsprofis, denen sich damit radikal neuartige Denkansätze zum Schutz geschäftskritischer Netzwerke und Ressourcen eröffneten — mitsamt der dort gespeicherten und gehosteten Dateien und Dokumente, der Kommunikations- und Produktivitätstools mit transformativem Potenzial.

Die revolutionäre Tragweite des Zero-Trust-Modells für die Cybersicherheit lässt sich jedoch erst ermessen, wenn man die Schwächen des Legacy-Ansatzes der Netzwerksicherheit kennt und die Entwicklung des Zero-Trust-Konzepts — von seiner erstmaligen Formulierung bis hin zur konsequenten Revision jahrzehntelang gültiger Prinzipien — vor diesem Hintergrund Revue passieren lässt.

Flache Netzwerke mit Perimetersicherheit

Zur Beschreibung von Legacy-Netzwerkarchitekturen und den entsprechenden Sicherheitsmaßnahmen wird gerne auf zwei Metaphern zurückgegriffen: „Hub and Spoke“ (Speichenarchitektur) bzw. „Castle and Moat“ (Festung mit Burggraben). Nicht zufällig stehen in beiden Fällen jahrhundertealte technische Errungenschaften Pate.

Als Speichenarchitektur wird die Anordnung mehrerer Satellitennetzwerke um eine zentrale „Nabe“ bezeichnet. Bei diesem Modell läuft der gesamte interne und externe Traffic über einen Security-Stack in einem zentralen Rechenzentrum, bevor er an sein eigentliches Ziel weitergeleitet wird. Dieser Ansatz funktionierte jahrzehntelang gut. Unter heutigen Vorzeichen — also der Verlagerung der IT-Infrastruktur in die Cloud, Umstieg auf hybride oder dezentrale Arbeitskonzepte, wachsende Bedeutung der Mobilität im Geschäftsalltag — erweist sie sich jedoch zunehmend als allzu kompliziert und teuer.

Das Bild der „Festung mit Burggraben“ beschreibt ein in sich abgeschlossenes Netzwerk, das so angelegt ist, dass Eindringlinge abgewehrt, befugten Usern jedoch Einlass gewährt wird. Sicherheitsappliances im organisationseigenen Rechenzentrum fungieren hier quasi als Wachposten. Das historische Verteidigungskonzept wurde letztlich durch die Verbreitung von Kanonen obsolet. Mit der Verlagerung vieler Anwendungen in die Cloud sowie der Umstellung von Präsenz- auf Remote-Arbeit, mit der sich die User zunehmend außerhalb der „Festung“ befanden, bot auch der virtuelle Burggraben mit Zugbrücke keinen ausreichenden Schutz mehr für Unternehmensnetzwerke.

VPNs und WLAN sorgten für weitere Komplikationen. Das Festungskonzept gab Administratoren nämlich keine Möglichkeit, die Bewegungsfreiheit von Gästen so einzuschränken, dass sie zwar Zugang zum Netzwerk erhalten, aber nicht auf sämtliche Anwendungen und Daten zugreifen können. Die Notwendigkeit, externe Endgeräte mit Unternehmensnetzwerken zu verbinden, ohne deren Sicherheit zu gefährden, ließ sich nur durch Segmentierung bewältigen.

Auf Dauer musste eine bessere Lösung her.

802.1X und das Problem der unbewachten Nebeneingänge

2001 veröffentlichte die IEEE Standards Association das 802.1X-Protokoll als Standard für die Netzwerkzugangskontrolle.

> „Ein Mittel zur Authentifizierung und Autorisierung von Geräten, die an einen LAN-Port mit Point-to-Point-Konnektivität angeschlossen sind, und zur Verhinderung des Zugriffs auf diesen Port, wenn das Verfahren zur Authentifizierung und Autorisierung fehlschlägt.“
>
> Definition des IEEE zum 802.1X-Protokoll →

Konkret bedeutete das, dass im Lieferumfang vieler drahtloser Geräte ein Supplicant bzw. Client inbegriffen war, der die Authentifizierung des Endgeräts ermöglichte, bevor eine Verbindung zum Netzwerk zugelassen wurde. Hinter diesem Vorstoß steckte die Absicht, kabelgebundene und drahtlose Netzwerke vor dem Zugriff nicht verwalteter Geräte und unbefugter User zu schützen. Am besten stellt man sich die Authentifizierung als Einlasskontrolle am Eingang zum Netzwerk vor.

Leider waren damit keineswegs alle Probleme gelöst. Interne Netzwerke basierten grundsätzlich auf der automatischen Einstufung aller User und Geräte als vertrauenswürdig. Entsprechend war der Versuch, nachträglich eine Authentifizierung bzw. Autorisierung zu erzwingen, mit hohem Aufwand verbunden. Eine effektive Netzwerkzugangskontrolle setzt voraus, dass sämtliche zugänglichen Ports gesperrt werden. In der Praxis scheiterte dies daran, dass längst nicht alle Geräte 802.1X-fähig waren. Durch die zunehmende Verbreitung vernetzter Geräte (Drucker, Ausweislesegeräte etc.) entstanden massive Sicherheitslücken. Das führte gewissermaßen dazu, dass zwar am Haupteingang eine Einlasskontrolle mit Überprüfung der Identität und Zugriffsberechtigungen durchgeführt wurde, aber mehrere (teilweise sogar Dutzende) Nebeneingänge vollkommen unbewacht blieben.

Der Fall von Jericho: Abschied vom Netzwerkperimeter

Der Trend zur zunehmenden Nutzung privater Endgeräte blieb in den folgenden Jahren ungebrochen. Entsprechend sahen sich die Organisationen gezwungen, zuverlässige Methoden zur Gewährleistung der Sicherheit von Geräten zu entwickeln, die nicht hinter Festungsmauern verschanzt sind. Parallel dazu wurde durch die Zunahme an verschlüsseltem Traffic die Wirksamkeit von Perimeter-Firewalls beeinträchtigt. Damit standen Organisationen vor der Wahl, entweder ihre Kapazitäten zur Entschlüsselung und Überprüfung massiv auszubauen oder aber verschlüsselten Traffic ungeprüft durchzulassen.

Um diesen Herausforderungen zu begegnen, entstand 2003 das Jericho Forum als Initiative führender europäischer IT-Experten, die sich intensiv mit den Themen User-Authentifizierung, Verschlüsselung, Identitätsmanagement und Richtliniendurchsetzung auseinandersetzte. Der offiziellen Gründung im Januar 2004 folgte die Veröffentlichung mehrerer Whitepaper und Positionspapiere, in denen die Arbeitsgruppe den Begriff der „Deperimeterisierung“ vorstellte und erläuterte.

Der Name nimmt Bezug auf die biblische Erzählung von der Zerstörung Jerichos durch die Israeliten, deren Posaunen die Stadtmauern zum Einsturz gebracht haben sollen. Das Forum verschrieb sich dem kaum weniger ehrgeizigen Ziel, eine Lösung für das Problem zu erarbeiten, ohne Netzwerkperimeter unternehmensweit einen sicheren Datenfluss zu gewährleisten.

Detaillierte Handlungsempfehlungen für die Governance perimeterloser Netzwerke wurden in den Jericho Forum Commandments veröffentlicht. Leider ging die Bereitstellung und Verwaltung der empfohlenen Kontrollmechanismen und Maßnahmen zur Risikominderung weit über die damaligen Kapazitäten der meisten Unternehmen hinaus.

„Zero Trust“ als neues Schlagwort

2010 veröffentlichte der Forrester-Analyst John Kindervag einen Artikel mit dem Titel „No More Chewy Centers: Introducing The Zero Trust Model Of Information Security“ — und hatte damit ein neues Schlagwort geprägt, das ein radikales Umdenken in Bezug auf Netzwerksicherheit signalisierte. Eine Kernaussage des Artikels lautete, dass kein Akteur mehr auf der

Grundlage seiner Präsenz im Netzwerk automatisch als vertrauenswürdig eingestuft werden darf.

„Damals kam sowas auf wie ‚Identität ist der neue Perimeter'", erinnert sich Lisa Lorenzin, Field CTO bei Zscaler und Zero-Trust-Expertin. „In der Praxis sah das so aus, dass man einen User authentifizierte und ihm dann anhand seiner Identität bestimmte Berechtigungen zuwies. Wenn wir Glück hatten, gelang es uns manchmal, ein paar kontextbezogene Daten zu erfassen: Haben wir es hier z. B. mit einem verwalteten oder nicht verwalteten Gerät zu tun? Auf der Grundlage dieser rudimentären Informationen wurde dann entschieden, welche Zugriffsberechtigungen der betreffende User erhalten sollte."

Ein gewisser Fortschritt war damit erreicht. Jedoch blieb die Unternehmenssicherheit auch weiterhin dem Grundsatz der Netzwerksicherung verhaftet. Noch war man nicht soweit, sich ganz davon zu lösen und völlig neue Wege einzuschlagen. Das Scheitern einer konsequenten Umsetzung der Zero-Trust-Prinzipien war damit vorprogrammiert, zumal immer noch das gleiche netzwerkbezogene Toolset zum Einsatz kam wie zuvor: 802.1X und RADIUS auf der Verbindungsebene, identitätsorientierte Firewalls auf der Netzwerkebene usw.

Mit anderen Worten: Netzwerkzugangskontrolle in neuem Gewand.

BeyondCorp reagiert und geht voran

Dann brachte eine spektakuläre Aktion chinesischer Hacker mit Verbindungen zu den Streitkräften der Volksrepublik neue Brisanz in die Diskussion um Vertrauen und Zugriffsberechtigungen. Anfang 2010 veröffentliche Google Details zu einer Anschlagsserie, die im Vorjahr eine Reihe prominenter High-Tech-Unternehmen ins Visier genommen hatte. Neben Google selbst zählten auch Akamai, Adobe und Juniper Networks zu den Opfern. Sicherheitsexperten von McAfee gaben der Anschlagsserie den Namen „Operation Aurora".

Damit hatten die Hacker freilich ins Wespennest der US-amerikanischen Entwickler-Elite gestochen und unabsichtlich die Arbeit an praxistauglichen Zero-Trust-Architekturen in den führenden Technologielaboren des Landes vorangetrieben. Google reagierte auf Operation Aurora mit der Entwicklung von BeyondCorp und verfolgte dabei im Wesentlichen das Ziel, **„die Zugriffskontrollen vom Netzwerkperimeter zu den einzelnen Usern zu verlagern, [...] um ein sicheres Arbeiten von so gut wie jedem beliebigen Standort ohne Einsatz herkömmlicher VPNs zu ermöglichen".**

„Google ist ein Unternehmen mit lauter Software-Entwicklern, das von Software-Entwicklern geleitet wird, über ein de facto unbegrenztes Budget verfügt und verglichen mit anderen Unternehmen wenig Legacy-Infrastruktur hat", merkt Lorenzin an. „Trotzdem brauchte man dazu sieben Jahre und sechs Whitepaper mit Empfehlungen für Design und Implementierung."

Trotz der gut dokumentierten Vorlage von Google blieb eine echte Zero-Trust-Architektur für die Mehrzahl der Unternehmen weiterhin unerreichbar. Ungeachtet aller Bemühungen, „anderen Organisationen den Weg zur Realisierung eigener Implementierungen eines Zero-Trust-Netzwerks zu ebnen", war es noch ein weiter Weg bis zur Verwirklichung dieser Zukunftsvisionen.

Aufgrund der wachsenden Beliebtheit von Cloud- und Mobil-Anwendungen befand sich mittlerweile ein Großteil der für User zugänglichen Daten außerhalb des Netzwerkperimeters. Ein Umdenken in Bezug auf die Sicherung dieser Daten und die Vergabe von Zugriffsberechtigungen war somit dringendst erforderlich.

CARTA und ZTNA: Gartner schreibt das nächste Kapitel

Die nächsten bedeutenden Fortschritte auf dem Weg zur Entwicklung eines allgemein gültigen Zero-Trust-Frameworks waren dem Forschungsunternehmen Gartner — genauer gesagt: der Veröffentlichung seines Continuous Adaptive Risk and Trust Assessment (CARTA) — zu verdanken. Das Positionspapier erschien 2010, als der Begriff „Zero Trust" in der Tech-Welt zwar im Umlauf, aber nicht unbedingt als Priorität präsent war.

Insbesondere wurde hier die Notwendigkeit thematisiert, Zugriffsberechtigungen nur basierend auf präzisen Informationen zur Identität und Rolle des Users sowie einer dynamischen Bewertung von Umgebung bzw. Kontext zu gewähren.

Lorenzin bezeichnet CARTA als „ein großartiges Modell, das sehr viel mehr Aufmerksamkeit verdient hätte".

Die dort formulierten Grundsätze fanden später Eingang in das ebenfalls von Gartner entwickelte ZTNA-

Framework (Zero Trust Network Access) — wobei interessanterweise die Betonung weiterhin auf Netzwerken als Zugriffsziel liegt. Obwohl die Veröffentlichung wenig unmittelbare Wirkung erzielte, darf der damit geleistete Beitrag zur weiteren Entwicklung des Zero-Trust-Konzepts keinesfalls unterschätzt werden, eben weil CARTA quasi das Fundament für ZTNA legte.

Ebenfalls von Gartner stammte die nächste wichtige Erkenntnis, nämlich die Feststellung einer zunehmenden Konvergenz der Bereiche Netzwerkarchitektur und Sicherheit. Aus dieser Beobachtung heraus entstand 2019 das SASE-Framework (Secure Access Service Edge). Die damit geschlossene Ehe zwischen beiden Kategorien wurde bereits 2021 mit der Einführung einer neuen Marktkategorie wieder geschieden, für die Gartner den Begriff „Secure Service Edge“ (SSE) prägte. Konkret handelte es sich um SASE abzüglich WAN.

Ungeachtet der verschiedenen Bezeichnungen und Akronyme hatte Gartner sich längst die Deutungshoheit über das Zero-Trust-Konzept gesichert. Entsprechend versuchten die unterschiedlichen Anbieter nun, ihre jeweiligen Lösungen möglichst überzeugend als ZTNA, SASE oder SSE zu verkaufen.

Offizielle Absegnung: Zero Trust hält Einzug in US-Regierungsbehörden

Mit der Veröffentlichung von NIST 800-207 als Standard für Zero-Trust-Architekturen setzte das National Institute for Standards and Technology (NIST) 2020 einen neuen Maßstab für Cybersicherheit, der den Fokus auf den Schutz von Ressourcen legt. Die Einstufung als vertrauenswürdig darf demnach nie automatisch erfolgen, sondern muss ständig neu überprüft werden.

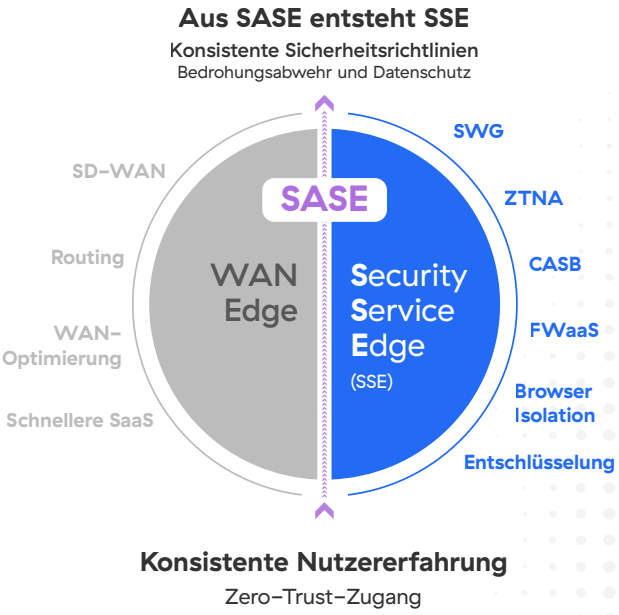
Die Altlasten von Perimeterschutz und VPN waren damit endgültig beseitigt. Der Schwerpunkt verlagerte sich vom Schutz des Netzwerks zum Schutz der User, Daten und Anwendungen, die über das Netzwerk miteinander interagieren. „Zero Trust“ stand nun unmissverständlich für kontextbasierte Zugriffsberechtigungen nach dem Prinzip der minimalen Rechtevergabe. Entsprechend erweiterte sich das Spektrum der möglichen Anwendungsfälle und Verbindungswege.

Der 800-207-Standard definiert zentrale Grundsätze und Annahmen für Zero Trust. Die drei wichtigsten Punkte (neben zahlreichen anderen) sind:

1. Keine Ressource wird automatisch als vertrauenswürdig eingestuft.

2. Sämtliche Kommunikationen werden standortunabhängig abgesichert. Verbindungen werden getrennt und Zugriffsanforderungen überprüft; diese Überprüfung erfolgt unter Berücksichtigung sämtlicher verfügbarer Kontextdaten zum User und zur jeweiligen Anforderung.

3. Ressourcen werden durchweg dynamisch authentifiziert und autorisiert, und Zugriff wird erst nach strikter Prüfung erteilt.



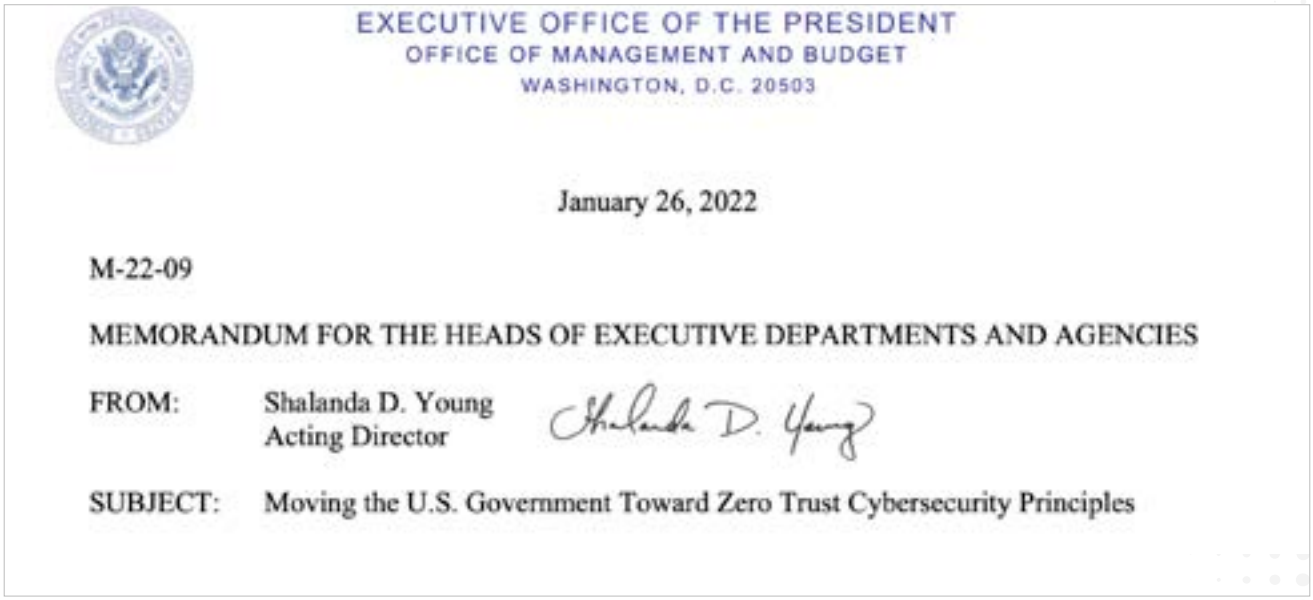
Der endgültige Tipping-Point war im Januar 2022 mit der Weisung M-22-09 des U.S. Office of Management and Budget erreicht. Die Behörde, die für die Umsetzung von Bundesprogrammen im Sinne der Exekutive zuständig ist, ordnete damit die Einführung von Zero-Trust-Architekturen in sämtlichen Regierungsbehörden bis 2024 an und legte präzise Meilensteine und Fristen für die Realisierung dieser Zielvorgabe fest.

Lorenzin begrüßt die neue Initiative: „Bisher gab es Handlungsempfehlungen. Es gab Administratormodelle. Mit der staatlichen Zero-Trust-Strategie reden wir nun endlich mal Tacheles."

Der 2021 bekannt gewordene Supply-Chain-Angriff auf die IT- Managementplattform SolarWinds, der Sicherheitsverletzungen bei mindestens neun US-Bundesbehörden verursachte — darunter die Ministerien für Inneres, Finanzen, Heimatschutz, Handel und Energie — war die wohl dreisteste und schädlichste Cyberattacke mit staatlicher Hilfe (in diesem Fall wird davon ausgegangen, dass der russische Geheimdienst seine Hände im Spiel hatte) seit Operation Aurora. Die US-Regierung reagierte darauf mit einem ausdrücklichen Bekenntnis zum Zero-Trust-Konzept als Leitstern ihrer offiziellen Cybersicherheitsstrategie.

Praktische Umsetzung des Konzepts

Die von Zscaler entwickelte Zero-Trust-Architektur orientiert sich eng am ZTA-Framework von NIST sowie an der Definition für SSE von Gartner. Über diese Branchenstandards hinaus beinhaltet das Zero-Trust-Konzept von Zscaler drei neue Denkansätze, die dazu beitragen, die praktische Umsetzung des Modells konsequent weiterzuführen.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

Zero Trust muss für den gesamten Traffic gelten

Ursprünglich wurde Zero Trust als neue Methode für den Schutz von Netzwerken konzipiert. Das Modell wurde dann auf Traffic außerhalb lokal installierter Unternehmensnetzwerke erweitert, bezog sich jedoch immer noch primär auf den ein-

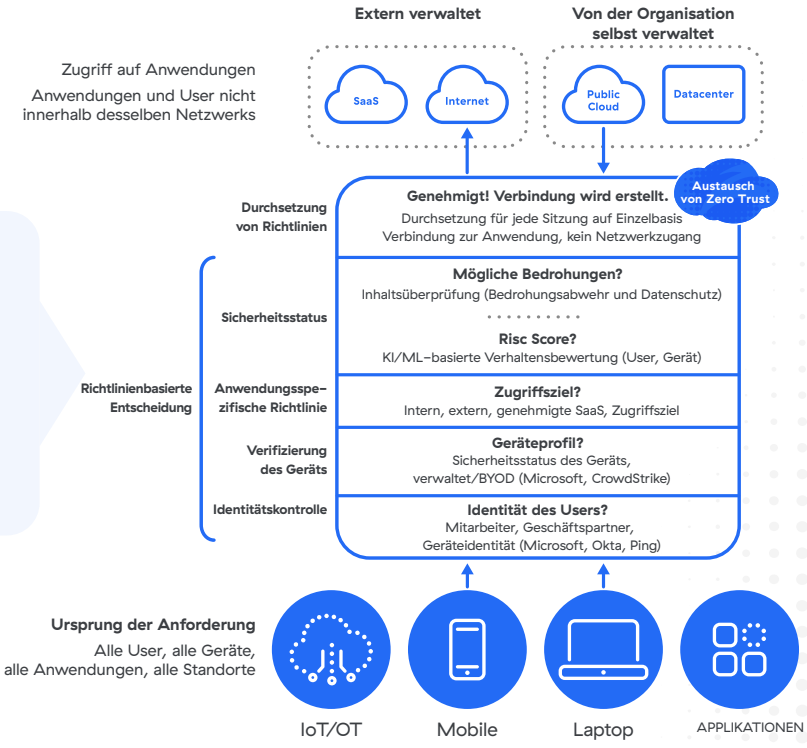
und ausgehenden Datenverkehr zu bzw. von unternehmenseigenen Anwendungen. Grundlage blieb weiterhin der Gedanke vom Netzwerk als zentralem Dreh- und Angelpunkt.

Inzwischen hat sich jedoch gezeigt, dass die Grundsätze des Zero-Trust-Konzepts für eine Vielzahl weiterer Anwendungsfälle gelten. Insbesondere betrifft dies den Schutz von SaaS-Anwendungen, von ein- und ausgehendem Traffic in öffentlichen Clouds sowie von Usern, die auf das öffentliche Internet zugreifen. Weiter ist zu beachten, dass der Traffic nicht nur von Usern, sondern auch von Workloads ausgehen kann. Zugriffsrichtlinien können transportunabhängig durchgesetzt werden, d. h. es spielt keine Rolle, über welchen Router bzw. welches Netzwerk (kabelgebunden oder kabellos, 4G oder 5G etc.) der Traffic fließt.

Zero-Trust-Prinzipien müssen auf den gesamten Traffic — unabhängig vom Ursprung und Zielort — angewandt werden. Andere Unterscheidungen, etwa zwischen vertrauenswürdigem und nicht vertrauenswürdigem Traffic oder zwischen Traffic innerhalb und außerhalb des Netzwerks, gehören längst der Vergangenheit an. Ähnlich obsolet ist auch die Klassifizierung von Verbindungen nach Ausgangs- und Zielort. Stattdessen müssen sämtliche Entitäten basierend auf Unternehmensrichtlinien direkt über eine Zero-Trust-Architektur verbunden werden — denn wenn das Internet als neues Unternehmensnetzwerk fungiert, sind sämtliche Verbindungen potenziell riskant.

Architektur der Zero Trust Exchange von Zscaler

Durchsetzung von Richtlinienentscheidungen für Einzelsitzungen in 150 RZ weltweit



1 Identität und Kontext sind die Voraussetzungen für Konnektivität

Identitätsprüfung ist das Kernprinzip des Zero-Trust-Konzepts. In der Vergangenheit wurden Identität und Konnektivität jedoch gerne verwechselt, was unweigerlich zum Scheitern des Modells führte. Identität ist nicht gleichbedeutend mit IP-Adressen, MAC-Adressen, Ports und Protocols.

OT-Geräte können sich von der Fabrik aus mit Netzwerken verbinden. User können sich vom Café aus einloggen. Das sagt aber noch nichts über ihre Vertrauenswürdigkeit aus. Verbindungen dürfen erst zugelassen werden, nachdem die Identität und der Kontext der betreffenden Entitäten überprüft wurden.

Wenn ein User Zugriff auf eine Ressource anfordert, müssen erstens Faktoren berücksichtigt werden, die sich auf seine Identität, seine Rolle oder Abteilung und sein Gerät beziehen, und zweitens die jeweils geltenden Sicherheitsrichtlinien. Was hat der User vor? Wo will er hin? Welche kontextbezogenen Faktoren können die Entscheidung beeinflussen, ihm Zugriff zu gewähren oder zu verweigern?

Kontext geht über Identität hinaus und wird kontinuierlich neu bewertet. Zu den weiteren Faktoren, die auf Anomalien untersucht werden können, zählen u. a. Geolocation, IP-Adresse, Sicherheitsstatus des Geräts und Tageszeit. Außerdem sollte eine Zero-Trust-Lösung Funktionen zur Entschlüsselung und Inline-Überprüfung des Traffics auf Bedrohungen und Exfiltrationsrisiken auch bei hohen Datenvolumen bereitstellen.

Mit der Zero Trust Exchange von Zscaler profitieren Unternehmen zudem von der laufenden Korrelation von Bedrohungsinformationen, die aus unserer Cloud sowie von Anbietern von Sicherheits- und Identitätsprüfungslösungen und anderen externen Technologiepartnern stammen. Diese Daten werden zur Ermittlung von Risiken und Unterstützung von Richtlinien- und Zugriffsentscheidungen ausgewertet.

2 Anwendungen (mitsamt ihrer jeweiligen Umgebungen) dürfen nur für befugte User sichtbar sein

Nachdem das Problem, vor der Gewährung von Zugriffsberechtigungen die Identität des Users zu überprüfen, erfolgreich gelöst wurde, stellt sich nun die nächste Herausforderung — diesen User mit den Ressourcen zu verbinden, auf die er Zugriff hat, ohne dass dadurch Sicherheitsrisiken entstehen. Dazu müssen zunächst Kontextdaten zu User, Gerät, Richtlinien und Umgebung erfasst und ausgewertet werden.

Durch Eliminieren der Ereignisbehandlungsroutinen für eingehende Remote-Verbindungen lässt sich die externe Angriffsfläche verkleinern. Ansonsten haben potenzielle Angreifer leichtes Spiel damit, anfällige VPN-Gateways oder exponierte Anwendungen zu identifizieren. VPNs, die auf eingehende Verbindungen warten, sind ein verlockendes Ziel für Bedrohungsakteure. Hier handelt es sich um ein anbieterunabhängiges Problem, das sich nur lösen lässt, indem man das Architekturmodell ändert.

Die Zero Trust Exchange von Zscaler lässt nur ausgehende Verbindungen zu: User und Anwendungsumgebung werden jeweils mit unserer Security Cloud verbunden, die dann über Mikrotunnel die Verbindung zwischen Anfragesteller und Zugriffsziel vermittelt.

Diese Vermittlungsinstanz fungiert als Puffer zwischen verifizierten Usern und den Ressourcen, auf die sie jeweils zugreifen dürfen. Durch granulare Richtlinien lässt sich gewährleisten, dass der User ausschließlich mit dem jeweils angeforderten Asset verbunden wird und auf keine weiteren Ressourcen zugreifen kann. Die laterale Bewegungsfreiheit innerhalb einer Umgebung wird dadurch radikal eingeschränkt.

3 Ausblick

Durch konsequente Anwendung der erläuterten Grundsätze können veraltete Vorstellungen endgültig überwunden werden. Dazu zählt sowohl der durch Firewalls gesicherte Netzwerkperimeter als auch die Verbindung externer Endgeräte über VPNs. Bei dem vorgestellten Konzept handelt es sich weder um die bloße Replizierung von Legacy-Sicherheitskontrollen in einer Cloud-basierten virtuellen Instanz, noch basiert es auf einem künstlichen Behelfskonstrukt zur Definition der Netzwerkgrenzen.

Eine ganzheitliche Architektur, die für die Implementierung von Zero-Trust-Sicherheit — für User, Workloads, Anwendungen, OT- und IoT-Geräte usw. — konzipiert wurde, reduziert Risiken, verbessert das Schutzniveau, optimiert die User Experience und eröffnet sehr viel bessere Möglichkeiten zur Bereitstellung zuverlässiger Sicherheitslösungen für Unternehmen.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de