Zero Trust im Rückblick: vom Whiteboard zum Weißen Haus

Zur Bewältigung aktueller wirtschaftlicher und sicherheitstechnischer Herausforderungen steigen immer mehr Organisationen auf Zero Trust um. Sie profitieren von einem zukunftsfähigen Ansatz, der entscheidende Vorteile gegenüber herkömmlichen Netzwerk- und Sicherheitsarchitekturen aufweist. Wie radikal neuartig das Zero-Trust-Konzept ist, wird im Rückblick auf seine Entstehungsgeschichte deutlich.

1987

Der Netzwerkperimeter als Festungsmauer

Software-Entwickler der Digital Equipment Corporation (DEC) veröffentlichen erstmals eine Studie zum Thema Firewall-Technologie und etablieren damit die „Festung mit Burggraben" als Standardmodell der Netzwerksicherheit.

1990

Rudimentäre Netzwerksegmentierung

Teilweise wurde versucht, Netzwerke mithilfe von VLANs oder Subnetzen zu segmentieren — bestenfalls eine Behelfslösung, die keine Authentifizierung, nur minimale Optionen zur Zugriffsbeschränkung und kaum interne Sicherheitsfunktionen unterstützt. Die Beschränkungen, die sich mit dieser Methode implementieren lassen, können mühelos umgangen werden.

2001

Network Access Control (NAC) als neue Komponente

Mit der Veröffentlichung des 802.1X-Protokolls als Standard für die Netzwerkzugangskontrolle trägt die IEEE Standards Association der zunehmenden Verbreitung von WLAN Rechnung. Das Protokoll sieht die Authentifizierung von Netzwerkverbindungen und die Vergabe von Zugriffsrechten auf Netzwerkebene (LAN/VLAN) vor, ist jedoch aufgrund seiner Komplexität nicht zur allgemeinen Implementierung geeignet.

2004

Deperimeterisierung als Vorläufer von Zero Trust

Das Jericho Forum wird gegründet. Die Arbeitsgruppe thematisiert die zunehmende Verlagerung von Usern und Anwendungen aus dem Unternehmensnetzwerk unter dem Stichwort der „Deperimeterisierung".

2010

Ein neuer Begriff für ein neues Konzept

In einem Forschungsbeitrag für Forrester Research prägt der Analyst John Kindervag den Begriff des Zero-Trust-Modells. Kindervags Modell sieht die Verlagerung der Authentifizierung und Cybersicherheit in den Datenpfad sowie eine Segmentierung zwischen einzelnen Sitzungen vor. Es bleibt weiterhin dem Paradigma des Netzwerkzugangs verhaftet, verschiebt den Sicherheitsperimeter jedoch ins Netzwerk.

2014

Google entwickelt ein eigenes Modell

Google reagiert mit der Entwicklung von BeyondCorp als neuem Konzept für die Sicherheitsarchitektur auf die Aurora-Angriffskampagne und leitet den unternehmenswiten Umstieg auf Zero Trust ein.

2016

Zscaler verlagert Zero Trust in die Cloud

Zscaler stellt die erste Cloud-basierte Zero-Trust-Lösung vor. Sie vereinfacht die Umstellung auf ein Zero-Trust-Konzept und unterstützt Organisationen bei der Minimierung ihrer externen Angriffsflächen und radikalen Einschränkung der lateralen Bewegungsfreiheit innerhalb des Netzwerks.

2019

ZTNA: Gartner setzt Zero Trust auf die Tagesordnung

Mit dem neuen Begriff des Secure Access Service Edge (SASE) rückt Gartner das Zero-Trust-Konzept — jetzt unter der Bezeichnung „Zero Trust Network Access" (ZTNA) — erneut in den Fokus.

2020

NIST veröffentlicht ein Standard-Framework für Zero Trust

Mit der Veröffentlichung der Leitlinie SP 800-207 als einheitliches Framework für den Aufbau von Zero-Trust-Architekturen leitet NIST einen Paradigmenwechsel ein, indem Zero Trust erstmals nicht mehr im Kontext des Netzwerkzugangs definiert wird.

2021

Gartner weist den Weg in eine sicherere Zukunft

Gartner definiert die Sicherheitskomponenten von SASE als neue Marktkategorie unter der Bezeichnung „Secure Service Edge" (SSE).

2022

US-Behörden werden zur Umstellung auf Zero Trust verpflichtet

Das Office of Management and Budget verpflichtet alle US-Bundesbehörden zur Umstellung auf Zero Trust bis 2024.

Für alle, die sich ausführlicher mit der Entstehungsgeschichte und zukünftigen Weiterentwicklung des Zero-Trust-Konzepts beschäftigen wollen:

Zum Whitepaper

zscaler | Experience your world, secured.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408 533 0288
www.zscaler.de