So klappt es mit Zero Trust

Um eine stringente Zero-Trust-Strategie durchzusetzen, bedarf es mehr als punktueller, nur unzureichend integrierter Sicherheitstools. Gefragt ist vielmehr ein vollständiger Ansatz, der alle Aspekte von Zero Trust, wie Benutzer, Anwendungen und die gesamte Infrastruktur, mit einbezieht.

Die Tage, in denen die Mitarbeitenden nur innerhalb des gut abgesicherten Firmennetzwerks tätig waren, sind in den meisten Unternehmen gezählt. Hybride Arbeitsformen, verteilte Infrastrukturen, eine Vielzahl genutzter Apps und Cloud-Dienste, Integration von IoT sowie unterschiedliche, teils persönliche Mobilgeräte bieten Cyberkriminellen eine stark erweiterte Angriffsfläche ausserhalb des traditionellen Netzwerkperimeters. Dieser Herausforderung kann man nur begegnen, indem bei jedem Zugriff auf Unternehmensressourcen auf implizites Vertrauen verzichtet und jede digitale Interaktion in allen Phasen kontinuierlich verifiziert wird – kurz: In der heutigen digital geprägten Arbeitswelt ist ein Zero-Trust-Ansatz die Cybersicherheits-Strategie der Wahl.

Zero Trust im ganzen Unternehmen

Manche Unternehmen nutzen für die Umsetzung einer Zero-Trust-Strategie verschiedene, schlecht untereinander integrierte Punktlösungen wie Endpoint Protection, Remote Access (VPN), Mehrfaktor-Authentifizierung und Data Loss Prevention, oft von unterschiedlichen Herstellern. Diese unterschiedlichen Sicherheitsvorkehrungen müssen aufwändig einzeln getestet, implementiert und gepatcht werden. Gleichzeitig fehlt es an personellen und finanziellen Ressourcen, um der sehr dynamischen Bedrohungslandschaft zu begegnen. Dies alles erschwert es, eine Zero-Trust-Strategie unternehmensweit durchzusetzen.

Eine unternehmensweit einsetzbare Lösung, die alle Aspekte von Cybersecurity und Zero Trust abdeckt, ist die bessere Alternative. Genau damit befasst sich Palo Alto Networks seit über zehn Jahren und ist zu drei Schlussfolgerungen gekommen:

1. Einbezug des Ganzen

Benutzer, Systeme, Netzwerk, Applikationen, Daten: Zero Trust darf sich nicht auf eine einzelne Technologie beschränken, sondern sollte das gesamte zur Sicherung des Unternehmens genutzte Ökosystem umfassen.

2. Schrittweises Vorgehen

Der Aufbau eines vollständigen Zero-Trust-Unternehmens ist nicht trivial – aber man kann mit einfachen Massnahmen beginnen, die sich schon mit den vorhandenen Sicherheitstools implementieren lassen.

3. Vorteile fürs Business

Der Zero-Trust-Ansatz bietet neben technischen Aspekten weitere Vorteile, die sich einfach und verständlich vermitteln lassen.

Für Benutzer, Anwendungen und Infrastruktur

Zero Trust eliminiert das implizite Vertrauen im gesamten Unternehmen und überprüft jede digitale Transaktion im gesamten Ablauf, sowohl für Benutzer als auch für Anwendungen und die ganze Infrastruktur. Der erste Schritt sind strenge Kontrollen zur Authentifizierung der Nutzeridentität und zur Einhaltung der Richtlinien, gepaart mit einer Einschränkung der Zugriffsrechte auf das absolut Notwendige.

Auch Anwendungen und Microservices sowie der gesamte Datenverkehr sind grundsätzlich nicht vertrauenswürdig und müssen ebenso während der ganzen Laufzeit kontinuierlich verifiziert werden. Analoges gilt für die komplette Infrastruktur, von Routern und Switches über die Geräte der Benutzer, Cloud- und IoT-Ressourcen bis hin zu den in der Lieferkette genutzten Ressourcen.

Palo Alto Networks stellt mit ihrem Plattformansatz ein umfassendes Sicherheitsportfolio zur Umsetzung einer Zero-Trust-Strategie bereit. Mit Lösungen wie Next-Generation-Firewalls, Sicherheitsdiensten aus und für die Cloud, ausgezeichnetem Endpunkteschutz sowie Secure-Access-Service-Edge-Produkten bietet der Hersteller eine voll integrierte Plattform, um alles zu sehen, zu überprüfen und zu sichern. Komplementiert wird das Portfolio durch umfangreiche Security-Dienstleistungen und ein starkes Partnernetzwerk mit Experten-Know-how. ■

Boll Engineering AG, CH-5430 Wettingen
✆ +41 (0)56 437 60 60
info@boll.ch, www.boll.ch