LISTICLE

Der Fünf-Punkte-Plan für eine ganzheitliche Zero-Trust-Architektur

München, 14. November 2023 – Zero Trust hat sich als Sicherheitskonzept in der IT-Branche etabliert. Consol zeigt, welche fünf Schritte für dessen erfolgreiche Einführung nötig sind. Der IT-Dienstleister erklärt auch, warum moderne Cloud- und Container-Szenarien dringend feingranulare Zero-Trust-Architekturen benötigen.

Für Unternehmen, die ihre Sicherheit steigern wollen, gibt es viele Stellschrauben, an denen sie drehen können. Eine davon ist die Implementierung einer Zero-Trust-Architektur. Das Konzept ist nicht neu und auch kein Allheilmittel, das alle Sicherheitsprobleme löst. Dennoch ist die praktische Umsetzung des auf Verschlüsselung und grundsätzlich eingeschränktem Vertrauen basierenden Paradigmas sinnvoll: Unternehmen müssen davon ausgehen, dass ein Gerät, eine Applikation oder ein User-Account irgendwann gehackt wird – Experten sprechen in diesem Zusammenhang von „Assume Breach“. Nehmen sie also an, dass sich ein Cyberkrimineller früher oder später Zugriff verschafft, ist es sinnvoll, die Rechte jeder einzelnen Ressource soweit es geht zu beschränken – auch in internen Netzen.

Gerade Cloud- oder Container-basierte Anwendungen sind hier gleichermaßen Fluch und Segen: Einerseits finden sich durch die in der Regel auf Microservices beruhenden Strukturen sehr viele Angriffsflächen für Hacker. Andererseits bietet gerade diese Vielzahl an Diensten und getrennten Anwendungsteilen hervorragende Voraussetzungen für Zero Trust. IT-Dienstleister Consol erklärt, welche fünf wesentlichen Aspekte Unternehmen bei der Implementierung einer Zero-Trust-Architektur berücksichtigen sollten.

1. Identifizieren der Schutzbereiche

Unternehmen, die ihre eigene IT-Infrastruktur nicht genau kennen, werden zwangsläufig Schlupflöcher für Hacker oder potenzielle Angriffsvektoren übersehen. Um also eine Zero-Trust-Architektur nachhaltig und effektiv zu gestalten, müssen sie ihre Schutzbereiche identifizieren. Dazu gehören etwa Datenspeicher, auf denen sie sensible Daten sichern, und die gesamte Anwendungslandschaft. Danach folgt die weitere Segmentierung, bei der Unternehmen kleinere Perimeter definieren können.

2. Überwachen und Aufzeichnen der Transaktionsflüsse

Sind die Mikroperimeter angelegt, gilt es, die Transaktionsflüsse aller sensiblen Daten zwischen Personen, Anwendungen, Services sowie die Verbindungen aus dem Unternehmensnetzwerk hinaus (etwa zu Kunden) zu mappen. Diese Übersicht hilft dabei, die Kommunikationswege abzusichern, aber auch die notwendigen Rechte richtig zu verteilen: Wenn wichtige Transaktionsflüsse durch zu restriktiven Zugriff unterbrochen werden, kann das im Zweifel eine Abteilung lahmlegen oder die korrekte Ausführung einer Anwendung verhindern. Über diesen Zweck hinaus gewährt das konstante Monitoring der Transaktionsflüsse die Möglichkeit, sie zu optimieren und so die Performance von Applikationen zu verbessern.

3. Definieren der Zero-Trust-Architekturen

Sobald Unternehmen ein klares Bild ihrer IT-Umgebungen und von den jeweiligen Transaktionsflüssen zwischen den Sicherheitsperimetern haben, folgt die Definition der Zero-Trust-Architektur. Dafür kommen softwaredefinierte Netzwerke und Sicherheitsprotokolle sowie physische oder virtuelle Firewalls zum Einsatz.

4. Formulieren der Richtlinien

Um sicherzustellen, dass nur autorisierte Anwendungen oder User Zugriff auf die jeweiligen Perimeter haben, müssen Unternehmen Zero-Trust-Richtlinien formulieren. Die Grundannahme an dieser Stelle ist: Alle Geräte, egal ob private oder unternehmenseigene, sind unsicher und damit nicht vertrauenswürdig. Um die Zugangsrechte sinnvoll zu verteilen, sollten Unternehmen die Kipling-Methode verwenden, die die Fragen „Wer?“, „Was?“, „Wann?“, „Wo?“, „Warum?“ und „Wie?“ umfasst – also „Wer oder was muss warum, wann, worauf und wie Zugriff erhalten?“

5. Betreiben der Zero-Trust-Infrastruktur

Die Implementierung allein reicht leider nicht aus, um Zero Trust zum Erfolg zu führen. Höchstmögliche Sicherheit erreichen Unternehmen nur, wenn sie ihre IT auch konstant auf ungewöhnliche Datenflüsse hin untersuchen und die Zero-Trust-Architektur immer wieder auf den Prüfstand stellen. Da die manuelle Überwachung und Anomalieerkennung nicht praktikabel ist, helfen Softwarelösungen mit KI-Unterstützung dabei, diese Aufgaben zu automatisieren.

„Der Spruch – Vertrauen ist gut, Zero Trust ist besser – gilt nach wie vor“, erklärt Lukas Höfer, Cloud Solutions Architect bei Consol. „Allerdings müssen Unternehmen heute nicht nur den Datenverkehr und die Kommunikation zwischen strikt getrennten Systemen kontrollieren. Da Angriffe auch von innen kommen können, müssen die gleichen strikten Zugriffskontrollen auch intern stattfinden – etwa zwischen in Containern gelagerten Microservices oder Cloud-Anwendungen.“

Weitere Informationen unter: https://www.consol.de/custom-it-solutions/build-operate/cloud-solutions/

Dieses Listicle und Bildmaterial sind abrufbar unter www.pr-com.de/companies/consol.

Über Consol

Die Consol Consulting & Solutions Software GmbH mit Hauptsitz in München begleitet seit mehr als 35 Jahren lokale und internationale Unternehmen mit passgenauen IT-Lösungen durch den gesamten Software-Lifecyle. High-End-IT-Beratung, agile Software-Entwicklung sowie Betrieb und Support sind die Eckpfeiler des Portfolios, das Consol unter Anwendung von modernsten Technologien ständig erweitert. Dazu zählen Open Source-Projekte wie Quarkus, OpenShift oder Tekton. Das Unternehmen entwickelt und vertreibt auch die Software Consol CM, eine Plattform zur Digitalisierung von Geschäftsprozessen. Bei der Umsetzung der Digitalisierungsstrategien seiner Kunden macht Consol IT-Umgebungen und Geschäftsprozesse fit für die Herausforderungen von morgen. Mit den Leitmotiven Exzellenz und höchste Qualität folgt Consol dem Ziel, Businesses weiter voranzubringen. Dabei fokussiert Consol Bereiche wie Cloud-native, Container, Microservice-Architekturen oder IT Automation.

Consol ist Red Hat Premier Partner und NGINX Preferred Partner. Strategische Partnerschaften bestehen außerdem zu AWS und Microsoft Azure. Zu den Kunden zählen Großunternehmen wie Haribo, Daimler oder Vodafone. Aktuell beschäftigt Consol rund 260 Mitarbeiter an seinen Standorten München, Düsseldorf, Wien, Krakau sowie San Francisco.

Weitere Informationen unter https://www.consol.de, https://cm.consol.de und https://blog.consol.de.

Pressekontakt

ConSol Consulting & Solutions Software GmbH
Isabel Baum
St.-Cajetan-Straße 43
D-81669 München
Fon: +49-89-45841-101
E-Mail: Isabel.Baum@consol.de
Web: https://www.consol.de und https://cm.consol.de

PR-COM GmbH
Nicole Oehl
Sendlinger-Tor-Platz 6
D-80336 München

Fon: +49-89-59997-758
E-Mail: nicole.oehl@pr-com.de
Web: www.pr-com.de