consol

BEST PRACTICES ZERO TRUST

CONSOL BEST PRACTICES

IT SECURITY

Traditionelle Sicherheitskonzepte prüfen die Identität und die Berechtigungen von Usern, Applikationen und Systemen in der Regel nur beim ersten Zugriff auf Firmenressourcen. Sind diese einmal verifiziert, können sie sich meist ungehindert im Netz bewegen.

Aufgrund der immer komplexeren Sicherheitsanforderungen und da immer mehr Menschen remote arbeiten, reicht es nicht mehr aus, nur den Netzwerkperimeter zu schützen. Es braucht anpassungsfähige Lösungen, die jede Zugriffsanforderung authentifizieren und verifizieren. Das Zero-Trust-Modell ist eines dieser zukunftsfähigen Sicherheitskonzepte.

Was sind die Grundsätze von Zero Trust?

Kontinuierliche Überwachung und Überprüfung

Zero Trust geht davon aus, dass es innerhalb als auch außerhalb eines Netzwerks Angreifer gibt. Keinem User oder Gerät wird automatisch vertraut. Zero Trust verifiziert die Identität und die Privilegien der Nutzer sowie die Identität und Sicherheit der Geräte. Anmeldungen und Verbindungen werden in regelmäßigen Abständen unterbrochen. User und Geräte müssen sich ständig neu verifizieren.

Geringste Privilegierung (minimaler Zugang)

Prinzip des Zero-Trust-Modells sind geringstmögliche Zugriffsberechtigungen. User erhalten nur so viel Zugriff, wie sie benötigen. Damit haben die Nutzer möglichst wenig mit allen sensiblen Teilen des Netzwerks zu tun. Die Implementierung des minimalen Zugangs erfordert eine sorgfältige Verwaltung der Nutzerrechte.

Kontrolle des Gerätezugriffs

Neben den Kontrollen des Nutzerzugriffs erfordert Zero Trust auch Kontrollen des Gerätezugriffs. Zero Trust überwacht, wie viele Geräte versuchen, auf das Netzwerk zuzugreifen und stellt sicher, dass jedes Gerät autorisiert ist.

Mikrosegmentierung

Zero Trust arbeitet auch mit Mikrosegmentierung. Dabei werden die Sicherheitsperimeter in kleine Zonen aufgeteilt. Dadurch wird der Zugriff auf separate Teile des Netzwerks auch separat verwaltet. Eine Person oder ein Programm mit Zugriff auf eine Zone, kann ohne zusätzliche Autorisierung auf keine der anderen Zonen zugreifen.

Laterale Bewegung verhindern

„Laterale Bewegung“ bedeutet, dass sich ein Angreifer innerhalb eines Netzwerks bewegt, nachdem er Zugang zu diesem erhalten hat. Der Zero-Trust-Ansatz wurde entwickelt, um Angreifer einzuschließen, sodass sie sich nicht lateral bewegen können. Dadurch kann ein Angreifer nicht zu anderen Mikrosegmenten innerhalb des Netzwerks überwechseln. Wird seine Anwesenheit entdeckt, wird das kompromittierte Gerät oder Nutzerkonto unter Quarantäne gestellt und von weiterem Zugriff abgeschnitten.

Multi-Faktor-Authentifizierung (MFA)

Bei MFA wird für die Authentifizierung eines Benutzers mehr als ein Nachweis herangezogen. Nur das Passwort reicht nicht aus. Der User muss beispielsweise einen Code eingeben, der auf ein anderes Gerät gesendet wurde. Somit liegen zwei Belege vor, die einen User eindeutig identifizieren.

Wie wird eine Zero-Trust-Architektur aufgebaut?

Der Zero-Trust-Ansatz verwendet vorhandene Netzwerkarchitekturen und benötigt keine aufwendigen Updates. Eine Zero-Trust-Architektur kann mit der Fünf-Schritte-Methode einfach bereitgestellt und gewartet werden.

1. Identifizieren Sie die Schutzoberfläche, einschließlich sensibler Daten und Anwendungen. Sie können die Kategorien „öffentlich“, „intern“ und „vertraulich“ verwenden. Daten, die es zu schützen gilt, werden in Mikroperimeter segmentiert und miteinander verknüpft. So baut sich ein umfassenderes Zero-Trust-Netzwerk auf.

2. Ordnen Sie die Transaktionsflüsse aller sensiblen Daten zu. So ermitteln Sie, wie Daten zwischen Personen, Anwendungen und externen Verbindungen wie Kunden verschoben werden. Anschließend werden Abhängigkeiten von Netzwerk- und Systemobjekten offengelegt und geschützt.

3. Definieren Sie eine Zero-Trust-Architektur für jeden Mikroperimeter, der auf Daten- und Transaktionsflüsse im Unternehmen basiert. Dies wird mit Software-defined Netzwerken (SDNs) und Sicherheitsprotokollen erreicht.

4. Erstellen Sie eine Zero-Trust-Richtlinie. Viele Unternehmen verwenden die Kipling-Methode, die das „Wer?“, „Was?“, Wann?“, Wo?“, „Warum?“ und „Wie?“ ihrer Richtlinien und ihres Netzwerks berücksichtigt. So kann eine Richtlinie durchgesetzt werden, sodass nur autorisierte Anwendungen oder User Zugriff auf die Schutzoberfläche erhalten.

5. Automatisierung, Überwachung und Wartung sind essentiell, um festzustellen, wo ungewöhnlicher Datenverkehr stattfindet. Ermitteln Sie, wo Anomalien auftreten und überwachen Sie alle Aktivitäten. Automatisieren Sie die Überprüfung und Analyse des

Protokolldatenverkehrs.

Was sind die Vorteile von Zero Trust?

1. Durch die Implementierung von Zero Trust wird die Angriffsfläche einer Organisation reduziert.

2. Im Falle eines Angriffs minimiert Zero Trust den Schaden. Durch die vorgenommene Mikrosegmentierung wird der Schaden auf einen begrenzten Bereich beschränkt. Dies senkt auch die Kosten für die Wiederherstellung.

3. Wenn Phishing-Angriffe stattfinden und Anmeldeinformationen gestohlen werden, verringert Zero Trust die Auswirkungen, da mehrere Authentifizierungsfaktoren notwendig sind.

4. Zero Trust reduziert durch die Überprüfung jeder Anfrage das Risiko, das von Sicherheitslücken ausgeht, einschließlich dem von IoT-Geräten, die oft schwer zu sichern und zu aktualisieren sind.

Was sind Anwendungsfälle von Zero Trust?

VPN ersetzen oder ergänzen: VPNs eignen sich nicht gut für Ansätze zur Autorisierung nach dem Prinzip des geringsten Privilegs. Die Anmeldung bei einem VPN gewährt einem User Zugriff auf das gesamte verbundene Netzwerk.

Remote-Arbeit sicher unterstützen: VPNs können zu Engpässen führen und die Produktivität von Remote-Mitarbeitern beeinträchtigen. Zero Trust dagegen erweitert die sichere Zugriffskontrolle auf Verbindungen von überall her.

Zugriff auf Cloud und Multi-Cloud kontrollieren: Ein Zero Trust Netzwerk verifiziert jede Anfrage, unabhängig von Quelle oder Ziel. Dies trägt auch dazu bei, die Nutzung nicht-autorisierter cloudbasierter Dienste einzudämmen, indem die Nutzung nicht genehmigter Apps kontrolliert und blockiert wird.

Dritte und Auftragnehmer onboarden: Zero Trust kann den eingeschränkten Zugriff nach dem Least-Privilege-Prinzip schnell auf externe Parteien ausweiten.

Neue Angestellte schnell onboarden: Zero Trust kann die schnelle Einarbeitung neuer interner User erleichtern, was es zu einer guten Lösung für schnell wachsende Unternehmen macht. VPN benötigt im Gegensatz dazu eventuell mehr Kapazität, um eine wachsende Zahl neuer User aufzunehmen.

Was sind die wichtigsten Best Practices für Zero Trust?

Netzwerk-Traffic und angeschlossene Geräte überwachen: Transparenz ist das A und O. Nur so können User und Rechner verifiziert und authentifiziert werden.

Geräte auf dem neuesten Stand halten: Patchen Sie Sicherheitslücken so schnell wie möglich. Zero Trust Netzwerke müssen den Zugriff auf Sicherheitslücken einschränken können.

Das Prinzip des minimalen Zugangs für alle Mitarbeitenden anwenden: Egal ob Führungskraft oder Mitglied eines IT-Teams, jede/r sollte so wenig Zugriff haben, wie benötigt. Das minimiert den Schaden bei Kompromittierung eines Endnutzerkontos.

Das Netzwerk aufteilen: Durch Mikrosegmentierung lässt sich das Netzwerk in kleinere Teile aufteilen. So können Sicherheitslücken früh geschlossen werden, bevor sie sich ausbreiten.

So vorgehen, als gäbe es keinen Netzwerkperimeter: Wenn ein Netzwerk nicht vollständig abgekapselt ist, sind die Punkte, an denen es das Internet oder die Cloud berührt zu zahlreich, um sie zu eliminieren.

Sicherheitsschlüssel für Mehr-Faktor-Authentifizierung verwenden: Hardware-basierte Sicherheits-Token sind sicherer als Soft-Token wie Einmalpasswörter, die über SMS oder E-Mail verschickt werden.

ConSol
Consulting & Solutions Software GmbH

St.-Cajetan-Straße 43
D-81669 München
Tel.: +49-89-45841-100
vertrieb@consol.de
www.consol.de
Folgen Sie uns auf LinkedIn:
@consol-software-gmbh

ConSol
Austria Software GmbH

Maysedergasse 2/25
A-1010 Wien, Österreich
Tel.: +43-1-9971392
info-austria@consol.com
www.consol-software.at
Folgen Sie uns auf LinkedIn:
@consol-austria-software-gmbh