Vertrauen ist gut, Kontrolle besser

Die globale Angriffsfläche der Unternehmen ist sehr dynamisch und verändert sich laufend. Dies fordert die Arbeit der Sicherheitsverantwortlichen und ist eine laufende Aufgabe. Von Angriffen sind weder kleine noch grosse Firmen sicher. Deshalb sind laufende Prävention, Überwachung und Kontrolle notwendig.

Lurata Reci, Armin Baumann

Zero Trust ist ein Sicherheitskonzept (erstmals 1994 von Paul Marsh verwendet), das jeden Benutzer und jedes Gerät im Netzwerk als unsicher betrachtet. Deshalb muss vor jedem Zugriff auf Informationen und Systeme, wie auch Public oder Private Cloud, ständig überprüft und authentifiziert werden. Dies sind:

- Identitäts- und Zugriffsmanagement
- Datenverschlüsselung
- Micro-Netzwerksegmentierung
- kontinuierliches Monitoring und Analyse von Benutzeraktivitäten
- Zugriffsanfragen und Netzwerkverkehr kontrolliert und einschränken

Das Modell verwendet das Prinzip der geringstmöglichen Rechte und Zugriffe und geht fast immer von einer möglichen Sicherheitsverletzung aus. Es kann in verschiedenen Umgebungen eingesetzt werden, einschliesslich Cloud-basierten, hybriden und On-Premise-Netzwerken. Besonders wichtig ist es für Systeme, in denen Mitarbeiter externen Zugriff benötigen (Cloud-basierte Dienste/Anwendungen). Firmenanwendungen und -Daten verlagern sich von lokalen Umgebungen zu hybriden und Cloud-Umgebungen. Herkömmliche Netzwerksteuerungen können nur noch bedingt oder gar

nicht mehr verwendet werden. Steuer- und Kontrollelemente müssen dorthin verschoben werden, wo sich die Daten befinden – auf mobile Geräte und Apps.

Die Mitarbeiter haben im Laufe der letzten Jahre den Sicherheitsperimeter enorm ausgeweitet durch «Arbeiten von überall». Somit wird von ausserhalb auf Daten des Unternehmensnetzwerks zugegriffen. Daten werden mit externen Mitarbeitern wie Partnern und Anbietern geteilt («Co-working»). Mehr als 70 Prozent der Datenverstösse werden durch Hacking mithilfe gestohlener Anmeldeinformationen verursacht. Durch eine adaptive, kontextbasierte Multi-Faktor-Authentifizierung kann davor bereits geschützt werden.

Das Zero-Trust-Konzept wurde von Forrester Research entwickelt und besteht aus sechs Schritten und soll helfen Unternehmen, die Sicherheit ihrer Netzwerke, den Datenschutz zu erhöhen und sich gegen Cyberangriffe zu schützen:

1. Identifizierung kritischer Assets: Bestimmen, welche Ressourcen, Daten und Anwendungen für das Unternehmen am wichtigsten sind und deren Schutz mit höchster Priorität. Sensible Daten sind zu verschlüsseln, damit sie bei Übertragung und Speicherung geschützt sind.
2. Erstellung von Zugriffskontrollrichtlinien: Definieren, wer auf welche Ressourcen zugreifen darf, basierend auf einer Vielzahl von Faktoren wie Benutzeridentität, Gerätetyp, Standort und Sicherheitsstatus.
3. Implementierung von mehrstufigen Authentifizierungsmethoden: Verwenden mehrerer Authentifizierungsmethoden, damit nur zugelassene Benutzer Zugriff erhalten. Dies durch eine IAM-Strategie, die sicherstellt, dass Benutzer nur auf deren benötigte Ressourcen zugreifen können und dass ihre Identität durch Multi-Faktor-Authentifizierung und starke Passwörter geschützt ist.
4. Umsetzung von Least-Privilege-Zugriff: Vergeben der erforderlichen Berechtigungen für jeden Benutzer, um seine Aufgaben auszuführen. Damit wird das Risiko von Missbrauch oder versehentlichem Zugriff auf nicht autorisierte Ressourcen vermindert.
5. Überwachung und Protokollierung: Kontinuierliches Überwachen des Netzwerkverkehrs und Protokollieren aller Zugriffsversuche, um verdächtige Aktivitäten schnell zu erkennen und darauf zu reagieren. Automatisieren der Überwachung und Durchsetzung von Sicherheitsrichtlinien, um sicherzustellen, dass diese ständig auf dem neuesten Stand sind und dass Bedrohungen schnell erkannt und abgewehrt werden können.
6. Implementierung von Segmentierung: Netzwerk in kleinere, logische Segmente aufteilen, um Angriffe zu begrenzen und den Zugriff auf kritische Ressourcen auf autorisierte Benutzer zu beschränken. Dadurch wird das Risiko minimiert, dass ein Angriff auf einen Teil des Netzwerks auf den Rest des Netzwerks übergreift.

Zero Trust kann eingesetzt werden, um eine höhere Sicherheit und Kontrolle des Netzwerkzugriffs zu erreichen wie z. B.:

- Datenschutz: Unternehmen und Organisationen, die personenbezogene oder vertrauliche Daten speichern oder verarbeiten. Diese Daten sind kontinuierlich abzusichern und zu kontrollieren.
- Dezentralisierte Arbeitsumgebungen: Die Kontrolle über den Netzwerkzugriff ist aufrechtzuerhalten, unabhängig davon, wo sich die Mitarbeiter befinden.
- Schutz von Cloud-basierten Anwendungen und Diensten: Der Zugriff auf diese Anwendungen und Dienste ist zu kontrollieren und zu überwachen.
- Schutz von IoT-Geräten (Internet der Dinge): Diese Geräte sind besser abzusichern und der Netzwerkzugriff zu kontrollieren.

Die Umsetzung von Zero Trust kann eine komplexe Aufgabe sein, die ein tiefes Verständnis der Architektur und der Ressourcen des Netzwerks erfordert. Es ist ratsam, erfahrene Sicherheitsexperten hinzuzuziehen, die bei der Implementierung unterstützen. Auch wenn Zero Trust eine effektive Methode zur Verbesserung der Netzwerksicherheit ist, kann es einige Herausforderungen und Probleme geben, die bei der Implementierung auftreten können:

- Komplexität: Die Implementierung erfordert eine umfassende Analyse und Überwachung der Benutzer- und Geräteaktivitäten sowie Zugriffskontrolle und -segmentierung nach Datenschutzprinzipien. Dies kann zu einer erhöhten Komplexität und Kosten führen, insbesondere wenn es um die Integration von verschiedenen Systemen und Anwendungen geht.
- Benutzererfahrung: Eine strikte Zugriffskontrolle und -segmentierung kann auch zu Einschränkungen in der Datenverarbeitung führen, wenn es um den Zugriff auf Anwendungen und Ressourcen geht. Es ist daher wichtig, gemäss den Datenschutzbestimmungen die Mitarbeiter zu informieren und zu sensibilisieren.
- Integration von Legacy-Systemen: Unternehmen können Schwierigkeiten bei der Integration in ihre bestehenden Legacy-Systeme haben. Dies kann zu Kompatibilitätsproblemen und Konflikten mit anderen Sicherheitslösungen führen.
- Datenverlust: Eine falsch konfigurierte Zero-Trust-Umgebung kann dazu führen, dass Benutzer Zugriff auf Daten erhalten, auf die sie nicht zugreifen sollten, oder dass sensible Informationen nach aussen gelangen. Es ist daher wichtig, eine umfassende Überwachung und Kontrolle von Daten und Zugriffen sicherzustellen und zu dokumentieren.
- Mangelnde Standardisierung: Es gibt keine einheitlichen Standards oder Richtlinien für die Implementierung von Zero Trust. Unternehmen müssen daher ihre eigenen Richtlinien und Best Practices an das bestehende und neue Datenschutzgesetz anpassen oder entwickeln, um sicherzustellen, dass ihre Zero-Trust-Implementierung effektiv und sicher ist. ■

KMU Swiss Symposium 2023

Ort: Campussaal Kultur + Kongresse, Brugg Windisch
Thema: Versorgungssicherheit… Der Stoff aus dem Träume sind?
Datum: 7. September 2023 (13:00 bis 20:00 Uhr)
Referenten und Referentinnen berichten aus ihren Erfahrungen und Erlebnissen und über aktuelle Situationen. Dies sind unter anderem: Doris Leuthard (Alt-BR), Dr. David W.F. Huang (Repräsentant Taiwan), Daniel Schöni (Schöni Transporte), Dr. Martin Keller (Fenaco), Jürg Brand (Von Roll Infratec), Stefan Winzenried (Janzz.technology) und zahlreiche Überraschungen.
Besonderes: Vor dem Start (11:45 bis 12:30 Uhr) finden zwei Prologe statt zu den Themen:
- Darknet
- Kunden analysieren und gewinnen mit Cloud Contact Center

Anmeldung: www.kmuswiss.ch/symposium
Impressionen: www.kmuswiss.tv