CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Zero Trust Security

Definition Zero Trust Security

“Das Zero-Trust-Modell ist ein **Sicherheitskonzept**, das auf dem Grundsatz basiert, **keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks zu vertrauen**. Es erfordert umfangreiche Maßnahmen zur Authentifizierung sämtlicher Anwender und Dienste sowie zur Prüfung des Netzwerkverkehrs.”

Funktionsweise

- Keine praktische Differenzierung zwischen Nutzern und Geräten innerhalb des internen Netzwerks
  - Grundprinzip: **“Nie vertrauen, immer verifizieren.”**
- Alles Unterliegt strengsten Sicherheitskontrollen
- Ziel: Risiko für Firmennetze und -anwendungen zu minimieren und neben externen Bedrohungen auch interne Gefahrenpotentiale auszuschließen
- Unterschied zu meisten anderen Sicherheitskonzepten:
  - Auch interner Datenverkehr wird bis aufs Äußerste überwacht und geprüft

Schlüsselkomponenten

Identitäts- und Zugriffsmanagement:

- Starke Authentifizierungsverfahren und rollenbasierte Zugriffskontrollen

Gerätemanagement:

- Sicherstellung, dass nur gesicherte und autorisierte Geräte auf Netzwerkressourcen zugreifen können

Netzwerksegmentierung:

- Trennung von Netzwerkbereichen zur Minimierung von lateraler Bewegung bei einem Sicherheitsvorfall

Schlüsselkomponenten

Datenverschlüsselung:

- Schutz sensibler Daten sowohl im Ruhezustand als auch während der Übertragung

Sicherheitsüberwachung:

- Kontinuierliche Überwachung und Analyse von Netzwerkaktivitäten zur frühzeitigen Erkennung und Reaktion auf Bedrohungen

Vorteile

Verbesserte Sicherheitslage:

- Reduzierung der Angriffsfläche und bessere Abwehr gegen Sicherheitsverletzungen

Flexibilität und Skalierbarkeit:

- Anpassungsfähig an verschiedenste Unternehmensgrößen und -strukturen

Eignung für moderne Arbeitsumgebungen:

- Unterstützung für Remote-Arbeit und Cloud-Dienste

Prävention gegen Insider-Bedrohungen:

- Schutz gegen Bedrohungen, die von innerhalb des Netzwerks kommen

Nachteile

Technische Komplexität:

- Integration verschiedener Sicherheitstechnologien und -systeme

Kultureller Wandel:

- Notwendigkeit zur Änderung der Sicherheitsmentalität und -praktiken im gesamten Unternehmen
    - Attraktivitätssteigerung von Arbeitsplätzen durch mehr Bequemlichkeit

Kosten und Ressourcen:

- Erfordert möglicherweise erhebliche Investitionen in neue Technologien und Fachwissen

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm