Zero Trust Security

Zero Trust Security geht davon aus, dass nichts sicher ist – auch nicht hinter der Firmen-Firewall. Darum wird jede Anfrage so geprüft, als käme sie aus einem offen zugänglichen Netzwerk. So werden Umgebungen, Nutzer, mobile Mitarbeiter, Geräte, Anwendungen und Daten an jedem Ort geschützt.

Ausgangslage

Mobilität und Digitalisierung verursachen mehr Zugriffe von Benutzern und Geräten auf Firmendaten. Die Überwachung wird anspruchsvoller und die Angriffsfläche ist grösser.

Lösung

Verhinderung von unberechtigtem Zugriff auf Daten und Dienste in Verbindung mit einer granularen Durchsetzung der Zugriffskontrolle. Dies geschieht in mehreren Schritten:

1. Authentisierung durch mehrere Faktoren (Identität, Integrität, …).
Jeder Datenverkehr, unabhängig vom Standort, gilt als bedrohlich, bis überprüft wurde, dass er autorisiert, kontrolliert und geschützt ist.

2. Autorisierung nur für bestimmte Netzwerke, Workloads, Applikationen und Daten.
Durchsetzung der Zugriffskontrolle auf Basis von minimaler Berechtigung (Least Privilege) und Mikrosegmentierung.

3. Kontinuierliche Überwachung und Reagieren auf Gefahren.
Überprüfung und Loggen aller Ressourcen und des gesamten Datenverkehrs auf bösartige Aktivitäten mit Echtzeitschutzfunktionen.

Wichtigste Erkenntnisse

1. Es gilt das Prinzip "Vertrauen ist gut, Kontrolle ist besser", egal, woher die Anfrage stammt und auf welche Ressource zugegriffen wird.

2. Hat sich der Endpunkt ausgewiesen, wird der Zugriff gemäss seinem Profil freigeschaltet und überwacht.

Darum Security by Netcloud
Netcloud hat das Wissen und die Erfahrung aus dutzenden Zero-Trust-Implementierungen.
Wir bieten die gesamte Lösung aus einer Hand an und decken von Beratung bis Betrieb alle Phasen ab.

Weitere Infos:

Success Story – Frankfurter Bankgesellschaft: Zero-Trust-Architektur

Experten-Interview: Workload Protection

Cisco Zero Trust Security-Übersicht

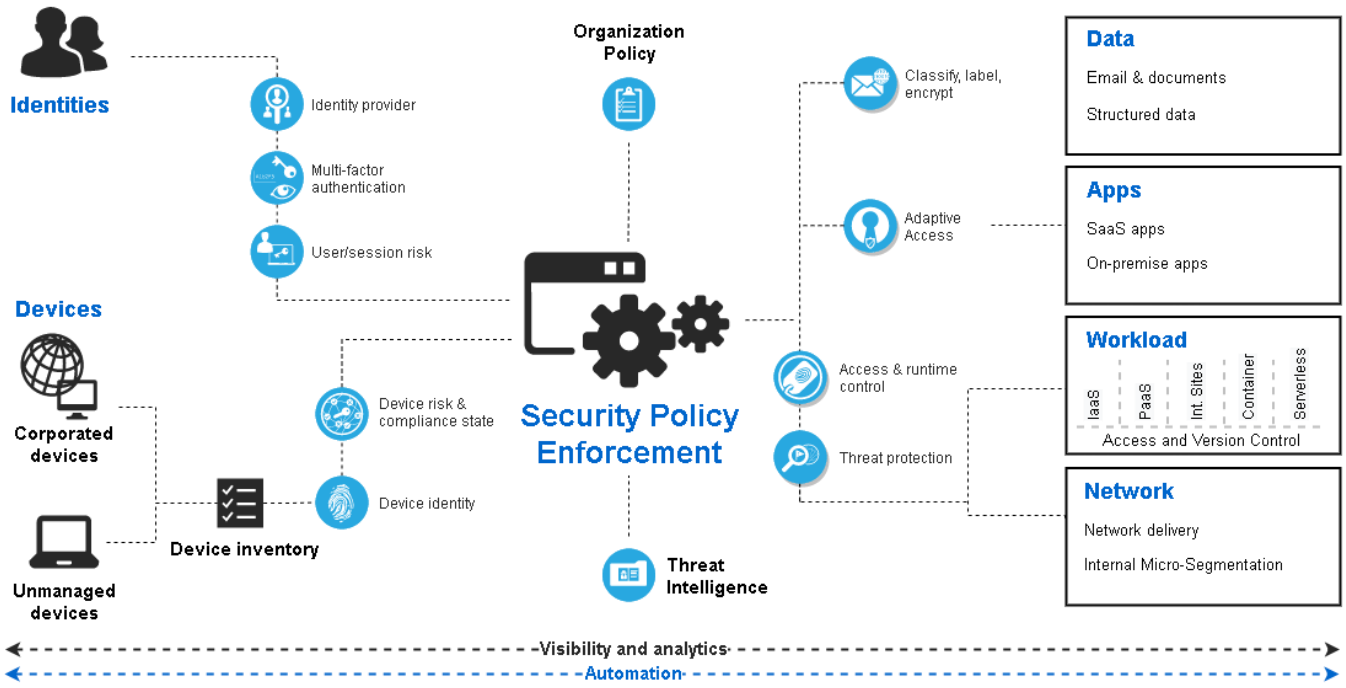

Abbildung 1: Zero Trust-Schema gemäss Microsoft

Identities	- Eine Identität (Mensch, Dienst oder IOT-Gerät) kann nur mit starker Authentifizierung auf eine Ressource zugreifen - Ist der Zugriff konform und typisch für diese Identität, folgt man dem Grundsatz "Least Privilege Access"
Devices	- Gerätezustand und Compliance (Richtlinien, z.B. aktueller Endpunktschutz, aktivierte Firewall) müssen für einen sicheren Zugriff überwacht und durchgesetzt werden
Data	- Daten sollten klassifiziert, gekennzeichnet und verschlüsselt werden - Der Zugriff soll auf Grundlage dieser Attribute eingeschränkt sein
Apps	- Kontrollen und Technologien nutzen, um Schatten-IT zu erkennen - Angemessene In-App-Berechtigungen (z.B. Sharepoint) gewährleisten - Abnormales Verhalten überwachen und bei Abweichungen einschränken - Benutzeraktionen (Entwickler, Administratoren, etc.) kontrollieren und Konfigurationseinstellungen validieren
Workloads	- Prüfen der Workloads auf aktuelle Version, sichere Konfiguration und Zugriff - Mittels Telemetrie Angriffe und Anomalien erkennen - Riskantes Verhalten sollte automatisch blockiert und alarmiert werden
Networks	- Visibilität und Segmentierung hindern Angreifer daran, sich seitlich (lateral) durch das Netzwerk zu bewegen