Secure Identity & Access

Benutzer, Geräte und SaaS Applikationen sind mittlerweile überall. Mit Secure Identity and Access können Identitäten (Endgeräte, Benutzer) validiert, sowie die Zugriffsrechte einfach verwaltet werden.

Ausgangslage

Ressourcen von Unternehmen sind oftmals global verteilt und sind über zahlreiche Wege zugänglich. Zugangswege müssen vor Missbrauch geschützt werden.

Lösung

Verhindern von unberechtigten Zugriffen auf Daten und Dienste mittels Zugriffskontrolle und granularer Berechtigungssteuerung.

1. Authentifizierung: Die Validierung von Identitäten, welche Zugang zum Netzwerk/Ressourcen erhalten möchten.
Oftmals mittels mehrerer Methoden (MFA).

2. Autorisierung: Nur berechtigte Identitäten erhalten Zugriff auf das Netzwerk/Ressourcen.
Hat sich die Identität ausgewiesen, wird der Zugriff gemäss seiner Rolle freigeschaltet und protokolliert.

3. Visibilität: Wer versucht mit welchen Mitteln auf welche Ressourcen zuzugreifen?
Geräte mit einem alten Softwarestand sind ein hohes Sicherheitsrisiko. Diese Visibilität kann anschliessend für Policies verwendet werden, um veraltete oder unsichere Systeme am Zugriff zu hindern.

Wichtigste Erkenntnisse

1. Alle Zugriffswege müssen kontrolliert werden, wenn möglich mittels mehrerer Methoden (MFA)

2. Erfolgreich validierte Identitäten erhalten den minimalen nötigen Zugang gemäss ihrer Rolle (Least Privilege).

3. Zugänge werden protokolliert und sind nachvollziehbar.

Darum Security by Netcloud
Netcloud hat Expertise im Cloud-, Security- und Netzwerkumfeld sowie Erfahrung aus zahlreichen Identity and Access-Implementierungen. Wir bieten die gesamte Lösung aus einer Hand an und decken von Beratung bis Betrieb alle Phasen ab.

Weitere Infos:

Produktbeschreibung – Cisco Identity Services Engine (ISE)

Produktbeschreibung – Cisco Duo

Infografik - Azure Cloud Identity and Access Mgmt

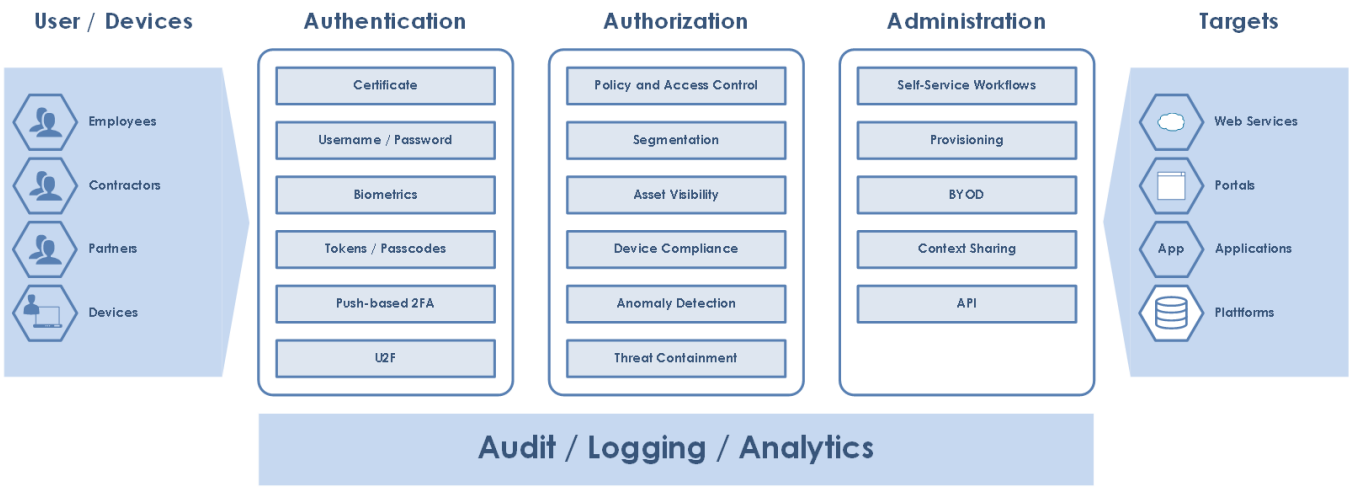

Abbildung 1: Übersicht Secure Identity and Access

User / Devices	- Zentrale Verwaltung und Validierung von Identitäten
Authentication	- Die Prüfung eines Identitätsnachweises auf seine Authentizität - Identitätsnachweise können auf unterschiedliche Art erbracht werden - Primäre Authentifizierung mittels Cisco Identity Services Engine (ISE) oder Azure AD - Multi-Faktor-Authentifizierung (MFA) mittels Cisco Duo oder Azure MFA
Authorization	- Das Gewähren des Zugangs zu den Privilegien, welche der erfolgreich nachgewiesenen Identität zustehen - Gewährte Ressourcen werden im Web-Portal zur Verfügung gestellt
Administration	- Geräte für MFA können selbst verwaltet werden (Self-Service) - Warnmeldungen bei veralteter Software - Unterstützung zur Behebung von nicht eingehaltenen Richtlinien
Targets	- Schützen von Zugängen On-Premise - Schutz von verschiedenen Applikationen (SaaS, Webportale, M365 etc.)
Audit / Logging / Analytics	- Das Protokollieren der Zugänge zum Netzwerk und / oder Zielsystem - Einsicht von Softwareständen und Sicherheitsrisiken