WHITEPAPER

NAC (Network Access Control)

Volle Kontrolle im Netzwerk

Zusammenfassung für Entscheider

In vielen KMU ist das Firmennetzwerk heute offen wie ein Büro ohne Zutrittskontrolle: Jeder, der das Gebäude betritt oder ein Kabel einsteckt, ist automatisch «drin».

Network Access Control (NAC) ist sinnbildlich wie eine intelligente Eingangsschleuse für das Netzwerk: Nur autorisierte Geräte kommen rein, neue oder unsichere Geräte werden zuerst geprüft und nur bekannte sowie autorisierte Geräte erhalten den notwendigen Zugriff.

Durch den Einsatz von NAC hat man zusätzlich zur erhöhten Sicherheit auch den Vorteil, dass Geräte automatisch im richtigen Netzwerk sind – unabhängig davon, wo diese eingesteckt werden – da aufgrund der Authentifizierung das Netzwerk zugeteilt wird.

Der NAC erweitert Cybersecurity auf den Netzwerklayer und somit auf den frühesten Kontrollpunkt und ist die logische Fortführung von Firewall, Netzwerksegmentierung sowie Endpoint Protection.

Bei Datimo setzen wir auf das Open-Source Produkt PacketFence, welches sehr flexibel und massgeschneidert parametriert werden kann. Im Zusammenspiel mit einer internen PKI (Public Key Infrastructure) für Computer- und Benutzerzertifikate und anderen Authentifizierungsquellen wie M365, Sponsor-E-Mail lassen sich auch Bring-Your-Own-Device Szenarien sicher und kontrolliert realisieren.

Die Implementierung von NAC ist sehr individuell – gerne erstellen wir ein massgeschneidertes Angebot für Sie.

Worum geht es?

Ein NAC-Server kontrolliert wer oder was Zugang zum Netzwerk bekommt. Statt «jeder darf rein, solange er ein Netzwerkkabel findet oder das WLAN-Passwort kennt» gibt es klare Regeln. Dies erfolgt u.a. über:

- Authentifizierung von Endgeräten
- Registrierung neuer Geräte
- Sicherheitsprüfungen (Benötigt ein Drittanbieterprodukt)
- Segmentierung der Netzwerkzonen
- Automatische Reaktionen bei Sicherheitsvorfällen

Warum ist das wichtig?

- Mehr Risiken durch BYOD, IoT und Gäste
- Gesetzliche Anforderungen steigen
- Angriffe beginnen oft intern oder durch eingeschleuste Geräte
- Bessere Übersicht
- Dynamische Netzwechsel je nach Autorisierungsstufe

Technische Architektur

NAC setzt sich aus einem Serverdienst (auch clusterfähig) und den Netzwerkkomponenten zusammen. Es gibt grundlegend die Deployment-Szenarien In-Band und Out-Of-Band, welche auch hybrid kombiniert werden können.

Zu den einzelnen Komponenten:

NAC-Server (hosted VM)
PacketFence wird typischerweise als VM betrieben und dient als zentrale Policy-Engine, RADIUS-Server, Webportal und Reporting-Einheit.

Netzwerkhardware per RADIUS und 802.1X oder Inband
PacketFence nutzt Standardprotokolle wie RADIUS, 802.1X und MAC Authentication. Der Switch fragt PacketFence wie ein Wachmann: «Darf dieses Gerät rein?». In der Autorisierungsantwort wird mitgeliefert, ob Zugriff gewährt wird und in welches Netz das Gerät verschoben werden soll.

Use-Cases

Das Thema NAC kann komplex und abstrakt wirken – mit folgenden Use-Cases wird das Thema verständlicher und greifbar.

Schutz sensibler Daten durch rollenbasierten Zugriff

Herausforderung:	Mitarbeiter aus verschiedenen Abteilungen (z.B. Buchhaltung, Vertrieb) benötigen unterschiedliche Netzwerkzugriffe. Keine einfache Möglichkeit, Zugriffsrechte durchzusetzen.
Lösung:	NAC erlaubt rollenbasierten Zugriff: Mitarbeiter erhalten nur Zugriff auf die für ihre Rolle relevanten Ressourcen. Gastgeräte haben nur Internetzugriff.
Vorteil:	Minimiert das Risiko eines Datenlecks. Klare Trennung von Zugriffen erhöht die Netzwerksicherheit.

Schwachstellenscans und Geräteisolierung

Herausforderung:	Geräte im Netzwerk könnten bekannte Schwachstellen enthalten. Kein automatisiertes System zur Geräteprüfung.
Lösung:	PacketFence integriert einen Schwachstellenscanner (z.B. Greenbone oder Nessus). Geräte mit Schwachstellen werden in Quarantäne verschoben und der Nutzer wird benachrichtigt.
Vorteil:	Reduziert das Risiko von Sicherheitsvorfällen. Transparente Kommunikation mit Nutzern über notwendige Massnahmen.

Sicheres Gäste-WLAN

Herausforderung:	Gäste benötigen Internetzugang, dürfen jedoch nicht auf interne Ressourcen zugreifen.
Lösung:	NAC bietet ein Captive Portal für Gäste, das nur eingeschränkten Internetzugang ermöglicht. Gästezugriff wird zeitlich begrenzt und protokolliert. Erlaubnis kann z.B. über ein Sponsor-E-Mail erfolgen.
Vorteil:	Sicherer Gästezugang ohne Kompromisse bei der internen Netzwerksicherheit. Einfache Verwaltung durch das IT-Team.

BYOD-Sicherheit

Herausforderung:	Mitarbeiter verwenden private Geräte, die potenziell unsicher sind.
Lösung:	Geräte müssen sich über das Captive Portal authentifizieren und werden auf Sicherheitsstandards geprüft (z.B. Updates, Antivirenstatus). Unsichere Geräte werden in Quarantäne isoliert.
Vorteil:	Sichere Integration von BYOD ohne zusätzliche Kosten für Geräte. Erhöhtes Sicherheitsbewusstsein bei Mitarbeitern.

Netzwerkzugang für IoT-Geräte

Herausforderung:	IoT-Geräte (z.B. Drucker, Kameras) haben oft keine Sicherheitsupdates und können Angriffspunkte bieten.
Lösung:	IoT-Geräte werden in ein separates VLAN mit eingeschränktem Zugriff verschoben. Regelmässige Überprüfung dieser Geräte auf Anomalien.
Vorteil:	Minimiert das Risiko, das durch unsichere IoT-Geräte entsteht. Trennung des IoT-Datenverkehrs erhöht die Netzwerksicherheit.

Compliance-Anforderungen umsetzen

Herausforderung:	Das Unternehmen muss Sicherheits- und Datenschutzvorgaben wie ISO 27001 einhalten.
Lösung:	NAC dokumentiert den Netzwerkzugang und speichert Protokolle. Regelmässige Berichte zeigen die Einhaltung der Sicherheitsrichtlinien.
Vorteil:	Nachweisbare Sicherheit für Audits. Unterstützt bei der Zertifizierung und dem Erhalt von Compliance-Standards.

Proaktive Angriffserkennung

Herausforderung:	Angreifer versuchen möglicherweise, sich unbefugt Zugriff zu verschaffen.
Lösung:	NAC erkennt und blockiert Geräte mit auffälligem Verhalten (z.B. ungewöhnlich hohem Datenverkehr oder fehlgeschlagene Anmeldungen). Automatische Benachrichtigung des IT-Teams bei verdächtigen Aktivitäten.
Vorteil:	Reduziert die Reaktionszeit bei Angriffen. Frühzeitige Erkennung verhindert potenziellen Schaden.

Benötigen Sie Unterstützung oder eine Beratung? Gerne stehen wir Ihnen zu Seite und erarbeiten ein individuelles Lösung für Sie.

Datimo | Optimo Service AG
Franz-Burckhardt-Strasse 11 | CH-8404 Winterthur
T +41 58 322 33 33 | support@datimo.ch | www.datimo.ch