Benutzerkonten vor Hackern schützen

Thomas Thaler

thomas.thaler@itelio.com

Agenda

Grundlagen

Was sind eigentlich diese Identitäten

Anwendung in der Praxis

Wie geht‘s denn wirklich

Bedrohungen

Wo liegt die Gefahr

Q&A

Noch Fragen?

Möglichkeiten

Wie können wir uns schützen

Was ist eine Identität

Eindeutige Benutzeridentifikation

Schlüssel zu personalisierten Informationen

Grundlage für Sicherheitsrichtlinien

Person – Identität = 1:n

Identität – Person = 1:1

Identity & Access Management

Benutzerauthentifizierung

Autorisierung

Rollenbasierte Zugriffssteuerung (RBAC)

Warum Identiäten schützen?

Identität = Zugriff

Datenschutz

Compliance

Vertrauen und Reputation

Sicherheitsvorfälle

Finanzielle Verluste

Bedrohungen für Identitäten

Phishing

Brute-Force-Angriffe

Pass-the-Hash

Man-in-the-Middle

Credential Stuffing

Social Engineering

Token-Hijacking

Insider Threats

Sind wir hilflos?

Festungsmodell

Strikte Teilung LAN und Internet

Starke Einschränkungen durch Verbote

Priorität liegt auf Vermeidung von Angriffspunkten

Citymodell

Hohe Flexibilität

Schnelle Reaktion auf Vorfälle

„Selbstlernend“ durch KI

Priorisierung auf Schadensbegrenzung

Zero Trust

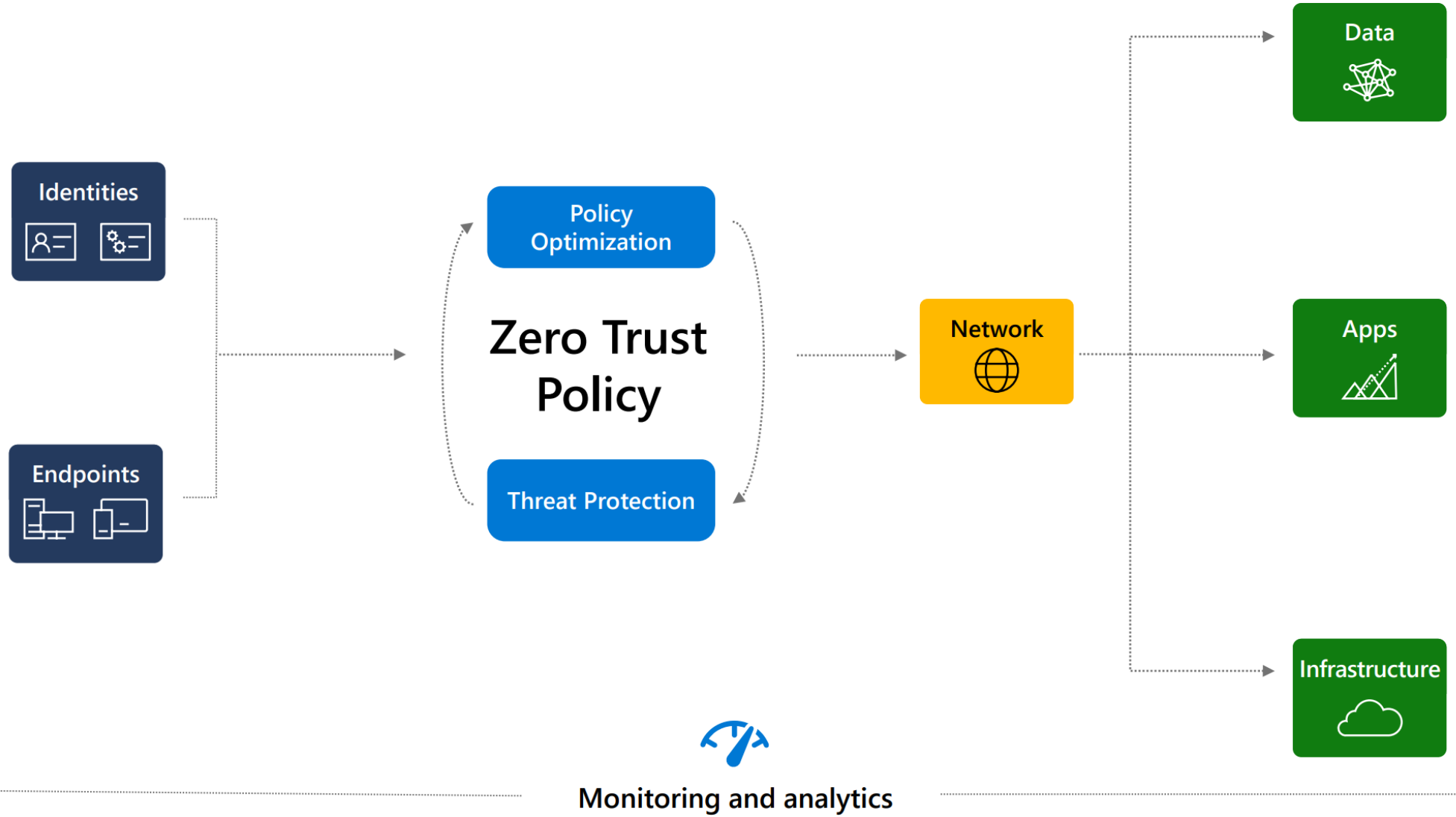
Ständige Verifizierung

Geringstmögliche Berechtigungen

Assume Breach

Microsoft Security

Zero Trust architecture



Multifaktor-Authentifizierung

Das weiß ich

Das habe ich

Das bin ich

Identität schützen

- Anwender mit ins Boot holen
- Anomalieerkennung
- Phishing-Resistenz aufbauen
- Awareness-Training

Privilegierte Rollen schützen

- Keine stehenden Berechtigungen
- Just-in-Time Zugriff
- Genehmigungsprozesse
- Mehrstufige Authentifizierung
- Zugriffsüberprüfungen
- Nachvollziehbarkeit und Auditing

Kontinuierliche Überwachung / Auditing

- Protokollanalyse
- Anomalieerkennung
- Incident-Response-Plan

Security Defaults

Standardeinstellungen

Grundlegender Schutz

Sollte immer eingesetzt werden

Conditional Access / RBCA

Benutzeranmeldungen kontrollieren

Zugriff auf Ressourcen steuern

Risiko bewerten und reagieren

Privileged Identity Management

Zeitlich begrenzter Zugriff

Überwachung von privilegierten Aktionen

Keine stehenden Berechtigungen

4-Augen-Prinzip

Passwortlose Authentifizierung

Microsoft Authenticator

FIDO2 Sicherheitsschlüssel

Windows Hello for Business

Defender for Identity

Ausweiten des Schutzes aufs lokale AD

Integration in Azure AD

Anomalieerkennung

Secure Score

Überprüfen von Einstellungen

Nachvollziehen von Änderungen

Ständige Überwachung

Änderungshinweise erhalten

Noch Fragen?