TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"T.I.S.P. Community Meeting 2022"

Berlin, 09.-10.11.2022

Zero Trust: Vision und Realität

Rudolf Schreiner

ObjectSecurity OSA GmbH

ObjectSecurity

- Standorte in San Diego (CA) und Falkensee, 20 Mitarbeiter
- Fokus: Risikomanagement in komplexen Systemen (Infrastruktur, Industrie, Verkehr, Automotive, Verteidigung, 5G, Lieferketten, KI)
- Entwicklung/Anwendung spezieller Werkzeuge/Technologien
  - Penetration Tests/Schwachstellenanalyse
  - Anomalies Detection
  - Zugriffskontrolle
  - **Implementierung von Zero Trust Architectures**
- Spezieller Ansatz: Automatisierung
  - Modellierung/Regelbasiert
  - Künstliche Intelligenz/Machine Learning

Agenda

- Die Frage heute:
- **Zero Trust : Nur ein neuer Hype oder wirklich nützlich?**
- Welche Herausforderungen führten zur Entwicklung von Zero Trust?
- Die Vision: Was ist Zero Trust?
- Die Realität (Wie) kann Zero Trust umgesetzt werden?

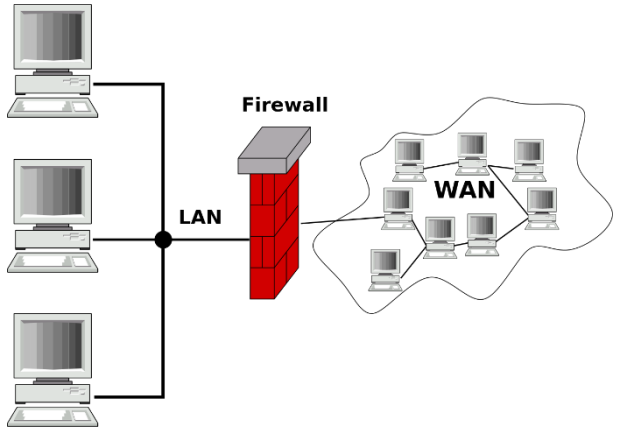
Ziele von IT Sicherheit im Unternehmen

- Wir betrachten das ganz praktisch
  - Cybersecurity ist kein Selbstweck
  - Alle IT und OT Systeme sollen *normal* funktionieren
    - Produkte herstellen, Rechnungen schreiben,…
  - Sensitive Daten sollen nicht in die falschen Hände geraten
    - Herstellungsverfahren, Kalkulationen,…
  - Angriffe sollen beschränkt bleiben
  - Nach einem Angriff sollen Systeme so schnell wie möglich wieder funktionieren
- Zur Erreichung dieser Ziele haben wir vorgesorgt…

Quelle: Wikipedia

Die Lebenslügen der IT Sicherheit

- Mir kann nichts passieren, weil:
  - „Ich habe eine Firewall“
    - Schützt nicht vor Insidern, Ausbreitung, diversen Angriffen
  - „Meine kritischen Systeme sind von aussen nicht zugänglich“
    - Wirklich?
  - „Alle System haben die letzten Updates“
    - Wirklich? Fertigung?
    - Zero Day Angriffe?
  - „Ich habe Backups“
    - Daten-Diebstahl?
    - DoS?
- Firewalls, Updates und Backups sind wichtig!
  - Aber reichen sie?
  - Nein!



Quelle: Wikipedia

Vertrauen ist gut...

- Vertrauen und Annahmen
  - Draussen, das Internet ist böse
  - Drinnen, das eigene Netzwerk ist sicher
  - Ich kann meine gute Welt von der bösen Welt trennen
  - Die bösen Angreifer sind alle draussen
  - Drinnen sind nur die Guten, die eigenen Mitarbeiter
  - Wenn ich Sicherheitsprodukte kaufe, dann bin ich geschützt
- In der Realität
  - Mitarbeiter machen unabsichtlich Fehler
  - Mitarbeiter sind nicht immer *gut*
  - Admins machen Fehler
    - Man versteht Produkte und ihre Grenzen nicht wirklich
    - Beispiel: VPN koppelt Trust Domains

Quelle: Wikipedia

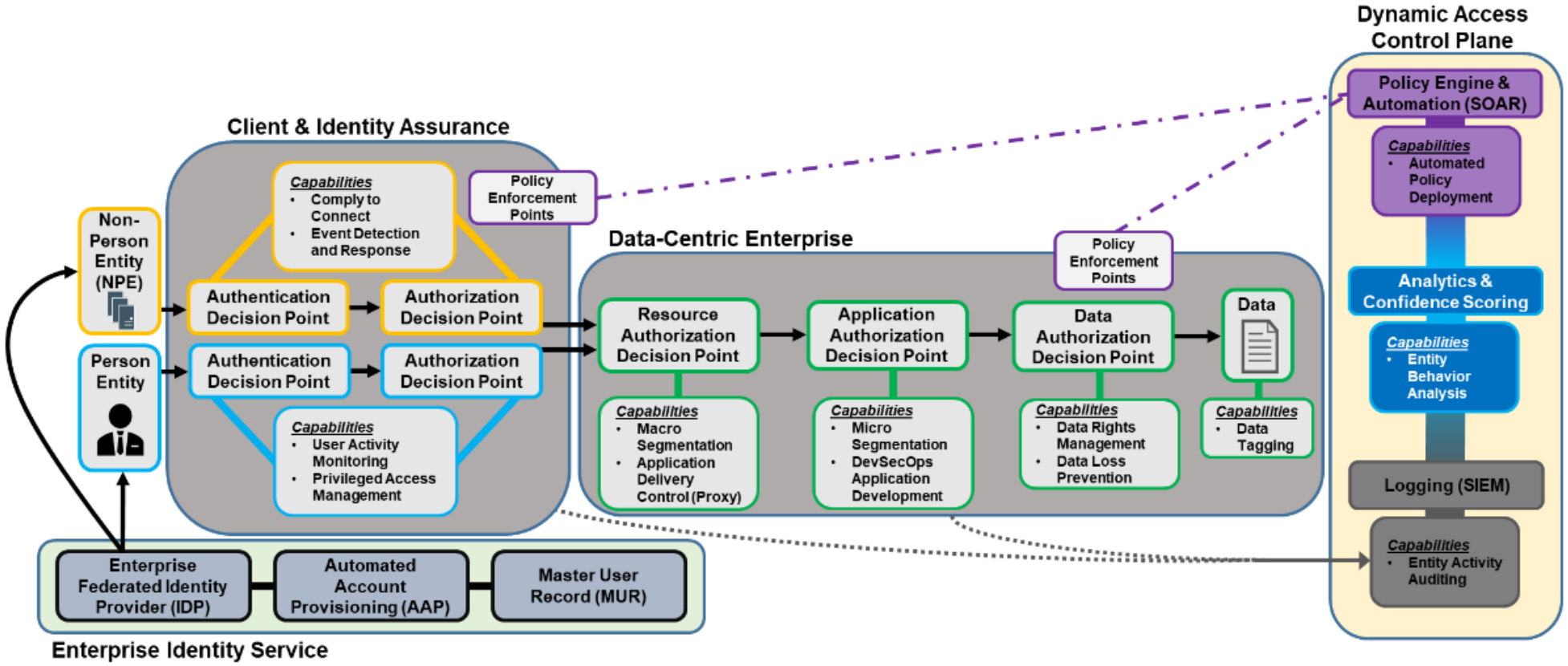
...Kontrolle ist besser! (W.I.Lenin)

- Oder: Trau, schau wem. (Äsop)
- Wir trauen nichts und niemanden!
- ***Vendors: Zero Trust*** *ist die Lösung aller Probleme!*
  - *Kaufen Sie das neue SuperTrust 1.0 von TrustTeck*
  - *Und alles wird gut!*
- Die nächste Silver Bullet kommt schon:
  - Künstliche Intelligenz
- *Intelligent Zero Trust*
  - *Unsere hochinnovative, patentierte KI implementiert automatisch Zero Trust und verteidigt Ihr System*
  - *Nur 9.99 im Monat pro Arbeitsplatz*
  - *Ihren Security Admin können Sie rauswerfen*
- Reality Check?

Zero Trust: Die Konzepte

- Zero Trust: Wir vertrauen nichts und niemanden
  - JEDE Aktion im System muss ausdrücklich authorisiert werden
    - Wer? Was? Oft auch warum, wann, wie, wo?
    - Nutzer und Gerät
  - Keine Unterscheidung zwischen
    - Drinnen und draussen
    - Vertrauenswürdig und nicht vertrauenswürdig
  - Kontinuierliches Monitoring und Risikoanalyse
    - Continuous Adaptive Risk and Trust Assessment (CARTA)
    - Continuous Diagnostics and Mitigation (CDM)
- Getrieben von
  - NIST: SP 800-207, Zero Trust Architecture
  - DOD: Zero Trust Reference Architecture

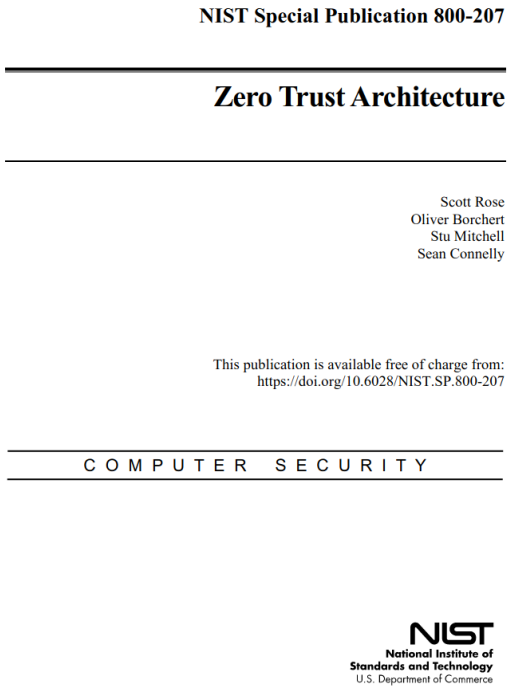
Zero Trust Architektur



DoD Zero Trust High Level Operational Concept

Zero Trust ist eine Herausforderung

- ZTA nach NIST SP 800-207/DOD ist sehr komplex
  - Kann auch zu Angriffspunkten führen
- Kein Produkt, sondern ein Prozess
- Basiert auf vielen komplexen Konzepten und Technologien
  - Dynamische Risikoanalyse
  - Sammlung aller benötigten Daten schwierig
  - Komplexe Datenanalyse
- Viele Herausforderungen, die gemeinhin wegabstrahiert werden
  - Integration in bestehende und neue Systeme
- Der Kern von Zero Trust ist hochkomplexe Zugriffskontrolle


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

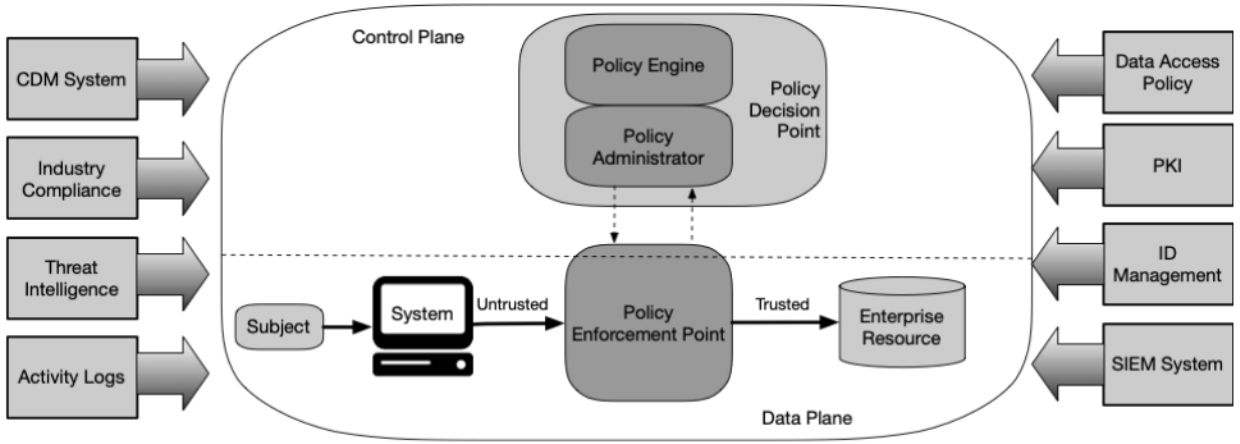
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Zero Trust: Komplexe Zugriffskontrolle

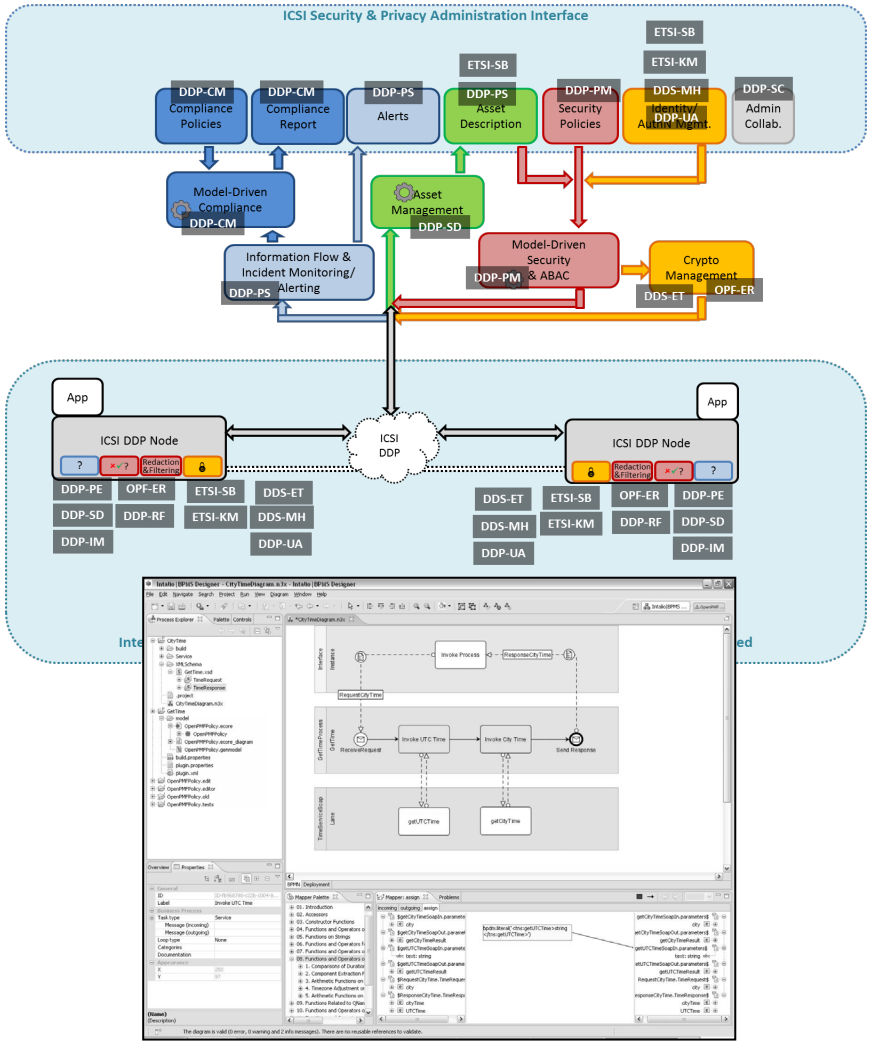
- Im Zero Trust Bildchen:
  - Alles ganz einfach…
  - Policy Enforcement Point (PEP)
  - Policy Decision Point (PDP)
- In der Realität: Zugriffskontrolle ist hochkomplex
  - Korrekte Policies
  - Korrekte Umsetzung an allen relevanten Stellen und Ebenen, jederzeit und konsistent



- Die Standards sind hier nicht hilfreich…

Zero Trust: Alter Wein in neuen Schläuchen?

- Der Kern von Zero Trust ist feingranuläre Zugriffskontrolle
- Wir machen das seit 20 Jahren
  - Telekommunikation
  - Flugsicherung
  - Intelligent Transport Systems
  - Intelligence/Predictive Policing
  - SoA/BPMN
- Herausforderungen:
  - Policy vs Technologie
  - Verteidigung in der Tiefe
  - Komplexität
  - Assurance



Zugriffskontrolle: 1. Herausforderung

- **Detallierte Beschreibung des Systems**
  - Alle Bestandteile
  - Alle Interaktionen
- Modellierung aller relevanten Informationen
  - Subjekte
  - Assets/Resourcen-Objects
  - Interaktionen
  - Systeme
- aus
  - Beobachtung des Systems
  - Vorhandenen Informationen (UML, BPMN, Directories,…)
  - Scannen, Reverse Engineering

Zugriffskontrolle: 2. Herausforderung

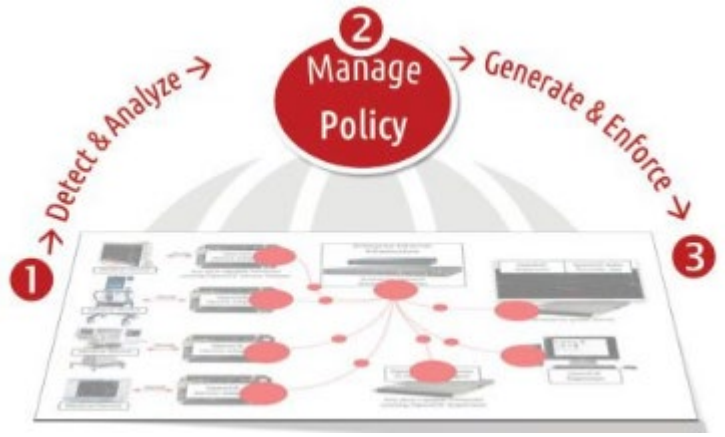
- **Definition der High Level Policies**
  - Wer darf wann was in welchem Context?
  - Definiert von Menschen
- Beispiele
  - Der behandelnde Arzt darf auf Patientenakten seiner Patienten zugreifen
  - Im Notfall darf jeder Arzt auf die Patientenakte zugreifen
- Wie beschreibe ich diese Regeln formal?
  - Role Based Access Control (RBAC)
  - Attribute Based Access Control (ABAC)
  - Proximity Based Access Control (PBAC)
- Korrekte Formulierung ist nicht so einfach
- Nicht direkt durchsetzbar

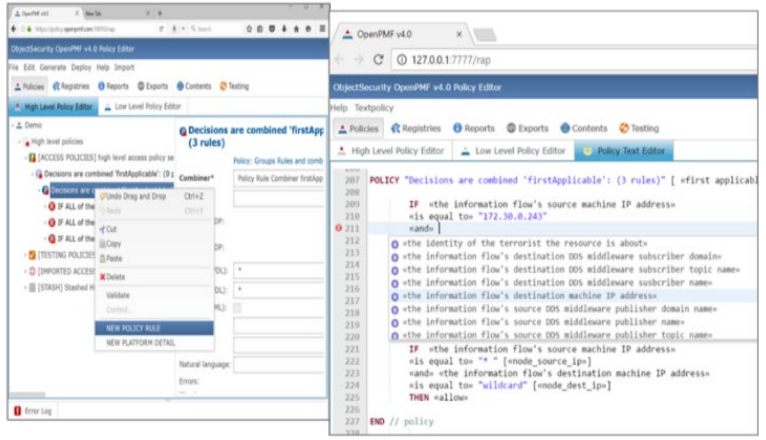
Zugriffskontrolle: 3. Herausforderung

- **Durchsetzung der Policies**
  - In allen Systemen
  - Auf allen Ebenen
- Erzeugung von Low Level Regeln
  - Netzwerke (Firewall ACL)
  - Middleware/Services (z.B. XACML)
  - Datenbanken
  - ….
- Nicht einfach
  - Konsistenz zwischen Systemen und Zeitpunkten
  - Semantische Brüche zwischen Ebenen
  - Sehr grosse Mengen von Regeln

Die Lösung: Model Driven Security

- Technisch alles machbar
- Implement z.B. in unserem OpenPMF Produkt
  - Systemmodellierung
  - Definition der Policies
  - Durchsetzung der Policies
- Und noch viel mehr
  - Policy Checker
  - Risiko Analyse
- Funktioniert grossartig
- **ABER…**





Die Lösung: Model Driven Security???

- In der Praxis kaum umsetzbar
  - Zumindest nicht in normalen Unternehmen
- Meist viel zu komplex und aufwändig
- Muss von Anfang an in Life Cycle integriert werden
- Muss von der kompletten Infrastruktur und allen Applikationen unterstützt werden
- Daher nur für sehr wenige Anwendungen/Umgebungen geeignet
- Aus den gewonnenen Erfahrungen kann man einiges für Zero Trust ableiten:
  - Die vorgeschlagene Kontrolle aller Zugriffe ist so einfach nicht umzusetzen
  - Von den anderen Herausforderungen ganz zu schweigen

Zero Trust in der Realität

- Zero Trust ist für die meisten Unternehmen derzeit kaum vollständig umsetzbar
  - Trotzdem viele wertvolle und umsetzbare Konzepte
- Was kann man praktisch tun?
  - Zuerst das eigene Denken ändern
- Das eigene System besser verstehen und dokumentieren
- Asset Management: Welche Werte/Assets-Resourcen habe ich?
  - Was will ich schützen?
  - Daten, Services, Systeme, Netzwerke,...
- Identity Management: Welche Subjekte habe ich?
  - Nutzer, Devices
- Verständnis der Interaktionen
  - Wer greift wann/womit zu?

Zero Trust in der Realität

- Access Management
  - Pragmatische Zugriffskontrolle
  - Besser simples RBAC als gar keine Zugriffskontrolle
  - Segmentierung in kleinere Trust Domains reduziert die Ausbreitung von Angriffen
- Security Information and Event Management
  - Detektion von Anomalien im internen Netz, nicht nur auf Firewalls und nicht nur Intrusions
- Nicht zuletzt:
  - Vertrauen Sie niemanden!
  - Auch wenn Sie gemeinsam im Kirchenchor singen!

Zusammenfassung

- Perimeter/Firewall-zentrische Sicherheit hat viele Schwächen
- Zero Trust ist konzeptionell sehr mächtig
  - Kein Vertrauen
  - Jeder Zugriff wird überprüft
- Praktische Umsetzung sehr aufwändig
  - Kein Produkt, sondern Prozess
  - Komplexe Technologien
- In vielen Fällen nicht umsetzbar
- Nicht jede Initiative des DoD ist für Sie relevant
- Viele Konzepte auch praktisch anwendbar und hilfreich