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

TeleTrusT-Konferenz

28.06.2022, Berlin

"Zero-Trust-Konzepte"

Dirk große Osterhues, Deutsche Bahn

Zero Trust@DB

Allgemeine Strategieprinzipien für die Deutsche Bahn

TeleTrusT-Konferenz | Deutsche Bahn AG | Dirk große Osterhues | Berlin | 28.06.2022

Zero Trust-Strategien

1. Motivatoren und ursächliche Herausforderungen
2. Säulen und Leitmotive von Zero Trust-Strategien
3. Ziele und Vorteile für den Deutsche Bahn-Konzern

Motivatoren und ursächliche Herausforderungen

Happy Birthday! 30 Jahre Perimeter Sicherheit: Das „Extern vs. Intern“ Paradigma

1980

Erste Paket Filter Firewalls (J. Mogul)

1988

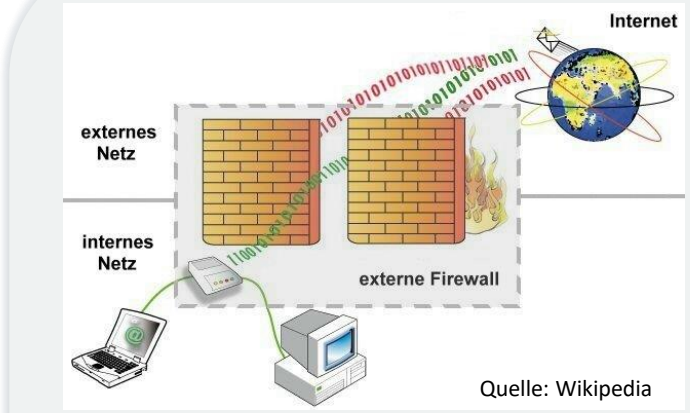
IETF unterscheidet „interne“ und “externe” Netze (RFC 1335)

1990

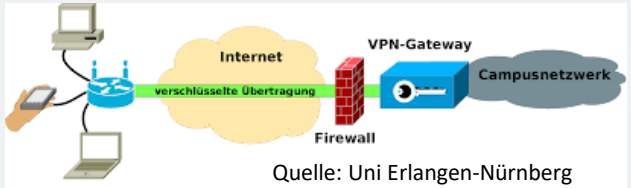
Erste Firewalls auf Anwendungsebene (Spafford, Cheswick, Ranum, Bellovin)

1992

Diverse Weiterentwicklungen von Firewalls



Quelle: Wikipedia



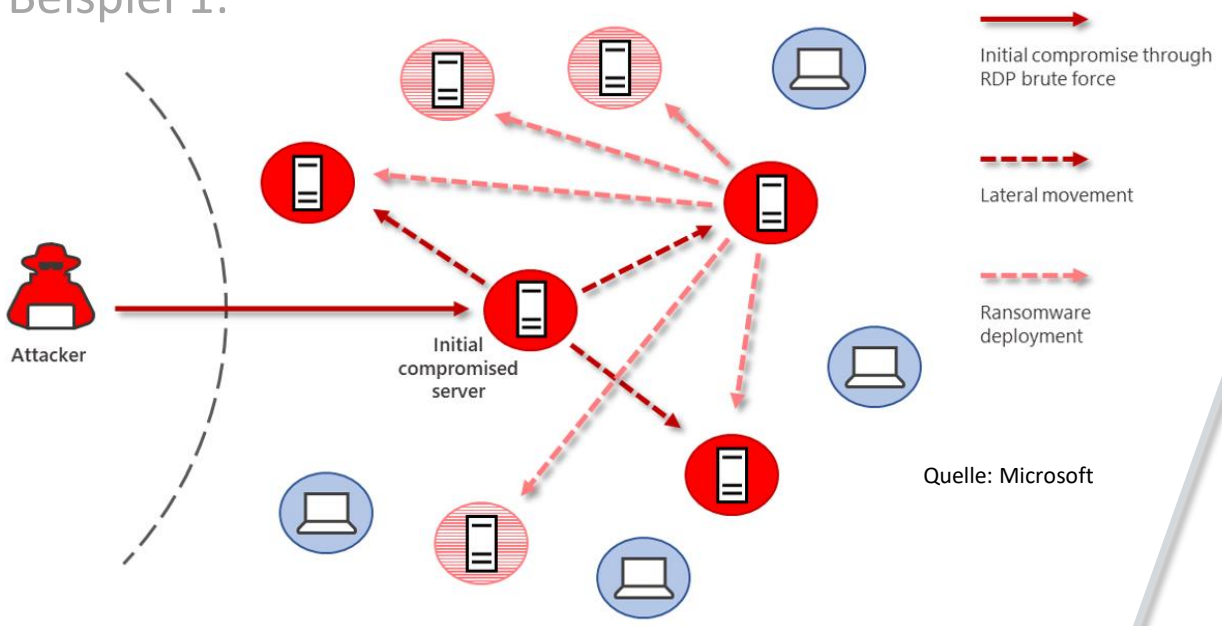
Quelle: Uni Erlangen-Nürnberg

2022

Motivatoren und ursächliche Herausforderungen

Probleme mit dem „Extern vs. Intern“-Paradigma: Zwei Beispiele

Beispiel 1:



Quelle: Microsoft

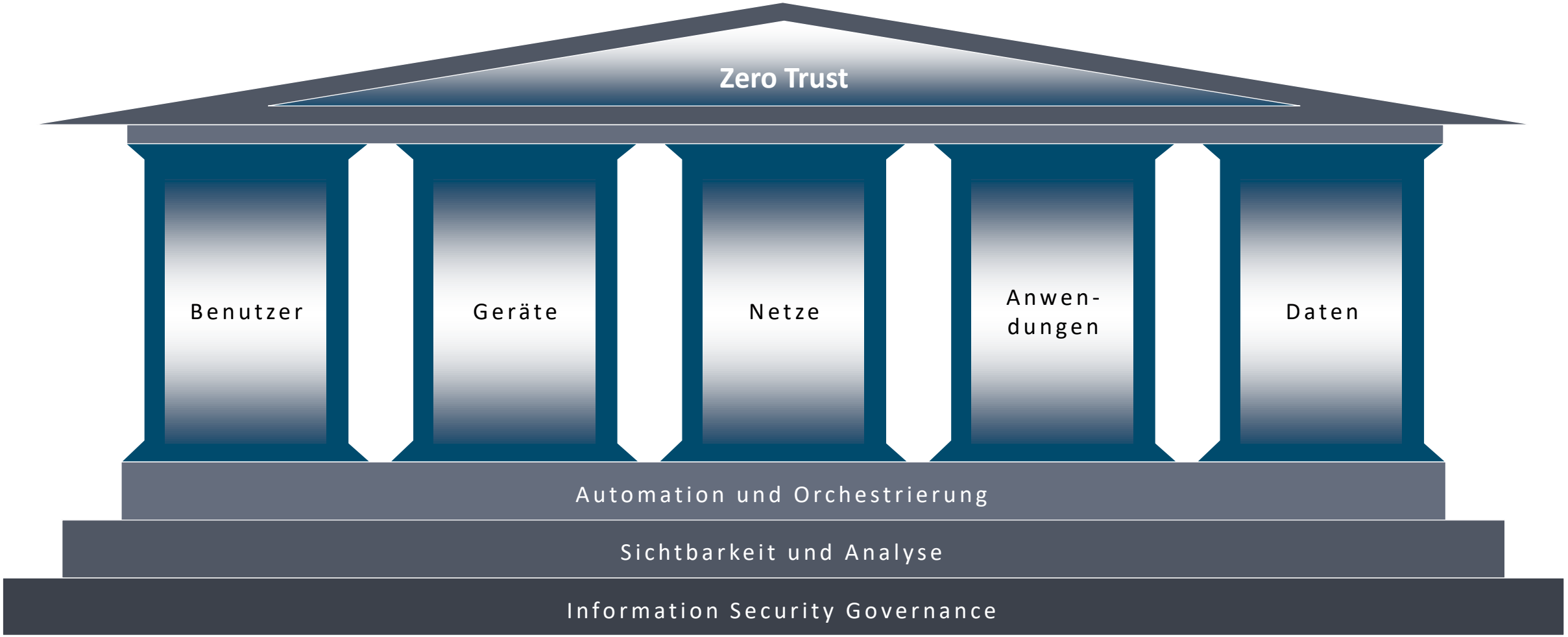
Harte Schale – weicher Kern.

Beispiel 2:

Wo ist „innen“?

Säulen und Leitmotive von Zero Trust-Strategien

Good Practice von Zero Trust-Ansätzen lässt sich in drei Leitmotive und fünf Domänen strukturieren



Ziele und Vorteile für den Deutsche Bahn-Konzern

5+1 industrieübliche Grundsätze verfolgt die Deutsche Bahn beim Design und der Implementierung ihrer Zero Trust-Strategie

Grundsatz +1:
Zero Trust ist keine einzelne Technologie und kein Produkt, sondern ein Paradigma.

Grundsatz 1:
Netze sind per se nicht vertrauenswürdig.

Grundsatz 2:
Zugriffe sind nur mit Authentifizierung möglich.

Grundsatz 3:
Zugriffe sind nur über einen sicheren Kanal möglich.

Grundsatz 4: Anomalien und Sicherheitsereignisse werden kontinuierlich erkannt.

Grundsatz 5: Authentifizierung und Autorisierung werden in Echtzeit an das aktuelle Risiko angepasst.

Ziele und Vorteile für den Deutsche Bahn-Konzern

Zero Trust bedeutet für die Deutsche Bahn eine resiliente, einheitliche und dabei für die Nutzenden einfach konsumierbare IT

Aktuell wachsen die Unsicherheiten:
IT-Landschaften werden komplexer - es gibt kein Innen und kein Außen mehr
- Angriffe werden ausgefeilter - Sicherheit wird teurer

Warum ist Zero Trust für die DB wichtig?

- Zur **Abwehr von Angriffen** sind getrennte Sicherheitsmechanismen in den Domänen nicht effektiv
- **Angriffe** (auch noch unerkannte) **müssen automatisch maximal möglich begrenzt** werden
- Sicherheitsmechanismen dürfen ein System **für Anwender:innen nicht unverwendbar machen**, aber Sicherheit bieten, wann und wo erforderlich
- **Aufwände reduzieren** durch übergreifende Funktionen

Auf was können wir uns bei Zero Trust freuen?

- **Flexibilität für das Business und Sicherheit** beim Arbeiten in einer heterogenen Welt mit Hybrid- und Multi-Cloud, On-Premises und Mobile Work
- **Einheitliche Bedienbarkeit** durch standardisierte Lösungen für sämtliche Anwendungen, z.B. SSO und zusätzliche Abfragen, sofern erforderlich
- **Schnellere und einfachere Umsetzungen** durch Automatisierungen und Orchestrierung von Sicherheitsmaßnahmen

Dirk große Osterhues
IT Security Governance Manager

Deutsche Bahn AG
An der Welle 3
60322 Frankfurt am Main

Mobil: 0170-100 6780