Webinar
Zero-Trust-Architektur
Das große Ganze zählt

Max Zöller

T·M·K
THOMAS MACK
KOMMUNIKATION GMBH

Zu meiner Person

Max Zöller

- 20+ Jahre Erfahrung im Bereich Kommunikation & Netzwerk
- Seit 2014 bei der TMK Thomas Mack Kommunikation
- Seit 2022 Geschäftsfeldleitung
- Verantwortungsbereich Informationssicherheit & Netze
- Zwischen Köln und Bonn, verheiratet, 2 Kinder

Agenda

T·M·K
THOMAS MACK
KOMMUNIKATION GMBH

01 Geschichte & Entwicklung von Zero Trust

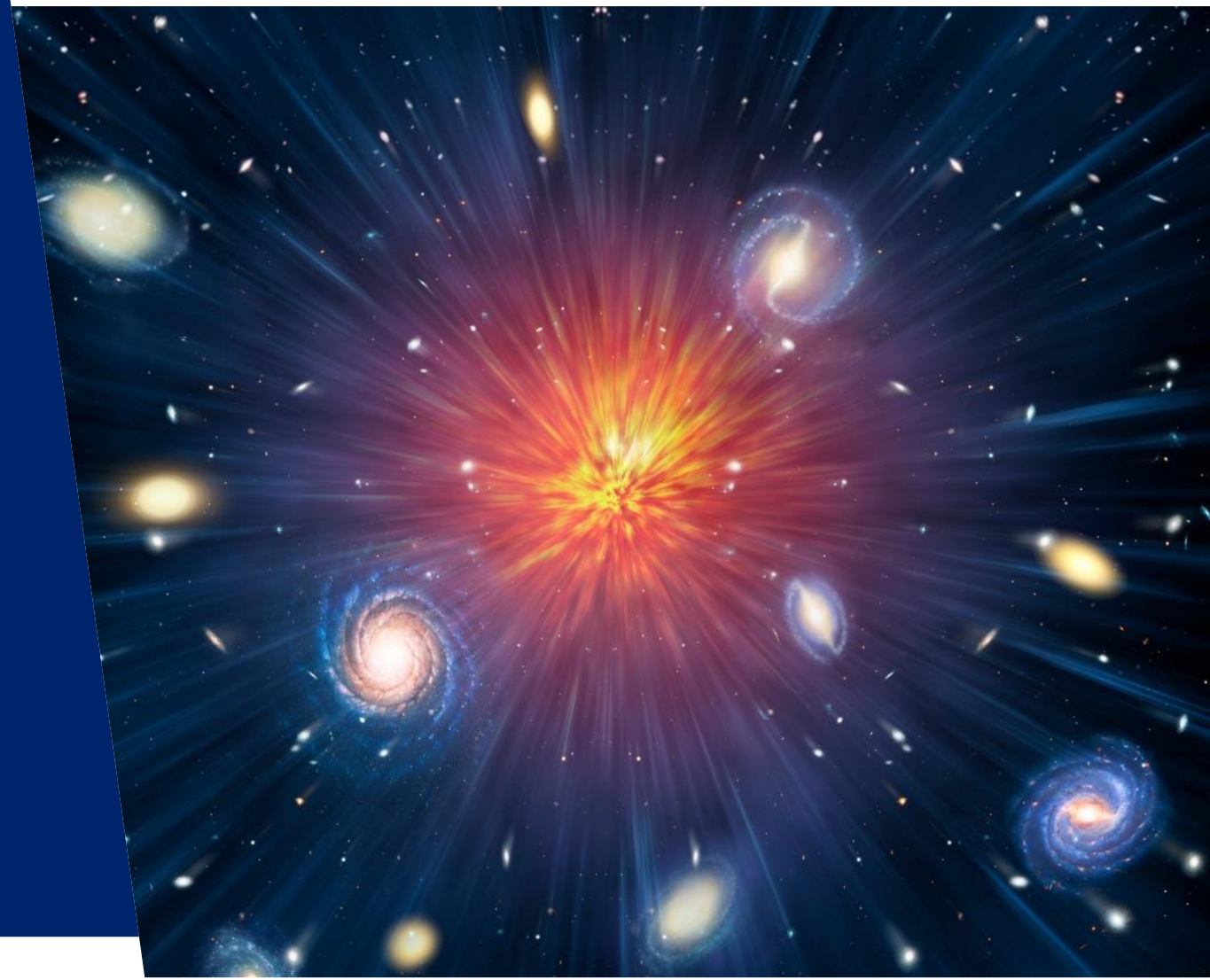
02 Der Zero-Trust-Ansatz

03 Zero Trust in der Praxis

04 Zero Trust in Ihrem Unternehmen?

Patagonien Chile Nationalpark Torres del Paine See

Geschichte & Entwicklung von Zero Trust



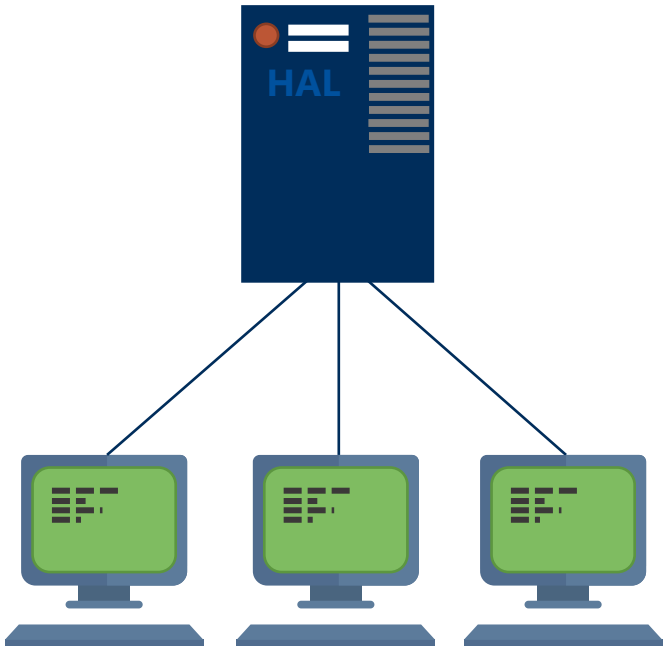
Die Vorzeit

Die Bedrohung war überschaubar

T·M·K
THOMAS MACK
KOMMUNIKATION GMBH

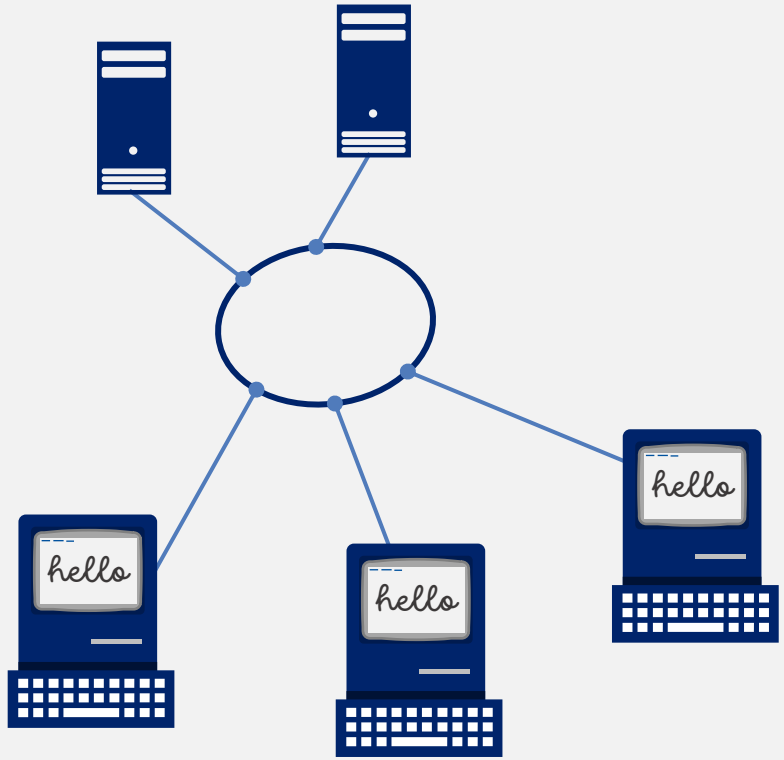
Mainframes und Terminals

Die Mutter der EDV



Local Area Networks

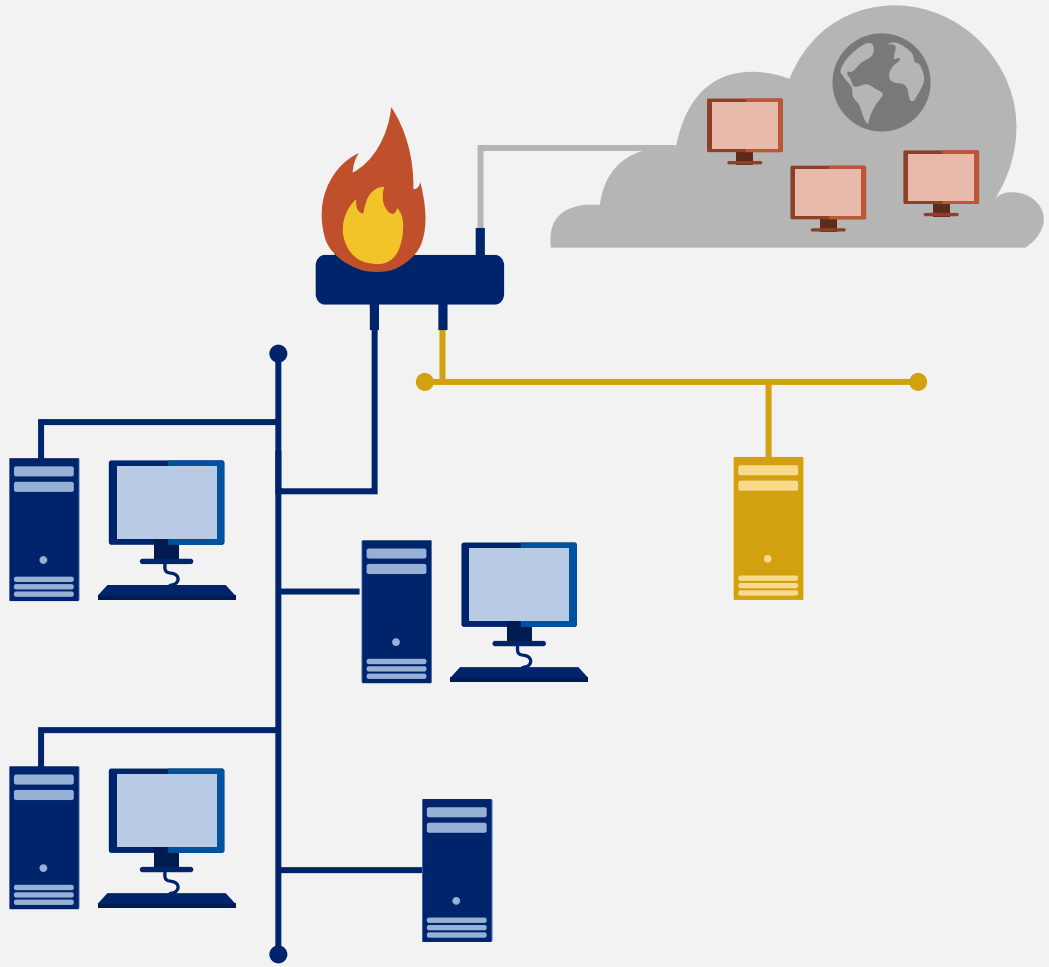
Personal Computer werden gesprächig



Das Internet und Firewalls

Das Perimeter Security Modell

- Legitimer Zugriff durch unbekannte Clients außerhalb des Kontrollbereichs
- Zentrale Benutzerverwaltung (Active Directory)
- Zugriff auf interne Ressourcen nur von innen
- Demilitarisierte Zone (DMZ) für Zugriffe von außen



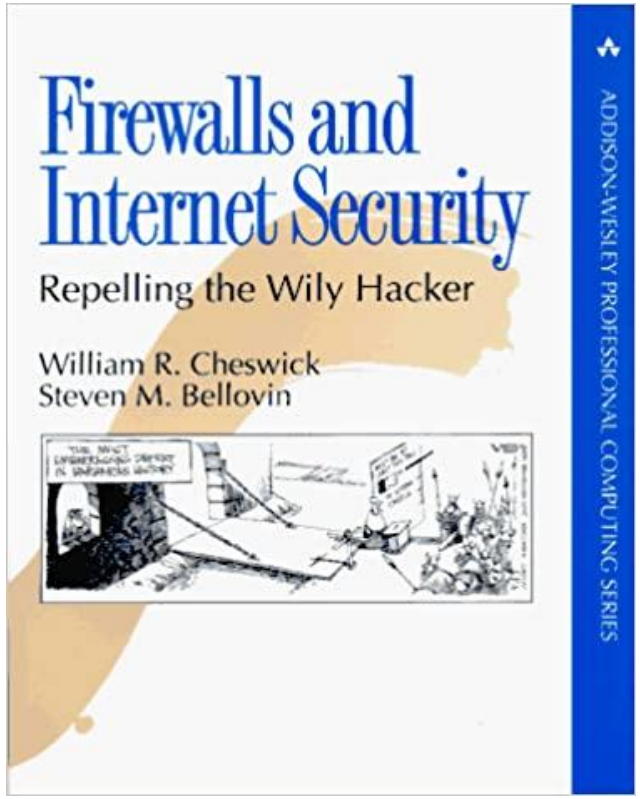
„Erfinder“ der Firewall

William Cheswick

Sie sind eine wirtschaftliche Lösung für schwache Host-Sicherheit. Ich möchte eine stärkere Host-Sicherheit sehen

Steven M. Bellovin

Eine Wache an der Eingangstür ist nicht mehr zeitgemäß, wenn es Tausende von Hintertüren gibt. […] Ich sage nicht, dass man die Wache an der Tür abschaffen soll. […] Aber die eigentliche Zugangskontrolle sollte auf dem Host erfolgen.



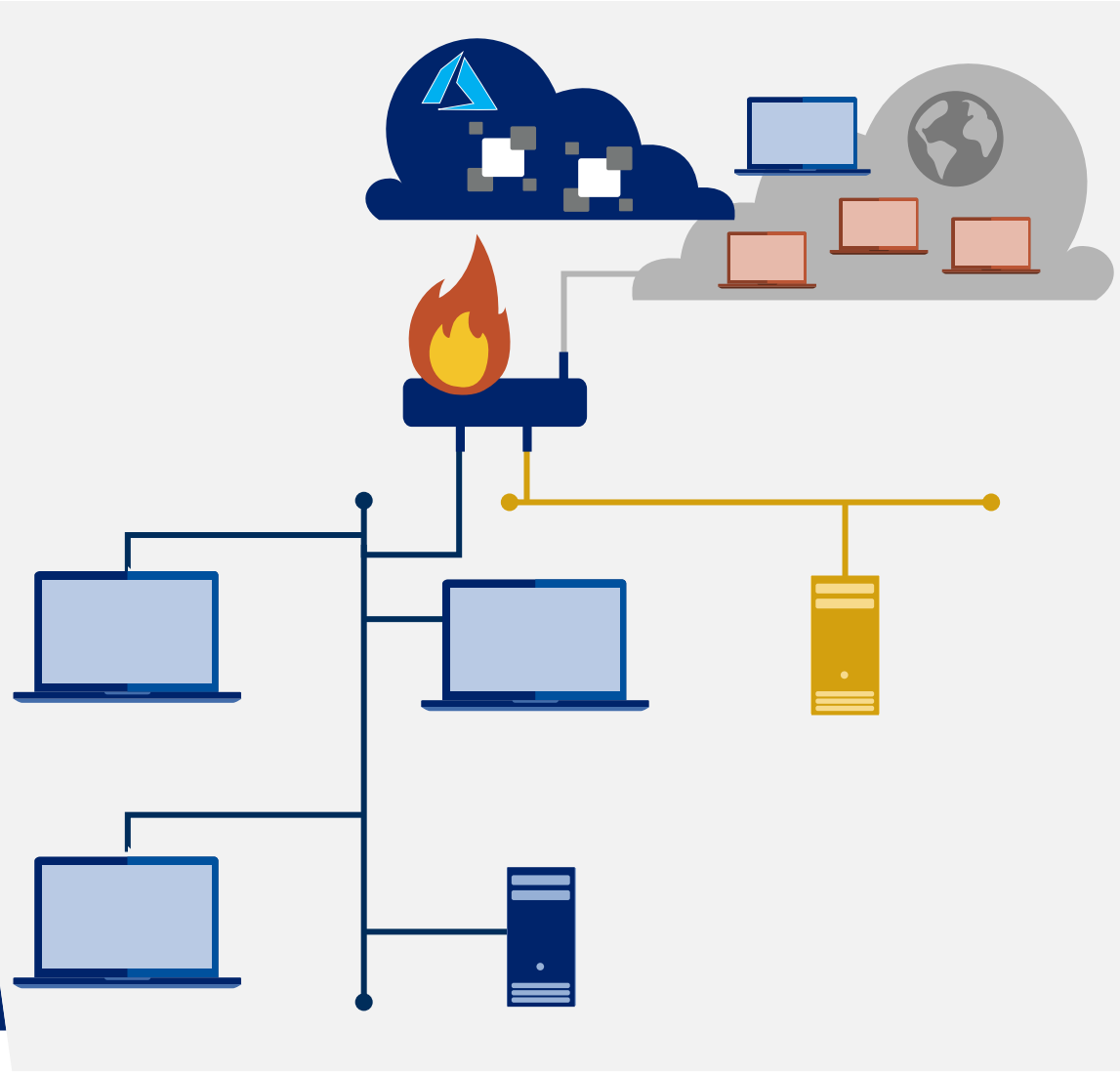
1994: Firewalls and Internet Security

Bilder Quellen: Bellovin: https://www.flickr.com/photos/newamerica/27656453014/ CC 2.0 Generic; Cheswick: https://www.cheswick.com/ches/speakerinfo.html
Zitat Quelle: https://www.darkreading.com/analytics/who-invented-the-firewall-

Die verteilte Infrastruktur

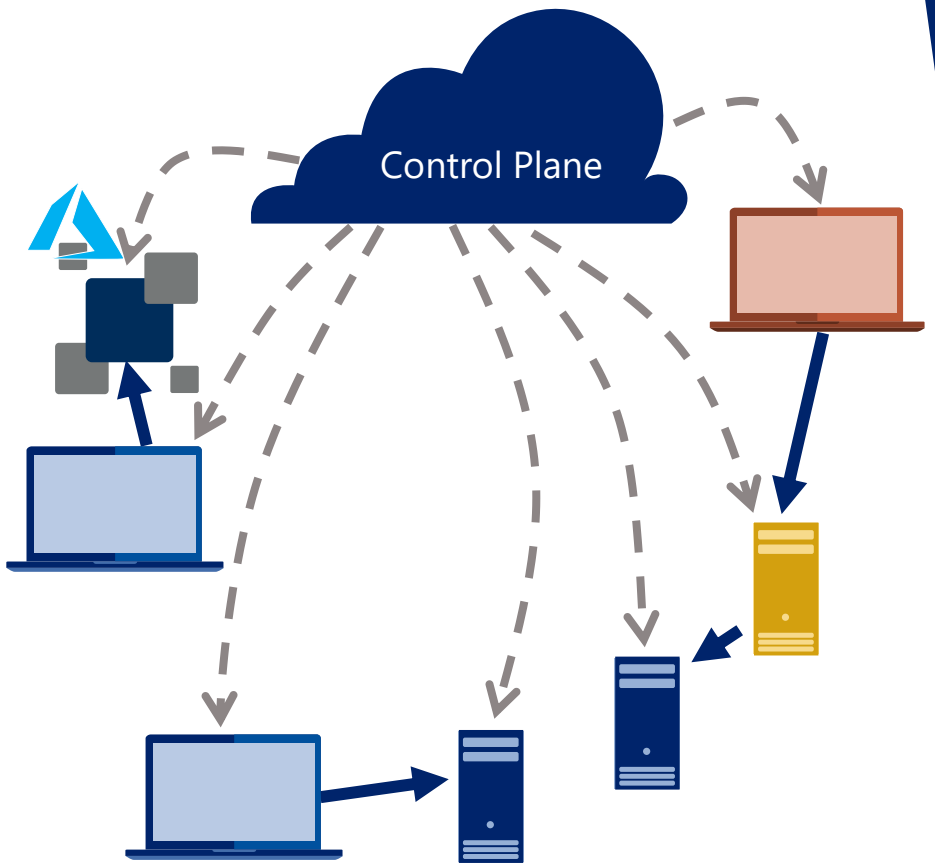
Die Herausforderung für ~~die Zukunft~~ heute

- Interne Benutzer greifen auch von außen auf interne Ressourcen zu
- Interne Ressourcen werden durch Cloud-Services bereitgestellt
- Benutzer sind mobil (Hybrid Workspace)
- Neue Technologien (z. B. SD-WAN)
- Wichtige Sicherheitsdienste kommen von außen (z. B. 2FA)



Die Zero Trust Idee

Vertrauen gesteuert über eine Control Plane



- Kein impliziertes Vertrauen
- Zugriffsanforderungen müssen durch Control Plane autorisierte werden
- Autorisierung basierend auf Anwender, Gerät und mehr
- Schützenswertere Ressourcen benötigen stärkere Authentifizierung
- Control Plane konfiguriert Data Plane dynamisch und automatisiert

Der Zero-Trust-Ansatz

Zero Trust Prinzipien

T·M·K
THOMAS MACK
KOMMUNIKATION GMBH

Verify explicitly
Jeder einzelne Zugriff wird authentifiziert und kontinuierlich überprüft.

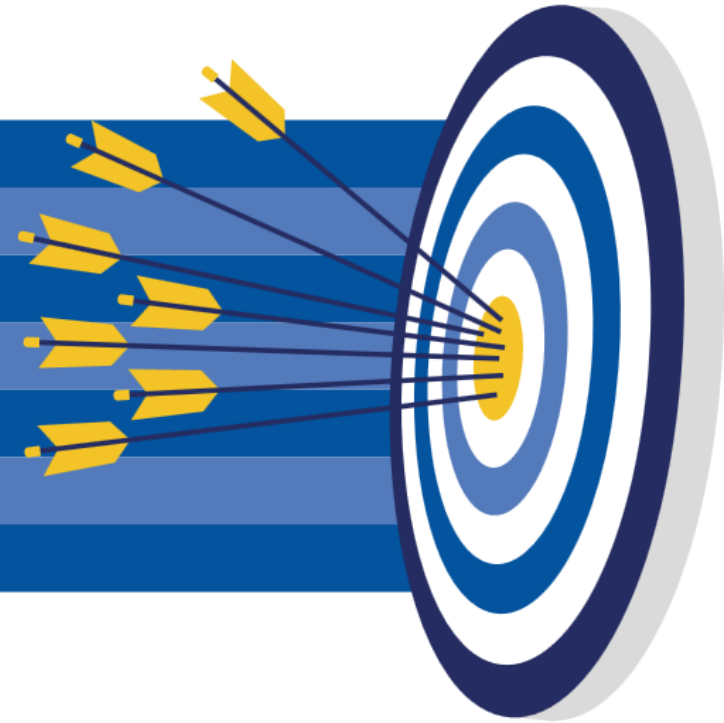
Use least privileged access
Nutzer erhalten nur die minimal notwendigen Zugriffsrechte für die spezifische Anfrage.

Assume breach
Es wird immer davon ausgegangen, dass der Angreifer bereits im System ist.

Wozu das Ganze?

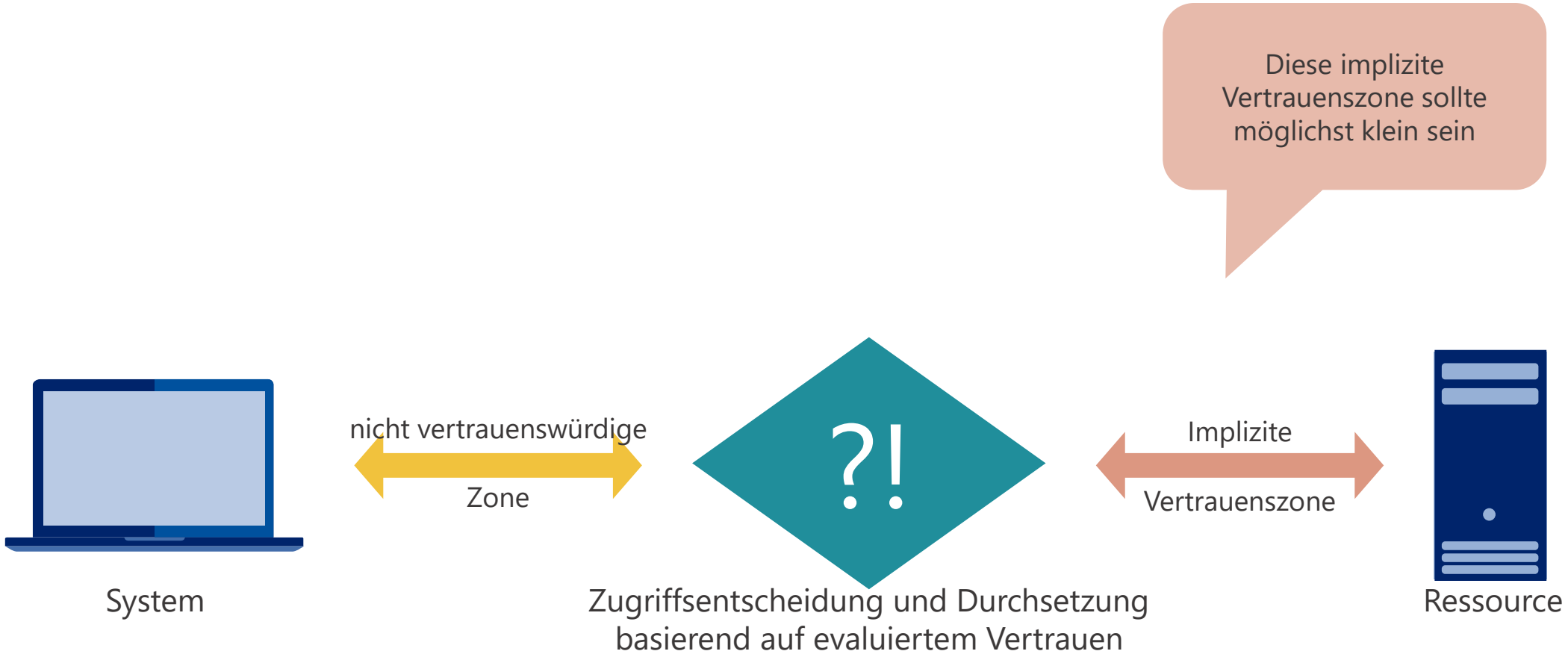
T·M·K
THOMAS MACK
KOMMUNIKATION GMBH

- Minimierung von Angriffsflächen
- Präventive Absicherung von Anwendungszugriffen
- Einheitliches Schutzniveau On-Premise oder in der Cloud
- Geringeres Risiko von Sicherheitsverletzungen
- Sicherer Hybrid-Arbeitsplatz
- Transparentere Einblicke in die digitale Umgebung
- Einheitliche Best Practices für Datenschutz und Governance



NIST Referenzarchitektur

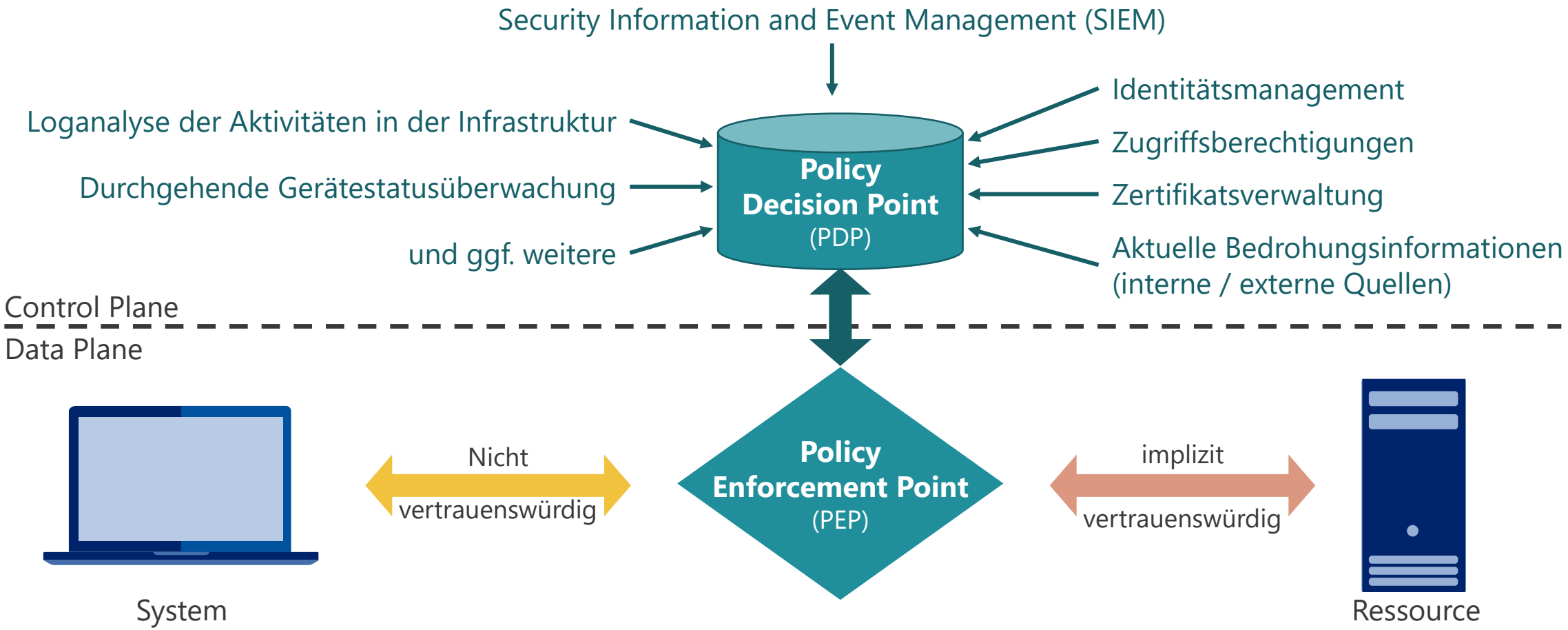
Logischer Aufbau - Einstieg



Quelle: Positionspapier Zero Trust vom BSI

NIST Referenzarchitektur

Logischer Aufbau - Erweitert



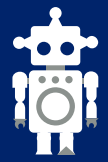
Quelle: Positionspapier Zero Trust vom BSI

Umsetzung von Zero Trust

Erstmal Misstrauen aber dann …

T·M·K
THOMAS MACK
KOMMUNIKATION GMBH

Vertrauen in Geräte



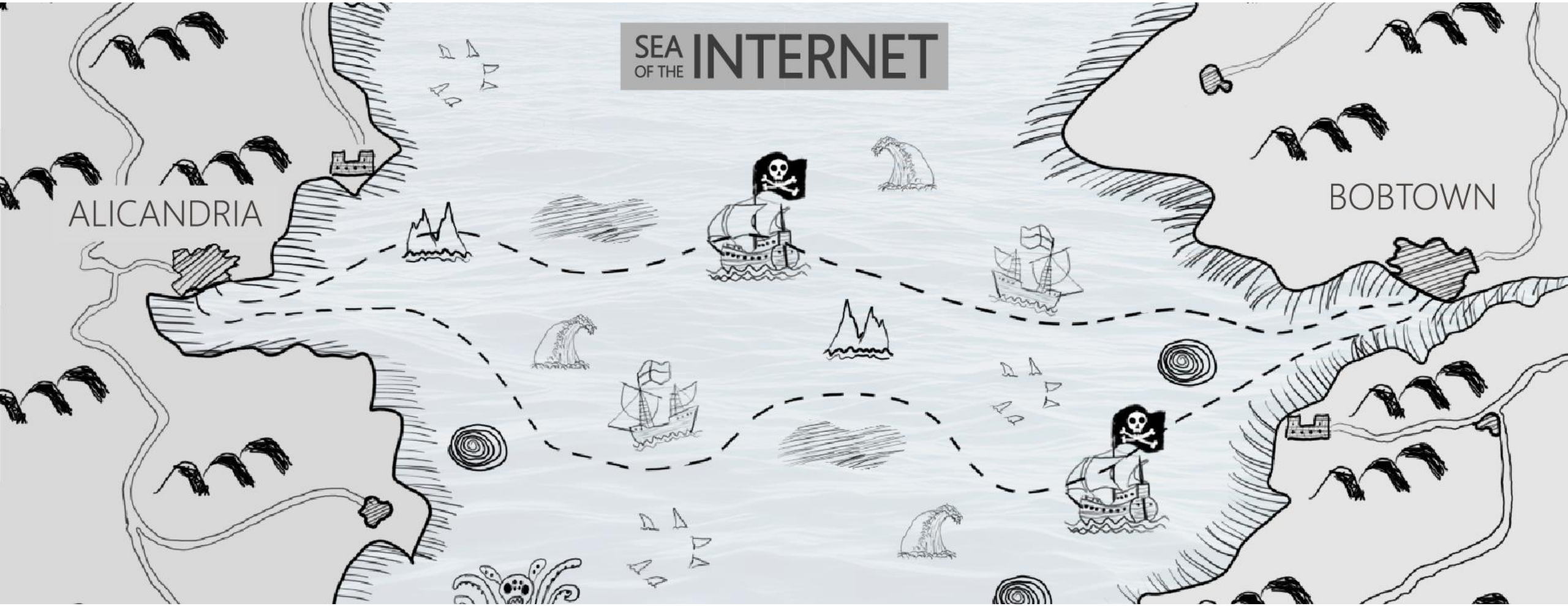
Vertrauen in Nutzer

Vertrauen in Applikationen

Vertrauen in den Netzwerkverkehr

… etablieren.

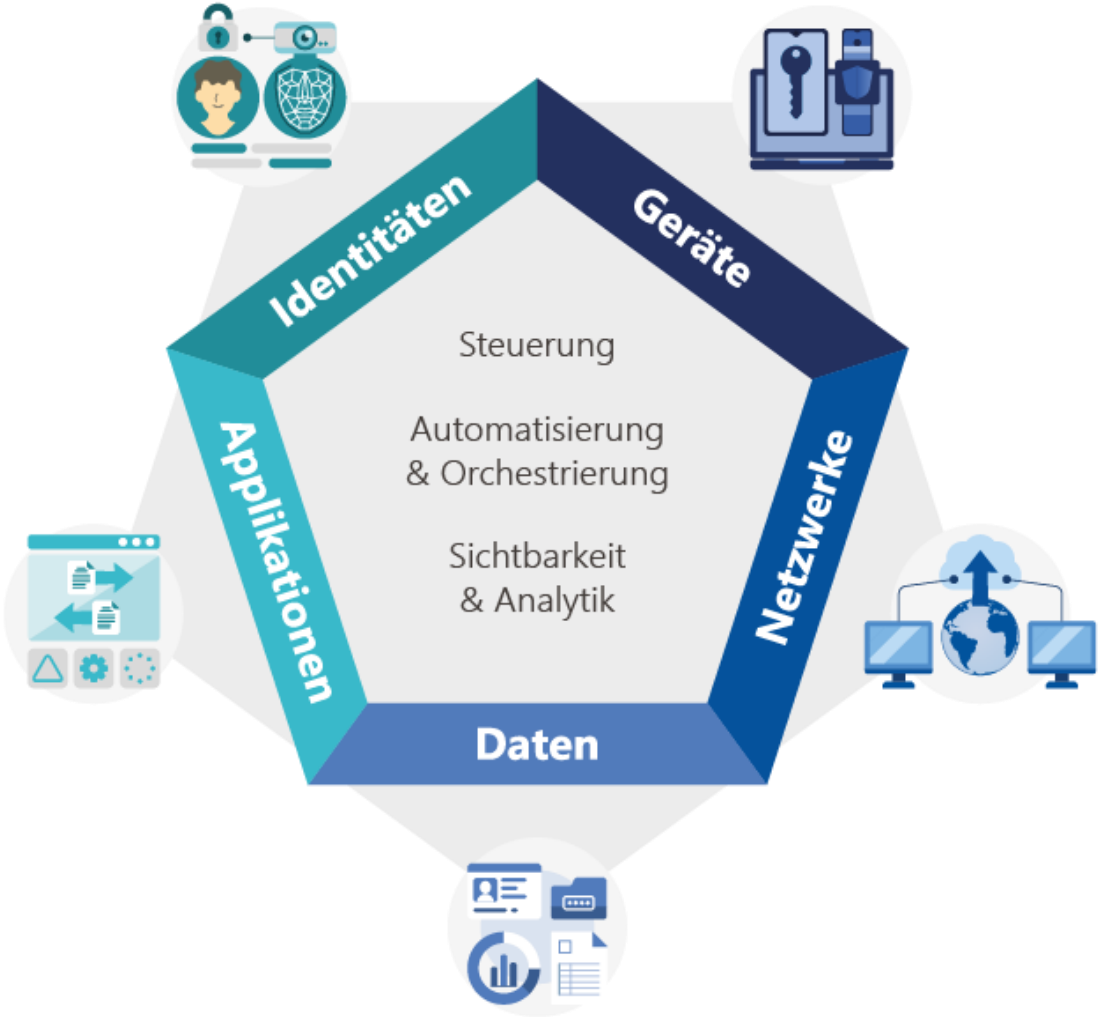
Das Threat Model von Zero Trust



Zero Trust in der Praxis

Reifegradmodell (nach CISA)

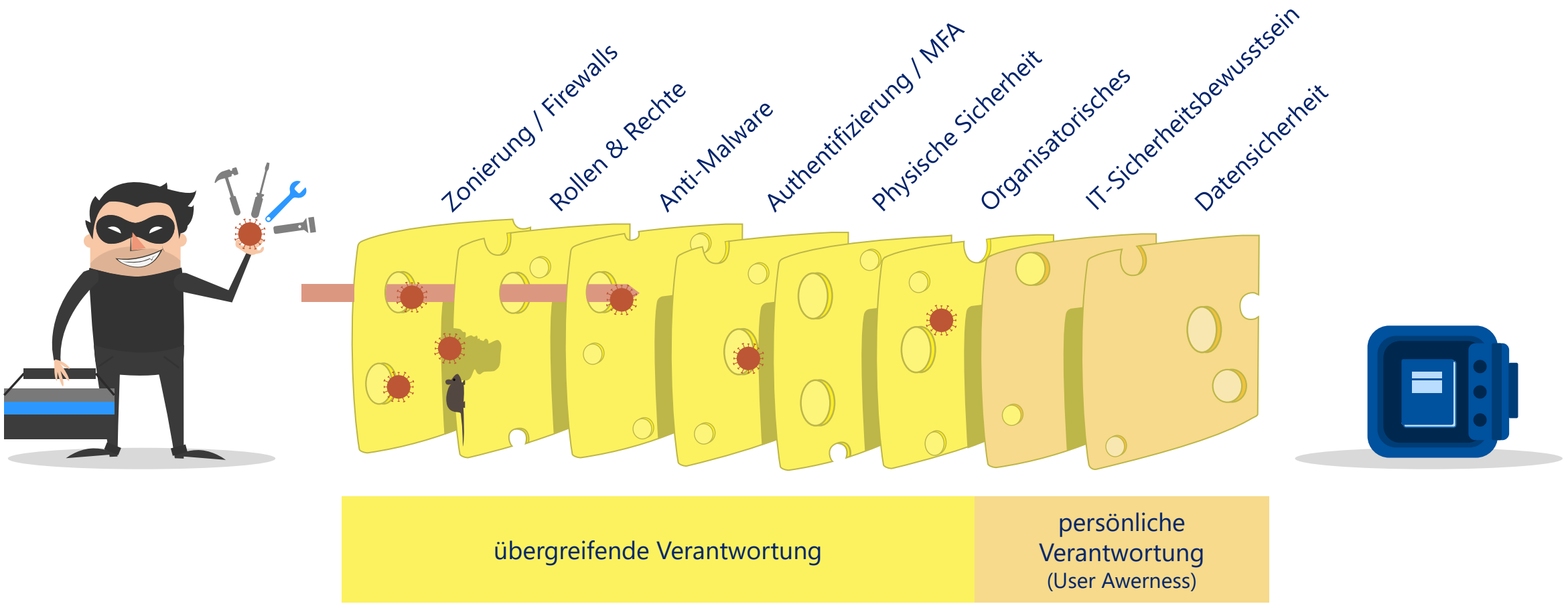
Die Pfeiler der Zero Trust Architektur



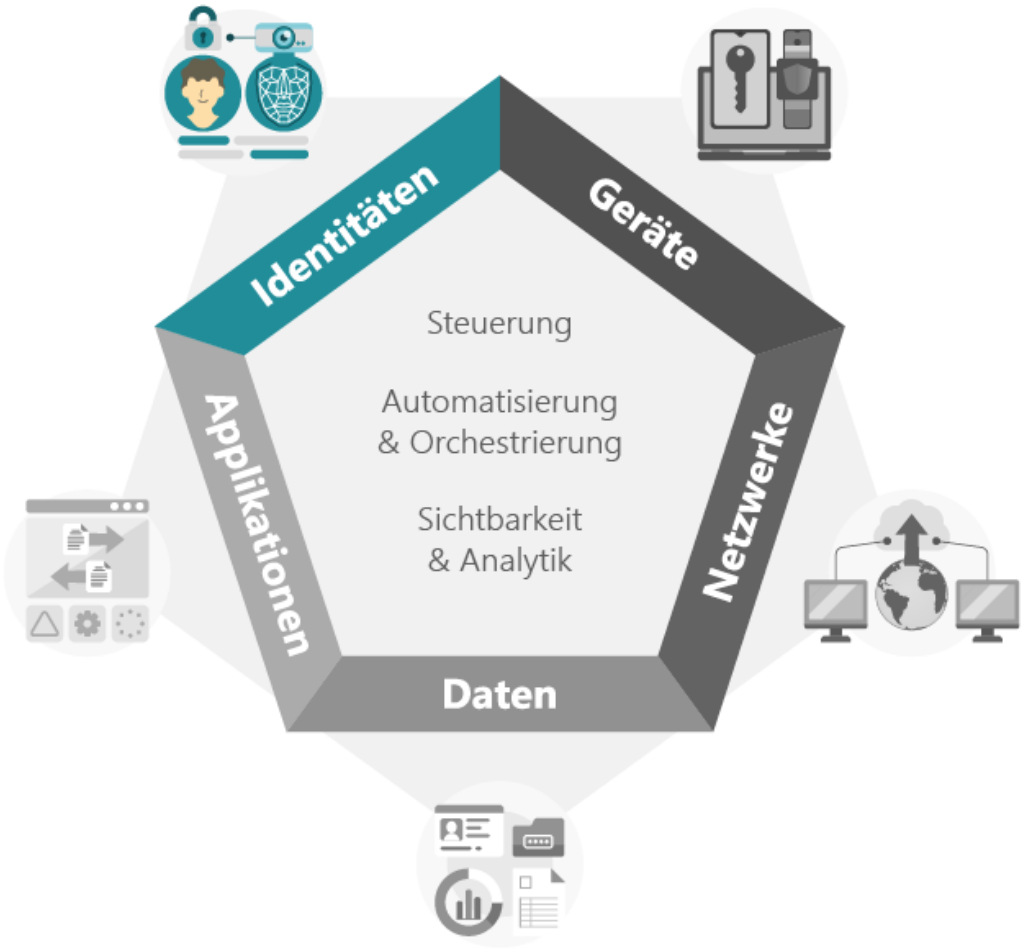
Quelle: Zero Trust Maturity Model der CISA

Defense in Depth

Schweizer Käse Modell

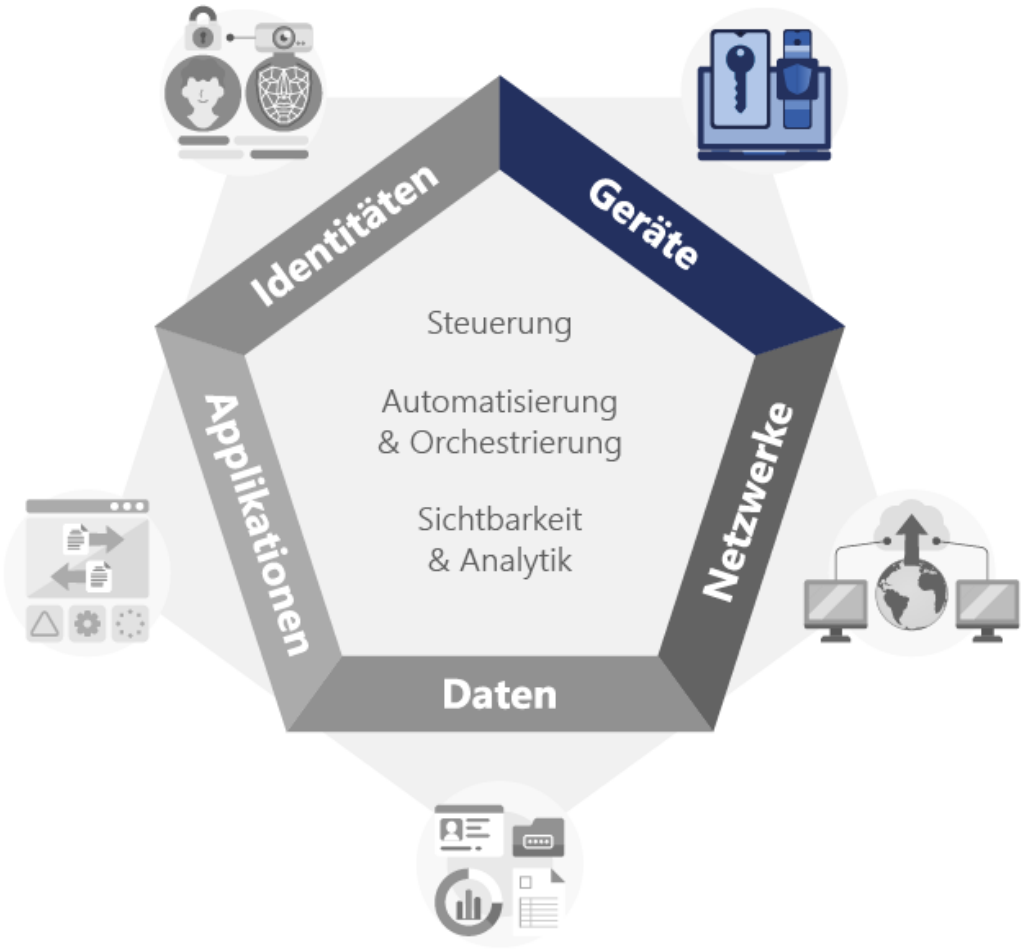


Teilbereich Identitäten



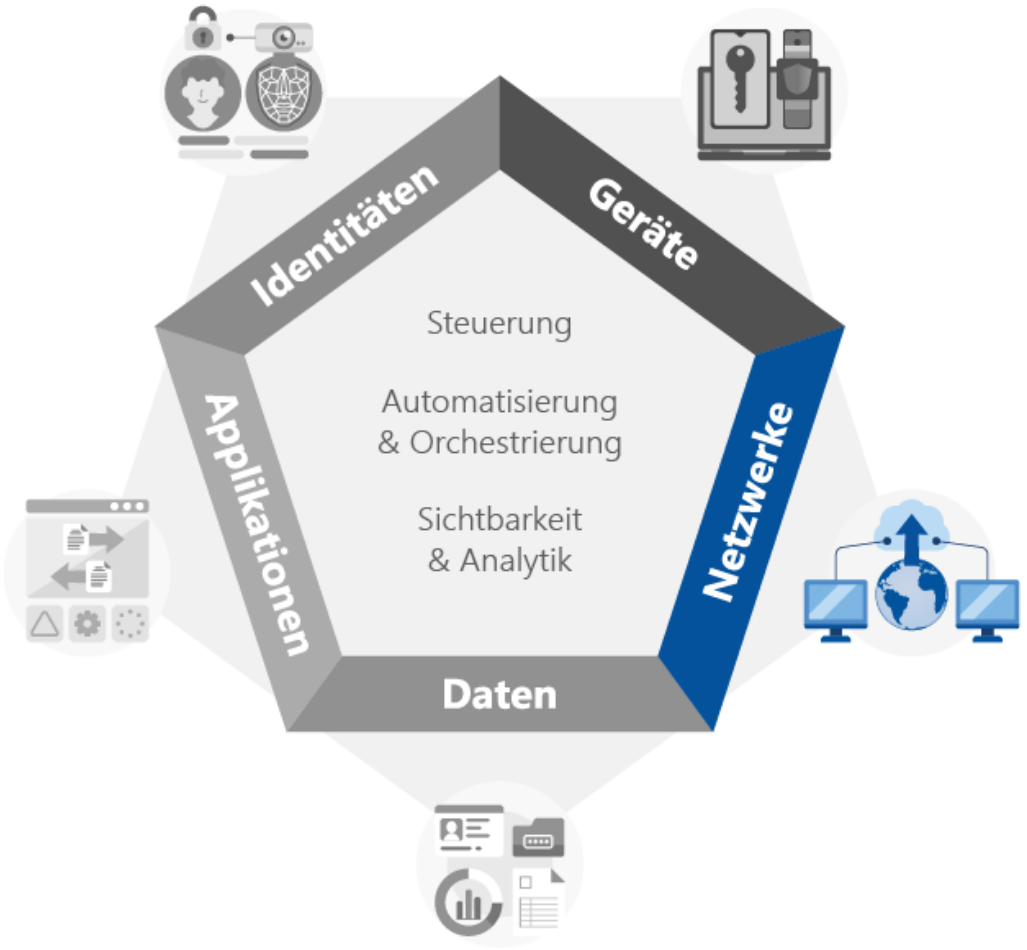
- Authentisierung
  (Password, MFA, Passkeys)
- Autorisierung
  (Rollen & Rechte)
- Identitätsprovider
- Identitätsverwaltung
- Single Sign-On
- Vertrauens Scores
- Identity Recovery Systeme
- Fehlerkultur
  (See Something, Say Something)

Teilbereich Geräte



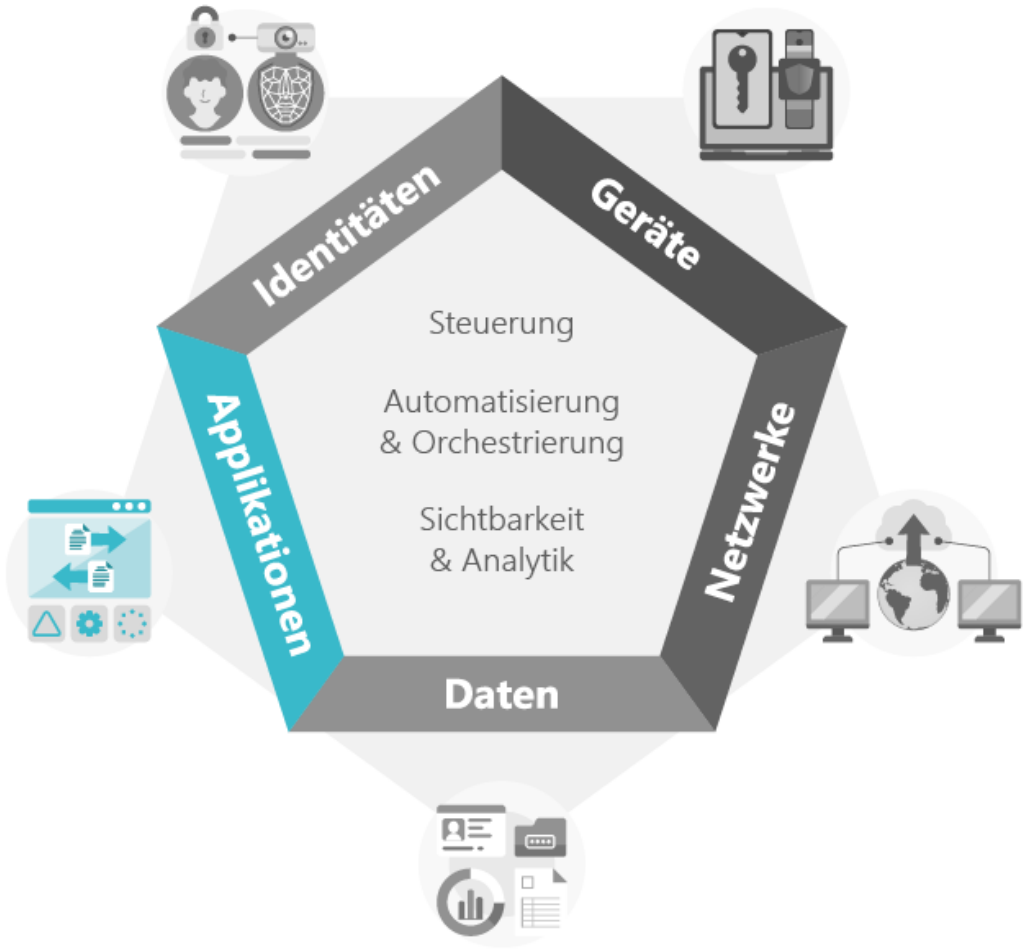
- Asset / Device Management
- sichere System Images (Härtung)
- negative „Vertrauenskurve“ (startet stark, nimmt über Zeit ab)
- Schwachstellenmanagement
- Überwachung Systemgesundheit
- digitale Zertifikate (HSM, TPM, X.509)

Teilbereich Netzwerke



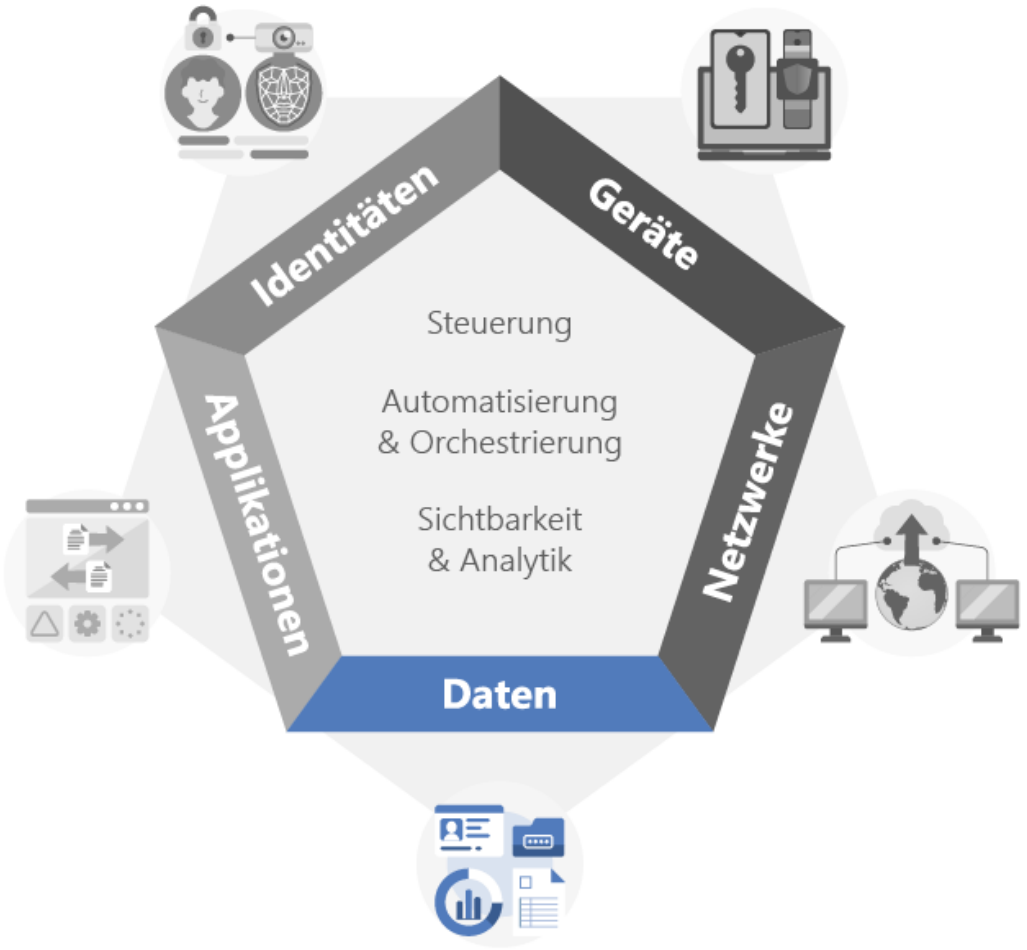
- Verschlüsselung & Authentisierung in Applikationen
- First Packet Problem (SPA – Single Packet Authentication)
- Segmentierung (Mikro & Makro)
- Intrusion Detection & Prevention Systeme (IDS/IPS)

Teilbereich Applikationen



- Klassifizierung
- Server Discovery / Server Trust
- Zugriffsrichtlinien
- Gegenseitige Authentifizierung / MTLS
- Lieferkette
- Härtung
- Least Priviledge / Isolation

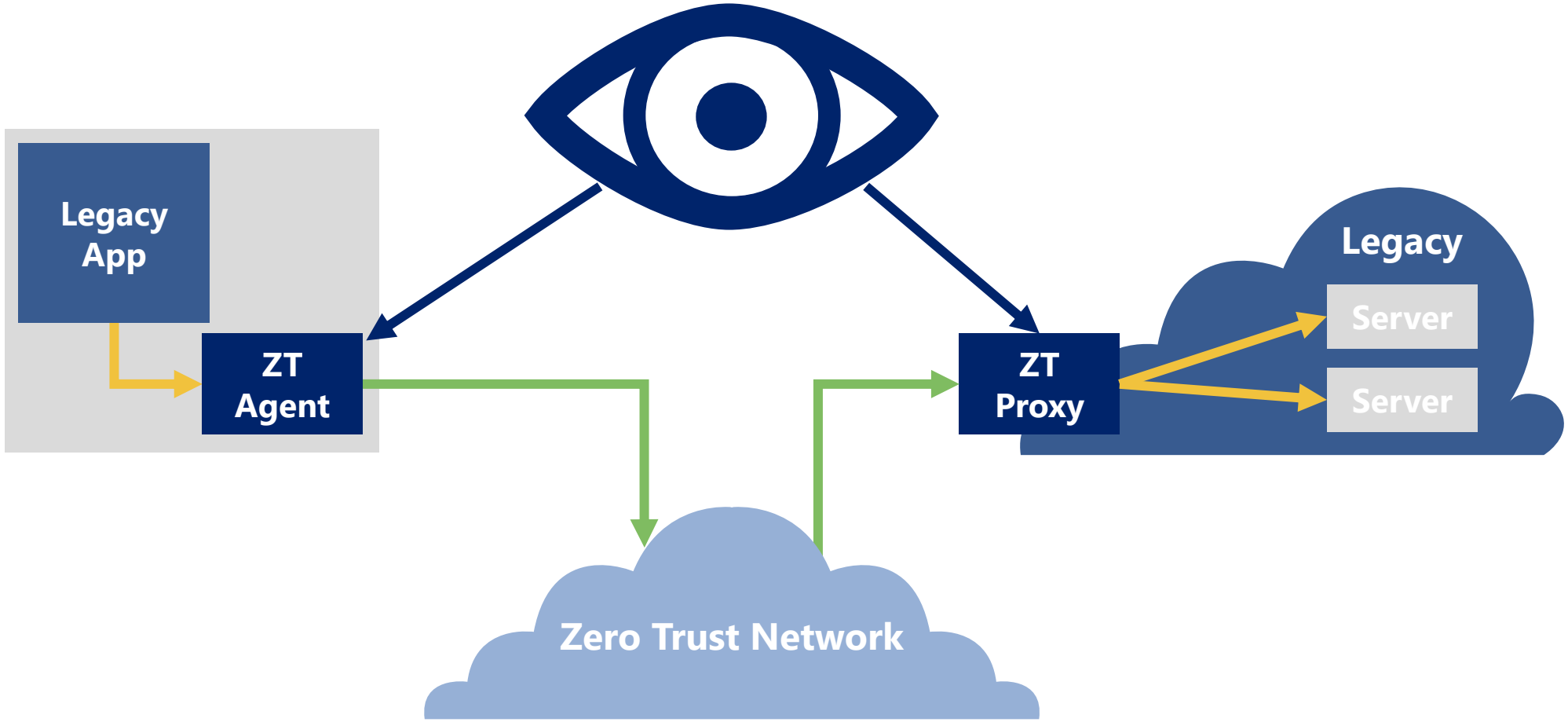
Teilbereich Daten



- Inventarisierung
- Klassifizierung & Zuordnung
- Zugriffsregeln (DLP)
- Verschlüsselung (at rest)

Legacy Gateway – Zero Trust Proxy

Device Agent/Gateway Model

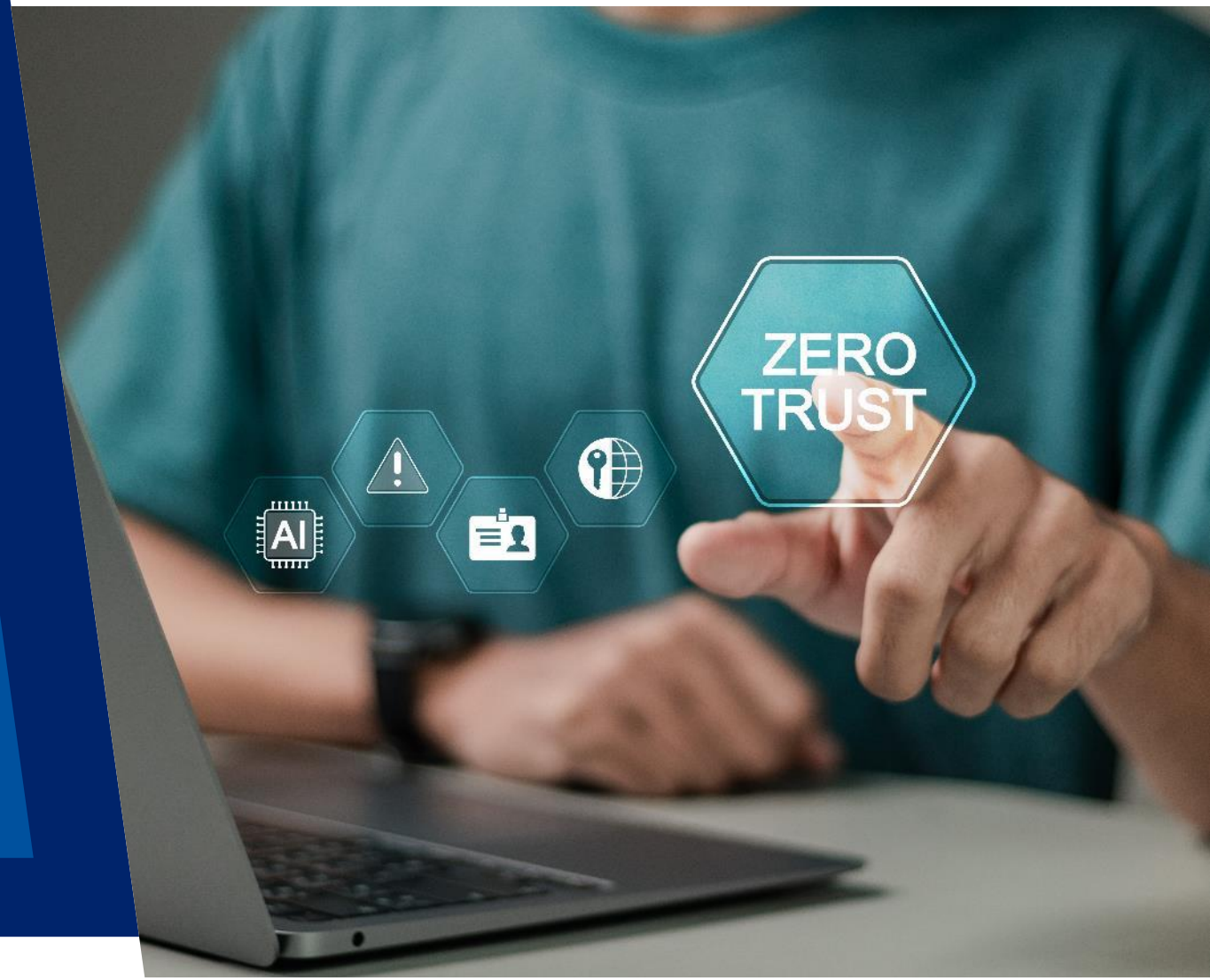


Quelle: NIST Zero Trust Reference Architecture (Device Agent/Gateway Model)

Zero Trust in Ihrem Unternehmen?

Security is a journey, not a destination.

Bruce Schneier

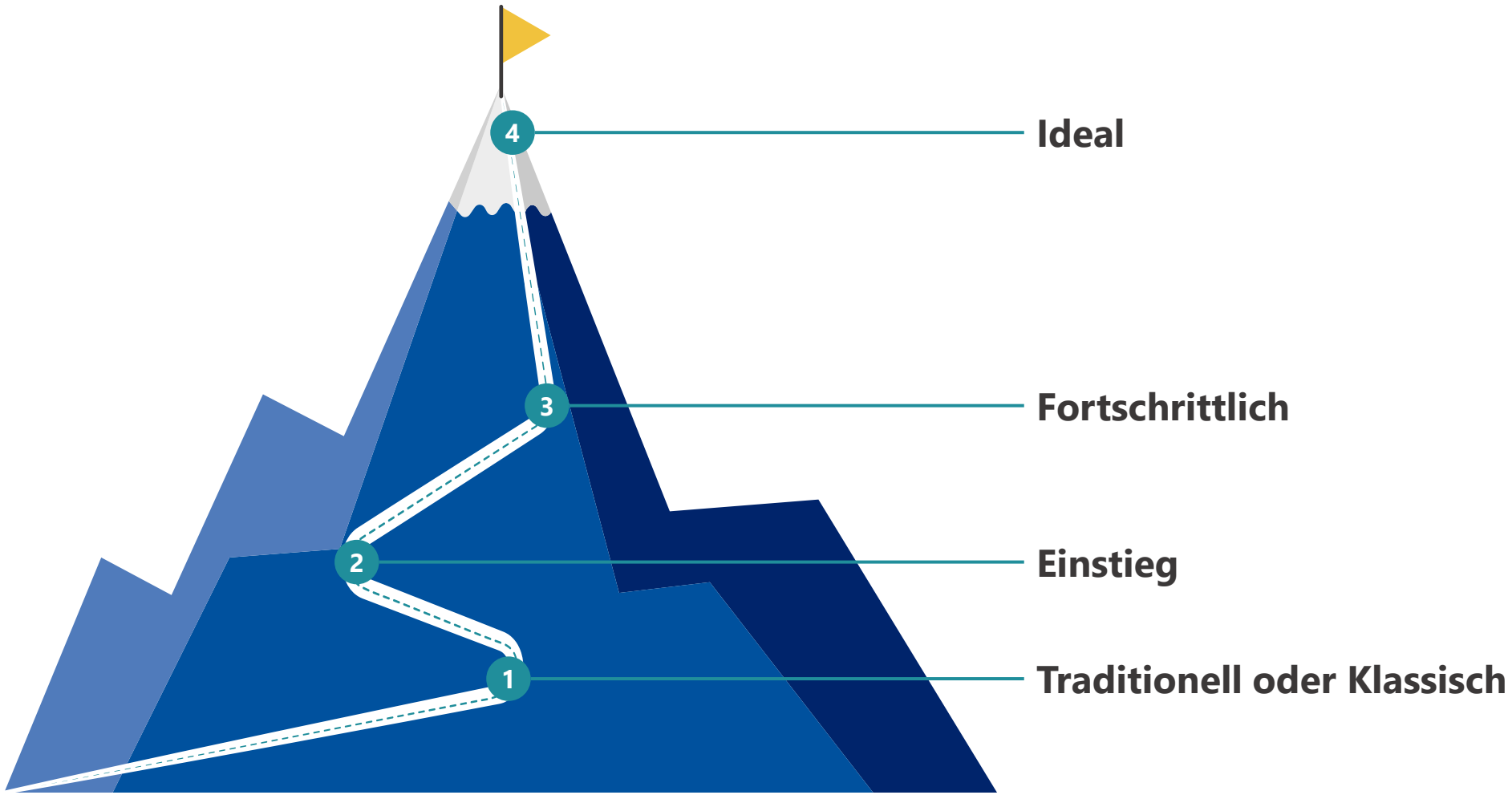


Fokuslösungen oder „Low Hanging Fruits“

- **Fokus auf IDM**
  - dynamische, risikobasierte Authentisierung
  - RBAC, ABAC
- **Fokus auf Segmentierung**
  - Mikrosegmentierung
  - Verhinderung von lateral Movement
- **Fokus auf Zugriff über Gateways**
  - Zero Trust Network Access (ZTNA)
  - Übergangslösung bis Infrastruktur vollständig ZT-fähig
- **Fokus auf Erkennung von Kompromittierungen**
  - Vor allem auf dem Endgerät: EDR und XDR

Reifegradmodell (nach CISA)

Reifegrade



Zero Trust Landkarte

- Erstellung einer Zero Trust Landkarte
- Inventarisierung vorhandener Sicherheitsmechanismen
- Aufnahme je Zero Trust Teilbereich
- Berücksichtigung der Bereiche
  - Basis-Sicherheit
  - Prävention
  - Erkennung und Reaktion

Formulierung eines Zielbildes

- Wie kann auf der Ausgangslage aufgebaut werden?
- Welche Bestandteile sollen kurz, mittel und langfristig eingeführt werden?
- Berücksichtigung Reifegrad und Kosten-Nutzen

Take Away

Zero Trust: Der Schlüssel für Ihre sichere Zukunft

- **Klarheit statt Illusionen:** Lassen Sie sich nicht blenden
- **Status quo verstehen:** Ihren Reifegrad realistisch einschätzen
- **Mit Weitblick handeln:** Ein Zielbild und eine Roadmap entwickeln
- **Nachhaltig wachsen:** Den Reifegrad kontinuierlich steigern

Zero Trust ist kein Trend – es ist eine Notwendigkeit

Beginnen Sie jetzt mit den richtigen Schritten, um Ihre Sicherheitsstrategie auf ein neues Niveau zu heben.

Neuer Weg 9
35516 Münzenberg
Deutschland

E-Mail: mail@tmk.de
Telefon: +49 6004 9148 0
Fax: +49 6004 9148 38
www.tmk.de