**Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung CIR**

# OmniSecure 2026

# „Methoden zu einer Zero Trust Interoperabilitätsarchitektur“

Oberstlt Ihloff

Berlin, 21.01.2026

BUNDESWEHR

# „One-Pager Zero Trust“

## Paradigmenwechsel:

| Zutritt zu IT regulieren | IT-/ Netzwerksicherheit | Data Centric Security | Zero Trust |
|---|---|---|---|
| *„VS auf PCs und Datenträgern schützen“* | *„Secure your network like a fortress“* | *„Das eigentliche Schutzgut sind die Informationen“* | *„Früher oder später werde ich kompromittiert.“* |

## InfoSichh aktuell in der Bw:

(statische) InfoSichh-Konfiguration
- Personell
- Materiell
- Organi-satorisch

+

Überwachung
- Server
- Client
- Netzwerk

+

Reaktion
- CSOC
- CERT

## Bei Zero Trust zusätzlich:

**Mikrosegmentierung**
→ Schadensbegrenzung

**(Teil-)Automatisierung Reaktionsfähigkeit**
→ Echtzeitreaktion

**DevSecOps-Cycle**
→ Zügige Behandlung von Schwachstellen

**Zugriffsentscheidung auf Basis Regelwerk statt Einzelmerkmal**
→ Intelligentere Sicherheitskonfiguration

### Mehrwert in der InfoSichh mit Fokus auf Hochwertgegner:

- *Effizienterer Einsatz von Fachpersonal*
- *Erhöhte Aufmerksamkeit*
- *Präzisere Maßnahmensteuerung*
- *Minimierung operativer Einschränkungen*

# Zero Trust und Interoperabilität – Der Zielkonflikt

Wie können nun zwei Organisationen, die

- **zentrale ZT Fähigkeiten** besitzen, wie
  - Eine Regelwerkbewirtschaftung über eine Zero Trust Engine
  - Teilautomatisierte Incident Response
  - Softwarepflege über einen DevSecOps-Cycle, und

- ein **ZT-fähiges IT-Service Portfolio** haben, welches
  - auf unterschiedlichen Ebenen mikrosegmentiert ist
  - sich über kryptographisch abgesicherte API Schnittstellen steuern lässt und
  - über eine trusted CI/CD Pipeline bewirtschaftet wird,

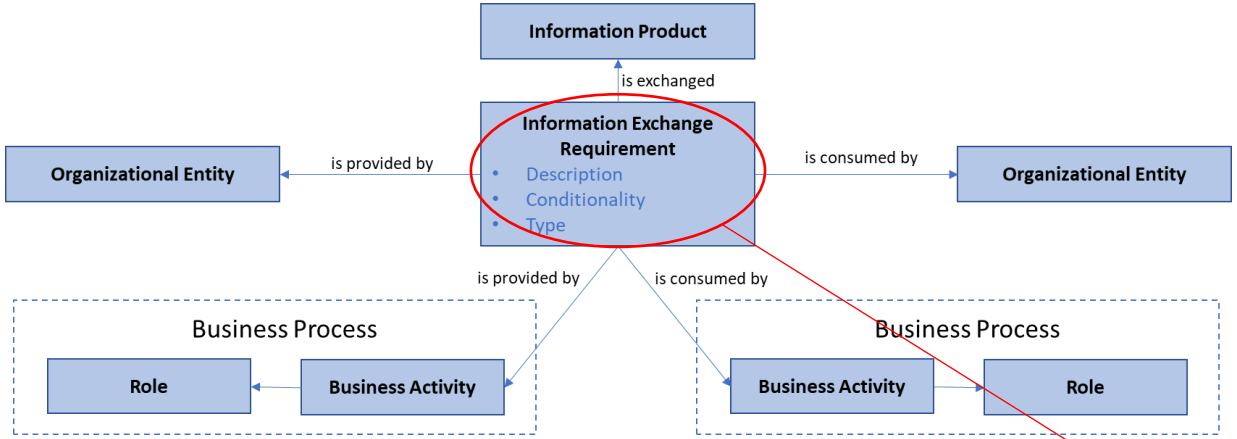
Technische und ablauforganisatorische Interoperabilitäts-anforderungen
*(Federation Requirements)*

zusammenarbeiten, ohne im jeweils anderen wieder eine intransparente Vertrauensumgebung zu schaffen?

Prozessschnittstellen
*(„Operationally driven …*

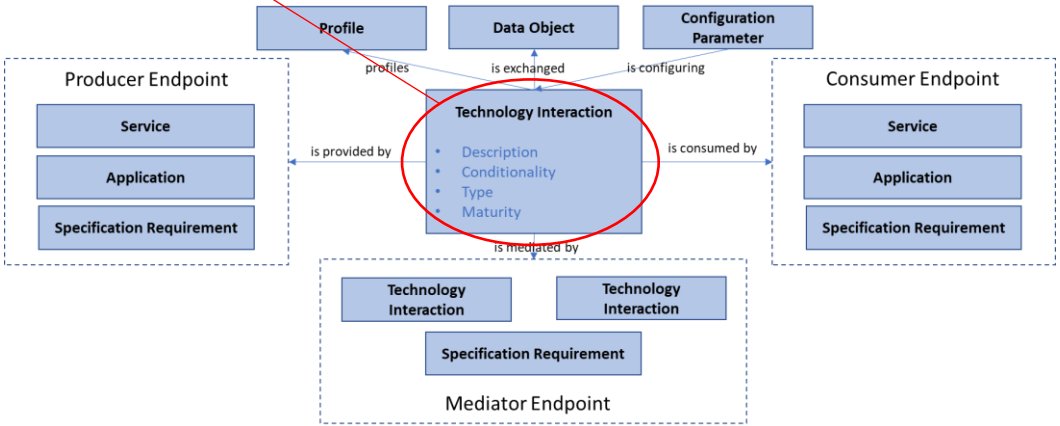
Technische Schnittstellen
*…and technically supported“)*

# Exkurs: FMN Spiral 6 Meta Modell



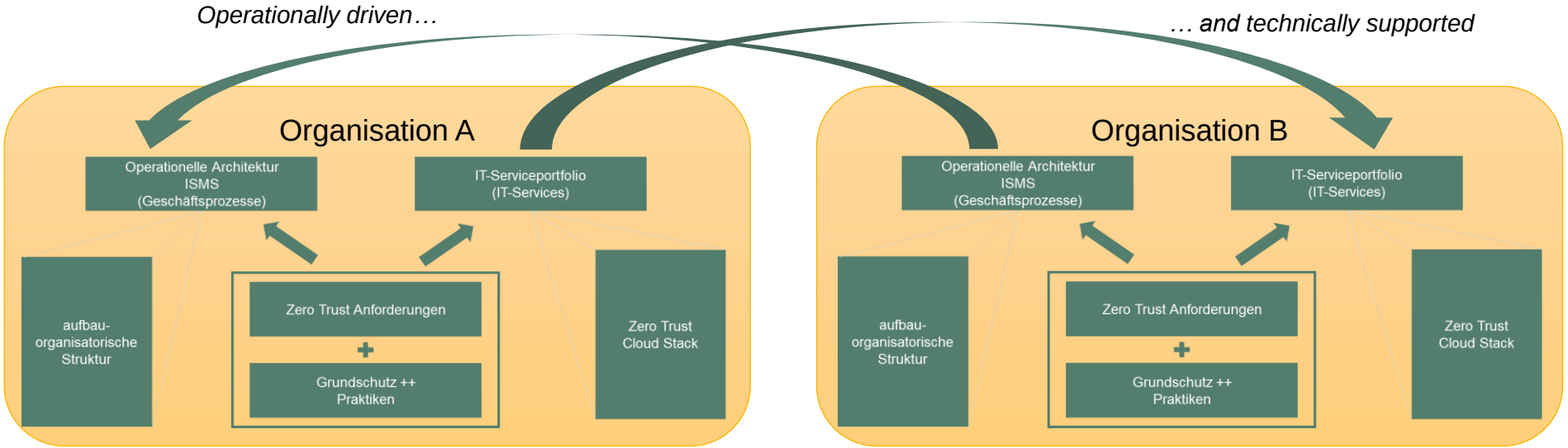

***Operationally driven…***

***… and technically supported***



# Zero Trust Interoperabilitätsarchitektur

*Durch die Einhaltung **prozeduraler und technischer Schnittstellenstandards** entwickeln zwei heterogene Organisationen **interoperable Zero Trust Fähigkeiten** und lösen über diesen Ansatz den **Zielkonflikt** zwischen Zero Trust und dem Erfordernis des digitalen Datenaustauschs*



# Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung CIR

Oberstlt Ihloff

Fontainengraben 150 | D 53123 Bonn

+49 (0) 228 5504 -7224 (Bw: 3402)

ZDigBwChdSt@bundeswehr.org

BUNDESWEHR