


Föderale Digitalstrategie



**Digitale
Transformation**




**Digitale
Infrastruktur**



**Digitale
Anwendungen**



Datennutzung



**Informations-
sicherheit**

Agenda

Standortbestimmung I – „Zero Trust“, was heißt hier „Zero Trust“ !?!

Vortragsblock: Zero Trust - Einleitung

Standortbestimmung II - ...und was machen Sie so?

Vortragsblock: Zero Trust – im Maschinenraum

Standortbestimmung III – Schön wäre wenn ...



Standortbestimmung I

„Zero Trust“, was heißt hier „Zero Trust“ !?!

Gehen Sie davon aus, dass Ihr Netz implizit vertrauenswürdig ist?

Ja

Nein

Was ist Zero Trust?

Eine technische Herausforderung

Eine organisatorische Herausforderung

Eine prozessuale Herausforderung



Zero Trust

Einleitung

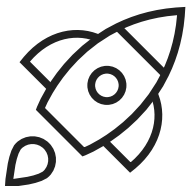
Zero Trust - Ausgangslage



Die Verwaltung wird digitaler, die Angriffsfläche wächst



Perimeter-Sicherheit reicht nicht mehr



Angriffe kommen von außen und innen



Die Frage ist nicht mehr: „Wer ist drin?“, sondern: „Wem vertraue ich und warum?“

Was ist Zero Trust?



never trust – always verify!

Zero Trust - Übersicht

1. Zero Trust ist ein **Paradigmenwechsel**
2. Konsequentes Zero Trust beschränkt den Aktionsradius des Angreifers
3. Zero Trust ist keine neue Technologie, sondern eine Kombination bestehender Technologien und Prozesse
4. Zero Trust ist die Basis für sichere Cloudanwendung



Standortbestimmung II ...

... und was machen Sie so?

Machen Sie schon Zero Trust?

Erste Erfahrungen

Teil der Zielarchitektur

Operativ umgesetzt

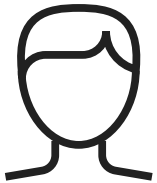


Zero Trust

Im Maschinenraum

Zero Trust – Die Aufbauten

Identität



- Starke Authentisierung MFA
- Identitätszentrierte Steuerung

Gerätevertrauen



- Gerätezustand (Patchlevel etc.)
- Manged vs. Unmanged

Netzwerk/ Microsegmentierung



- Weg vom „flachen Netz“
- Zugriff nur auf das, was nötig ist

Monitoring & Analyse



- Kontinuierliche Bewertung
- Anomalieerkennung

Richtlinien und Kontext



- Zugriff abhängig vom Risiko

Zero Trust – der Rumpf

1. Zero Trust Implementierung & -Administration setzt geschultes Personal voraus
2. Die Implementierung von Zero Trust ist ein Migrationspfad
3. Es gibt keine originären „Zero Trust-Produkte“
4. Zero Trust muss in der ganzen(!) Organisation gelebt werden
5. Zero Trust Architekturparadigma fordert und fördert eine stärkere Zusammenarbeit über Organisationsgrenzen hinweg

Warum ist Zero Trust für die Verwaltung besonders relevant?

1. Kontext IT-Planungsrat
2. Argumentationsline für Entscheider
3. Für Experten

Die Route zur Umsetzung

1. Phase 1 – Transparenz schaffen
2. Phase 2 – Identitäten stärken
3. Phase 3 – Zugriff neu denken
4. Phase 4 – Monitoring gezielt nutzen



Standortbestimmung III

Schön wäre, wenn ...

Wenn Sie heute starten würden, womit würden Sie beginnen?

Beratung suchen

Personal einstellen

Assets inventarisieren

Was wünschen Sie sich vom BSI?

(Branchen-/sektorspezifische) Umsetzungspläne

Deutschlandweite Orchestrierung in staatlichen Einrichtungen

Erfolgskontrolle/Monitoring, Coaching

Zero Trust ist kein Zielzustand, sondern ein Weg!

zero-trust@bsi.bund.de



Yona Raekow

Fachbereichsleiterin

yona.raekow@bsi.bund.de

+49 228 9582 6051

<https://www.bsi.bund.de>



René Salamon

Sachbearbeiter (Zero Trust)

Zero-trust@bsi.bund.de

+49 228 9582 5142

<https://www.bsi.bund.de>



Danke!



Noch Fragen ?