Bundesministerium
für Digitales und
Staatsmodernisierung

Omnisecure – 19.–21.01.2026

# Eckpunkte einer Zero Trust IT-Sicherheitsinfrastruktur des Bundes

# Zero-Trust

## Übersicht

- Anforderungen an die verwaltungsübergreifende Kommunikation
- Anforderungen an die IT-Sicherheitsarchitektur des Bundes
- Zero-Trust Architekturdimensionen
- Zero-Trust Lösungsansätze für die IT-Sicherheitsarchitektur des Bundes
- Zero-Trust Eckpunkte für die IT-Sicherheitsarchitektur des Bundes

# Zero-Trust

## Anforderungen an die verwaltungsübergreifende Kommunikation -Übersicht

- Beachtung u.a. „neuer“ Gesetzesvorgaben Network and Information Security 2 – **NIS2** und Cyber Ressilience Act - **CRA** der EU
- Bestehende gesetzliche (BSIG, UP Bund (BSI)) und Leitlinien (NATO ZT Policy, Netzstrategie 2030,… )
- Veränderte IT-Sicherheitslage – Bsp. Erfolgreiche Ransomware Angriffe
  => Ausfall von IT-Dienstleistern – Angriffe erfolgen von Innen (Lt. Bitkom Schadensbericht 2025 ~ 280 Mrd. € Schaden)
- Zunehmende durchgängige Verschlüsselung der Nutzerverkehre
  => Erschwerung bzw. Verhinderung zentraler Abwehr von Schadsoftware an Netz-Außengrenzen / Perimeter
- Föderierte IT-Strukturen (NOOTS, RegMo, Multicloud,…)
  => Unterschiedliche Zuständigkeiten bzw. Verantwortlichkeiten – Bsp. Lieferketten in der Industrie, Gematik, föderaler Datenaustausch,…

=> Ergänzung klass. Netz-Perimeterstruktur durch Steuerung der (Nutzer)verkehre unter Beachtung der jeweiligen Identität inkl. Rechte + Datensensitivität <-> **Zero-Trust**

# Zero-Trust – Gestiegene Bedrohungslage [1)]

## Anforderungen an die IT-Sicherheitsarchitektur des Bundes

a) **Nutzerautorisierung:**

• Vermeidung unautorisierter Zugriff auf schutzbedürftige Daten durch Beachtung des Schutzbedarf der Daten. Mögliche weitere Attribute sind Standort und/oder Zeit

b) **Begrenzung der Netzausbreitung:**

• Begrenzung Netz-Kompromittierung durch architektonische Maßnahmen (bspw. dyn. Netz- bzw. Mikrosegmentierung mittels „Maschinenidentitäten“)

c) **Minimierung des Zugriffs:**

• Feingranulare Zuteilung von Zugriffsberechtigungen

d) **Reaktionsmechanismen:**

• Minimierung von Schadensauswirkungen, durch automatisierte Reaktionen (bspw. Entzug oder Reduzierung von Zugriffsrechten) => Minimierung „Blast Radius“



[1)] Siehe aktuelle BSI, BKA und BfV Berichte

# Zero-Trust - Arbeiten in **föderierten** Systemen

## Anforderungen an die IT-Sicherheitsarchitektur des Bundes

e. **Mandantentrennung**:
   - Bei zentraler Bereitstellung von IT-Lösungen und Daten.
   - Unterschiedliche Nutzergruppen, erhalten physisch oder logisch **getrennte IT-Lösungen** und Datenressourcen, um unautorisierten Datenzugriff zu verhindern
   - Erforderliche **Kommunikationsbeziehungen** und Zusammenarbeitsformen werden unter Beachtung der IT-Sicherheitsanforderungen bzw. Vorgaben ermöglicht

f. **Zugriffsauthentifizierung über Prozessketten**:
   - Gegenseitige (übergreifende) Authentifizierung von Anwendungen unter Beachtung der aufrufenden Nutzeridentität (On Behalf)

# Zero-Trust - **Mobiles Arbeiten**

Anforderungen an die IT-Sicherheitsarchitektur des Bundes

**e. Sicherer Netz-Fernzugriff:**

- Netz-Fernzugriffe erfolgen sicher
- Steuerbarkeit gemäß Berechtigungen und Schutzbedarf der IT-Ressourcen

**f. Verwaltung der Gerätevielfalt:**

- Endgeräte müssen erfasst und kategorisiert werden können

**g. Echtzeitüberwachung von Endgeräten:**

- Durchgängige Überwachung des Compliance- und Gerätezustands von Endgeräten (bspw. Einhaltung der Sicherheitsstandards - Status Betriebssystems, Anti-Viren oder Anti-Malware)
- Echtzeitrisikoanalyse als Entscheidungsgrundlage für Zugriffsentscheidung

# Zero-Trust - **Cloudbasierte** Anwendungsbereitstellung

Anforderungen an die IT-Sicherheitsarchitektur des Bundes

**e. Sicherheit in Multi-Cloud-Umgebungen:**

- Verwaltungsweite standardisierte Zugriffsvergabe
- Authentifizierung zwischen Anwendungen als auch eine Echtzeitrisiko-analyse bei Zugriffsanfragen
- Beachtung der jeweiligen Identitäten und Rechte

**f. Dev (Sec) Ops:**

- Integration von Sicherheitsmaßnahmen in allen Phasen der Softwareentwicklung („Development“, „Security“, „Operations“)

=> Frühzeitige Zusammenarbeit Anwendungsentwicklung und Betrieb

# Zero-Trust - **NIS-2** [1)]

## Anforderungen an die IT-Sicherheitsarchitektur des Bundes

**e. Risikomanagementmaßnahmen:**

• **Bundeskanzleramt** und **Bundesministerien** müssen geeignete Maßnahmen zur Gewährung der **Integrität** und **Vertraulichkeit** von IT-Systemen ergreifen (Bspw. Konzepte für Risikoanalysen, Einsatz von Verschlüsselung und Multi-Faktor- oder kontinuierliche Authentifizierung)

**f. Meldepflichten:**

• Meldung erheblicher Sicherheitsvorfälle (inkl. Verdachtsfälle ) innerhalb von 24 Stunden an zuständige Stelle (IT -> BSI),

• Gefolgt von einer Fortschrittsmeldung und Abschlussmeldung

• Fortlaufende Dokumentation der Sicherheitsvorfälle



[1)] Bundestagsdrucksache 20/13184 - Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) – 13.11.2025

# Zero-Trust - **NATO** Sicherheitsstandards

## Anforderungen an die IT-Sicherheitsarchitektur des Bundes

**e. Anschlussfähige, Zero Trust befähigte Schnittstellen nationaler IT-Verfahren:**

• Umsetzung der NATO Föderations- und Zero-Trust Vorgaben für Alle, die (digitale) Schnittstellen zu NATO Stellen oder NATO Partnern unterhalten.

**f. Implementierung von NATO Dateneinstufungsstandards:**

• Alle Stellen, die eingestufte Informationen mit der NATO freigegeben, speichern, verarbeiten oder übertragen müssen perspektivisch NATO Daten[1)] und Zero-Trust Vorgaben umsetzen



[1)] U.a. zur Syntax von vertrauenswürdigen Labels gemäß *Standardization Agreement* (STANAG 4774) und deren kryptographische Bindung an Datenobjekte (STANAG 4778)

# Zero-Trust - Zusammenfassung

## Anforderungen an die IT-Sicherheitsarchitektur des Bundes

| Kateg. | Rahmenbedingungen an die IT-Sicherheitsarchitektur des Bundes | Anforderungen | | |
|---|---|---|---|---|
| Gestiegene Bedrohungslage | Gestiegene Qualität und Quantität der Angriffe | a. Nutzerautorisierung | b. Begrenzung der Netzwerkausbreitung | c. Minimierung des Zugriffs |
| | | d. Reaktionsmechanismen | | |
| Veränderte Nutzerbedarfe | Arbeiten in föderierten Systemen | e. Mandantentrennung | f. Zugriffsauthentifizierung über Prozessketten | |
| | Mobileres arbeiten | g. Sicherer Netzwerk-Fernzugriff | h. Verwaltung der Gerätevielfalt | i. Echtzeitüberwachung von Endgeräten |
| | Agile und Cloudbasierte Anwendungsbereitstell. | j. Sicherheit in Multi-Cloud-Umgebungen | k. Dev (Sec) Ops | |
| Externe Vorgaben | Übergreifende Sicherheitsstandards | l. NIS-2 Authentifizierungs-anforderungen | m. NIS-2 Meldepflichten | |
| | Behördenspezifische Sicherheitsstandards | n. Implementierung von Zero Trust an den NATO-Schnittstellen | | |

# Zero-Trust - Lösungsansätze

## Zero-Trust Architekturdimensionen

Einteilung der Zero-Trust Lösungsansätze in folgenden Architekturdimensionen:

- **Identitäten,**
- **(End)geräte,**
- **Netze,**
- **Anwendungen und**
- **Daten**

# Zero-Trust - Lösungsansätze

## Architekturdimension - **Identitäten**

**Identitätsverwaltung** - Zuweisung Rollen und Berechtigungen durch IAMs

⇒ Granulare Zugriffskontrolle

Föderation - Einheitliche organisatorische und technische Standards => Gegenseitige Verifizierung von Identitäten (IDP)

**Authentifizierung** - Kontinuierliche Verifizierung der Identität - ggf. adaptive Multi-Faktor-Authentifizierung

**Autorisierung** - Rechtzuweisung nach Authentifizierung; ggf. Nutzung dynamischer Attributen (Zeitpunkt, geografischer Standort, Nutzerverhalten, Gerätezustand etc.)

**Zugriffsverwaltung** - Zeitlich begrenzte beschränkte Zugriffe „Just-In-Time“ und „Just-Enough“

**Überwachung** - Echtzeitanalyse des Nutzerverhalten (z. B. Login-Zeiten, verwendetes Gerät, Standort, Schutzbedarf der Daten,...)

# Zero-Trust - Lösungsansätze

## Architekturdimension - **Endgeräte**

**Gerätemanagement -** Automatisiertes Assetmanagement (GMS) -> zentrale Verwaltung und „Kontrolle “dienstlicher Endgeräte

Föderation – „Einheitliches“ Gerätemanagement

=> Gegenseitiges Vertrauen – Systemübergreifende Verifizierung und Nutzung von Geräten

**Compliance-Zustand** - Automatisierte kontinuierliche Überwachung der Sicherheitsvorgaben dienstlicher und privater Endgeräte, (Bspw. Aktualität des Betriebssystems oder den AV-Status)

**Geräteautorisierung -** Beachtung des Compliance-Zustandes und ggf. weiterer Attribute bei Zugriff

**Endpunktsicherheit -** Schutz für alle Geräte durch Integration von Endpoint Protection[1)], sowie Detection und Response[2)] - Berücksichtigung bei Zugangsentscheidungen

**Integrität (End-)Geräte** - Sicherstellung der Integrität der (End-)Geräte entlang der Lieferkette - Verhinderung maliziöser (End-)Geräte



[1)] Endpoint Protection bietet grundlegenden Schutz vor bekannten Bedrohungen wie Malware und Viren durch Integration von Antiviren-Software, Anti-Malware oder SW-Firewalls

[2)] Detection and Response sammelt kontinuierlich Daten von Endgeräten und verwendet Analysen, um verdächtiges Verhalten zu erkennen und automatisch Gegenmaßnahmen durchzuführen

# Zero-Trust - Lösungsansätze

## Architekturdimension – **Netze**

**Netzinventarisierung** - Netzsegmente werden kontinuierlich inventarisiert einschließlich einer Kategorisierung nach erforderlichem Schutzbedarf - Einteilung in Kategorien (bspw. Resort, Behörde, Dienst) und klassifiziert (bspw. öffentlich, föderiert, intern)

**Mikrosegmentierung** - Feingranulare Aufteilung von Netzsegmenten, mittels „Maschinenidentitäten“, ermöglicht szenariospezifischen Datenaustausch - Umfasst physische und logische Segmentierungen, die isolierte Netzbereiche oder benutzergruppenspezifische Zugriffsrechte, je nach Sicherheitsanforderung (bspw. Schutzbedarf der Daten) ermöglichen

**Netzwerkmanagement** - Netzverbindungen erfolgen auf Basis von Relevanz, Risikobewertung und Kritikalität der Anfragen und der zu übertragenen Daten. (Bsp. Software-Defined Networking (SDN))

**Netzverkehrsverschlüsselung** - Datenaustausch über verschlüsselte Netzverbindungen (Beachtung Stand der Technik <-> Kryptoagilität)

**Anomalieerkennung** - Kontinuierliche automatisierte, auf Kontext und Metadaten basierende Erkennung von Abweichungen unterstützt den Schutz des Netzes (Bsp. Erkennung von Lateral Movement)

# Zero-Trust – Lösungsansätze 1/2

## Architekturdimension – **Anwendungen**

**Anwendungszugriffsberechtigung** - Zugriffsautorisierungen basieren auf Echtzeitrisikoanalysen (Beachtung anfragender Berechtigungen + Nutzungsverhaltensanalysen - Analysen überwachen kontinuierlich den Zugriff
=> Erkennung von Abweichungen => Mögliche Einschränkung des Zugriffs

**Anwendungszugänglichkeit** - Anwendungszugriffe über Kommunikations-Netze

Sicherheitszustand des **internen** und des **externen** Netzes **gleichwertig** betrachtet

Zugriffsberechtigungen minimal und attributbasiert (Nutzungsbedarf, Schutzbedarf der Anwendung / Daten, Anfrage-Standort,...)

**Anwendungsschutz** - Integration von Sicherheitsrichtlinien in Anwendungsabläufe - Anwendungsspezifische Schutzmaßnahmen (bspw. Web Application FW und Mikrosegmentierung) schützen ausgewählte Anwendungskomponenten

# Zero-Trust – Lösungsansätze 2/2

Architekturdimension – **Anwendungen**

**Authentisierung zwischen Anwendungen**- Gegenseitige basierte Authentisierung (MFA ) - Berücksichtigung bspw. Zeitpunkt + geografischen Standort

Gegenseitige Authentisierung folgen einheitlichen Standards <-> Systemübergreifende Verifizierung => Föderation

**Anwendungsentwicklung & -bereitstellung** - Gewährleistung der Sicherheit während gesamtem Entwicklungszyklus

**Integrität Anwendungen** - Sicherstellung der Integrität der Anwendungen entlang der Lieferkette -> Verhinderung maliziöser Anwendungen

# Zero-Trust – Lösungsansätze 1/2

## Architekturdimension – **Daten**

**Datenzugriffsberechtigung** - Gewährung des Zugriff nur für den benötigten Zeitraum („Just-in-Time“) und benötigtem Umfang („Just-Enough“) - Basierend auf Echtzeitrisikoanalysen erfolgt Zugriffsüberwachung um ggf. den Zugriff einzuschränken oder nicht zu gewähren

**Zentrale Inventarisierung**- Daten werden kontinuierlich inventarisiert, einschließlich Kategorisierung nach erforderlichem Schutz (bspw. Geschäfts-, Kunden- und Finanzdaten, VS-Einstufung) und Klassifizierung (bspw. öffentlich, intern, vertraulich, geheim)

# Zero-Trust – Lösungsansätze 2/2

## Architekturdimension – **Daten**

**Blockierung verdächtiger Datenexfiltration** - „Inventarisierung und Klassifizierung“

Erfasst alle Daten und „stuft“ sie entsprechend dem Schutzbedarf ein

DLP-Mechanismen (Data Loss Prevention) überwachen den Datenverkehr, erkennen verdächtige Aktivitäten, um Abweichungen bzw. Anomalien zu identifizieren um ggf. den Zugriff einzuschränken oder nicht zu gewähren

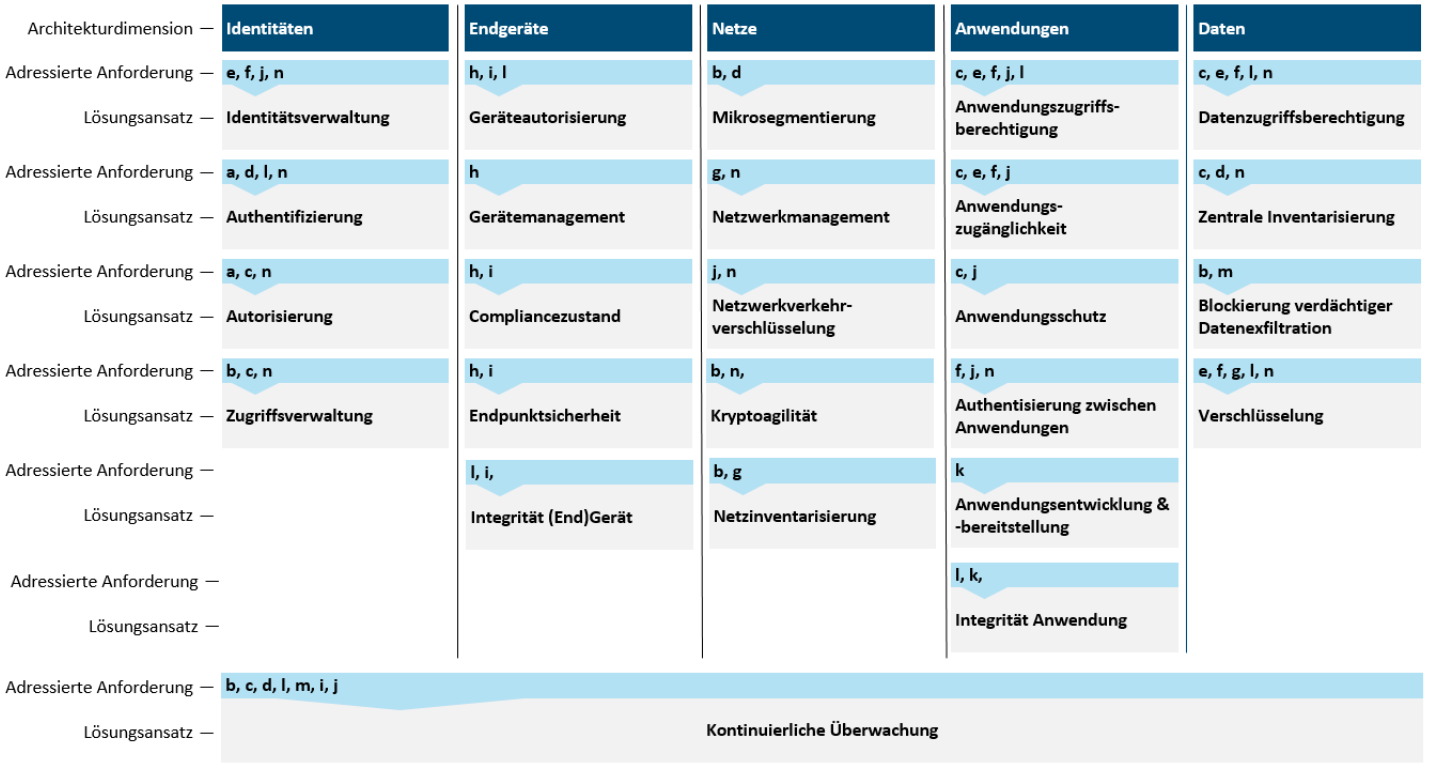
**Verschlüsselung** - Datenverschlüsselung und -authentisierung in Ruhe (At Rest) und in Übertragung (In Transit)

⇒ Schutz der Daten auf Speichermedien und bei Übertragung

Zugriff nur für autorisierte Benutzer auf entschlüsselte Daten

**Kryptoagilität** – Reaktionsmöglichkeit auf kurzfristige kryptografische Entwicklungen

# Zero-Trust - Lösungsansätze und adressierte Anforderungen der IT-Sicherheitsarchitektur des Bundes



# Zero-Trust

## Zero-Trust Eckpunktepapier für die IT-Sicherheitsarchitektur des Bundes (V.1.0)

**Eckpunkt 1: Es wird von einem erfolgreichen "Einbruch" („Assume Breach“) ausgegangen,** dessen Schadenauswirkungen durch mehrstufige IT-Sicherheitsmaßnahmen begrenzt werden können. Die klassische Perimeter Absicherung ist daher durch einen mehrstufigen, alle IT-Ressourcen der IT des Bundes umfassenden Ansatz zu ergänzen.

**Eckpunkt 2: Es existiert kein implizites Vertrauen.** Jeder Zugriff auf IT-Ressourcen der IT des Bundes ist fortlaufend zu validieren. Im Sinne von Zero-Trust werden interne und externe Zugriffsanfragen prinzipiell gleichbehandelt. Transparenz zwischen kommunizierenden IT-Komponenten bzw. IT-Systemen ist, insbesondere in föderierten Strukturen, elementare Voraussetzung für eine gemeinsame Vertrauensbasis.

**Eckpunkt 3: Gewährung minimaler Rechte.** Jeglicher Zugriff auf IT-Ressourcen der IT des Bundes, sind nach dem Prinzip „Kenntnis nur wenn nötig“ grundsätzlich mit den minimalen Rechten für die Ausübung konkreter Aufgaben und Tätigkeiten zu gewähren. Dieses Prinzip ist auf alle Identitäten anzuwenden (z.B. Nutzer, Provider, Anwendungen/Systeme).

# Zero-Trust

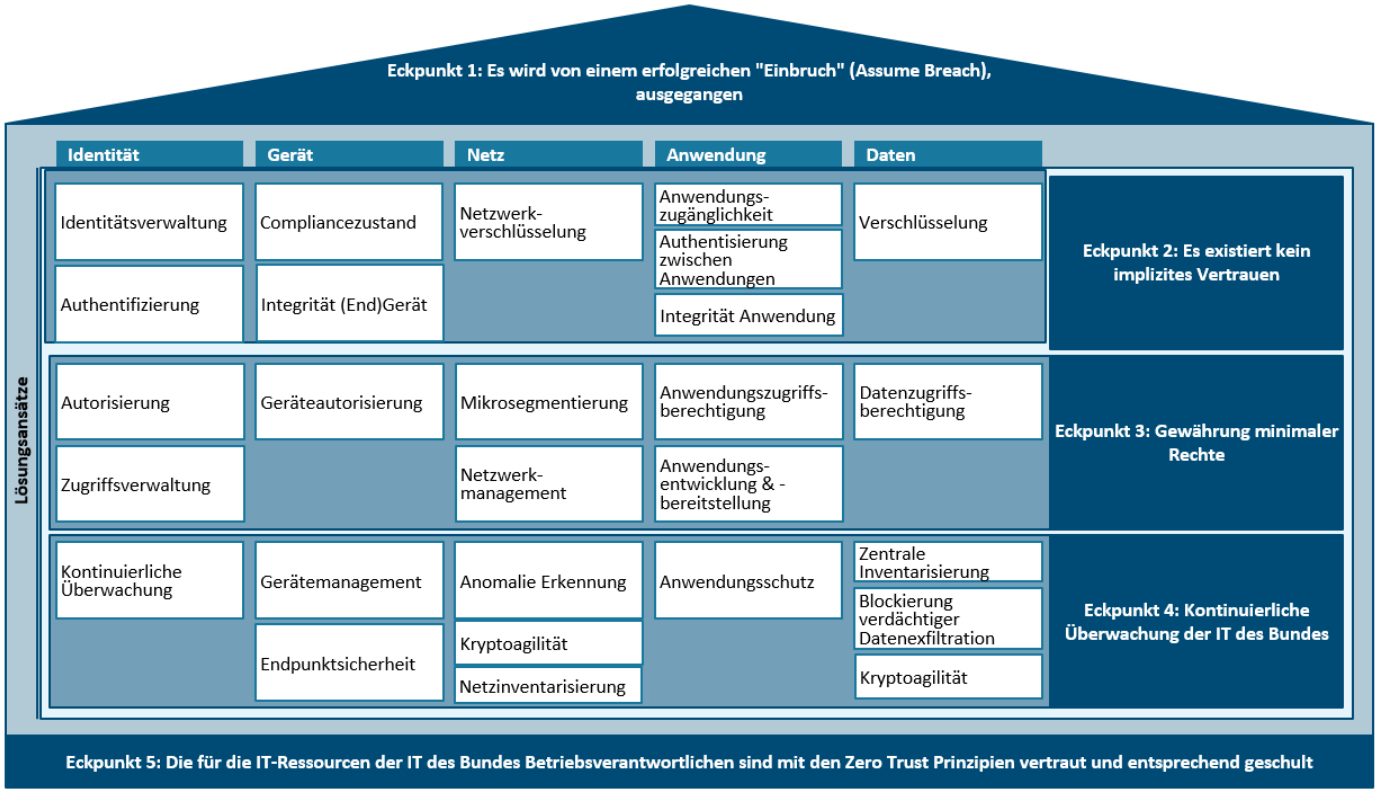
## Zero-Trust Eckpunktepapier für die IT-Sicherheitsarchitektur des Bundes (V. 1.0)

**Eckpunkt 4: Kontinuierliche Überwachung der IT des Bundes.** Jeglicher Zugriff auf IT-Ressourcen der IT des Bundes ist anhand festgelegter Attribute sowie dynamischer Regelwerke kontinuierlich zu überwachen. Solche Überwachung schafft die Basis, um Anomalien frühzeitig zu erkennen und zu behandeln.

**Eckpunkt 5: Die für die IT-Ressourcen der IT des Bundes Verantwortlichen sind mit den Zero-Trust Prinzipien vertraut und entsprechend geschult.** In ihrer Verantwortung liegt es den Paradigmenwechsel von perimeterbasierten Sicherheitsansätzen hin zu Zero-Trust Ansätzen und den damit kulturellen und organisatorisch notwendigen Wandel zu unterstützen. Prozesse und Richtlinien unterstützen die Zero-Trust Etablierung in allen Bereichen der Bundesverwaltung. Transparenz ist hier im Sinne der gegenseitigen Bereitstellung von für eine Zugriffsentscheidung relevanter Informationen zwischen Parteien zu verstehen.

# Zero-Trust Lösungsansätze für die IT-Sicherheitsarchitektur des Bundes

ZT-Lösungsansätze gemäß dem CISA Zero-Trust Reifegrad Modell in fünf Architektur-dimensionen **Identitäten, Endgeräte, Netze, Anwendungen und Daten** geordnet



# Kontakt

Bundesministerium
für Digitales und
Staatsmodernisierung

**Dienstsitz**
Bundesministerium für Digitales und
Staatsmodernisierung
Englische Straße 30
10587 Berlin

**Postanschrift**
Bundesministerium für Digitales und
Staatsmodernisierung
Alt-Moabit 140
10557 Berlin

Axel Munde
Referat DS I1
Axel.Munde@bmi.bund.de
Axel.Munde@bmds.bund.de
030 18 681 17989

Bundesministerium
für Digitales und
Staatsmodernisierung