Eckpunkte einer **Zero-Trust-IT-Sicherheitsarchitektur** des Bundes

Bundesministerium
für Digitales und
Staatsmodernisierung

Kurzfassung

Die IT des Bundes ist fortlaufend mit veränderten Rahmenbedingungen konfrontiert. Diese Rahmenbedingungen entstehen derzeit insbesondere aus einer gesteigerten Bedrohungslage (bspw. durch Cyberangriffe staatlicher Akteure), veränderten Nutzerbedarfen der Mitarbeitenden der Bundesverwaltung (bspw. durch die Zunahme von mobilem Arbeiten), kollaborativen ressortübergreifendem Arbeiten und externen Vorgaben (bspw. EU oder NATO). Die IT-Sicherheitsarchitektur des Bundes muss fortlaufend an diesen veränderten Rahmenbedingungen ausgerichtet werden. Die in diesem Dokument dargelegte Betrachtung zeigt auf, dass eine Anwendung der Zero-Trust-Prinzipien gemäß Zero-Trust-Architekturparadigma1 den Schutz sämtlicher IT-Ressourcen (u.a. Netze, Anwendungen und Daten) der IT des Bundes deutlich erhöhen kann.

Als Zielkorridor für die Ausgestaltung einer Zero-Trust-IT-Sicherheitsarchitektur lassen sich für die IT des Bundes fünf Eckpunkte ableiten:

Eckpunkt 1: Es wird von einem erfolgreichen "Einbruch" 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. Insbesondere in föderierten IT-Strukturen, sollten interne und externe Zugriffsanfragen gleichbehandelt werden. Eine einmalige Authentifizierung (z. B. an der Perimetergrenze) ist nicht mehr ausreichend. Zugriffe müssen stattdessen laufend, unter Beachtung der aktuellen Sicherheitslage neu geprüft, erteilt und ggf. angepasst werden. Sichere Authentifizierungsmethoden (z. B. Multi-Faktor-Authentifizierung) werden für alle Identitäten angewendet. Transparenz[2] 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

[1] Unter Beachtung der in der NATO durch die Mitgliedsstaaten getroffenen Definitionen.
[2] Transparenz ist hier im Sinne der gegenseitigen Bereitstellung von für eine Zugriffsentscheidung relevanter Informationen zwischen Parteien zu verstehen.

Rechten für die Ausübung konkreter Aufgaben und Tätigkeiten zu gewähren. Dieses Prinzip ist auf alle Identitäten anzuwenden (z.B. Nutzer, Provider, Anwendungen/Systeme). Die Zuordnung von Berechtigungen wird fortlaufend überprüft und ggf. bedarfsgerecht angepasst. Die Autorisierung erfolgt für jeden Zugriff erneut.

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. Zu möglichen Attributen gehören Zeitpunkt oder geografischer Standort des Zugriffs.

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. Die Betriebsverantwortlichen sind mit „Zero-Trust“ vertraut, verstehen die Prinzipien und sind darin geschult, diese konsequent in ihrem Arbeitsalltag umzusetzen. Technologische Zero-Trust-Lösungsansätze werden effektiv durch Prozesse in der Organisation unterstützt.

Die vorgenannten Eckpunkte dienen als Zielkorridor für einen noch durchzuführenden nachgelagerten Prozess, um die bisherige IT des Bundes an eine Zero-Trust-IT-Sicherheitsarchitektur heranzuführen. Im Rahmen des nachgelagerten Prozesses sind gesetzliche und untergesetzliche Vorgaben, bestehende Standards, Architekturvorgaben, die Anforderungen der Dienste- und Betriebskonsolidierung und des Deutschland-Stacks sowie die Anforderungen der Ressorts zu betrachten und in einen angemessenen Ausgleich zu bringen. Basis für eine konkrete und angemessene Umsetzung wird eine modulare Reifegradanalyse und schrittweise Identifikation von Maßnahmen zur Erreichung des Zielbildes sein. Dabei ist das Proportionalitätsprinzip anzuwenden.

Inhalt

1.Einleitung

Im Jahr 2022 hat das Bundesministerium des Innern und für Heimat (BMI) eine Cybersicherheitsagenda vorgestellt, welche die digitalpolitischen Ziele des BMI für den Bereich Cybersicherheit konkretisiert. Eine in der Cybersicherheitsagenda definierte Maßnahme zur Umsetzung eines höchstmöglichen Schutzniveaus in der Cybersicherheit ist die Anpassung der IT-Sicherheitsarchitektur des Bundes an die bestehende Bedrohungslage.[3]

Gegenwärtig orientiert sich die IT des Bundes an traditionellen Architekturparadigmen wie dem Perimeterschutz. Das bedeutet, dass bspw. die Weitverkehrsnetze des Bundes durch Sicherungsmaßnahmen an Netzaußengrenzen („Perimeter“) geschützt werden. In den von der öffentlichen Hand betriebenen Netzen sind darüber hinaus ergänzende Sicherheitsmaßnahmen umgesetzt, eine Vergabe von Berechtigungen, nach dem Prinzip der minimalen Rechte, erfolgt in der Regel nicht konsequent. Angreifer könnten, so durch eine Überwindung des Perimeters, beispielsweise durch laterale Bewegung[4] und zugehöriger Rechteausweitung, potenziell unbeschränkten Zugriff auf IT-Ressourcen (Identitäten, Daten, Anwendungen, Netze und Geräte) der IT des Bundes erlangen.

Dem gegenüber besteht für die IT des Bundes eine veränderte Bedrohungslage, die insbesondere durch in Anzahl und Qualität stark gestiegener Cyberangriffe gekennzeichnet ist. Daneben verändern sich auch die fachlichen Anforderungen an die IT des Bundes selbst z.B. durch die Betriebs- und Dienstekonsolidierung Bund mit cloudbasierter Anwendungsbereitstellung, einer zunehmenden Nutzung mobiler Endgeräte, ressortübergreifender Zusammenarbeit sowie Anforderungen aus Richtlinien, wie zum Beispiel der Network and Information Security Directive (NIS-2) der Europäischen Union.

Zur Umsetzung der Cybersicherheitsagenda des BMI ist daher eine Weiterentwicklung der IT-Sicherheitsarchitektur des Bundes notwendig.[5] Die in diesem Dokument beschriebenen Eckpunkte schaffen hierfür einen Zielkorridor, in dem die durch die NATO-Mitgliedsstaaten vereinbarten sechs Zero-Trust Prinzipien Beachtung finden können.

Die Anwendung insbesondere des „Assume Breach“-Ansatzes, erfordert, im Unterschied zum traditionellen Perimeterschutz IT-Sicherheitsarchitekturen unter Einbeziehung aller Ressourcen ganzheitlich neu zu betrachten. Deshalb wird keinem Nutzer, Endgerät und keiner Anwendung implizit vertraut. Stattdessen wird jeder Zugriff fortlaufend verifiziert. Für eine Integration der Prinzipien des Zero-Trust Architekturparadigmas müssten die haushälterischen Voraussetzungen nachhaltig geschaffen und technologische, organisatorische und kulturelle Veränderungsmaßnahmen getroffen werden. Dieses Dokument fokussiert sich im Wesentlichen auf die technologischen Lösungsansätze.

---

[3] vgl. Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (2022), Seite 10

[4] Als laterale Bewegung ist gemeint, dass ein Angreifer sich nach Überwindung des Perimeterschutzes seitwärts im Netz bewegen und auf weitere Daten, Anwendungen und Endgeräte zugreifen kann.

[5] vgl. Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (2022), Seite 10

Durch die angestrebte Integration der Zero-Trust-Eckpunkte, unter Beachtung der NATO Zero-Trust-Prinzipien und weiterer relevanter Rahmenwerke und Vorgaben in die IT-Sicherheitsarchitektur des Bundes, soll ein bestehender Perimeterschutz so weiterentwickelt werden, dass Identität und Berechtigung von Nutzenden, Geräten, Anwendungen und Netzen fortlaufend geprüft und validiert werden. Auf dieser Grundlage sind nachvollziehbare und vorhersagbare Zugriffsentscheidungen möglich.

Dieses Eckpunktepapier beschreibt Zero-Trust-Lösungsansätze entlang der Ressourcen und IT-Sicherheitsarchitekturdimensionen **Identitäten**, **Daten**, **Anwendungen**, **Netze** und (**End)Geräte** und benennt Eckpunkte für eine nachgelagerte Übersetzung in konkrete Maßnahmen und Umsetzung innerhalb der IT des Bundes.

Im Anschluss an diese Einleitung werden geltende Rahmenwerke und Vorgaben beschrieben (Kapitel 2). Auf Basis identifizierter Rahmenbedingungen leiten sich Anforderungen ab (Kapitel 3), die von einer IT-Sicherheitsarchitektur IT des Bundes berücksichtigt und adressiert werden müssen (Kapitel 4) und durch die Eckpunkte einer Zero-Trust-IT-Sicherheitsarchitektur des Bundes (Kapitel 5) adressiert werden können.

2.Rahmenwerke und Vorgaben, Referenzwerke und Standards

Der Gestaltungsraum einer IT-Sicherheitsarchitektur des Bundes wird durch Rahmenwerke, BSI-Vorgaben und gesetzliche Vorschriften gesetzt. Verfügbare Rahmenwerke, Vorgaben und technische Referenzwerke und Standards werden im Folgenden auf Basis der bestehenden Dokumentenlage beschrieben.

2.1 Rahmenwerke für die IT-Sicherheitsarchitektur des Bundes

In der **Nationalen Sicherheitsstrategie** der Bundesrepublik Deutschland aus dem Jahr 2023 wird Cybersicherheit als elementarer Baustein zur Umsetzung eines integrierten Sicherheitsansatzes charakterisiert. Vor diesem Hintergrund hat sich die Bundesregierung das Ziel gesetzt, ihre „Cybersicherheits-architektur [zu] modernisieren und ihre Fähigkeiten zur Abwehr von Cyberangriffen [zu] stärken“, um auf die veränderte Bedrohungslage im Bereich Cyber angemessen reagieren zu können[6]. Die im vorliegenden Dokument beschriebenen Eckpunkte einer Zero-Trust-IT-Sicherheitsarchitektur sind ein Be-standteil einer modernisierten Cybersicherheitsarchitektur und sollen die nationale Sicherheitsstrategie für die IT des Bundes in diesem Zusammenhang konkretisieren.

Die **Netzstrategie 2030** aus dem Jahr 2018 priorisiert Informationssicherheit als „oberste[s] Ziel für die Gestaltung der Netzinfrastrukturen“ der öffentlichen Verwaltung.[7] Dieses Eckpunktepapier definiert Grundlagen zur Etablierung einer modernen IT-Sicherheitsarchitektur des Bundes, die in der Netzstrategie nicht definiert wurden. Im Sinne des Zero-Trust-Architekturparadigmas sind die Eckpunkte nicht auf Netzinfrastrukturen begrenzt, sondern betrachten als Ressourcen neben Netzen auch Identitäten, Endgeräte, Anwendungen und Daten der IT des Bundes.

Die **Cybersicherheitsagenda** des BMI aus dem Jahr 2022 (WP 20) basiert auf den digitalpolitischen Zielen und Maßnahmen des BMI bis 2025 und umfasst den Geltungsbereich des Ministeriums sowie der nachgeordneten Behörden. Vor dem Hintergrund des Krieges in der Ukraine, der Aktivitäten staatlicher Akteure und der „Zeitenwende“ beschreibt die Cybersicherheitsagenda die Notwendigkeit einer resilienten IT-Sicherheitsarchitektur für die Aufrechterhaltung der staatlichen und wirtschaftlichen Funktionsfähigkeit. Die Cybersicherheitsagenda fordert eine sofortige „Stärkung der Cyber-Resilienz von Bundesbehörden [und] weiteren staatlichen Infrastrukturen“ zum Schutz vor Cyberangriffen und Sabotageakten.[8] Hierzu soll die IT-Sicherheitsarchitektur durch die Implementierung von „Security by Design and by Default“ modernisiert werden.[9] Dieses Eckpunktepapier schafft zu

[6] vgl. Nationale Sicherheitsstrategie (2023), Seite 15
[7] vgl. Eckpunkte einer Netzstrategie 2030 (2018), Seite 5
[8] vgl. Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (2022), Seite 5
[9] vgl. Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (2022), Seite 10

diesem Zweck eine ressortübergreifende, gemeinsame Grundlage für die Weiterentwicklung der IT-Sicherheitsarchitektur des Bundes.

2.2 Vorgaben für die IT-Sicherheitsarchitektur des Bundes

Auf gesetzlicher Ebene definiert insb. das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) Vorgaben für die IT-Sicherheitsarchitektur des Bundes. Darin wird bspw. das BSI als zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes festgelegt und z.B. Regelungen zur Kontrolle, Abwehr von Schadprogrammen und Gefahren oder Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit getroffen. So legt das BSI gem. BSIG §8 (1) im Benehmen mit den Bundes-Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest. Das BSIG soll durch das derzeit im parlamentarischen Verfahren befindliche Umsetzungsgesetz zur Network and Information Security Direktive 2 (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)[10] grundlegend erweitert werden.

Untergesetzlich definiert die verbindliche **Leitlinie für Informationssicherheit in der Bundesverwaltung (UP Bund)** die wesentlichen Rahmenbedingungen an die Informationssicherheit in der Bundesverwaltung. Hierzu zählen insb. ein Informationssicherheitsmanagement nach BSI-Standards (200-1 bis 200-3), die Umsetzung des IT-Grundschutz des BSI und die Einhaltung der Mindeststandards für die Bundesverwaltung (nach §8 BSIG). Im Rahmen des „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ werden einige der Regelungsbestandteile auch für oberste Bundesbehörden auf gesetzlicher Ebene verankert.

Die **Directive on Security of Network and Information Systems** (NIS-2), 2022 durch das Europäische Parlament verabschiedet und hätte bis spätestens Oktober 2024 durch die nationalen Regierungen in nationales Recht umgesetzt werden müssen, ist eine Weiterentwicklung der ersten NIS-Richtlinie aus dem Jahr 2016.[11] Ziel der NIS-Richtlinie ist die Umsetzung eines hohen IT-Sicherheitsniveaus im privaten und öffentlichen Sektor innerhalb der gesamten Europäischen Union. Die obersten Bundesbehörden werden grundsätzlich explizit in den Geltungsbereich der NIS-2-Richtlinie einbezogen. Für die Umsetzung der NIS-2-Richtlinie ist unter anderem die Implementierung von Multi-Faktor-Authentifizierung oder kontinuierlicher Verifizierung Nutzender, als erster Zero-Trust-Umsetzungsschritt, sowie die Einhaltung von erweiterten Meldepflichten nötig.[12] Solche Anforderungen werden aufgegriffen und im Folgenden in Anforderungen an eine IT-Sicherheitsarchitektur des Bundes überführt.

---

[10] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Die EU-NIS-2-Richtlinie (NIS2UmsuCG) wurde am 13. November 2025 vom Deutschen Bundestag beschlossen.

[11] vgl. EU-Richtlinien zur Netzwerk- und Informationssicherheit (2024)

[12] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Die EU-NIS-2-Richtlinie (NIS2UmsuCG) wurde am 13. November 2025 vom Deutschen Bundestag beschlossen.

Im November 2023 haben die NATO-Mitgliedsstaaten im Consultation, Command and Control Board die **NATO Zero Trust Policy**[13] verabschiedet. Diese beschreibt für das Umfeld der NATO Enterprise und der NATO-Mitgliedsstaaten ein gemeinsames Verständnis des Zero-Trust Paradigmas.

In Erweiterung international etablierter Zero-Trust-Modelle wurden sechs Prinzipien formuliert, die Handlungsleitend sein sollen:

1 **„Assume Breach“**: Entscheidungen werden unter der Annahme getroffen, dass Systeme kompromittiert sind.

2 **„Never Trust, Always Verify“**: Subjekten (z.B. Nutzer, Geräte, Applikationen) wird nicht ungeprüft vertraut. Vor allen Zugriffen auf Ressourcen wird deren Identität bestätigt.

3 **„Verify Explicitly and Continuously“**: Einmal erteilte (Zugriffs-)Rechte werden nicht zeitlich unbegrenzt erteilt.

4 **„Apply Least Privilege“**: Zugriffsrechte auf Ressourcen sollen stets auf das notwendige Mindestmaß reduziert werden.

5 **„Probabilistic and Explainable Security Decisions“:** Zugriffsentscheidungen erfolgen basierend auf messbaren Sicherheitsparametern, welche die Verlässlichkeit einer Entscheidung repräsentieren. Entscheidungssysteme, insb. beim Einsatz von KI-Systemen, sind stehts erklärbar.

6 **„Transparency“**: Die effektive Umsetzung von Zero-Trust in föderierten Umgebungen benötigt die Bereitschaft zur Transparenz zwischen den Föderationspartnern (Bereitstellung von Informationen, um die Entscheidung des Partners zu unterstützen).

Weiterhin wird betont, dass diese Prinzipien auf drei Handlungsebenen im jeweiligen Kontext angewandt werden sollen, um:

a) die Sicherheitskultur,

b) die Unternehmens-Governance sowie

c) die digitale Umgebung

weiterzuentwickeln.

Mit der Einführung des Zero-Trust Paradigmas will die NATO den Schutz eigener IT-Systeme im föderierten Umfeld erhöhen, den sicheren Zugriff auf Ressourcen in der Allianz beschleunigen und neue technische Möglichkeiten erschließen.

Zero-Trust ist ein Enabler für die angestrebte Fähigkeit zur Durchführung von Multi-Domain-Operations, dem zivil-militärisch gemeinsamen Handeln innerhalb der Allianz. Alle Ressorts,

[13] Das C3B ist seit Dezember 2024 umbenannt als NATO Digital Policy Committee (DPC)

deren Stellen NATO-Informationen verarbeiten oder an die NATO übertragen wollen, haben die Policy und zukünftige Regelungen zu beachten.

Darüber hinaus bestehen weitere gesetzliche Rahmenbedingungen, insbesondere zum Datenschutz, die gemäß DSGVO, bei der Verarbeitung personenbezogener Daten gelten. Insbesondere für tiefergehende Verhaltensanalysen, wie bspw. der Echtzeitanalyse von Verhaltensmustern sind Regeln (Policy) zu definieren, die dem Datenschutz der betroffenen Personen angemessen Rechnung tragen. Zero-Trust baut auf einer ressourcenzentrierten Betrachtung der IT-Sicherheitsarchitektur auf. Fokus liegt hierbei auf den Schutzzielen Integrität und Vertraulichkeit. Bei der Umsetzung des Zero-Trust-Ansatzes in konkrete Regeln (Policy) sollte neben den genannten Schutzzielen aber auch die Möglichkeit der Nutzung von IT-Ressourcen für die Nutzenden betrachtet werden.

2.3 Technische Referenzwerke und Modelle für Zero-Trust

Die **Zero Trust Architecture** des National Institute of Standards and Technology (NIST; 2020) ist die Referenzarchitektur zur Umsetzung des Zero-Trust-Architekturparadigmas in der Bundesverwaltung der Vereinigten Staaten. Es werden konkrete Architekturelemente für die Verwaltung von Attributen und Regeln, (Policy Administration Point – PAP), Festlegung anzuwendender Regeln (Policy Decision Point – PDP) und Anwendung der Regelwerke (Policy Enforcement Point – PEP) im Rahmen der fortlaufenden Autorisierung von Zugriffsentscheidungen darin definiert. Die Grundannahmen der NIST-Referenzarchitektur liegen auch der Entwicklung der Lösungsansätze und Eckpunkte in diesem Eckpunktepapier zu Grunde.

Das **Zero-Trust-Reifegradmodell** der Cybersecurity and Infrastructure Security Agency (CISA) aus dem Jahr 2023 beschreibt einen möglichen Ansatz zur Integration von Zero-Trust in IT-Bestandsumgebungen. Das Modell wird u. a. für die Integration der Zero-Trust-Komponenten in die IT-Sicherheitsarchitektur der Bundesverwaltung der Vereinigten Staaten angewendet.[14]

Das **Positionspapier Zero Trust 2023** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) adaptiert die Standards des Zero-Trust Reifegradmodells der CISA und ergänzt diese um auf den deutschen Kontext zugeschnittene Regelungen, wie bspw. Anforderungen an den Umgang mit Verschlusssachen.[15] Das Positionspapier Zero-Trust 2023 soll sowohl für die Industrie als auch für die öffentliche Verwaltung anwendbar sein. Dieses Eckpunktepapier übernimmt diejenigen Teile des Zero-Trust-Positionspapiers, die sich speziell auf die Anforderungen und Rahmenbedingungen der IT des Bundes fokussieren.

[14] vgl. Memorandum for the Heads of Executive Departments and Agencies (2022)
[15] vgl. Positionspapier zu Zero Trust des BSI (2023)

Die in Kap. 2.3 gen. Modelle bzw. Dokumente nutzen die Architekturdimensionen **Identitäten**, **(End)Geräte**, **Netze**, **Anwendungen** und **Daten**. Diese werden auch in diesem Eckpunktepapier genutzt.

3.Rahmenbedingungen und Anforderungen an eine IT-Sicherheitsarchitektur des Bundes

Die IT des Bundes ist mit veränderten Rahmenbedingungen konfrontiert, aus denen spezifische Anforderungen an eine IT-Sicherheitsarchitektur des Bundes abgeleitet werden. Ein zusammenfassender Überblick ist in Abbildung 1 dargestellt.

Kateg.	Rahmenbedingungen an die IT-Sicherheits-architektur des Bundes	Anforderungen an die IT-Sicherheitsarchitektur des Bundes		
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		

Abbildung 1: Rahmenbedingung und Anforderungen an die IT-Sicherheitsarchitektur des Bundes

3.1 Gestiegene Bedrohungslage

Die IT des Bundes ist bereits seit vielen Jahren einer kontinuierlich gestiegenen Bedrohungslage ausgesetzt, welche durch Cyberangriffe mit Ransomware, Phishing, Spam-Emails[16] oder DDoS-Angriffe gekennzeichnet ist. Aus der Perspektive des BSI ist Ransomware die größte Cyberbedrohung[17], wobei technologische Entwicklungen wie Künstliche Intelligenz die Effektivität dieser Angriffe steigern können. Weiterhin stellen sogenannte Advanced Persistent Threats (APT) eine erhebliche Gefahr für die IT des Bundes dar. Diese langfristig geplanten und ressourcenintensiven Angriffe zielen darauf ab, dauerhaften Zugang zu besonders schutzbedürftigen Netzen und den dort verfügbaren Daten zu erlangen.[18] Insbesondere seit Anfang 2022, dem Beginn des russischen Angriffskrieges gegen die Ukraine verzeichnet das Bundesamt für Verfassungsschutz (BfV) eine besondere Zunahme hochversierter Cyberangriffe durch staatlich gesteuerte Akteure auf IT-Dienstleister, die Behördennetze betreuen.

Die in jüngster Zeit erneut erheblich gestiegene Bedrohungslage ist auf eine erhöhte Anzahl von Cyberaktivitäten staatlich gesteuerter Akteure (APT) zurückzuführen, wie beispielsweise

[16] vgl. Die Lage der IT-Sicherheit in Deutschland 2023 (2023), Seiten 67 bis 68
[17] vgl. Die Lage der IT-Sicherheit in Deutschland 2023 (2023), Seite 47
[18] vgl. Die Lage der IT-Sicherheit in Deutschland 2023 (2023)

russischer oder chinesischer Nachrichtendienste.[19] Das BfV betont, dass chinesische Cyberspionage „hochprofessionell und mit enormen Ressourcenaufwand“ betrieben wird,[20] was sich in technisch versierten Cyberangriffen auf Regierungsinstitutionen und damit auf die IT des Bundes manifestiert. Diese Angriffe zielen darauf ab, dauerhaften Zugriff auf die Netze und den dort verfügbaren Daten zu etablieren und Informationen über politische Meinungsbildungs- und Entscheidungsprozesse sowie Positionen der Bundesregierung mit Auswirkungen u. a. auf den chinesischen Staat zu erlangen. Diese Angriffe waren laut BfV in Deutschland bereits erfolgreich.[21]

Zusätzlich erstrecken sich auch Cyberangriffe russischer Akteure, darunter die entsprechenden Nachrichtendienste, überwiegend auf „Regierungsstellen, Parlamente und Personen in der Politik, Parteien, Streitkräfte“ mit dem vorrangigen Ziel der „kontinuierliche[n] Informationsbeschaffung“, umfassen aber auch Sabotageakte zur Destabilisierung der Regierungsstrukturen.[22] So werden auch klassische Phishing-Angriffe auf E-Mail-Konten „im politischen Raum in Deutschland“ durchgeführt, mit dem Ziel Zugang zu persönlichen Informationen zu erlangen.[23] Das von den russischen Nachrichtendiensten ausgehende Gefährdungspotential wird durch den BfV als hoch eingeschätzt und geht von einer hohen Dunkelziffer nicht erkannter, qualitativ hochwertiger Cyberangriffe aus.[24]

Ergänzend zu den genannten Gefährdungen, bildet die Manipulation genutzter (End)Geräte, Netzwerkkomponenten oder Anwendungen entlang der Lieferkette[25] eine nicht zu unterschätzende konkrete Gefährdung für die Sicherheit der IT des Bundes.

Vor dem Hintergrund dieser sich verschärfenden Bedrohungslage, den daraus resultierenden Gefährdungen ergeben sich unter Beachtung der Zero-Trust-Prinzipien folgende Anforderungen an eine IT-Sicherheitsarchitektur des Bundes:

a. **Nutzerautorisierung:** Um unautorisierten Zugriff auf schutzbedürftige Daten der IT des Bundes zu vermeiden, sind bei der Zugriffsentscheidung die Eigenschaften aller Ressourcen mit Bezug auf den Schutzbedarf der Daten zu berücksichtigen. Mögliche weitere zu berücksichtigende Attribute sind beispielsweise geografischer Standort oder Zeit.

b. **Begrenzung der Netzausbreitung:** Die Kompromittierung von Netzen muss durch architektonische Maßnahmen verhindert bzw. begrenzt werden, beispielsweise durch Netz- bzw. Mikrosegmentierung, auf Grundlage von „Maschinenidentitäten“.

c. **Minimierung des Zugriffs:** Zugriffsberechtigungen müssen möglichst feingranular zugeteilt werden können, um Schadensauswirkungen reduzieren zu können.

---

[19] vgl. Verfassungsschutzbericht 2023 (2024), Seiten 323 bis 325
[20] vgl. Verfassungsschutzbericht 2023 (2024), Seite 326
[21] vgl. Verfassungsschutzbericht 2023 (2024), Seiten 323 bis 325
[22] vgl. Verfassungsschutzbericht 2023 (2024), Seiten 311 bis 315
[23] vgl. Verfassungsschutzbericht 2023 (2024), Seiten 314 bis 315
[24] vgl. Verfassungsschutzbericht 2023 (2024), Seiten 317 bis 318
[25] U.a. Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung.; ETSI TR 103 937 V1.1.1 (2024-08) - Cyber Security (CYBER); Cyber Resiliency and Supply Chain Management; BSI - Produktzertifizierung: Programm IT-Sicherheitszertifizierung Common Criteria (CC)

d. **Reaktionsmechanismen:** Um Schadensauswirkungen von Angriffen zu minimieren, müssen automatisierte Reaktionen ausgelöst werden können, wie bspw. der Entzug oder die Reduzierung von Zugriffsrechten.

3.2 Veränderte Nutzerbedarfe

In den letzten Jahren hat sich die Arbeitswelt der Mitarbeitenden der Bundesverwaltung weiterentwickelt. Die Arbeit in föderierten Systemen, mobiles Arbeiten und die Nutzung cloudbasierter IT-Anwendungen verändern die IT des Bundes und stellen auch Anforderungen an eine IT-Sicherheitsarchitektur des Bundes.

Aus den Anforderungen von NIS-2 ergeben sich Bedarfe für Maßnahmen für unterschiedliche Beteiligtengruppen. Dazu gehören vor allem regelmäßige Schulungen mit entsprechenden Angeboten je nach Betroffenheit, allgemeinen Sensibilisierungen für Bedrohungen der jeweiligen Sicherheitsstufen, Darstellung der Verantwortung und Rollen je nach Betroffenheit und Risikosituation, die Dokumentation der Aktivitäten und die Zugänglichkeit für alle zur Teilnahme verpflichteten Beteiligten in einer geeigneten medialen Form.

3.2.1 Arbeiten in föderierten Systemen

Durch die IT-Konsolidierung Bund wird die IT des Bundes ressortübergreifend gebündelt, vernetzt, standardisiert und modernisiert.[26] So war es Ziel der Dienstekonsolidierung, dass maximal zwei IT-Lösungen je Funktionalität zur Verfügung stehen. In der Folge sollen rund 168 Bundesbehörden und bis zu 276.000 Beschäftigte der unmittelbaren Bundesverwaltung zentralisierte IT-Ressourcen und konsolidierte Anwendungen nutzen.[27] Im Ergebnis der IT-Betriebskonsolidierung werden gemeinsame Hardware-Plattformen genutzt. Durch die hierbei entstehenden dringend erforderlichen Kommunikationsbeziehungen zwischen Ministerien, Behörden und Dienstleistern erhöht sich zugleich aber auch die Angriffsfläche der IT des Bundes. Zusätzlich entsteht durch die Zentralisierung der IT-Ressourcen die Gefahr möglicher Kaskadeneffekte. Für die IT-Sicherheitsarchitektur des Bundes ergeben sich folgende Anforderungen, die ebenso relevant sind für das Arbeiten im föderalen Kontext als auch darüber hinaus Beachtung finden sollten:

e. **Mandantentrennung:** Die zentrale Bereitstellung von IT-Lösungen und Daten erfordert in der Regel eine strikte Mandantentrennung. Dabei erhalten verschiedene Nutzergruppen, wie beispielsweise unterschiedliche Behörden, 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:** In föderierten Systemen müssen sich Anwendungen gegenseitig authentifizieren, um sicherzustellen, dass sowohl die Nutzenden als auch aufrufende Anwendungen die nötigen Berechtigungen haben, Prozesse auszulösen und auf Geräte, andere Anwendungen oder Daten zuzugreifen. Dafür sind durchgängige

[26] vgl. Artikel des BMI zur IT-Konsolidierung des Bundes (2023)
[27] vgl. Artikel des BMI zur IT-Konsolidierung des Bundes (2023)

Mechanismen notwendig, die diese Zugriffe innerhalb der Prozessketten authentifizieren.

3.2.2 Mobiles Arbeiten

In der öffentlichen Verwaltung hat sich die Nutzungshäufigkeit der Arbeit von Zuhause in den letzten Jahren nicht zuletzt durch die Corona-Krise stark erhöht[28] und soll in der gesamten Bundesverwaltung noch weiter ausgebaut werden.[29] Die Anzahl an Fernzugriffen auf die IT des Bundes von außerhalb der Dienstsitze der Bundesverwaltung ist deutlich gestiegen. Zusätzlich steigt auch die Anzahl der genutzten Endgeräte,[30] ebenso wie die Nutzung privater Endgeräte, bspw. durch Reservisten der Bundeswehr, die ihr privates Smartphone für dezidierte dienstliche Anwendungen nutzen. Bei der Verwendung privater Endgeräte im dienstlichen Kontext sind entsprechende Regeln (Policy) zu formulieren. Für die IT-Sicherheitsarchitektur des Bundes ergeben sich daher folgende Anforderungen:

g. **Sicherer Netz-Fernzugriff:** Netz-Fernzugriffe auf die IT des Bundes müssen sicher erfolgen können. Zur Erhöhung der Sicherheit müssen Berechtigungen und Zugriffe über Fernzugriff gemäß Nutzerbedarf und Schutzbedarf der IT-Ressourcen steuerbar sein.

h. **Verwaltung der Gerätevielfalt:** Durch die gestiegene Anzahl und Vielfalt an Endgeräten steigt die Komplexität der Geräteverwaltung der IT des Bundes. Endgeräte, welche mit der IT des Bundes interagieren, müssen erfasst und kategorisiert werden können.

i. **Echtzeitüberwachung von Endgeräten:** Eine durchgängige Überwachung des Compliance- und Gerätezustands von Endgeräten (bspw. Einhaltung der Sicherheitsstandards wie Status des Betriebssystems und Aktivierung von Anti-Viren- oder Anti-Malware-Programmen) sowie eine Echtzeitrisikoanalyse müssen als Entscheidungsgrundlage für die Zugriffsentscheidung dienen.

3.2.3 Cloudbasierte Anwendungsbereitstellung

Auf Basis von Multi-Cloud Lösungen und offener Schnittstellen wird eine interoperable und modulare Cloud Infrastruktur für die öffentliche Verwaltung gemäß der Deutschen Verwaltungscloud-(DVC)-Strategie und der IT-Strategie des Bundes umgesetzt.[31] Durch die Standardisierung soll eine Interoperabilität bereits bestehender, beispielsweise der Bundescloud und der Betriebsplattform Bund, als auch neuer Cloud-Lösungen sichergestellt werden. Die zunehmende Bereitstellung und Nutzung von Cloud-Lösungen wird durch einen „Cloud-First“-Entwicklungsansatz vorangetrieben.[32] Für die IT-Sicherheitsarchitektur des Bundes ergeben sich daher folgende Anforderungen:

j. **Sicherheit in Multi-Cloud-Umgebungen:** Durch die vermehrte Nutzung von Cloud-Diensten sind sowohl eine bundesverwaltungsweit standardisierte Zugriffsvergabe für Nutzende, eine Authentifizierung zwischen Anwendungen als auch eine Echtzeitrisikoanalyse bei Zugriffsanfragen notwendig. Zur Reduktion von Angriffsflächen sollte der Zugriff auf

---

[28] vgl. Pressemitteilung des statistischen Bundesamtes zur Zahl der Erwerbstätigen, die im Home-Office arbeiten (2023)
[29] vgl. Artikel des BMI zum flexiblen Arbeiten in der Bundesverwaltung (2023)
[30] vgl. Artikel des BSI zu Mindeststandard des BSI für Mobile Device Management (2022)
[31] vgl. Artikel des Beauftragten der Bundesregierung für Informationstechnik zu Deutsche Verwaltungscloud (2024)
[32] vgl. ITZBund IT-Strategie (2023), Seite 6

Cloudbereiche unter Beachtung der jeweiligen Identitäten und Rechte bestimmt werden.

k. **Dev(Sec)Ops:** Durch die Anwendung von Dev(Sec)Ops als agiles Framework, welches Sicherheit in allen Phasen des Lebenszyklus der Softwareentwicklung integriert („Development“, „Security“, „Operations“), müssen Sicherheitsmaßnahmen frühzeitig in der Anwendungsentwicklung und in Zusammenarbeit mit dem Betriebsteam umgesetzt werden.

3.3 Externe Vorgaben

3.3.1 Übergreifende Sicherheitsstandards

Mit Zustandekommen des NIS-2 Umsetzungsgesetztes[33] würden sich folgende Anforderungen an eine IT-Sicherheitsarchitektur des Bundes ergeben:

l. **Risikomanagementmaßnahmen:** Das Bundeskanzleramt und die Bundesministerien sind verpflichtet, geeignete Maßnahmen zu ergreifen, um Integrität und Vertraulichkeit der informationstechnischen Systeme zu gewährleisten. Dazu zählen beispielsweise Konzepte für Risikoanalysen, Einsatz von Verschlüsselung und Multi-Faktor- oder kontinuierliche Authentifizierung.[34]

m. **NIS-2 Meldepflichten:** Verdachtsfälle für erhebliche Sicherheitsvorfälle müssen innerhalb von 24 Stunden an die zuständige Stelle[35] gemeldet werden, gefolgt von einer Fortschrittsmeldung und Abschlussmeldung. Dazu müssen Sicherheitsvorfälle fortlaufend dokumentiert, transparent gemeldet, protokolliert und nachvollzogen werden können.[36]

3.3.2 NATO-Vorgaben

Bereits jetzt ist Deutschland verpflichtet, relevante NATO-Vorgaben national dort umzusetzen, wo NATO-Informationen im behördlichen Bereich verarbeitet werden oder ein Austausch mit NATO-Dienststellen erfolgt.

Mit der NATO-Zero-Trust Policy ist ein wesentlicher Schritt zur Einführung einer übergreifenden und föderierten IT-Architektur in der NATO mit seinen Schnittstellen in die NATO-Mitgliedsstaaten getan.

Daraus ergeben sich folgende Anforderungen an eine IT-Sicherheitsarchitektur des Bundes für die betroffenen behördlichen Bereiche:

n. **Anschlussfähige, Zero-Trust-befähigte Schnittstellen nationaler IT-Verfahren:** Alle Stellen, die im Kontext der NATO unmittelbare digitale Schnittstellen zu NATO-Stellen oder

---

[33] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Die EU-NIS-2-Richtlinie (NIS2UmsuCG) wurde am 13. November 2025 vom Deutschen Bundestag beschlossen.

[34] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Die EU-NIS-2-Richtlinie (NIS2UmsuCG) wurde am 13. November 2025 vom Deutschen Bundestag beschlossen.

[35] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Die EU-NIS-2-Richtlinie (NIS2UmsuCG) wurde am 13. November 2025 vom Deutschen Bundestag beschlossen.

[36] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Die EU-NIS-2-Richtlinie (NIS2UmsuCG) wurde am 13. November 2025 vom Deutschen Bundestag beschlossen.

NATO-Partnern unterhalten, müssen die Föderations- und Zero-Trust-Vorgaben der NATO umsetzen.

o. **Implementierung von NATO-Dateneinstufungsstandards:** Alle Stellen, die eingestufte NATO-Informationen oder national eingestufte Information für die NATO freigegeben, speichern, verarbeiten oder übertragen, müssen zunehmend Daten-[37] und Zero-Trust-Vorgaben der NATO umsetzen.

[37] U.a. zur Syntax von vertrauenswürdigen Labels gemäß Standardization Agreement (STANAG 4774) und deren kryptographische Bindung an Datenobjekte (STANAG 4778) und BSI - VS – Anforderungsprofil Digitales Labelling.

4.Eignung des Zero-Trust-Architekturparadigmas für die IT-Sicherheitsarchitektur des Bundes

Inwiefern eine Zero-Trust-IT-Sicherheitsarchitektur die identifizierten Anforderungen des Bundes adressieren kann, soll im Folgenden beschrieben werden. Dazu wird die Eignung der Lösungsansätze des Zero-Trust-Architekturparadigmas den Anforderungen der IT-Sicherheitsarchitektur des Bundes gegenübergestellt. Die Zero-Trust-Lösungsansätze sind gemäß dem CISA-Zero-Trust-Reifegrad- bzw. dem BSI-Zero-Trust Integrations-Modell den fünf Architekturdimensionen **Identitäten**, **(End)Geräte**, **Netze**, **Anwendungen** und **Daten** zugeordnet.

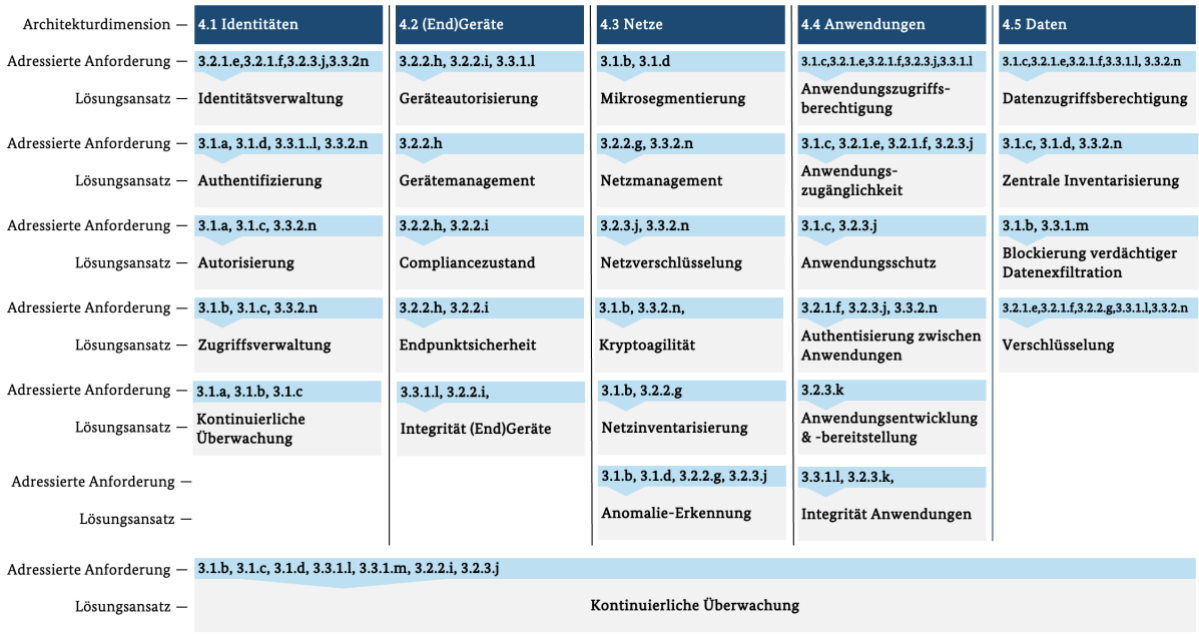

Abbildung 2: Zero-Trust-Lösungsansätze und adressierte Anforderungen der IT-Sicherheitsarchitektur des Bundes

Für alle Architekturdimensionen (Identitäten, (End)Geräte, Netze, Anwendungen und Daten) gilt, dass durch eine kontinuierliche Überwachung, jegliche Aktivität durch Echtzeitanalysen untersucht und bewertet (z. B. Login-Zeiten, verwendetes Gerät, abgelehnte Zugriffsanfragen) wird.

4.1 Architekturdimension – Identitäten

In der Architekturdimension Identitäten ordnet das Zero-Trust-Architekturparadigma folgende Lösungsansätze ein:

Identitätsverwaltung: Identitäten, Rollen und Verantwortlichkeiten werden durch Identitätsprovider verwaltet und verifiziert. In Abhängigkeiten von Identitäten werden Rollen und Berechtigungen zugewiesen. Auf diese Weise wird eine granulare Zugriffskontrolle ermöglicht. In föderierten Systemen müssen Identitätsprovider einheitlichen technischen und organisatorischen Standards folgen, damit sie sich gegenseitig vertrauen und Identitäten systemübergreifend verifiziert und genutzt werden können.

Authentifizierung: Eine kontinuierliche, adaptive Multi-Faktor-Authentifizierung gewährleistet die Verifizierung der Identität nicht nur bei der Erteilung des ersten Zugriffs, sondern fortlaufend während der gesamten Dauer des Zugriffs. Zusätzliche Authentifizierungsfaktoren zur Sicherheitsverstärkung können dynamisch ausgewertet werden.

Autorisierung: Autorisierungsprozesse, die – nach erfolgreicher Authentifizierung – auf dynamisch belegten Attributen wie bspw. Zeitpunkt, geografischer Standort, zuvor beobachtetem Verhalten oder Gerätezustand basieren - nach erfolgreicher Authentifizierung - verbessern den Schutz vor unbefugtem Zugriff.

Zugriffsverwaltung: Zugriffe werden zeitlich begrenzt und beschränkt auf die zur konkreten Aufgabenerfüllung notwendigen IT-Ressourcen („Just-in-Time“ und „Just-Enough“).

Kontinuierliche Überwachung: Nutzerverhalten wird durch Echtzeitanalysen analysiert (z. B. Login-Zeiten, verwendetes Gerät, Standort, Schutzbedarf der Daten).

Mit diesen Lösungsansätzen können u. a. die Anforderungen Nutzerautorisierung (3.1.a), Begrenzung der Netzausbreitung (3.1.b), Minimierung des Zugriffs (3.1.c), Reaktionsmechanismen (3.1.d), Mandantentrennung in föderierten Systemen (3.2.1.e), Zugriffsauthentifizierung über Prozessketten (3.2.1.f), Sicherheit in Multi-Cloud-Umgebungen (3.2.3.j) sowie Risikomanagementmaßnahmen (3.3.1.l) und Meldepflichten (3.3.1.m) nach NIS-2 adressiert werden.

4.2 Architekturdimension – (End)Geräte

In der Architekturdimension (End)Geräte ordnet das Zero-Trust-Architekturparadigma folgende Lösungsansätze ein:

Gerätemanagement: Dienstliche Endgeräte werden zentral verwaltet. Ein automatisiertes Assetmanagement ermöglicht fortlaufende Kontrolle. In föderierten Systemen muss das Gerätemanagement aller Partner einheitlichen Standards folgen, damit sie sich gegenseitig vertrauen und Geräte systemübergreifend verifiziert und genutzt werden können.

Compliance-Zustand: Automatisierte Compliance-Mechanismen prüfen und aktualisieren kontinuierlich die Einhaltung von Sicherheitsvorschriften für dienstliche und private Endgeräte, beispielsweise die Aktualität des Betriebssystems oder den Antivirus-Status.

Geräteautorisierung: Zugriffe werden auf Basis des Compliance-Zustandes und ggf. weiterer Attribute erteilt.

Endpunktsicherheit: Zentralisierte Sicherheitslösungen bieten umfassenden Schutz für alle Endgeräte durch die Integration von Endpoint Protection[38] sowie Detection und Response[39].

[38] Endpoint Protection bietet grundlegenden Schutz vor bekannten Bedrohungen wie Malware und Viren durch Integration von Antiviren-Software, Anti-Malware oder Firewalls.
[39] Detection and Response sammelt kontinuierlich Daten von Endgeräten und verwendet Analysen, um verdächtiges Verhalten zu erkennen und automatisch Gegenmaßnahmen durchzuführen.

Hierdurch werden präventive Maßnahmen gegen bekannte Bedrohungen und fortgeschrittene Erkennung und Reaktion auf verdächtige Aktivitäten kombiniert und finden Eingang bei Zugangsentscheidungen.

Integrität (End)Geräte: Sicherstellung der Integrität der (End)Geräte entlang der Lieferkette[40]. Hierdurch wird verhindert, dass mögliche Gefährdungen der Sicherheit der IT des Bundes durch maliziöse (End)Geräte, verursacht werden.

Mit diesen Lösungsansätzen können u. a. die Anforderungen Verwaltung der Gerätevielfalt (3.2.2.h), Echtzeitüberwachung von (End)Geräten (3.2.2.i) und Risikomanagementmaßnahmen (3.3.1.l) adressiert werden.

4.3 Architekturdimension – Netze

In der Architekturdimension Netze ordnet das Zero-Trust-Architekturparadigma folgende Lösungsansätze ein:

Netzinventarisierung: Alle Netzsegmente werden kontinuierlich inventarisiert einschließlich einer Kategorisierung nach erforderlichem Schutzbedarf. Netze werden in Kategorien (bspw. Ressort, Behörde, Dienst) eingeteilt und klassifiziert (bspw. öffentlich, föderiert, intern).

Mikrosegmentierung: Durch eine feingranulare Aufteilung von Netzsegmenten, auf Grundlage der „Maschinenidentitäten“, wird ein szenariospezifischer Datenaustausch ermöglicht. Dies schließt physische und logische Segmentierung ein, die isolierte Netzbereiche oder benutzergruppenspezifische Zugriffsrechte je nach Sicherheitsanforderung (bspw. Schutzbedarf der Daten) ermöglicht.

Netzmanagement: Die Bereitstellung von Netzverbindungen erfolgt auf Basis von Relevanz, Risikobewertung und Kritikalität der Anfragen und der übertragenen Daten. Die Durchsetzung findet bspw. durch Software-Defined Networking statt.

Netzverschlüsselung: Datenaustausch erfolgt grundsätzlich über verschlüsselte Netzverbindungen. Die Verschlüsselung hat dem Stand der Technik und sofern zutreffend den Vorgaben der Verschlusssachenanweisung (VSA) zu entsprechen. Beim Einsatz der Netzverschlüsselung ist auf **Kryptoagilität** zu achten, um auf kurzfristige kryptografische Entwicklungen reagieren zu können.

Anomalie-Erkennung: Eine kontinuierliche automatisierte, auf Kontext und Metadaten basierende Erkennung von Abweichungen vom „Normalzustand“ unterstützt den Schutz des Netzes (Bsp. Erkennung von Lateral Movement).

Mit diesen Lösungsansätzen können u. a. die Anforderungen Begrenzung der Netzausbreitung (3.1.b), Reaktionsmechanismen (3.1.d), sicherer Netz-Fernzugriff (3.2.2.g), Sicherheit in Multi-

[40] U.a. Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung; ETSI TR 103 937 V1.1.1 (2024-08) - Cyber Security (CYBER); Cyber Resiliency and Supply Chain Management; BSI - Produktzertifizierung: Programm IT-Sicherheitszertifizierung Common Criteria (CC)

Cloud-Umgebungen (3.2.3.j) sowie Risikomanagementmaßnahmen (3.3.1.l) und Meldepflichten (3.3.1m) adressiert werden.

4.4 Architekturdimension – Anwendungen

In der Architekturdimension Anwendungen ordnet das Zero-Trust-Architekturparadigma folgende Lösungsansätze ein:

Anwendungszugriffsberechtigung: Zugriffsautorisierungen für Anwendungen basieren auf Echtzeitrisikoanalysen, die sowohl die anfragenden Berechtigungen als auch das aktuelle Risikoprofil durch Nutzungsverhaltensanalysen berücksichtigen. Diese Nutzungsverhaltensanalysen überwachen kontinuierlich die Zugriffsmuster und erkennen Abweichungen, die eine Einschränkung des Zugriffs erforderlich machen können.

Anwendungszugänglichkeit: Anwendungszugriffe sind über Netze möglich, wobei der Sicherheitszustand sowohl des internen als auch des externen Netzes als gleichwertig betrachtet wird. Zugriffsberechtigungen werden minimal und attributbasiert vergeben, abhängig von Faktoren wie bspw. dem Zugangsbedarf, dem Schutzbedarf der Anwendung und dazugehöriger Daten oder dem Standort der Anfrage.

Anwendungsschutz: Sicherheitsrichtlinien sind direkt in die Anwendungsabläufe integriert. Anwendungsspezifische Schutzmaßnahmen, wie bspw. Web Application Firewalls und Mikrosegmentierung, schützen ausgewählte Anwendungskomponenten. Eine Kapselung der Anwendungen, z.B. in Containern, Sandboxen oder mit Mandatory-Access-Control-Mechanismen verhindert weitreichende unbefugte Zugriffe eventueller Angreifer bei Ausnutzung anwendungsspezifischer Schwachstellen.

Authentisierung zwischen Anwendungen: Anwendungen authentisieren sich gegenseitig durch den Einsatz von starken, Multifaktor basierten Methoden. Die Authentifizierung berücksichtigt u.a. Attribute wie Zeitpunkt und geografischen Standort der Anfrage. Authentisierungen zwischen Anwendungen müssen einheitlichen Standards folgen, damit sie sich gegenseitig vertrauen können und systemübergreifend verifiziert und genutzt werden können.

Anwendungsentwicklung und -bereitstellung: Die Sicherheit von Anwendungen wird durchgängig während des gesamten Entwicklungszyklus sichergestellt, unter Einsatz von Methoden wie SAST[41], DAST[42] und IAST[43]. Der Bereitstellungsprozess erfolgt automatisiert ohne Administratorzugriff, wobei unveränderliche Images verwendet werden, die nach ihrer Bereitstellung nicht mehr unbemerkt modifiziert werden können. Über Attestierung und Verifikation der Images wird sichergestellt, dass keine Veränderungen erfolgt sind.

---

[41] SAST: Static Application Security Testing, um den Quellcode auf Sicherheitslücken zu analysieren, bevor der Code kompiliert wird

[42] DAST: Dynamic Application Security Testing, um laufende Anwendungen zu testen und Schwachstellen im laufenden Betrieb zu identifizieren

[43] IAST: Interactive Application Security Testing, um Sicherheitslücken sowohl im Quellcode als auch während der Laufzeit zu erkennen

Integrität Anwendungen: Sicherstellung der Integrität der Anwendungen entlang der Lieferkette. Hierdurch wird verhindert, dass mögliche Gefährdungen der Sicherheit der IT des Bundes durch maliziöse Anwendungen, verursacht werden.

Mit diesen Lösungsansätzen können u. a. die Anforderungen Minimierung des Zugriffs (3.1.c), Mandantentrennung (3.2.1.e), Zugriffsauthentifizierung über Prozessketten (3.2.1.f), Sicherheit in Multi-Cloud-Umgebungen (3.2.3.j) und Risikomanagementmaßnahmen (3.3.1.l) adressiert werden.

4.5 Architekturdimension – Daten

In der Architekturdimension Daten ordnet das Zero-Trust-Architekturparadigma folgende Lösungsansätze ein:

Datenzugriffsberechtigung: Der Zugriff auf Daten wird streng kontrolliert und nur für den benötigten Zeitraum („Just-in-Time“) und nur in unbedingt benötigtem Umfang gewährt („Just-Enough“). Basierend auf Echtzeitrisikoanalysen wird fortlaufend der Zugriff überwacht, um ungewöhnliche Zugriffsmuster zu erkennen und bei Risikoindikationen wie bspw. Zugriff zu unüblichen Zeiten oder von ungewöhnlichen geografischen Orten den Zugang einzuschränken oder nicht zu gewähren.

Zentrale Inventarisierung: Alle Daten werden kontinuierlich inventarisiert, einschließlich einer Kategorisierung nach erforderlichem Schutz. Daten werden in Kategorien (bspw. Geschäfts-, Kunden- und Finanzdaten, VS-Einstufung) eingeteilt und klassifiziert (bspw. öffentlich, intern, vertraulich, geheim).

Blockierung verdächtiger Datenexfiltration: Durch umfassende Inventarisierung und Klassifizierung sind alle Daten erfasst und entsprechend ihrem Schutzbedarf eingestuft. DLP-Mechanismen (Data Loss Prevention) überwachen den Datenverkehr in Echtzeit, erkennen verdächtige Aktivitäten und nutzen maschinelles Lernen sowie KI zur Analyse des normalen Verhaltens von Benutzern und Systemen, um Abweichungen und Anomalien zu identifizieren und im Risikofall den Zugriff einzuschränken oder nicht zu gewähren.

Verschlüsselung: Alle Daten werden sowohl in ruhendem Zustand („At Rest“) als auch während der Übertragung („In Transit“) verschlüsselt und authentisiert. Dies gewährleistet, dass Daten auf Speichermedien und bei der Übertragung über Netze hinweg geschützt sind und nur autorisierte Benutzer Zugriff auf die entschlüsselten Daten haben. Beim Einsatz der Verschlüsselung ist auf **Kryptoagilität** zu achten, um auf kurzfristige kryptografische Entwicklungen reagieren zu können.

Mit diesen Lösungsansätzen können u. a. die Anforderungen Minimierung des Zugriffs (3.1.c), Reaktionsmechanismen (3.1.d), Mandantentrennung (3.2.1.e), Zugriffsauthentifizierung über Prozessketten (3.2.1.f), sicherer Netz-Fernzugriff (3.2.2.g), Sicherheit in Multi-Cloud-Umgebungen (3.2.3.j) sowie Risikomanagementmaßnahmen (3.3.1.l) und Meldepflichten (3.3.1.m) nach NIS-2 adressiert werden.

5.Zero-Trust-Eckpunkte der IT-Sicherheits-Architektur des Bundes

Die beschriebenen Zero-Trust-Lösungsansätze können die identifizierten Anforderungen an eine IT-Sicherheitsarchitektur des Bundes grundsätzlich erfüllen. Allerdings erfordert die Etablierung einer Zero-Trust basierten IT-Sicherheitsarchitektur in der komplexen IT-Bestandslandschaft des Bundes große Aufwände. Für eine vollständige Integration der genannten Zero-Trust-Lösungsansätze müssten in der IT-Sicherheitsarchitektur des Bundes voraussichtlich tiefgreifende Anpassungen in allen Architekturdimensionen vorgenommen werden – den Identitäten (bspw. Etablierung einer Authentifizierungsstelle), (End)Geräten, Weitverkehrsnetzen des Bundes (bspw. Erweiterung des bestehenden perimeterbasierten Ansatzes), Anwendungen (bspw. Umsetzung von „Always-Verify“ Komponenten in den Diensten) und bei der Datenhaltung.

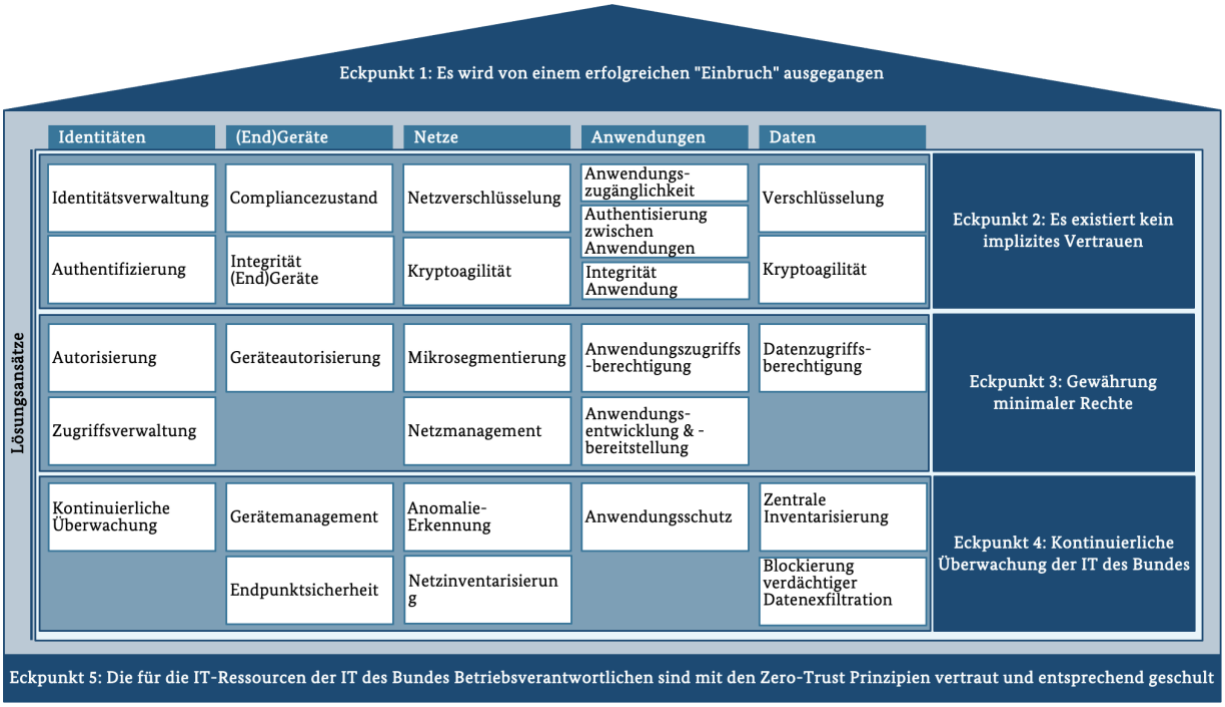

Abbildung 3: Zero-Trust-Eckpunkte der IT-Sicherheitsarchitektur des Bundes

Die folgenden Eckpunkte dienen als Zielkorridor für einen noch durchzuführenden nachgelagerten Prozess, um die bisherige IT des Bundes an eine Zero-Trust IT-Sicherheitsarchitektur heranzuführen. Im Rahmen des nachgelagerten Prozesses sind gesetzliche Vorgaben, bestehende Standards, Architekturvorgaben, die Anforderungen der Dienste- und Betriebskonsolidierung und des Deutschland-Stacks sowie die Anforderungen der Ressorts zu betrachten und in einen angemessenen Ausgleich zu bringen.

Eckpunkt 1: Es wird von einem erfolgreichen "Einbruch" ausgegangen, dessen Schadenauswirkungen durch mehrstufige IT-Sicherheitsmaßnahmen begrenzt werden können. Die klassische Perimeter Absicherung ist daher durch einen mehrstufigen, alle IT-Ressourcen (u.a. Netze, Daten und Anwendungen) der IT des Bundes umfassenden Ansatz zu ergänzen.

Eckpunkt 2: Es existiert kein implizites Vertrauen. Jeder Zugriff auf IT-Ressourcen (u.a. Netze, Daten und Anwendungen) der IT des Bundes ist fortlaufend zu validieren: Insbesondere in föderierten IT-Strukturen, sollten interne und externe Zugriffsanfragen gleichbehandelt werden. Eine einmalige Authentifizierung (z. B. an der Perimetergrenze) ist nicht mehr ausreichend. Zugriffe müssen stattdessen laufend, unter Beachtung der aktuellen Sicherheitslage neu geprüft, erteilt und ggf. angepasst werden. Sichere Authentifizierungsmethoden (z. B. Multi-Faktor-Authentifizierung) werden für alle Identitäten angewendet. Transparenz[44] 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). Die Zuordnung von Berechtigungen wird fortlaufend überprüft und ggf. bedarfsgerecht angepasst. Die Autorisierung erfolgt für jeden Zugriff erneut.

Eckpunkt 4: Kontinuierliche Überwachung der IT des Bundes. Jeglicher Zugriff auf IT-Ressourcen der IT des Bundes ist anhand festgelegter Attribute bzw. sowie dynamischer Regelwerke kontinuierlich zu überwachen. Solche Überwachung schafft die Basis, um Anomalien frühzeitig zu erkennen und zu behandeln. Zu möglichen Attributen gehören Zeitpunkt oder geografischer Standort des Zugriffs.

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. Die Betriebsverantwortlichen sind mit „Zero-Trust“ vertraut, verstehen die Prinzipien und sind darin geschult, diese konsequent in ihrem Arbeitsalltag umzusetzen.

[44] Transparenz ist hier im Sinne der gegenseitigen Bereitstellung von für eine Zugriffsentscheidung relevanter Informationen zwischen Parteien zu verstehen.

Technologische Zero-Trust-Lösungsansätze werden effektiv durch Prozesse in der Organisation unterstützt.

6.Ausblick

Wie in den vorangegangenen Eckpunkten dargelegt, können die Anforderungen an die IT-Sicherheitsarchitektur des Bundes durch eine maßvolle Integration des Zero-Trust-Paradigmas besser erfüllt werden. Mit Integration der Zero-Trust-Eckpunkte in die IT-Sicherheitsarchitektur des Bundes, besteht die Möglichkeit, dass auf Grund systemübergreifender IT-Sicherheitsregeln, eine Reduzierung der Gesamtsystemkomplexität, durch eine eventuelle Reduzierung von Sicherheitsregeln, einhergeht.

Die Implementierung einer auf Zero-Trust basierenden IT-Sicherheitsarchitektur in der bestehenden IT ist ein mehrstufiges Vorhaben. Die Integration wird mehrere Jahre in Anspruch nehmen und mit teils signifikanten Aufwänden sowohl im technischen als auch im organisatorischen Umfeld verbunden sein. Die Umsetzung wird schrittweise erfolgen, weshalb sich eine rechtzeitige Planung mit einer entsprechenden Haushaltsfürsorge empfiehlt.

Basierend auf dem durch die Eckpunkte definierten Rahmen, wird in einem nachgelagerten Prozess ein Zielbild für eine zukünftige IT-Sicherheitsarchitektur des Bundes unter Beachtung laufender IT-Maßnahmen konzipiert. Die Konzeption erfolgt unter enger Einbeziehung der Bundesressorts. Insbesondere muss eine enge Abstimmung und ein enges Zusammenwirken, unter Beachtung der geltenden gesetzlichen und untergesetzlicher Vorgaben, bestehender Standards und Architekturvorgaben sowie Anforderungen der Ressorts und zusammen mit den dafür zuständigen Beteiligten (bspw. BSI, Verbund der IT-Dienstleister, BfDI) erfolgen.

Nach Abstimmung des Zielbildes werden in Abstimmung mit den Ressorts und den beteiligten Institutionen Maßnahmen zur Erreichung definiert und anschließend umgesetzt. Zu diesen Maßnahmen sollte eine Marktsichtung, basierend auf den hier gen. Eckpunkten gehören, da davon auszugehen ist, dass sich architektonische Zero-Trust Anforderungen perspektivisch durch marktverfügbare IT-Systeme umsetzen lassen. Hierzu gehören beispielsweise dynamische Entscheidungssysteme, die auf Grundlage messbarer Sicherheitsparameter KI-unterstützte Zugriffsentscheidungen treffen. Allerdings sollte bei der Nutzung KI-unterstützter Systeme darauf geachtet werden, dass die Entscheidungen stehts erklärbar sind. Da Entscheidungssysteme, angelehnt an die Definition in §2 Ziffer 21 des Entwurfes zum NIS-2-Umsetzungsgesetz, als „kritische Komponenten“ zu werten sind, sind für Auswahl Einsatz der Entscheidungssysteme die Aspekte der Herstellerintegrität, der möglichen mittelbaren oder unmittelbaren Kontrolle des Herstellers durch Drittstaaten und die Vereinbarkeit des Einsatzes mit den Sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der EU und der Bündnispartner mit einer besonderen Gewichtung zu berücksichtigen.

Neben technologischen Maßnahmen sind auch organisatorische Maßnahmen und Anpassungen notwendig. Insbesondere sind die kritischen zentralen Geschäftsprozesse der jeweiligen Organisationen zu betrachten. Als Basis hierfür empfiehlt sich die Durchführung einer Reifegradanalyse, unter Beachtung gesetzlicher Vorgaben, auf Basis des Reifegradmodells („Maturity Modell“) der CISA bzw. des BSI-Integrationsmodells für die IT des Bundes. Diese Analyse kann modular innerhalb der Architekturdimensionen, unter

Berücksichtigung möglicher Wechselwirkungen zwischen den Dimensionen, erfolgen. Hierbei wird der aktuelle Zero-Trust-Reifegrad entlang der Architekturdimensionen erhoben („Startposition“) und anschließend notwendige Maßnahmen zur Erreichung des gewünschten Zielzustandes abgeleitet. Die Maßnahmen werden einer finanziellen Bewertung, der praktischen Umsetzbarkeit unter Berücksichtigung der fachlichen Anforderungen an die IT des Bundes und verfügbaren Ressourcen und Haushaltsmittel unterzogen. Auf Basis dieser Aufwandsbetrachtung können Maßnahmen parallel oder sequenziell im Rahmen eines pilothaften Vorgehens umgesetzt werden.

Glossar

Architekturdimension – Anwendungen im Kontext der IT des Bundes: Anwendungen im Kontext der IT des Bundes umfassen „Systeme von Behörden, Computerprogramme und Dienste, die lokal, auf mobilen Geräten und in Cloud-Umgebungen ausgeführt werden“.[45]

Architekturdimension – Daten im Kontext der IT des Bundes: Daten im Kontext der IT des Bundes umfassen „alle strukturierten und unstrukturierten Dateien und Fragmente, die sich in föderierten Systemen, Geräten, Netzen, Anwendungen, Datenbanken, Infrastrukturen und Backups befinden oder befunden haben (einschließlich lokaler und virtueller Umgebungen) sowie die zugehörigen Metadaten“.[46]

Architekturdimension – (End)Geräte im Kontext der IT des Bundes: Ein Endgerät im Kontext der IT des Bundes bezieht sich auf jegliche „Ressource (einschließlich seiner Hardware, Software, Firmware usw.)“, die sich mit einem Netz verbinden kann, „einschließlich Server, Desktop- und Laptop-Computer, Drucker, Mobiltelefone, IoT-Geräte, Netzausrüstung und mehr“. Hierbei ist zunächst unwesentlich, ob die Geräte direkt durch die Bundesverwaltung verwaltet werden, oder es sich um externe Geräte handelt (beispielsweise im Rahmen von „Bring Your Own Device“).[47]

Architekturdimension – Identitäten im Kontext der IT des Bundes: Eine Identität im Kontext der IT des Bundes bezieht sich auf ein „Attribut oder eine Gruppe von Attributen, die einen Benutzer oder eine Entität“ einer Bundesbehörde oder externen Kooperationseinrichtung „eindeutig beschreiben, einschließlich nicht-personenbezogener Entitäten“.[48]

Architekturdimension – Netze im Kontext der IT des Bundes: Ein Netz im Kontext der IT des Bundes bezieht sich auf ein „offenes Kommunikationsmedium, einschließlich typischer Kanäle“ wie interne Behördennetze, Weitverkehrsnetze des Bundes, „drahtlose Netze und das Internet umfasst sowie andere potenzielle Kanäle wie Mobilfunk und anwendungsspezifische Kanäle, die zur Übertragung“ von Daten verwendet werden.[49]

---

[45] Übersetzt und angelehnt an das Zero Trust Reifegradmodell der CISA (2023), Seite 23
[46] Übersetzt und angelehnt an das Zero Trust Reifegradmodell der CISA (2023), Seite 26
[47] Übersetzt und angelehnt an das Zero Trust Reifegradmodell der CISA (2023), Seite 16
[48] Übersetzt und angelehnt an das Zero Trust Reifegradmodell der CISA (2023), Seite 13
[49] Übersetzt und angelehnt an das Zero Trust Reifegradmodell der CISA (2023), Seite 20

Cybersicherheit: Cybersicherheit betrifft die Sicherheit aller Aspekte der Informations- und Kommunikationstechnik und erstreckt sich auf den gesamten Cyberraum. Dieser umfasst alle mit dem Internet und ähnlichen Netzen verbundenen Technologien sowie die darauf basierende Kommunikation, Anwendungen, Prozesse und Informationen.[50]

Cybersicherheitsarchitektur: Die Cybersicherheitsarchitektur eines Landes umfasst alle Akteure - Behörden, Plattformen, Organisationen - die laut nationaler Cybersicherheitspolitik zum Ökosystem gehören.[51]

Datenschutz: Zielt auf den Schutz der Rechte und Freiheiten von Personen bei der Verarbeitung ihrer personenbezogenen Daten ab. Datenschutzrisiken werden daher stets aus der Perspektive der betroffenen Personen betrachtet. Verarbeitungen müssen rechtmäßig, nach Treu und Glauben, nachvollziehbar, zweckgebunden, auf das notwendige Maß beschränkt, auf der Basis richtiger Daten und die Integrität und Vertraulichkeit wahrend erfolgen. Zusätzlich dürfen personenbezogene Daten in der Regel nur so lange in einer Form gespeichert werden, die eine Identifizierung der betroffenen Personen erlaubt, wie dies erforderlich ist. Die Einhaltung dieser Grundsätze muss nachweisbar sein. [52]

DDoS: Bei DDoS-Angriffen (Distributed Denial of Service) werden von vielen verschiedenen Quellen aus koordinierten Anfragen an ein Ziel gesendet, um dessen Dienste durch Überlastung außer Betrieb zu setzen.[53]

Föderiertes System: Ein föderiertes System übergreift separierte Systeme (Netz, Applikationen, Daten, Identitäten), wie bspw. den Systemen verschiedener Bundesministerien und nachgeordneter Behörden oder föderale Systeme. Um den Datenaustausch zu ermöglichen, werden Compliance-Regeln übergreifend eingehalten und überwacht.

Informationssicherheit: Informationssicherheit zielt auf den Schutz von Informationen ab, die auf Papier, in IT-Systemen sowie auf Datenträgern oder im Gedächtnis gespeichert sind. Dabei stehen u. a. die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit im Vordergrund.[54]

IT-Sicherheitsarchitektur: Eine IT-Sicherheitsarchitektur bildet aus Richtlinien, Technologien und Kontrollmechanismen einen Rahmen, um den gewünschten IT-Sicherheitszustand eines Systems zu erreichen. Die IT-Sicherheitsarchitektur legt klare Prozesse und Verantwortlichkeiten fest und sorgt dafür, dass alle Sicherheitsmaßnahmen kohärent und effektiv zusammenwirken, um den Zustand der IT-Sicherheit zu erreichen. Dieser Zustand der IT-Sicherheit zielt darauf ab, Risiken durch Bedrohungen und Schwachstellen in der IT zu

[50] vgl. Glossar des Positionspapiers zu Cybersicherheit für Weltrauminfrastrukturen des BSI (2022), Seite 16
[51] vgl. Glossar des Positionspapiers zu Cybersicherheit für Weltrauminfrastrukturen des BSI (2022), Seite 16
[52] Angelehnt an das Standarddatenschutzmodell der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz 2024)
[53] vgl. Artikel des BSI zu DoS- und DDoS-Attacken (2024)
[54] vgl. Glossar des Positionspapiers zu Cybersicherheit für Weltrauminfrastrukturen des BSI (2022), Seite 16

minimieren und die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen.[55]

Phishing: Beim Phishing werden E-Mails an das Opfer versendet, das dazu gebracht werden soll, einen maliziösen Link anzuklicken oder schutzbedürftige bzw. vertrauliche Daten wie Passwörter oder Transaktionsnummern (TANs) preiszugeben.[56] Phishing beschränkt sich dabei nicht nur auf konventionelle E-Mails, sondern kann auch per SMS, Telefon oder QR-Code stattfinden.[57]

Ransomware: Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese IT-Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom“) wieder freigeben.[58]

Spam: Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung. Häufig enthalten Spam-Nachrichten jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder sie werden für Phishing-Angriffe genutzt.[59]

[55] Angelehnt an die Definition zu IT-Sicherheit im Glossar des Positionspapiers zu Cybersicherheit für Weltrauminfrastrukturen des BSI (2022), Seite 16
[56] vgl. Verfassungsschutzbericht 2023 (2024), Seite 315
[57] vgl. Artikel des BSI zu Phishing (2024)
[58] vgl. Verfassungsschutzbericht 2023 (2024), Seite 317
[59] vgl. Die Lage der IT-Sicherheit in Deutschland 2023 (2023), Seite 92

Abbildungs-verzeichnis

Abkürzungs-verzeichnis

APT – Advanced Persistent Threats

BMDS – Bundesministerium für Digitales und Staatsmodernisierung

BMI – Bundesministerium des Innern

BSI – Bundesamt für Sicherheit in der Informationstechnik

CISA – Cybersecurity and Infrastructure Security Agency

DDOS – Distributed Denial of Service

DVC – Deutsche Verwaltungscloud

DSGVO – Datenschutz-Grundverordnung

IoT – Internet of Things

NdB – Netze des Bundes

NIS-2 – Network and Information Security Directive

NIST – National Institute of Standards and Technology

Literaturverzeichnis

Auswärtiges Amt. (Juni 2023). Nationale Sicherheitsstrategie. Berlin.

Bundesamt für Sicherheit in der Informationstechnik. (02. August 2022). Cybersicherheit für Weltrauminfrastrukturen. Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik. (26. 06. 2023). Positionspapier Zero Trust 2023. Bundesamt für Sicherheit in der Informationstechnik. Von Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik. (2023). Die Lage der IT-Sicherheit in Deutschland 2023. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

Bundesamt für Sicherheit in der Informationstechnik. (05.09.2022). Mindeststandard des BSI für Mobile Device Management. Von Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mobile_Device_Management/Mobile_Device_Management_node.html

Bundesamt für Sicherheit in der Informationstechnik. (08. April 2024). DoS- und DDoS-Attacken. Abgerufen am 24. Juli 2024 von Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service.html

Bundesgesetzblatt (05.12. 2025). Bundesgesetzblatt Teil I - Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung - Bundesgesetzblatt

Bundesamt für Sicherheit in der Informationstechnik. (01. 03. 2024). EU-Richtlinien zur Netzwerk- und Informationssicherheit. Abgerufen am 16. 07 2024 von Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinien/nis-richtlinie_node.html

Bundesamt für Sicherheit in der Informationstechnik. (23. Juli 2024). Phishing - how much is the phish!? Von https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html

Bundesministerium des Innern und für Heimat. (Juni 2022). Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Berlin.

https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=5

Bundesministerium des Innern und für Heimat. (02. November 2023). Flexibles Arbeiten. Von Bundesministerium des Innern und für Heimat: https://www.bmi.bund.de/DE/themen/oeffentlicher-dienst/arbeiten-in-der-bundesverwaltung/flexibles-arbeiten/flexibles-arbeiten-artikel.html

Bundesministerium des Innern und für Heimat. (2. November 2023). IT-Konsolidierung des Bundes. Von https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/it-konsolidierung/it-konsolidierung-node.html

Bundesministerium des Innern und für Heimat. (2024). Verfassungsschutzbericht 2023. Berlin: Bundesministerium des Innern und für Heimat.

Bundesministerium des Innern, für Bau und Heimat. (Juni 2018). Eckpunkte einer Netzstrategie 2030. Berlin: Der Beauftragte der Bundesregierung für Informationstechnik.

Bundesministeriums des Innern und für Heimat. (21. Mai 2024). Deutsche Verwaltungscloud. Der Beauftragte der Bundesregierung für Informationstechnik: https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/deutsche-verwaltungscloud-strategie/deutsche-verwaltungscloud-strategie-node.html

Cybersecurity and Infrastructure Security Agency. (April 2023). Zero Trust Maturity Model.

Executive Office of the President - Office of Management and Budget. (26. Januar 2022). Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. Memorandum for the Heads of Executive Departments and Agencies. Washington D.C.

Informationstechnikzentrum Bund. (März 2023). ITZBund IT-Strategie. Bonn: Informationstechnikzentrum Bund.

National Institute of Standards and Technology. (August 2020). Zero Trust Architecture. NIST Special Publication 800-207. U.S. Department of Commerce.

NATO Secretary. (23. 11. 2023). NATO Zero Trust Policy. Sweden: North Atlantic Council. Referenziert in: "Control Board (C3B) approves Digital Transformation Implementation Strategy". Abgerufen am 04. Oktober 2024 von NATO.int: https://www.nato.int/cps/en/natohq/news_214878.htm

Statistisches Bundesamt. (11. Juli 2023). Knapp ein Viertel aller Erwerbstätigen arbeitete 2022 im Homeoffice. Abgerufen am 18. Juli 2024 von Statistisches Bundesamt: https://www.destatis.de/DE/Presse/Pressemitteilungen/Zahl-der-Woche/2023/PD23_28_p002.html

Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung - Bearbeitungsstand: 25.07.2025 12:08

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung*)

Datenschutzkonferenz. (2024). Das Standard-Datenschutzmodell.

https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V3_1.pdf

VS – Anforderungsprofil Digitales Labelling

BSI-VS-AP-0023.pdf

ETSI TR 103 937 V1.1.1 (2024-08) - Cyber Security (CYBER); Cyber Resiliency and Supply Chain Management

TR 103 937 - V1.1.1 - Cyber Security (CYBER); Cyber Resiliency and Supply Chain Management

BSI - Produktzertifizierung: Programm IT-Sicherheitszertifizierung Common Criteria (CC)

CC-Produkte Version 4.3 vom 01.04.2025

Impressum

Herausgeber
Bundesministerium für Digitales und Staatsmodernisierung, 10557 Berlin
Internet: http://www.bmds.bund.de/

Stand
Dezember 2025

Weitere Publikationen der Bundesregierung zum
Herunterladen und zum Bestellen finden Sie unter:

http://www.publikationen-bundesregierung.de/

Bundesministerium
für Digitales und
Staatsmodernisierung

#WirMachen

bmds.bund.de