Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Positionspapier Zero Trust 2023

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.12	26.06.2023	TK12	Erstveröffentlichung

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: zero-trust@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

Management Summary

Zero Trust beschreibt ein aus dem „Assume Breach“-Ansatz entwickeltes Architekturdesign-Paradigma, welches im Kern auf dem Prinzip der minimalen Rechte (engl. „Least Privileges“) aller Entitäten (Nutzer, Geräte, Systeme, ...) in der Gesamtinfrastruktur (auf allen Ebenen) basiert. Durch Umsetzung von Zero Trust-Prinzipien lassen sich vorranging Anwendungszugriffe in einer IT-Infrastruktur robuster gegen verschiedenartige Angriffe gestalten und so die Resilienz der Daten und der von diesen abhängigen Geschäftsprozessen steigern. Durch die kritische Hinterfragung des bisher oftmals gesetzten impliziten Vertrauens in Entitäten innerhalb des internen Netzes werden bisher nicht betrachtete Risiken für die IT-Infrastruktur transparent. Hierdurch können dann auch entsprechende Gegen- und Härtungsmaßnahmen abgeleitet werden, die - abhängig vom Vertrauen - nur die notwendigen Zugriffe einräumen. Schwachstellen in der IT-Infrastruktur und Angriffe können durch diese Prinzipien früher sichtbar gemacht werden, um diese bei Zugriffsentscheidungen automatisch zu berücksichtigen und mögliche Schäden zu begrenzen. In der Regel steht beim Einsatz von Zero Trust Mechanismen der Schutz der Integrität und Vertraulichkeit der Daten der Geschäftsprozesse einer Organisation im Fokus und nicht die Verfügbarkeit der Geschäftsprozesse selbst.

Das Architekturdesign-Paradigma ist kein definierter Standard, der sich mit Hilfe von einzelnen Produkten vollumfänglich realisieren ließe. Hierdurch gestaltet sich die Interoperabilität von Produktfunktionalitäten aufwendig. Das Paradigma liefert vielmehr Leitprinzipien für Prozesse, Identitäten, den Aufbau von Systemen und die Interaktion dieser. Die Leitprinzipien können genutzt werden, um aus ihnen bedarfsgerechte Maßnahmen für den Schutz der Daten der eigenen Geschäftsprozesse in der IT-Infrastruktur abzuleiten. Dies erfordert folglich eine ganzheitliche Betrachtung der IT-Sicherheit der gesamten Organisation und damit auch die Mitarbeit von weiteren Organisationseinheiten neben der originären IT-Bereiche und dem Management für Informationssicherheit (ISMS). Bestehen Bestrebungen oder Notwendigkeiten einer stärkeren Zusammenarbeit über Organisationsgrenzen hinweg, sind neben individuellen Ansätzen auch organisationsübergreifende Zero-Trust-Architekturen zu betrachten.

1 Kernbotschaften

- Durch Zero Trust-Ansätze können Anwendungszugriffe besser präventiv abgesichert werden und insbesondere das Schadensausmaß von Angriffen weiter reduziert werden.
- Zero Trust vereint bekannte Sicherheitsmaßnahmen und Best-Practices, deren Umsetzung aufgrund der gestiegenen Bedrohungslage immer wichtiger wird, in einem ganzheitlichen Ansatz.
- Die Schutzwirkung bezieht sich vorrangig auf die Schutzziele Integrität und Vertraulichkeit und nicht Verfügbarkeit.
- Eine ganzheitliche, wirksame Umsetzung von Zero Trust-Prinzipien ist ein langfristiges Vorhaben und erfordert ebenso hohen wie dauerhaften finanziellen sowie personellen Ressourcenaufwand.
- Bei einer organisationsübergreifenden Vernetzung müssen die Zero Trust-Konzepte ggf. organisationsübergreifend verbindlich abgestimmt werden.
- Die Interoperabilität von Produktfunktionalitäten ist für eine erfolgreiche Zero Trust-Umsetzung elementar und stellt heute, u.a. aufgrund fehlender Standardisierungen, noch eine große Herausforderung dar.

2 Einleitung

Der Begriff „Zero Trust“ findet derzeit sowohl im Bereich der konzeptionellen und architekturellen Betrachtungen als auch bei Produkt- und Herstellerspezifischen Darstellungen Verwendung. Das Verständnis des Begriffs ist dabei jedoch nicht immer deckungsgleich. Dies erschwert es, einen ganzheitlichen Überblick - u.a. bzgl. der tatsächlichen Umsetzbarkeit der grundlegenden, konzeptionellen Ansätze - zu erlangen und in der weiteren Diskussion mit unterschiedlichen Beteiligten einheitlich zu verwenden. Insbesondere die kontextspezifischen, dynamischen Zugriffsrichtlinien sind konzeptionell noch verhältnismäßig neue Ansätze. Eine ganzheitliche Umsetzung in allen Bereichen der IT-Infrastruktur ist u.a. aufgrund bisher fehlender Standardisierungen und Produktverfügbarkeiten derzeit noch unrealistisch. Die Produkte, die von verschiedenen Herstellern unter dem Label „Zero Trust“ beworben werden, stellen derzeit lediglich einen Teil der Funktionalität einer idealen Zero Trust-Architektur zur Verfügung. Dennoch lässt sich die Resilienz gegen Angriffe auf die eigene IT-Bestandsinfrastruktur auch heute schon durch die Integration von Zero Trust-Prinzipien gezielt stärken. Ein Grundverständnis des Zero Trust-Ansatzes ist hierfür zwingende Voraussetzung. Das vorliegende Dokument hat daher das Ziel, diese konzeptionellen Grundlagen aus Sicht des BSI zu vermitteln, eine Diskussionsgrundlage bereitzustellen und erste Ansätze für die Umsetzung einzelner Aspekte zu skizzieren. Ergänzend werden erste organisationsübergreifende Zero Trust-Ansätze betrachtet.

3 Motivation

Bisherige, traditionelle Sicherheitsarchitekturbetrachtungen konzeptionieren für eine Organisation klassisch unterschiedlich vertrauenswürdige Netzzonen. Die Segmentierung und der Zugriff in die jeweiligen Zonen erfolgt in der Regel mehrschichtig über Firewalls und von extern, ggf. auch unter Verwendung von Virtual Private Networks (VPNs). Ein häufig vorzufindendes Beispiel ist die Unterteilung in eine demilitarisierte Zone (DMZ) mit direkter Anbindung an das Internet und das interne Netz. Dabei gilt die DMZ, in der sich u.a. aus dem Internet erreichbare Webserver befinden können, als weniger vertrauenswürdig als die interne Zone, in der sich Arbeitsplatzrechner der Beschäftigten und organisationsinterne Fachverfahren finden. Diese Zonensegmentierung folgt den Ansätzen des „Defense in Depth“ und ist als Analogie vergleichbar mit einer Zonierung, wie sie früher physisch beim Bau und der Absicherung einer Burgfestung vorgenommen wurde, wobei mehrschichtige Komponenten und die gezielte Regulierung von Zugangspunkten den ungewollten Zugang zum Inneren erschwerten. Diese im Fokus zonenbasierte Absicherung der eigenen IT-Landschaft hat seit vielen Jahren Bestand und gilt seit langem als Standard für den Aufbau von sicheren Infrastrukturen. Dementsprechend basieren heutzutage viele Sicherheitskonzepte vorrangig hierauf.

Durch die Entwicklungen der letzten Jahre sind neue Risiken entstanden, die in den bisherigen Sicherheitskonzepten in dem Umfang (noch) nicht berücksichtigt wurden. Diese sind sowohl der gestiegene Vernetzungsbedarf, auch über Organisationsgrenzen hinweg, als auch die verstärkte Integration von externen Diensten in internen Geschäftsprozessen. Hierdurch werden sicherheitsrelevante Kommunikationsbeziehungen immer komplexer und bieten eine vergrößerte Angriffsfläche. Außerdem haben sich in der Breite Angreifende in den genutzten Techniken weiterentwickelt, sodass die ungezielte Kompromittierung eines einzelnen internen Arbeitsplatzrechners häufig mit verhältnismäßig geringem Aufwand zu einer vollständigen Kompromittierung der gesamten IT-Infrastruktur führt. Weitergehende, moderne Absicherungskonzepte, bspw. nach dem „Assume Breach“-Ansatz, werden genutzt, jedoch fehlt es häufig an der stringenten Umsetzung notwendiger, vor allem umfassender Absicherungen innerhalb der als vertrauenswürdig definierten Zonen. Da man sich fälschlicherweise durch die Segmentierung des internen Netzes sicher(er) fühlt, werden dort vielfach keine oder nur geringe Sicherheitsmaßnahmen etabliert. Interne Netze sind nicht auf die frühzeitige Erkennung von Schwachstellen sowie die Erkennung deren Ausnutzung ausgelegt. Das Vertrauen in die Sicherheit des internen Bereichs liegt dabei primär im Schutz durch den Perimeter. Gleichzeitig erfordern sowohl die Ermöglichung von Vernetzung über Organisationsgrenzen hinweg als auch die verstärkte Nutzung von externen Diensten Sicherheitsfunktionen des Netzperimeters, für die dieser in der Regel nicht ausgelegt ist. Beispielsweise führt das Einbinden eines externen Dienstes mittels Ende-zu-Ende-Verschlüsselung oder proprietärer Protokolle in die lokale Sicherheitsinfrastruktur zu einem sicherheitstechnischen „Kurzschluss“ des Perimeterschutzes. Dadurch wird der bisherige Grundsicherheitspfeiler der klassischen Architektur, der Perimeter, aufgeweicht. Um diesen veränderten Anforderungen gerecht werden zu können - ohne durch den weiter aufweichenden Perimeter die gesamte interne Infrastruktur zu gefährden - haben sich verschiedene alternative Absicherungskonzepte abseits des reinen Perimeterschutzes und des Zonierungsansatzes entwickelt. Diese führten letztendlich zu der Erkenntnis, dass eine grundlegend andere Betrachtung bei der Absicherung von Infrastrukturen und der in ihnen übertragenen, verarbeiteten und gespeicherten Daten notwendig ist.

Die Herausforderungen bei der Absicherung von IT-Infrastrukturen sind vielfältig und erfordern, um der Komplexität möglichst effektiv begegnen zu können, ein strukturiertes Vorgehen. Dies gilt insbesondere bei Absicherungsansätzen, bei denen sich Maßnahmen sowohl über mehrere technische als auch prozessuale Bereiche einer oder mehrere Organisationen erstrecken. Aus diesem Grund wird in diesem Dokument ein erster Ansatz in Form eines Zero Trust-Integrationsmodells vorgestellt, mit dem Ziel die für die Integration von Zero Trust-Prinzipien relevanten IT-Infrastrukturbereiche zu identifizieren und notwendige Maßnahmen sinnvoll zu strukturieren.

4 Historie

Der Begriff "Zero Trust" wurde das erste Mal 1994 von Stephen Paul Marsh in seiner Dissertation "Formalising Trust as a Computational Concept" definiert. 2003 hat das Jericho Forum - eine Gruppe aus CISOs (Chief Information Security Officers) verschiedener großer Unternehmen sowie staatlicher und wissenschaftlicher Organisationen - den Begriff "de-perimeterization" geprägt. Sie beschäftigten sich schon damals mit der Fragestellung, wie Informationssicherheit in komplexen IT-Architekturen, in denen Netzgrenzen zunehmend verschwimmen und klassische Perimeter-orientierte Sicherheitskonzepte nicht mehr ausreichen, gewährleistet werden kann. Der Begriff "de-perimeterization" bezeichnet dabei das Verschwinden von Netzgrenzen. Sie schlussfolgerten, dass interne Netze neben Firewalls weitere Absicherungsmechanismen im Sinne eines "Defense in depth"-Ansatzes benötigen.

2010 hat der Forrester Analyst John Kindervag den Begriff "Zero Trust" in seinem heute häufig referenzierten Whitepaper "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security" aufgegriffen. Dieses Whitepaper fasst die Ideen, die zu der Zeit bereits in Fachkreisen, u.a. angestoßen durch das Jericho Forum, diskutiert wurden, in einem Zero Trust-Modell zusammen. Dieses sieht vor, dass die Komponenten innerhalb eines Netzeswerks zunächst analysiert werden müssen, um das Vertrauen in sie ermitteln zu können, bevor ihnen Zugriff auf Ressourcen gewährt wird. Forrester hat dieses Konzept über die Jahre weiterentwickelt und 2019 das "Zero Trust eXtended" (ZTX) Framework veröffentlicht, welches sowohl die Daten, die Geschäftsprozesse als auch die Identitäten als zentrale Komponenten eines Zero Trust-Modells definiert.

Google startete etwa 2010 nach einem spezialisierten und gezielten Angriff auf ihre Infrastruktur (Operation Aurora) mit einer Initiative, die eigene Infrastruktur nach Zero Trust-Prinzipien umzugestalten Die Konzeptionierung der Zero Trust-Architektur mit dem Namen "BeyondCorp" sah dabei vor, dass der Netzperimeter des Unternehmens vollständig aufgehoben wird und kein vertrauenswürdiges internes Netz mehr existiert. Dies hat Google größtenteils realisiert und Details hierzu 2014 in mehreren Forschungsberichten veröffentlicht, die auf großes Interesse stießen. Im selben Jahr stellte die Cloud Security Alliance die Software Defined Perimeter (SDP) Architektur mit mehreren Deploymentmodellen vor. Die Architektur an sich ist dabei neu, baut aber auf bekannten Sicherheitsmaßnahmen auf. Sie hat große Schnittmengen mit dem durch Google verfolgten Ansatz BeyondCorp und Zero Trust-Prinzipien im Allgemeinen.

Einen weiteren Fokus auf den Themenkomplex Zero Trust legte 2019 das US National Institute of Standards and Technology (NIST), indem es eine Special Publication (SP) zu "Zero Trust Architecture" [1] veröffentlichte. Diese erläutert logische Architekturansätze und Zero Trust-Prinzipien für verschiedene Infrastrukturen (bspw. on-premises, hybrid, cloud-only, multi-cloud-only). Dabei orientierte NIST sich teilweise an den Ansätzen der Cloud Security Alliance für die SDP-Architektur. So finden sich bspw. starke Ähnlichkeiten zwischen der SDP-Architektur und der von NIST präsentierten logischen "enclave-based" Architektur. Im Anschluss an diese Veröffentlichung wurde in einem Teil des NIST, dem US National Cybersecurity Center of Excellence (NCCoE), ein Projekt zur Realisierung solcher Architekturansätze gestartet. Dabei werden in einer Gruppe bestehend aus Beauftragten von Unternehmen, staatlichen und wissenschaftlichen Institutionen gemeinsam konkrete Umsetzungsbeispiele erarbeitet. Die Umsetzungen erfolgen dabei unter Verwendung von bereits auf dem Markt verfügbaren Produkten und unter Berücksichtigung der definierten Standards und "Best Practices".

In den letzten zwei Jahren haben insbesondere US-amerikanische Behörden, u.a. durch eine Forderung nach der Umsetzung von Zero Trust-Architekturen in der Executive Order 14028 von Präsident Biden, den Themenkomplex aufgegriffen und weiter ausgearbeitet. Die Cybersecurity and Infrastructure Security Agency (CISA) hat bspw. Ende 2021 das "Zero Trust Maturity Model" [2] veröffentlicht. In diesem wird eine mögliche Roadmap für US-amerikanische Behörden erläutert, welche bei der Entwicklung einer individuellen Zero Trust-Strategie, also der Umsetzung der Executive Order 14028, unterstützen soll. Das Maturity Modell enthält insgesamt fünf Kern- und drei Querschnittsbereiche, welche von CISA jeweils

nochmal in "traditionelle", "fortgeschrittene" und "optimale" Umsetzungsmöglichkeiten von Zero Trust-Architekturansätzen eingeteilt werden. Aufbauend auf der Executive Order 14028 und CISAs "Zero Trust Maturity Model" hat die US-amerikanische Behörde Office of Management and Budget (OMB) eine "Federal Zero Trust Strategy" veröffentlicht. Das Ziel dieses Dokuments ist es, den US-amerikanischen Behörden eine gemeinsame Baseline für den ersten Schritt in Richtung Umsetzung von Zero Trust-Prinzipien zu geben.

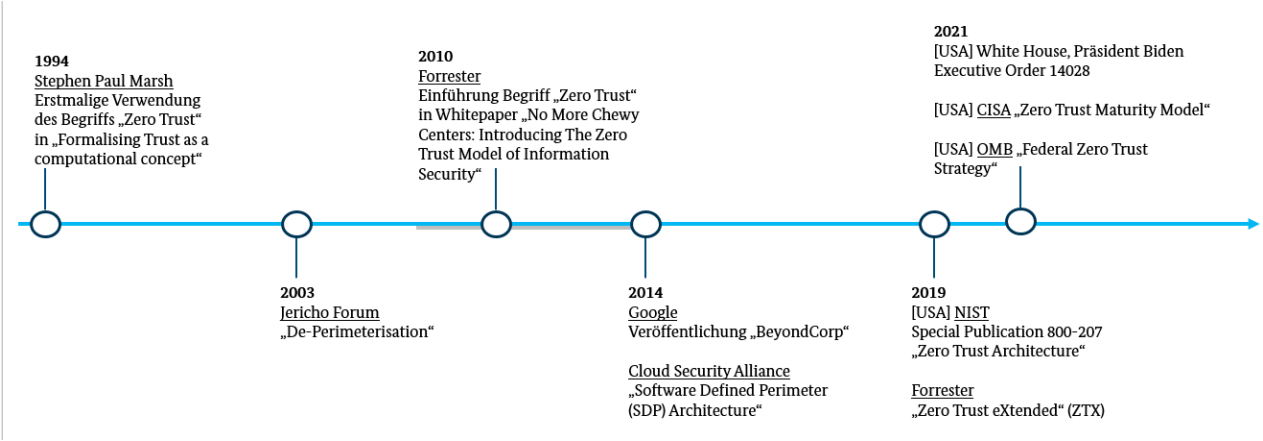

Abbildung 1- Zeitlinie Zero Trust Begriff

Die ganzheitliche Betrachtung in Form einer Zero Trust-Architektur an sich ist ein neuer Ansatz, welcher jedoch auf bereits bewährten Sicherheitsmaßnahmen aufbaut. Das heißt, viele Aspekte einer Zero Trust-Architektur sind singulär betrachtet schon länger bekannte und empfohlene Sicherheitsmaßnahmen (bspw. das Prinzip der minimalen Rechte und eine Mikrosegmentierung des internen Netzes). Neu in einer Zero Trust-Betrachtung ist der holistische Ansatz, in welchem diese Sicherheitsmaßnahmen, mit einem Fokus auf den Schutz der Daten bedarfsgerecht kombiniert werden, um für jeden Zugriff auf die Daten einen zu jedem Zeitpunkt angemessen starken Vertrauensnachweis auf Basis von dynamischen Zugriffsrichtlinien, kontinuierlicher Überwachung und Risikoanalysen fortwährend ermitteln und bewerten zu können.

5 Definition Zero Trust

Der Begriff „Zero Trust“ beschreibt ein aus dem „Assume Breach“-Ansatz entwickeltes Architekturdesign-Paradigma, welches im Kern auf dem Prinzip der minimalen Rechte (engl. „Least Privileges“) aller Entitäten (Nutzer, Geräte, Systeme, ...) in der Gesamtinfrastruktur (auf allen Ebenen) basiert. Das heißt, es existiert kein implizites Vertrauen zwischen allen Entitäten.

Bei notwendiger Kommunikation von Entitäten muss ein Vertrauen durch verlässliche Nachweise und Prüfungen jedes Mal neu aufgebaut werden („earned trust“). Durch diese Designprinzipien und mit Hilfe von kontinuierlicher Vertrauensbetrachtung wird das Sicherheitsrisiko für Vertraulichkeit und Integrität minimiert. Einschränkungen bei der Verfügbarkeit werden dabei in Kauf genommen.

1. Aus dem fehlenden impliziten Vertrauen folgt, dass jede Entität sich authentisieren und autorisiert werden muss, um Zugriff auf Ressourcen zu erhalten. Dabei spielt vor allem starke Authentifizierung eine entscheidende Rolle.
2. Das Prinzip der minimalen Rechte bedeutet, dass nur die Entitäten Zugriff erhalten, die auch Zugriff benötigen. Dies bedingt, dass Ressourcen in möglichst kleine Einheiten unterteilt und Berechtigungen möglichst feingranular vergeben werden müssen. Der kleinere Radius beschränkt im Fall von böswilligem Zugriff den unkontrollierten Abfluss, die Manipulation von Daten und eine laterale Ausbreitung.
3. Bei der Betrachtung existiert keine Differenzierung von innerhalb oder außerhalb des eigenen Netzes mehr. Hierdurch wird das interne Netz immer als unsicher erachtet und das erteilte Vertrauen nie dauerhaft gewährt. Auf Basis von dynamischen Zugriffsrichtlinien, kontinuierlicher Überwachung und Risikoanalysen wird das Vertrauen fortwährend bewertet und über Zugriffe jeweils neu entschieden.

6 Referenzarchitektur nach NIST

Die der Definition zu entnehmenden Zero Trust-Prinzipien erzwingen nicht genau eine bestimmte Architektur. Sie sind vielmehr als Leitprinzipien für Prozesse, Identitäten, den Aufbau von Systemen und die Interaktion dieser zu sehen. Diese Leitprinzipien können genutzt werden, um aus ihnen bedarfsgerechte Maßnahmen für den Schutz der Ressourcen in der eigenen Infrastruktur abzuleiten. Eine Architektur nach Zero Trust-Prinzipien fokussiert dabei den Schutz der Ressourcen (v.a. Daten, Systeme, Anwendungen) und nicht - wie im klassischen Perimeter-Modell - den Schutz ganzer Netzsegmente an den internen Netzgrenzen. Dieser Fokus hat architekturell zur Folge, dass der Zugriffsschutz näher an die zu schützende Ressource selbst rückt und so die impliziten Vertrauenszonen verkleinert werden. Die Funktionen der Zugriffsentscheidung und deren Durchsetzung werden dabei durch eine oder mehrere Komponenten übernommen.

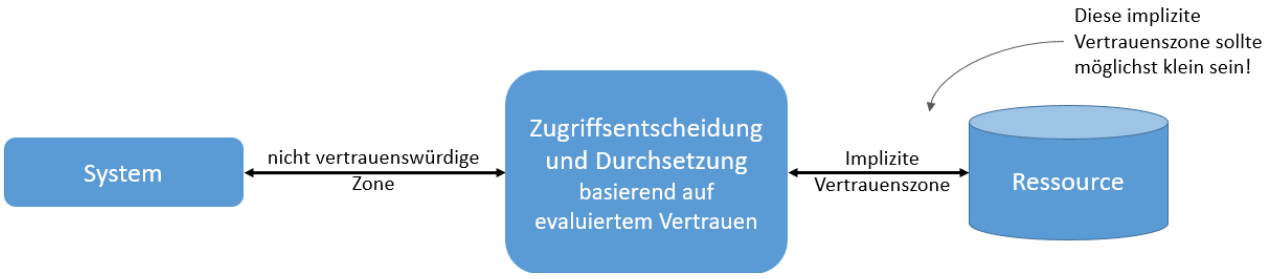

Abbildung 2 - Logische Musterarchitektur - Aufbau 01

Angelehnt an die logischen Architekturvorschläge des NIST aus der Veröffentlichung NIST Special Publication 800-207 "Zero Trust Architecture" [1] werden im folgenden logische Komponenten einer Zero Trust-Architektur eingeführt. Die daraus resultierende hier vorgestellte logische Musterarchitektur dient der Verdeutlichung der Prinzipien. Die konkrete Ausprägung der Integration der Zero Trust-Prinzipien, und damit auch die abgeleitete Architektur, ist dabei immer abhängig vom Bedarf der jeweiligen Organisation oder mehrerer zusammengeschlossener Organisationen mit einer einheitlichen, verbindlichen und globalen Architektur. In einem losen Verbund ist hingegen nur die Abstimmung der Schnittstellen nötig.

NIST spricht für die Funktionalität der Zugriffsentscheidung von sogenannten "Policy Decision Points" (PDP). Die PDP-Komponente stellt sicher, dass die Zugriffsanfrage valide ist. Der PDP (mit den beiden Teilkomponenten „Policy Adminstrator“ (PA) und „Policy Engine“ (PE)) kann dabei ein lokaler Bestandteil des Unternehmens oder ein extern gehosteter Dienst sein. Für die Evaluierung nutzt sie die Zugriffsrichtlinie der Organisation und erhält aus verschiedenen Quellen möglichst qualitativ hochwertige Informationen, auf deren Grundlage sie eine Bewertung des Vertrauensnachweises durchführt. Ist der Vertrauensnachweis stark genug, kann der PDP eine – möglicherweise eingeschränkte - Zugriffserlaubnis ausstellen und diese dem sogenannten „Policy Enforcement Point“ (PEP) mitteilen.

Der PEP sorgt im Anschluss für die Durchsetzung der Entscheidung, die der PDP getroffen hat. Diese beiden Komponenten (PDP und PEP) können gemeinsam als eine logische Komponente vor einer Ressource betrieben werden. In größeren Infrastrukturen skaliert dies häufig aber nur, wenn der PDP zentral betrieben wird, um die Zugriffsrichtlinien auf die Ressourcen zentralisiert verwalten zu können.

Zusätzlich sollte eine (logische und ggf. physische) Trennung zwischen der Kommunikation, die für die Kontrolle und die Konfiguration des internen Netzes notwendig ist, und der Kommunikation, die zur Nutzung von Anwendungen verwendet wird, erfolgen. Hierbei wird in Architekturen mit Zero Trust-Prinzipien des NIST von der "Control Plane" und der "Data Plane" gesprochen. Die Zero Trust-Prinzipien werden dabei nur in der "Data Plane" wirksam umgesetzt, während die "Control Plane", und damit die Administration der IT-Systeme, weiterhin vorwiegend auf Basis eines Perimeter-Modells abgesichert wird (vgl. Abbildung 3).

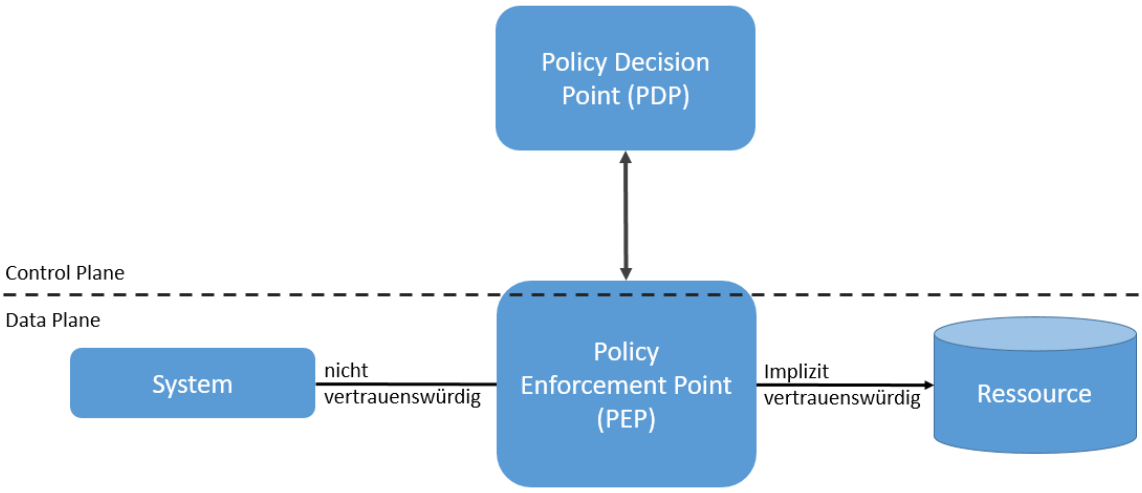

Abbildung 3 - Logische Musterarchitektur - Aufbau 02

Die qualitativ möglichst hochwertigen Informationen für die vom PDP vorgenommene Evaluierung des Vertrauens können aus unterschiedlichen Quellen hinzugezogen werden. Beispielsweise können zentrale Loganalysen zum Verhalten der zum Zugriff verwendeten Systeme, Informationen zum Gerätestatus oder aktuelle Bedrohungsinformationen in die Entscheidung mit einfließen. Hierbei gibt es keine festen Vorgaben, welche Informationen hinzugezogen werden müssen. Wichtig ist, dass der PDP eine gute, für die Organisation spezifisch relevante Informationsgrundlage zur Evaluierung erhält. Abbildung 4 zeigt beispielhaft Quellen, die für die Evaluierung des Vertrauens durch den PDP hilfreich sein könnten.

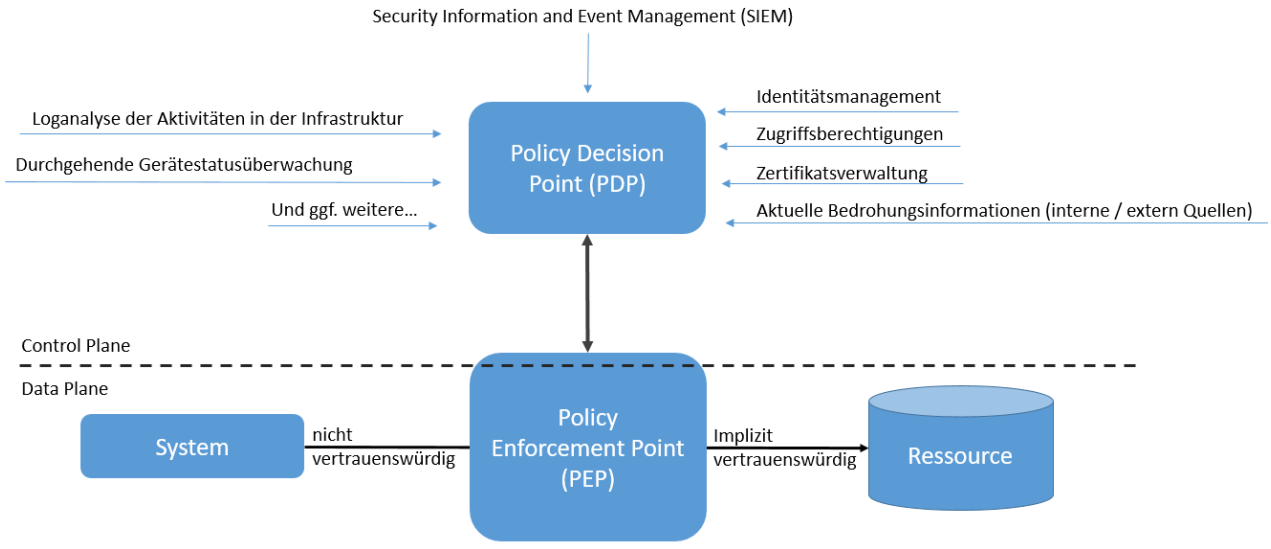

Abbildung 4 - Logische Musterarchitektur - Aufbau 03

Ein Ressourcenzugriff in einer logischen Zero Trust-Architektur soll im Folgenden an einem Beispielszenario verdeutlicht werden:

Eine Person möchte mit einem von der Organisation zur Verfügung gestellten System (bspw. einem durch die Organisation verwalteten Laptop) auf eine Unternehmensressource (bspw. eine Fachanwendung) zugreifen. Abbildung 5 visualisiert die Kommunikationsschritte. Dabei sind die aktiv für die Zugriffsentscheidung und -konfiguration beteiligten Komponenten farblich hervorgehoben.

1. Die Zugriffsanfrage wird vom lokalen PEP-Agenten auf dem Laptop entgegengenommen und an den PDP, konkret an die PDP Teilkomponente Policy Administrator (PA), weitergeleitet.
2. Der PA leitet die Anfrage zur Bewertung innerhalb des PDPs an die Policy Engine (PE) weiter.
3. Wenn die Anfrage durch die PE autorisiert wurde, konfiguriert der PA einen Kommunikationskanal zwischen dem PEP-Agenten und dem entsprechenden PEP-Gateway der Ressource. Die Konfiguration für diesen Kommunikationskanal enthält Informationen wie die IP-Adresse (Internet Protocol) des Systems, Portinformationen, Sitzungsschlüssel oder ähnliche Sicherheitsartefakte.
4. Der PEP-Agent und das PEP-Gateway der Ressource stellen dann eine Verbindung her, und der verschlüsselte Anwendungs-/Dienstdatenfluss beginnt. Die Verbindung zwischen dem PEP-Agenten und dem PEP-Gateway der Ressource wird beendet, wenn der Arbeitsablauf abgeschlossen ist, oder wenn der PA sie aufgrund eines Sicherheitsereignisses unterbindet (z.B. Session Zeitüberschreitung, fehlgeschlagene Neuauthentifizierung).

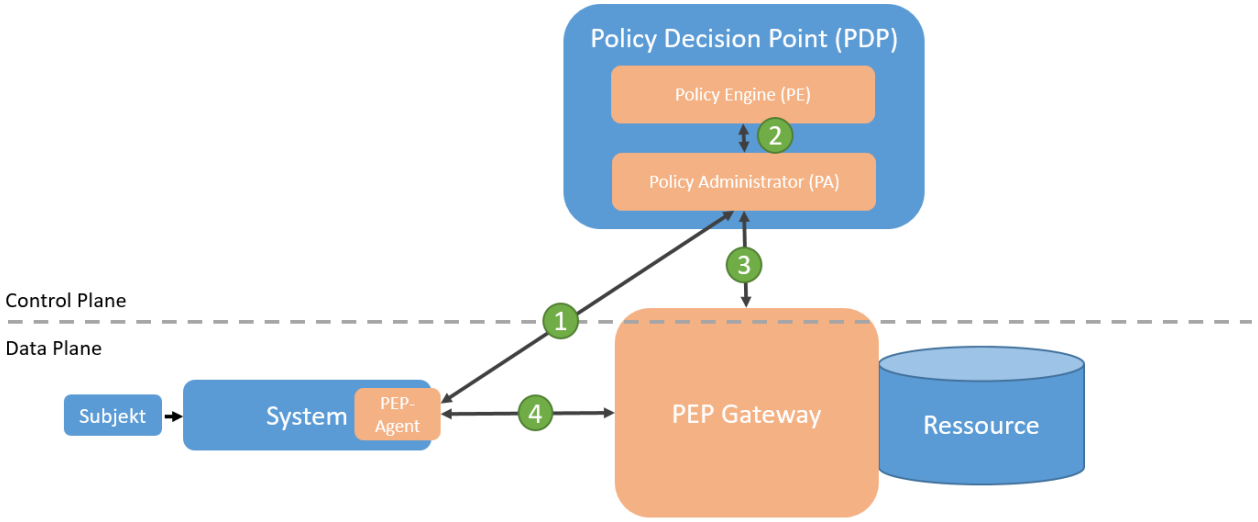

Abbildung 5 - Beispielablauf für einen Ressourcenzugriff

7 Integrationsmodell

Dieses Kapitel beschreibt einen möglichen Ansatz zur Integration von Zero Trust-Prinzipien in Bestandsumgebungen. Hierzu wird der Ansatz eines Zero Trust-Integrationsmodells eingeführt, welches nach fünf themenspezifischen Säulen strukturiert ist. Innerhalb jeder themenspezifischen Säule werden die Zero Trust-Prinzipien und ihre schrittweise Integration mit insgesamt drei Reifegraden erläutert. Dieses Integrationsmodell baut teilweise auf dem „Zero Trust Maturity Model“ der Cybersecurity and Infrastructure Security Agency (CISA) [2] auf und besteht aus insgesamt fünf Säulen mit den Querschnittsfunktionalitäten „Detektion“ und „Anforderungen an VS “.

Jede Säule enthält Funktionen, die bei einer Integration von Zero Trust-Prinzipien in Bestandsumgebungen zu berücksichtigen sind. Die querschnittlichen Aspekte der Funktion „Detektion & Reaktion“ finden sich in den vier Säulen „Identität“, „Gerät“, „Netz“ und „Anwendung“. Die querschnittlichen Aspekte der Funktion „Anforderungen an VS“ finden sich in jeder der fünf Säulen (vgl. Abbildung 6).

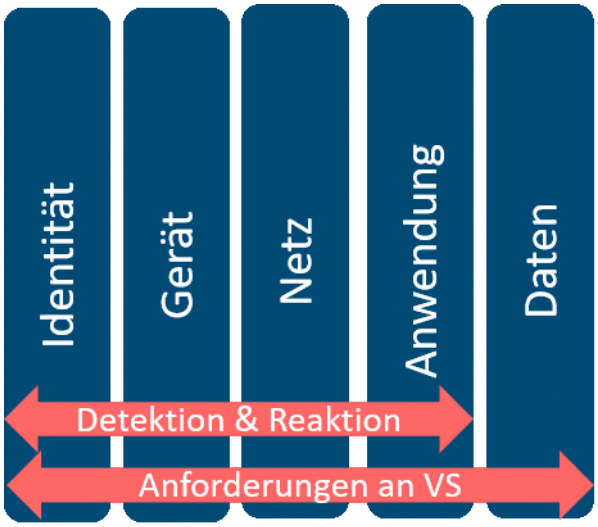

Abbildung 6 - Visualisierung der Säulen und Querschnittsfunktionen des Zero Trust Integrationsmodells

Abbildung 7 gibt eine Gesamtübersicht der säulenspezifischen als auch Querschnitts-Funktionen des Zero Trust-Integrationsmodells

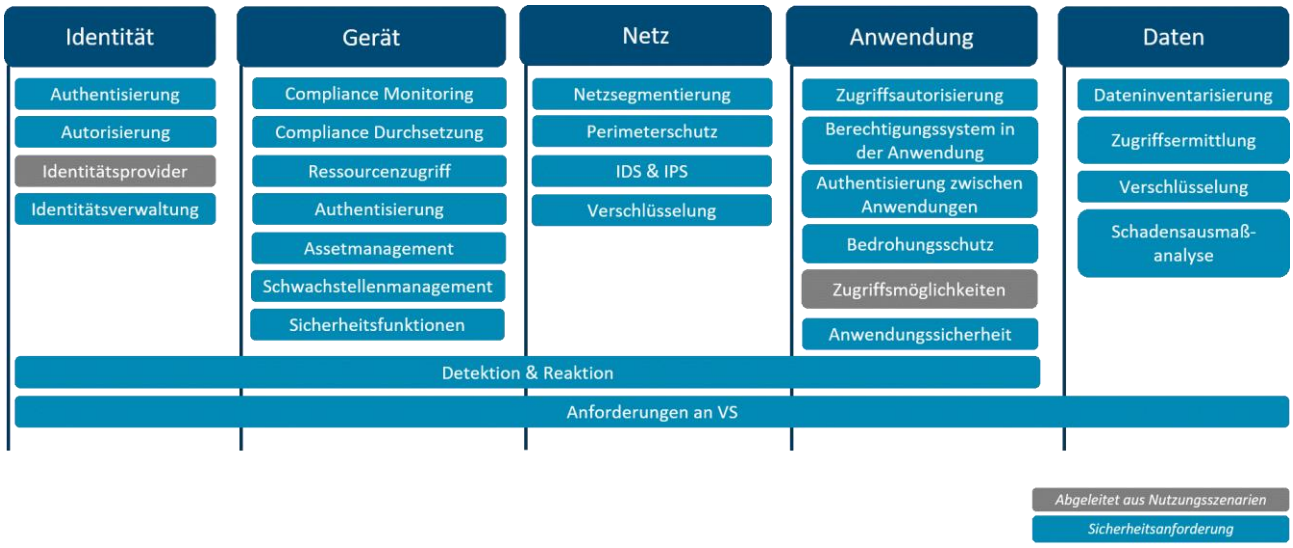

Abbildung 7 - Visualisierung der Säulen und Funktionen des Zero Trust-Integrationsmodell

Für jede Säule werden drei aufeinander aufbauende Reifegrade der Zero Trust-Integration betrachtet, die den Umsetzungsgrad von Zero Trust-Prinzipien in Bestandsumgebungen spezifizieren. Diese jeweiligen Abschnitte werden im Folgenden als Grundlage für die folgenden Maßnahmen grob wie folgt definiert:

- Klassisch (KL): In der Infrastruktur erfolgen hauptsächlich manuelle Konfigurationen und manuelle Zuweisungen von Attributen auf Grundlage von statischen Sicherheitsrichtlinien. Es existiert ein zentrales Identitätsmanagement, dieses wird allerdings nicht für die Verwaltung aller Identitäten in der Infrastruktur eingesetzt. Das Sicherheitsniveau für die Identifizierung und Authentifizierung von Entitäten ist (ohne Betrachtung weiterer netztechnischer Sicherheitsmaßnahmen) nicht durchgängig hoch bzw. hängt größtenteils von statischen Faktoren ab. In einzelnen Teilen wird das Least-Privilege-Prinzip bereits umgesetzt. Die Sichtbarkeit in/über die Infrastruktur ist in Teilen vorhanden, jedoch nicht ganz- und einheitlich umgesetzt. Die Incident Response- und Mitigationsprozesse sind größtenteils manuell.
- Fortschrittlich (FO): Es existieren einige säulenübergreifende Koordinationen, eine zentrale Sichtbarkeit in/über die Infrastruktur und ein zentrales Identitätsmanagement. Sicherheitsrichtlinien werden basierend auf Input und Output säulenübergreifenden durchgesetzt. Das Sicherheitsniveau für die Identifizierung und Authentifizierung von Entitäten ist in weiten Teilen (ohne die Notwendigkeit weiterer netztechnischer Sicherheitsmaßnahmen) hoch bzw. integriert bereits einige dynamische Faktoren und kontinuierliche (Re-)Authentifizierung, einige Incident Response Prozesse werden mit vordefinierten Mitigationen umgesetzt, in weiteren Teilen der Umgebung wird Least-Privilege bereits umgesetzt.
- Ideal (ID): Es existiert ein vollständig automatisiertes Zuweisen von Attributen zu Ressourcen, die dynamische Sicherheitsrichtlinien basieren auf automatisierten Triggern. Es existieren Maßnahmen, um eine Säulen-übergreifende Kompatibilität zu gewährleisten. Hierbei sind offene Standards hilfreich. Es existiert eine zentrale Sichtbarkeit in der Infrastruktur inkl. historischer Informationen. Es erfolgt ein dynamischer Zugriff auf Assets nach dem Prinzip der geringsten Rechte. Das Sicherheitsniveau für die Identifizierung und Authentifizierung von Entitäten ist durchgängig hoch und hängt nie ausschließlich von statischen Faktoren ab. Das Sicherheitsniveau der Identifizierung und Authentifizierung ist vollständig unabhängig von dem des Netzes. Das erforderliche Vertrauen in die Komponenten und Prozesse zur Identifizierung, Authentisierung, Authentifizierung etc. kann durch eine Zertifizierung oder vergleichbare Nachweise verbessert werden.

Jede der Säulen kann zunächst unabhängig von den anderen weiterentwickelt werden. Dies ermöglicht eine schrittweise Integration von Zero Trust Prinzipien in Bestandsumgebungen. Ressourcen (sowohl personell als auch finanziell) können bedarfsgerecht auf die jeweiligen Umsetzungen in verhältnismäßig kleinen Schritten geplant werden. Dort, wo Überschneidungen oder Abhängigkeiten zwischen den Säulen identifiziert werden, muss auf Kompatibilität geachtet werden. Inwieweit in jeder Funktion Zero Trust-Prinzipien umgesetzt werden sollen, muss für eine spezifische Architektur in einer anschließenden Bewertung festgelegt werden.

7.1 Voraussetzungen

Um eine ganzheitliche Umsetzung technischer Maßnahmen zu ermöglichen, müssen vor der Planung konkreter Maßnahmen die zu schützenden Ressourcen zunächst identifiziert werden. Insbesondere bei der Identifikation der zu schützenden Ressourcen aus den Geschäftsprozessen ist die Mitarbeit von weiteren Organisationseinheiten neben der IT und dem Management für Informationssicherheit (ISMS) notwendig. Folgende Aspekte sind Voraussetzung, damit eine schrittweise Umsetzung der Aspekte in einer klassischen Umgebung möglich wird:

1. **Identifizieren und priorisieren der zentralen Geschäftsprozesse der Organisation**
   Für Zero Trust-Architekturen wird dabei eine deutlich differenziertere Ausarbeitung der Geschäftsprozesse nötig, als sie derzeit in vielen Organisation vorliegt. Diese muss insbesondere die Kernprozesse einer Organisation abbilden, die über die Definition der unterstützenden Prozesse bspw. der IT hinausgehen.
2. **Identifizieren aller involvierten Parteien innerhalb der Organisation**
   Hierbei soll herausgearbeitet werden, welche Organisationseinheiten in den jeweiligen Geschäftsprozessen involviert sind. Dabei ergeben sich auch die Rollen, welche später u.a. als Grundlage für die Zugriffsentscheidungen des PDPs gegenüber konkreten Entitäten dienen.
3. **Identifizieren von weiteren Vorgaben**
   Bei der Umsetzung sind Vorgaben zu berücksichtigen, die sich aus Gesetzen, Verordnungen oder anderen Rechtseinflüssen ergeben können und ggf. Einfluss auf die umzusetzenden Maßnahmen bzw. deren Reihenfolge haben.
4. **Identifizieren aller involvierten Ressourcen (v.a. Daten, Systeme, Anwendungen) der Organisation**
   Nach der Erarbeitung der Geschäftsprozesse müssen aus diesen die involvierten Ressourcen abgeleitet werden. Dies ist insbesondere bei Zero Trust-Architekturen Voraussetzung, um im Folgenden feingranulare Zugriffsregeln festlegen zu können.
5. **Formulierung von Sicherheitsrichtlinien, die die Zero Trust-Maßnahmen enthalten**
   Diese Formulierungen sollen als Grundlage für spätere Zugriffsentscheidungen, welche Entitäten unter welchen Bedingungen auf die Ressourcen zugreifen dürfen, dienen. Aus diesen leiten sich dann maschinenlesbare Attribute ab, die bspw. im PDP ausgewertet werden können.
6. **Markterkundung**
   Ein ganzheitlicher Einsatz von Zero-Trust macht eine umfassende Markterkundung nach geeigneten Produkten nötig, denn nicht alle Produkte umfassen alle Zero-Trust-Funktionen. So ist zu Beginn detailliert zu prüfen, ob bestimmte Produkte überhaupt in einem Zusammenwirken einen ausreichenden Erfolg versprechen. Herstellerspezifische Kernkompetenzen können eventuell nur Teile des Gesamtbedarfes abdecken. So könnten sich Hersteller von Netzkomponenten eher auf die Verbindungsherstellung der Kommunikationsteilnehmer konzentrieren, ohne eine erweiterte Möglichkeit der parametrisierten Prüfung von Zugriffsrechten abzudecken. Andersherum sind Hersteller bestimmter Rechtezugriffsysteme eventuell nicht in der Lage, eine ausreichende Verbindungssteuerung innerhalb der Zero Trust Architektur zu etablieren.
7. **Priorisierung der Umsetzung**
   Dabei sind u.a. Aspekte wie die Abhängigkeit von Clientkomponenten bzw. dessen Sicherheitszustand, das Vorhandensein von adäquaten Loginformationen und (offenen) Protokollschnittstellen sowie notwendige Prozessänderungen zu berücksichtigen.

8 Bewertungen und Herausforderungen

8.1 Bewertung des ZTA-Paradigmas

Die Zero Trust-Prinzipien helfen die Anwendungszugriffe robuster gegen verschiedenartige Angriffe zu gestalten. Ihre Umsetzung verhindert Angriffe nicht vollständig, sie kann aber dazu beitragen, das Schadensausmaß verschiedenartiger Angriffe deutlich zu reduzieren. Durch die kritische Hinterfragung des bisher gesetzten impliziten Vertrauens in Entitäten innerhalb des internen Netzes werden bisher nicht betrachtete Risiken für die Anwendung und die hierin zu schützenden Daten transparent. Hierdurch können dann auch entsprechende Gegenmaßnahmen abgeleitet werden, die abhängig vom Vertrauen nur die notwendigen Zugriffe einräumen. Schwachstellen in der IT-Infrastruktur und Angriffe können durch diese Prinzipien früher sichtbar gemacht werden und es kann angemessen reagiert werden, um mögliche Schäden zu begrenzen. Durch die dadurch gesteigerte Resilienz der eigenen IT-Infrastruktur können Anwendungen auch außerhalb des Perimeters verstärkt genutzt oder integriert werden (z.B. auch von Dritten betriebene Anwendungen), sowie eigene Anwendungen breiter verfügbar gemacht werden, ohne dass das Sicherheitsniveau der gesamten Infrastruktur dadurch reduziert wird.

Wesentlicher Fokus des Zero Trust-Architekturparadigmas ist der Schutz der Vertraulichkeit und Integrität der Daten der Geschäftsprozesse einer Organisation. Die Datenverfügbarkeit wird nur indirekt durch eine Begrenzung des Schadensausmaßes adressiert. Beispielsweise kann die beabsichtigte massenhafte Verschlüsselung oder Löschung von Daten schnell erkannt, automatisch eingegrenzt und damit entsprechende Angriffe gestoppt werden. Jedoch verhindert die Anwendung der Zero Trust-Prinzipien keine Denial of Service (DoS)-Angriffe auf Geräte oder Anwendungen bzw. zugehörige Policy Enforcement Points (PEPs). Durch die funktionale Anforderung, die Anwendungen breit(er) erreichbar zu machen, entsteht ein größeres Risiko für DoS-Angriffe auf diese Anwendungen und die weiteren für den Zugriff benötigten Komponenten. Für diese Schutzfunktion wird daher langfristig, auch im idealen Zustand, eine zentrale Abwehr erforderlich bleiben.

Die zentralen Komponenten sind generell ein kritisches Element in jeder Infrastruktur, auch in einer Zero Trust-Infrastruktur. In der in Kapitel 6 vorgestellten Referenzarchitektur sind dies das zentrale Identitätsmanagement, der Policy Decision Point (PDP), die Zertifikatsverwaltung, Inventare und die zentrale Detektion, die besonders in allen drei Schutzzielen geschützt werden müssen und innerhalb einer Zero Trust-Implementierung eine besondere Vertrauensstellung haben. Sowohl in Bestandsinfrastrukturen als auch Infrastrukturen nach Zero Trust, stellen Schwachstellen in den entsprechenden Komponenten immer ein erhebliches Risiko dar. Durch die in der Regel größere Zentralisierung in Zero Trust-Architekturen ist dieses dort ggf. höher.

Die komplexeren Zugriffsregeln in einer Zero Trust-Infrastruktur führen dazu, dass für erfolgreiche Angriffe mehr Aufwand erforderlich wird. Beispielsweise reicht es in einer Bestandsinfrastruktur häufig aus Kontoname und Passwort zu kennen, um von einem beliebigen Client Zugriff auf ein erreichbares System zu erlangen. Dagegen könnten zukünftig weitere Kriterien wie der Zustand der verwendeten Geräte (Server & Client), Nutzerverhalten, Zugriffszeitpunkt und Authentisierungsstärke kontextspezifisch in die Zugriffsentscheidung einfließen. Diese Bedingungen müssen Angreifende zukünftig zunächst (er)kennen und im Angriffssinne manipulieren. Um auch solche komplexeren Angriffe zu erkennen, müssen die Detektionsmechanismen laufend angepasst werden.

Eine besondere Herausforderung bei der Erkennung von Angriffen stellen Innentäter dar, da diese zunächst einmal alle erforderlichen Berechtigungen im Rahmen ihrer Tätigkeit für den Zugriff auf Daten besitzen. Zero Trust-Prinzipien können nicht vollständig verhindern, dass Innentäter Daten ausleiten, können jedoch das Schadensausmaß begrenzen. Die Analyse des Nutzungsverhaltens kann dabei helfen ungewöhnliche Zugriffe zu erkennen, sodass diese eingeschränkt werden können. Außerdem sollte der Zugriff sowieso nur auf die für die jeweilige Tätigkeit notwendigen Daten gestattet werden, so dass hierdurch ebenfalls die Zugriffsmöglichkeiten eingeschränkt sind (Prinzip der minimalen Rechte).

8.2 Herausforderungen bei der Umsetzung

Dieses Kapitel erläutert einige der Herausforderungen bei der Umsetzung bzw. Integration von Zero Trust-Prinzipien in bestehende IT-Infrastrukturen anhand eines fiktiven Zugriffsszenarios auf eine Anwendung. Einige der Herausforderungen zur Umsetzung werden in diesen Beispielen bereits als erfolgreich etabliert angenommen. Insbesondere die Voraussetzungen einer detaillierten und umfassenden Dateninventarisierung sowie das Wissen der Organisation bzgl. notwendiger Datenkommunikation werden hier als gegeben angekommen. Das heißt, die Organisation weiß bereits u.a., welche Netzkommunikation zulässig ist, welche Entitäten Zugriff auf welche Ressourcen benötigen und, wo sich hochsensible Daten in der IT-Infrastruktur befinden. Solange eine Organisation die grundlegenden Voraussetzungen für die Integration von Zero Trust Prinzipien nicht erfüllt, ist die Wahrscheinlichkeit, dass Integrationsansätze scheitern bzw. die IT-Sicherheit ggf. sogar nachteilig beeinflussen werden hoch. Auch kann sich eine nicht ausreichend auf die Geschäftsprozesse der Organisation konzeptionierte und sinnvoll strukturierte Integration von Zero Trust Prinzipien ggf. negativ auf die Arbeitsabläufe der Beschäftigten und damit die Produktivität der Organisation auswirken.

Eine Folge von Zero Trust ist, dass zukünftig Zugriffe auf die Anwendungen und damit auch die Daten feingranularer gesteuert werden. Die feingranulare Zugriffssteuerung kann in den Anwendungen selbst stattfinden und durch andere IT-Komponenten (auch unterhalb der Anwendungsschicht) ergänzt werden. Für einige der Zugriffssteuerungen müssen auch die Anwendungen und verwendeten Protokolle angepasst werden.

Um diese vielfältigen und weitreichenden Herausforderungen der Umsetzung zu verdeutlichen, werden im Folgenden verschiedene, sehr spezifische, stark abgegrenzte Zugriffsbeispiele auf Web-basierten Anwendungen skizziert. Sie sind ein partieller Ansatz, der beispielhaft zeigen soll inwiefern sich einzelne Zero Trust-Aspekte in Bestandsumgebungen integrieren lassen. Diese Betrachtungen sind nicht abschließend, sondern skizzieren viel mehr einen ersten Ansatzpunkt, um einzelne Umsetzungsmöglichkeiten exemplarisch darzustellen und sich einer spezifischen Realisierung von Zero Trust-Prinzipien zu nähern.

Folgende Aspekte wurden bei diesen Zugriffsbeispielen als gegeben angenommen:

1 Es existiert eine Inventarisierung für alle Entitäten der Organisation. Die in den Anwendungsfällen verwendeten Entitäten (Anwendung 1, Endgerät 1, Gerätemanagement und Konto A) sind bereits registrierte Entitäten in der Organisation. Alle hierfür notwendigen Schritte (bspw. Installation von Agenten, Ausrollen von Zertifikaten) wurden vorgenommen.

2 Es existiert eine Richtlinie, die führend ist für die Regelung der Zugriffe von Entitäten. Tabelle 1 zeigt einen beispielhaften Auszug verschiedener Zugriffsszenarien, wie sie in der Organisation vorliegen können für die generelle interne Netzkonnektivität der Entitäten „Anwendung 1“ (AW 1) und „Endgerät 1“ (EG 1) zum internen Netz der Organisation.

ID	Entität	Registriert	Authentisierung erfolgreich	Compliance-Vorgaben erfüllt	Zugriffszeitpunkt	Gewünschtes Zugriffsergebnis
N-0	AW 1	Ja	Ja	Ja	*	Zugriff zum internen Netz
N-1	AW 1	Ja	Ja	Nein	*	Limitierter Zugriff zum internen Netz
N-2	AW 1	Ja	Nein	n/a	*	Kein Zugriff zum internen Netz
N-3	AW 1	Nein	n/a	n/a	*	Kein Zugriff zum internen Netz
N-4	EG 1	Ja	Ja	Ja	werktags 6:00-18:00 Uhr	Zugriff zum internen Netz
N-5	EG 1	Ja	Ja	Nein	werktags 6:00-18:00 Uhr	Limitierter Zugriff zum internen Netz
N-6	EG 1	Ja	Nein	n/a	werktags 6:00-18:00 Uhr	Kein Zugriff zum internen Netz
N-7	EG 1	Nein	n/a	n/a	werktags 6:00-18:00 Uhr	Kein Zugriff zum internen Netz
N-8	EG1	Ja	Ja	Ja	werktags 22:00-06:00 Uhr	Zunächst kein Zugriff zum internen Netz, weiteren Authentisierungsfaktor anfordern, bei erfolgreicher Authentisierung mit dem weiteren Faktor Zugriff zum internen Netz.
…	…	…	…	…		…

Tabelle 1 - Auszug Zugriffsszenarien auf das Netz

ID	Entität	Zugriff mit	Zugriff auf	Authentisierungsstatus			Compliance-Vorgaben erfüllt		Gewünschtes Zugriffsergebnis
				Konto	Endgerät	Anwendung	Endgerät	Anwendung	
R-0	Konto A	EG 1	AW 1	Authentisierung erfolgreich	Bereits aktiv authentisiert	Bereits aktiv authentisiert	Ja	Ja	Zugriff auf die Anwendung
R-1	Konto A	EG 1	AW 1	Authentisierung nicht erfolgreich	Bereits aktiv authentisiert	Bereits aktiv authentisiert	Ja	Ja	Kein Zugriff auf die Anwendung
R-2	Konto A	EG 1	AW 1	Authentisierung erfolgreich	Bereits aktiv authentisiert	Bereits aktiv authentisiert	Nein	Ja	Nur Lesender Zugriff auf die Anwendung
R-3	*	*	AW 1	*	*	*	*	Nein	Kein Zugriff auf die Anwendung
…	…			…	…	…	…	…	…

Tabelle 2 - Auszug Zugriffsszenarien auf Ressourcen

Tabelle 2 zeigt einen beispielhaften Auszug der Zugriffsszenarien, wie sie in der Organisation vorliegen können für den Zugriff der Entitäten „Konto A“ und „Endgerät 1“ auf „Anwendung 1 (AW 1)“. Zur Vereinfachung wird hierbei nur geprüft, ob das Endgerät die Compliance-Vorgaben erfüllt hat. Damit kann in dem skizzierten Anwendungsfall Person A mit Konto A bei erfolgreichen Authentisierung von jedem Endgerät der Organisation auf die Anwendung 1 zugreifen, sofern es die Compliance-Vorgaben erfüllt. Eine feste Bindung an spezifische Endgeräte ist auch denkbar. Da in diesem Anwendungsfall die über die Anwendung 1 verfügbaren Daten als nicht besonders schützenswert kategorisiert wurden, wird im Fall nicht erfüllter Compliance-Vorgaben des verwendeten Endgeräts (ID R-2) ein limitierter, lediglich lesender- statt gar kein- Zugriff auf die Anwendung 1 gewährt. Die Zugriffsentscheidung könnte bspw. für eine Anwendung 2 mit als sensibel kategorisierten Daten bei nicht erfüllten Endgeräte-Compliance-Vorgaben im Zugriffsergebnis den Zugriff von diesem Endgerät vollständig verhindern.

Die für die Zugriffsentscheidungen jeweils notwendigen Kriterien sind abhängig vom Anwendungsfall und müssen daher in den Organisationen individuell erarbeitet werden. Beispielsweise könnte R-2 in Tabelle 2 für den Fall, dass die Verfügbarkeit der Anwendung 1 von der Organisation für wichtiger als die Erfüllung der Compliance-Vorgaben durch die Anwendung definiert wird, auch im Fall von fehlender Erfüllung der Compliance-Vorgaben durch die Anwendung ein - ggf. limitierter Zugriff - gestattet werden. Im Sinne eines Zero Trust-Ansatzes sollten die gewählten Kriterien und ihre Auswertung nicht dazu führen, dass sich die Zugriffsanforderungen zwingend für alle Zugriffe von allen Endgeräten auf alle Anwendungen und Daten mit beliebiger Datenklassifizierung statisch erhöhen. Vielmehr sollten Zugriffsanfragen bedarfsgerecht mit den für den Zugriffskontext notwendigen Kriterien bewertet werden. Diese dynamische, kontextspezifische Auswertung von Attributen für Zugriffsentscheidungen ist ein zentraler Bestandteil eines Zero Trust-Ansatzes. Vor allem die notwendige Dynamik und die resultierende Komplexität stellen sowohl für die initiale Integration, als auch in der perspektivischen kontinuierlichen Pflege, eine Herausforderung dar.

8.3 Erweiterung um echtzeitfähige Informationsquellen

Tabelle 1und Tabelle 2 beschreiben Beispiele für Zugriffsbedingungen, welche bei der initialen Zugriffsanfrage, sowohl zum internen Netz allgemein als auch spezifisch zur Anwendung 1, vorliegen müssen. Die auf dieser Grundlage genehmigten Zugriffe werden in der Regel erst nach Ablauf einer statisch vorgegebenen Laufzeit erneut evaluiert. Ein Vertrauensverlust in eine der Entitäten wird erst bei einer erneuten Evaluierung nach Ablauf der statisch definierten Laufzeit des genehmigten Zugriffs berücksichtigt. Um die Arbeit mit den Anwendungen für Beschäftigte möglichst komfortabel zu gestalten, werden hier häufig längere Laufzeiten (bspw. die Zeit eines Arbeitstages) gewählt. Bei diesem statischen Ansatz wird der kontinuierliche Prüfaspekt des Zugriffsvertrauens im Zero Trust Sinne noch nicht berücksichtigt. Die bisher statische Gültigkeit einer Session kann jedoch ebenfalls dynamischer und damit bedarfsgerechter nach Zero Trust-Prinzipien gestaltet werden.

Im Folgenden wird die Nutzung einer für die Authentisierung an einen Identitätsprovider angebundenen Anwendung durch eine Person A dargestellt. Diese meldet sich nach Aufruf der Anwendung und Weiterleitung an den konfigurierten Identitätsprovider erfolgreich mit ihrem Konto A an (vgl. Tabelle 2 ID R-0). Sie erhält daraufhin Zugriff auf die Anwendung. Die Anwendung erzeugt eine aktive Session für das Konto A mit einer definierten Laufzeit und hält diese in ihrem Sitzungsmanagement vor. Während dieser aktiven Session tritt ein Ereignis ein, welches eine Deaktivierung des Kontos A im Identitätsprovider zur Folge hat. Dieses Ereignis kann bspw. die Detektion eines ungewöhnlichen Nutzungsverhaltens sein oder eine Konfiguration der Personalverwaltung im Personalinformationssystems in Folge einer Freistellung oder Kündigung der Person A. Diese Deaktivierung des Kontos A kann entweder durch eine zur Verwaltung des Kontos A berechtigten Person oder automatisiert durch ein Event einer weiteren Infrastruktur-Komponente erfolgen. Weitere IT-Infrastruktur-Komponenten können bspw. ein Personalinformationssystem oder eine Detektionskomponente sein. In bisherigen IT-Infrastrukturen besitzt die Anwendung in der Regel keine Kenntnis über die Deaktivierung des Kontos A im Identitätsprovider und weiß so nicht, dass das Vertrauen in die aktive Sitzung ggf. nicht mehr gerechtfertigt

ist. Der Zugriff mit der aktiven Session ist daher in bisherigen IT-Infrastrukturen mit der Restzeit der statisch definierten Laufzeit weiterhin möglich. Nach Zero Trust-Prinzipien sollte dieser Vertrauensverlust, ausgelöst durch die Deaktivierung des Kontos A, in der Zugriffsentscheidung unmittelbar berücksichtigt werden. So kann im Fall einer Kompromittierung das Schadensausmaß reduziert werden.

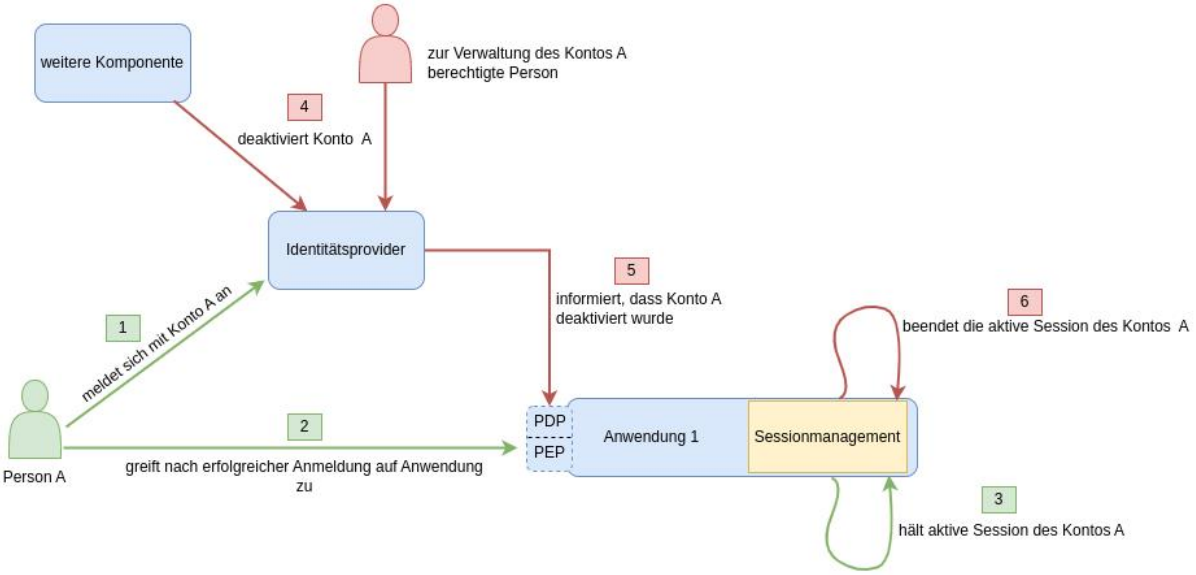

Abbildung 8 - Visualisierung Nutzung mit Echtzeitinformationsquelle 1

Bestrebungen wie die Spezifikation des „Shared Signal“ Frameworks der OpenID Foundation [3] bieten hier erste Ansätze, solche Events zu definieren und in einem standardisierten Format auszutauschen, um auf solche Events zeitnah reagieren zu können. Das Shared Signals Framework ermöglicht dabei den standardisierten Austausch von vordefinierten Events mit (teilweise optionalen) vordefinierten Eigenschaften (bspw. „das Konto A wurde deaktiviert, weil ein Hijacking-Angriff detektiert wurde“) zwischen verschiedenen IT-Infrastruktur Komponenten.

Diese Erweiterung um eine Echtzeitinformationsquelle skizziert neben dem Szenario aus der vorherigen Erweiterung zusätzlich die Nutzung eines Gerätemanagementsystems. Die Anwendung wird im Fall von Events, die im Gerätemanagement ausgelöst werden - ähnlich wie vom Identitätsprovider im Anwendungsfall 01 - vom Gerätemanagement über dieses Event informiert. Beispielsweise kann das Gerätemanagement der Anwendung mitteilen, wenn sich der Geräte-Compliance-Status eines für den Zugriff auf die Anwendung verwendeten Gerätes verändert hat. Die u.s. Grafik visualisiert den Kommunikationsablauf.

Auch hier können Bestrebungen wie die Spezifikation des „Shared Signal“ Frameworks der OpenID Foundation erste Ansätze bieten, um in der Anwendung auf Events des Gerätemanagements zu reagiert. [4] So könnte die Anwendung bei einem Event zur Änderung des Compliance-Status bspw. eine dedizierte Session des Kontos A von Client X terminieren während mögliche weitere Sessions des Kontos A von anderen Clients aktiv bleiben.

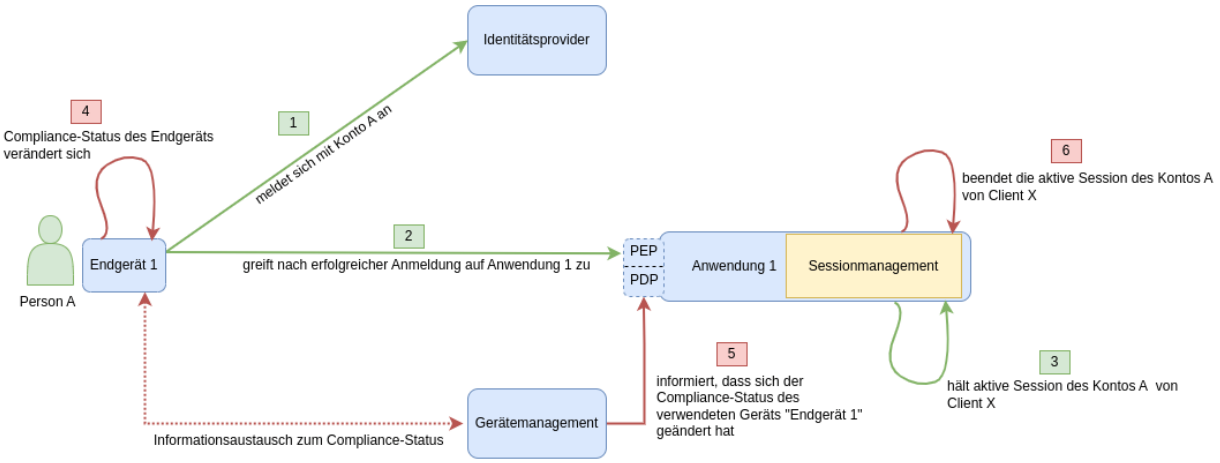

Abbildung 9 - Visualisierung Nutzung mit Echtzeitinformationsquelle 2

Diese stark begrenzten Nutzungsbeispiele sind in bestehenden IT-Infrastrukturen wie in den Abbildungen 8 und 9 bereits singulär umsetzbar. Die Komplexität steigt jedoch schnell an, wenn Zugriffe auf mehrere Anwendungen nach Zero Trust-Prinzipien abgesichert werden sollen. Hier kann es daher sinnvoll bzw. notwendig sein die Zugriffsbedingungen in einem zentralen PDP zu verwalten.

Die theoretischen Möglichkeiten zur Auswertung von Zugriffen und die damit verbundene Komplexität können ebenfalls Herausforderungen für Organisationen sein. Hier kann es helfen, sofern sich bereits stellenweise Möglichkeiten anbieten, einzelne Zugriffe auf bestimmte Anwendungen schon mal mit weiteren Attributen abzusichern. Dies birgt auf der einen Seite das Risiko, dass sich dadurch mit der Zeit viele verschiedene Implementierungen ergeben und aufgebaute Zugriffsevaluierungen ggf. noch einmal vereinheitlicht werden müssen. Auf der anderen Seite ermöglicht dieser Ansatz einer Organisation erste Erfahrungen mit der Implementierung der Konzepte zu machen. Diese können helfen besser abzuschätzen, welche Implementierungen in der eigenen IT-Infrastruktur sinnvoll und realistisch sind.

Darüber hinaus kann eine stellenweise Implementierung auch helfen der Herausforderung einer fehlenden Standardisierung zu begegnen. Derzeit existiert kein Standard, wie bspw. der Informationsaustausch für die Auswertung der Zugriffsszenarien auf das interne Netz oder auf die Ressourcen zwischen Komponenten technisch zu realisieren ist. Daher ist neben der inhaltlichen Ausgestaltung der Zugriffsrichtlinien auch die konkrete Implementierung individuell und abhängig von der Verfügbarkeit geeigneter Produkte zu realisieren.

9 Organisationsübergreifende Betrachtung

Unsere bisherigen Betrachtungen, aber auch Veröffentlichungen von Dritten, bzgl. Zero Trust-Architekturen fokussieren vor allem auf die Architekturbetrachtungen für IT-Infrastrukturen einer einzelnen Organisation. Allerdings ist das Zero Trust-Architekturparadigma vor allem auch motiviert und getrieben durch die in Kapitel 4 bereits erwähnten Bestrebungen einer stärkeren Zusammenarbeit über Organisationsgrenzen hinweg. Dies kann eine Zusammenarbeit zwischen unterschiedlichen, unabhängigen Unternehmen / (Bundes/Landes-) Behörden sein oder zwischen hierarchisch strukturierte Organisationseinheiten (bspw. Konzerne oder „Die Bundesverwaltung“).

Dies führt zwingend zu der Frage, ob und wenn ja, wie sich organisationsübergreifende Zero Trust-Architekturen oder individuelle Ansätze konzeptionieren lassen. Das Positionspapier hat die Herausforderungen der individuellen Ausgestaltung von Zero Trust Prinzipien wie bspw. die Erstellung bedarfsgerechter, dynamischer Zugriffsrichtlinien innerhalb einer Organisation bereits beschrieben.

Erweitert man die Betrachtung von einer Organisation auf organisationsübergreifende Kommunikation, so ergeben sich zusätzliche, vor allem organisatorische Herausforderungen und Abhängigkeiten. Ein multi-organisationaler Ansatz erfordert zunächst ein grundsätzliches gemeinsames Verständnis der Zero Trust-Prinzipien. Aus diesem grundsätzlichen gemeinsamen Verständnis ergeben sich aber nach der Integration von Zero Trust-Prinzipien nicht zwingend vergleichbare IT-Infrastrukturen. Wie auch heute schon sind die Sicherheitsniveaus, die IT-Infrastrukturen verschiedener Organisationen aufweisen nur schwer vergleichbar und immer unterschiedlich. Während eine Organisation, getrieben vom Schutz der Daten ihrer Geschäftsprozesse, für die identifizierten Gefährdungen bestimmte organisatorische Mitigationsmaßnahmen vorsieht und eine gewisse Menge an Restrisiken akzeptiert, kann eine zweite Organisation Gefährdungen für die Daten ihrer Geschäftsprozesse anders einschätzen und diese daher ggf. strikter durch technische Maßnahmen schützen wollen.

In einer bidirektionalen Vertrauensbeziehung auf Basis von Zero Trust-Prinzipien zwischen zwei Organisationen werden einige dieser Unterschiede auch technisch transparent gemacht. Bisher wurde bspw. organisatorisch vereinbart, dass beide Organisationen Sicherheitsupdates innerhalb einer bestimmten Frist einspielen. Zukünftig kann die eine Organisation prüfen, ob dies technisch tatsächlich erfolgt ist und entsprechende Maßnahmen ergreifen (bspw. kein oder limitierter Zugriff, Meldung an die andere Organisation oder Risikoakzeptanz im eigenen ISMS).

Abbildung 10 visualisiert einen Auszug eines solchen Szenarios beispielhaft. Clients der Organisation 1 sollen Zugriff auf Daten, die über die Anwendung bei Organisation 2 zur Verfügung gestellt werden, erhalten. Organisation 2 folgt den Zero Trust Prinzipien und evaluiert bei Zugriffsanfragen u.a., ob das zugreifende Endgerät die Compliance-Vorgaben der Organisation 2 erfüllt. Diese Informationen werden im Gerätemanagementsystem (GMS) der Organisation gesammelt. Um diese Evaluierung zu ermöglichen, stellt Organisation 2 einen Agenten des GMS zur Verfügung, welchen Organisation 1 auf den Clients, die zum Zugriff auf die Anwendung vorgesehen sind, installiert. In diesem Szenario kontrolliert Organisation 2 sowohl das Gerätemanagementsystem, welches Informationen für die Evaluierung der Umsetzung der Compliance-Vorgaben erhebt, als auch den Betrieb des PDPs, welcher die Richtlinien für einen Zugriff auf die Anwendung vorgibt.

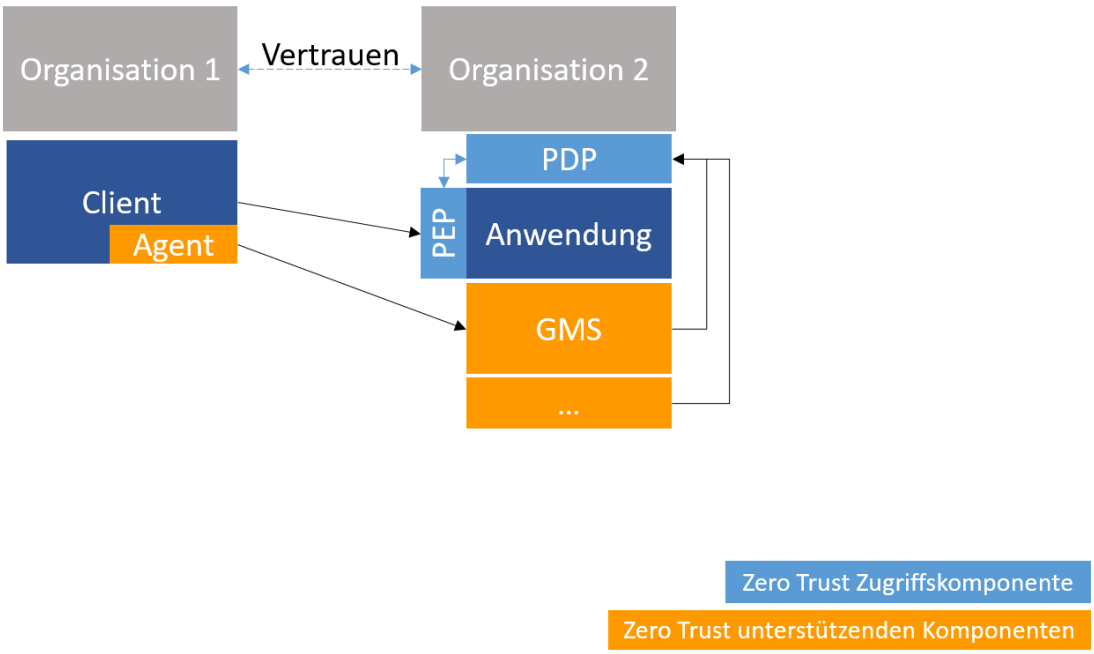

Abbildung 10 - Individuelles, bidirektionales Vertrauen zwischen Organisationen

Dieses Vorgehen skaliert jedoch nicht beim Einsatz unterschiedlicher Lösungen und in der Breite, da die Komplexität bei der individuellen Evaluierung jeder weiteren Organisation, die ggf. alle anderen bisherigen Evaluierungen ebenfalls beeinflussen kann, stark ansteigt. Bei einem multi-organisationalen Ansatz kann es daher hilfreich sein die für die Zugriffsevaluierung grundlegenden Anforderungen zentralisiert zu realisieren. Durch eine Zentralisierung ergibt sich zunächst eine gemeinsame, konsistente Grundlage. Auf dieser können, entweder ebenfalls zentral oder ggf. in den jeweiligen Organisationen, Zugriffsrichtlinien entwickelt werden. Die sich daraus ergebende Hierarchie ist in der Regel sehr flach und verfügt meist nur über zwei Ebenen.

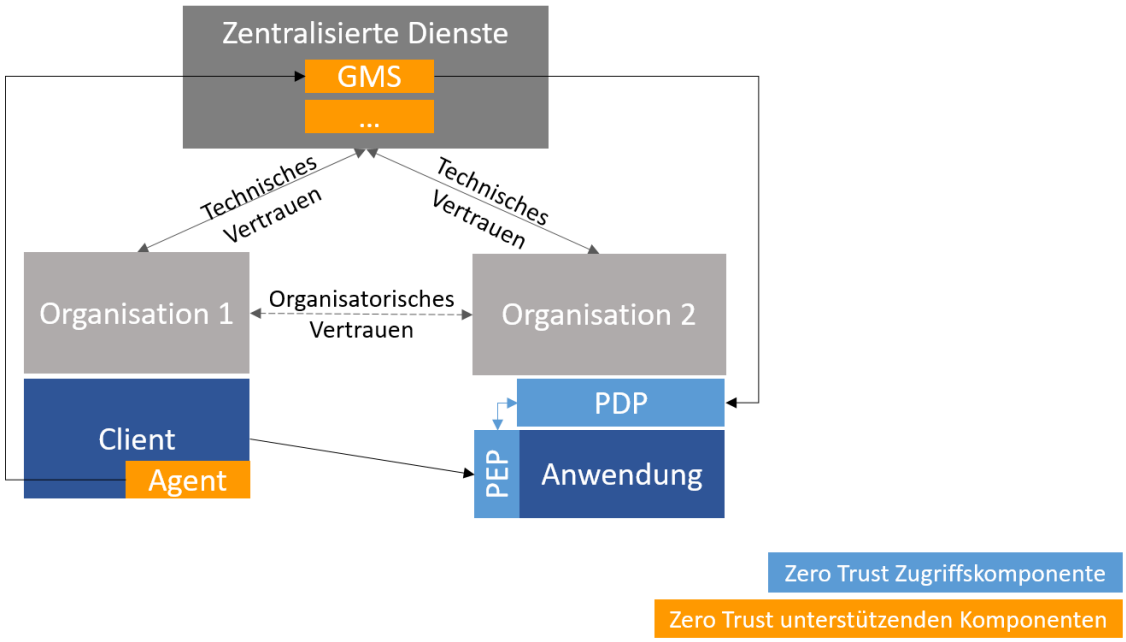

Abbildung 11 - Zentralisierte Dienste mit individuellem PDP

Abbildung 11 visualisiert ein Szenario, in welchem das Gerätemanagement als ein zentraler Dienst betrieben wird. Hier wird zentral für die Organisation vorgegeben, welche Informationen der Geräte vorliegen müssen. Somit ist zunächst eine einheitliche, organisationsübergreifende Datengrundlage für weitere Evaluierungen der Umsetzung von Compliance-Vorgaben möglich. In diesem Szenario wird die

Zugriffsentscheidungen allerdings weiterhin im PDP der Organisation 2 vorgenommen. Somit kann diese weiterhin entscheiden, welche Attribute für den Zugriff auf die Anwendung wie ausgewertet werden.

In dem Szenario, welches Abbildung 12 visualisiert, wird auch der PDP zentral betrieben. Dies ermöglicht neben der zentralen Datengrundlage auch eine zentrale, einheitliche Steuerung von organisationsübergreifenden Zugriffsrichtlinien. Auch Organisation 2 kann ihrerseits Informationen an zentralisierte Dienste, wie bspw. ein Schwachstellenmanagement, liefern. Die Informationen des Schwachstellenmanagements zum Status der Anwendung können im PDP ebenfalls berücksichtigt werden. Dies schafft auch die Möglichkeit für Organisation 1 in Teilen zu prüfen, ob die Daten in der Anwendung bei Organisation 2 gemäß den Compliance-Vereinbarungen geschützt sind.

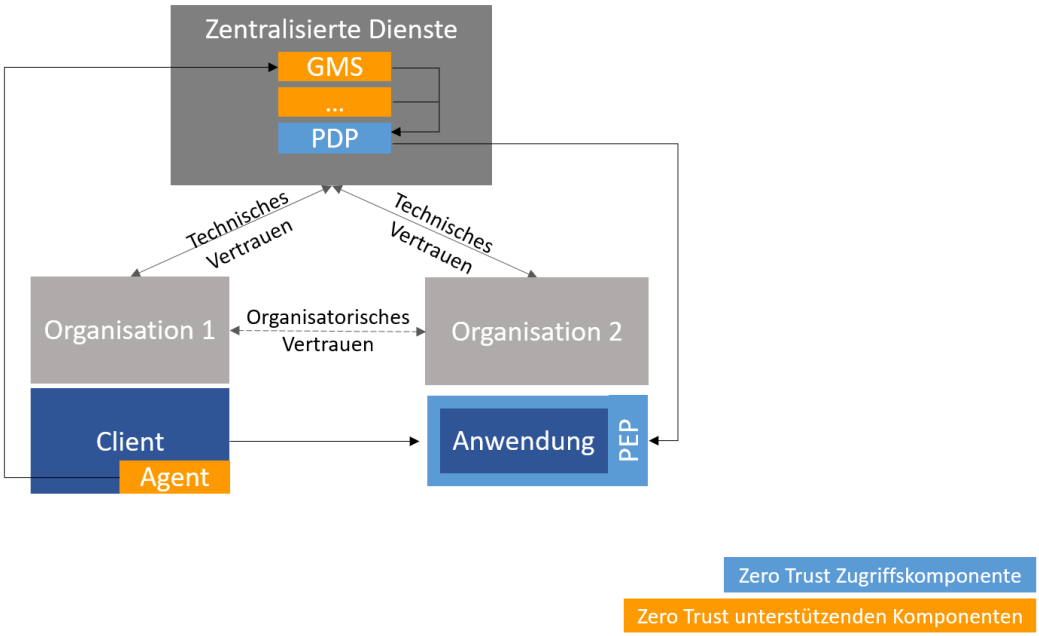

Abbildung 12 - Zentralisierte Dienste mit zentralisiertem PDP

Auch, wenn sich, wie bereits einleitend erwähnt, mit derzeitig auf dem Markt befindlichen Produkten noch nicht der volle Zero Trust Funktionsumfang realisieren lässt, kristallisiert sich insbesondere das in Abbildung 12 dargestellte Szenario heraus.

Organisationen sollten im ersten Schritt prüfen, ob der Grad der Vernetzung mit anderen Organisationen technisch eine Abstimmung der Zero Trust-Konzepte erfordert. Sofern die eigenen Anforderungen dies erfordern, sollte individuell bewertet werden, mit welchem Konzeptionierungsansatz diese Anforderungen am besten realisiert werden können. Den identifizierten Multiorganisationsansatz sollten sie dann für eine langfristige Planung verfolgen. Insbesondere für hierarchisch strukturierte Organisationseinheiten scheint der Architekturansatz in Abbildung 12 sehr effizient und effektiv. Zentrale Voraussetzung für den erfolgreichen Betrieb ist hierbei allerdings u.a. die Abstimmung der Zuständigkeiten und Verantwortlichkeiten zwischen den Organisationen und dem Betrieb der zentralisierten Dienste.

10 Zusammenfassung

Basierend sowohl auf der medialen Aufmerksamkeit, die der Themenkomplex Zero Trust derzeit auf sich zieht, als auch den bereits genannten sicherheitstechnischen und organisatorischen Vorteilen, die die Integration von Zero Trust-Prinzipien mit sich bringt, kann der Eindruck entstehen, dass nun zwingend für jede Organisation dringender operativer Handlungsbedarf besteht. Allerdings sollte bei der ganzheitlichen Integration von Zero Trust-Prinzipien strukturiert vorgegangen werden, die Integration muss zwingend sorgfältig geplant werden, um sich den bereits erwähnten Implementierungsherausforderungen erfolgreich zu stellen. Für eine wirksame und zielführende Integration von Zero Trust-Prinzipien in bestehende IT-Infrastrukturen sind insbesondere die Vorarbeiten (vgl. u.a. Kapitel 7 Integrationsmodell) erfolgskritisch. Daher sollte der initiale Fokus auf einer Bestandsaufnahme der eigenen, bestehenden IT-Infrastruktur liegen und u.a. eine Identifizierung sowohl der Identitäten, der organisationskritischen Daten, der Systeme und der Geschäftsprozesse erfolgen. Auf dieser Basis können im nächsten Schritt bedarfsgerechte Richtlinien entworfen werden, die die Grundlage für Zugriffsevaluierungen der Policy Engine bilden. Die Richtlinien können sich dabei auf die gesamte Organisation beziehen oder zunächst auch nur auf einen Teilbereich (bspw. auf als kritisch identifizierte Geschäftsprozesse) angewendet werden.

Bei einer Integration in große Organisationen wie Konzerne oder eine Bundes-/Landes-Verwaltung kommt weiterer vorangehender zentralisierter Planungs- und Abstimmungsbedarf hinzu. Des Weiteren müssen stark verteilte Betriebsteile mit sehr hohen Aufwendungen zur Standardisierung der nötigen Zero Trust-Funktionen und Policies rechnen. Eine solche Standardisierung ist jedoch zwingend vor einer globalen Implementierung durchzuführen, um eine spätere Interoperabilität überhaupt zu erzeugen. Das Fehlen solcher Standardisierungen führt zu einem nicht mitigierbaren Zwangsvertrauen in alle Teile der Organisation. Hierbei werden alle etablierten Maßnahmen der teilnehmenden Organisationsteile auf das Sicherheitsniveau des schwächsten Teilnehmenden reduziert sowie kosten- und ressourcenintensive Aufwände zerstört. Die Zero Trust Methoden führen aufgrund der geforderten Nachweise zu einer absoluten Transparenz der Sicherheitsniveaus der unterschiedlichen Teilnehmenden.

Ist die Bestandsaufnahme der eigenen, bestehenden IT-Infrastruktur unvollständig, führt diese unvollständige Sichtbarkeit mit hoher Wahrscheinlichkeit mindestens zu Verfügbarkeitsproblemen von Geschäftsprozessen, wenn Zugriffsanfragen von der Policy Engine aufgrund unvollständiger oder falscher Informationen verweigert werden. Die unvollständigen oder falschen Informationen können allerdings auch dazu führen, dass fälschlicherweise zu viele Zugriffe genehmigt werden, was sich ebenfalls negativ auf die IT-Sicherheit der Organisation auswirkt. Die Schaffung verlässlicher Informationsgrundlagen ist daher ein essentieller erster Schritt für Organisationen, die eine Integration von Zero Trust-Prinzipien anstreben. Auch ist für eine erste Integration von Zero Trust-Prinzipien die Aufrechterhaltung bereits vorhandener Sicherheitsmaßnahmen dringend geboten.

Der Zero Trust-Ansatz ist, nachdem die initialen Voraussetzungen und Richtlinien definiert und etabliert wurden, dynamisch und - im Verhältnis zu den Vorarbeiten - einfach zu erweitern, so dass eine Organisation flexibel auf Veränderungen der IT-Sicherheitslage oder eigener Prozessanpassungen reagieren kann. Diesen Zustand in einer bestehenden IT-Infrastruktur zu erreichen erfordert eine strukturierte Vorgehensweise und eine der Komplexität des Vorhabens angepasste Verfügbarkeit von Ressourcen und Zeit. Diese müssen auch kontinuierlich über die initiale Umsetzung hinaus zur Verfügung gestellt werden. Organisationen werden daher realistisch betrachtet über längere Zeit weiterhin statische Zugriffsentscheidungen für einige Teile ihrer IT-Infrastruktur parallel zu Zugriffsentscheidungen nach Zero Trust-Prinzipien in ersten anderen Bereichen treffen.

11 Ausblick / Weiteres Vorgehen

Das BSI plant eine Marktsichtung zur Analyse von Zero Trust-Funktionen in Produkten durchzuführen. Zusätzlich wird das BSI weiterhin die IT-Grundschutz-Anforderungen – auch unter Berücksichtigung von Zero Trust-Prinzipien - weiterentwickeln. Ein weiterer notwendiger Folgeschritt ist die Erarbeitung von Umsetzungsansätzen für zielgruppenspezifische Einsatzumgebungen und spezifische Randbedingungen.

Organisationen können aber bereits jetzt schon, unabhängig von weiteren Konkretisierungen, Zero Trust, etwa in ihren Risikoanalysen, berücksichtigen. Dies kann auch heute schon bei der gesteigerten Bedrohungslage erforderlich sein.

12 Weiterführende Informationen

1 NIST SP 800-207 Zero Trust Architecture, August 2020 https://csrc.nist.gov/publications/detail/sp/800-207/final, abgerufen am 09.03.2023

2 CISA Zero Trust Maturity Model, Juni 2021 https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf, abgerufen am 09.03.2023

3 OpenID Spezifikation Shared Signals Framework, Juni 2021 https://openid.net/specs/openid-sse-framework-1_0-ID1.html, abgerufen am 09.03.2023

4 OpenID Spezifikation OpenID Continuous Access Evaluation Profile 1.0 - draft 02, August 2021 https://openid.net/specs/openid-caep-specification-1_0.html, abgerufen am 09.03.2023

Glossar

Abkürzung	Bedeutung / Beschreibung
ABAC	Attribute Based Access Control
ALG	Application Layer Gateway
AV	Anti-Virus
„Assume Breach“-Ansatz	Der „Assume Breach“-Ansatz nimmt an, dass erfolgreiche Angriffe auf die eigene Infrastruktur unvermeidbar sind. Unter Berücksichtigung dieser Annahme werden dann die notwendigen Sicherheitsmaßnahmen für die eigene Infrastruktur erarbeitet.
CISA	Cybersecurity and Infrastructure Security Agency (USA)
Defense-in-depth	Eine Absicherungsstrategie, welche mehrere Absicherungsmechanismen über mehrere Ebene und Dimensionen einer Organisation vorsieht. Defense-in-depth sieht den Einsatz von heterogene Sicherheitsmaßnahmen vor, um Angriffe, die gezielt eine Maßnahme erfolgreich angreifen, dennoch durch weitere Sicherheitsmaßnahmen zu mitigieren.
Entität	Eine Entität ist ein eindeutig identifizierbares, einzelnes Informationsobjekt. Entitäten können sowohl reale Dinge oder Personen, als auch abstrakte Objekte sein. Im Kontext von Zero Trust können Entitäten Personen, Identitäten, Daten, Geräte, Netze oder Systeme sein.
GW	Gateway
DMZ	Demilitarisierte Zone
ISMS	Information Security Management System (dt. Managementsystem für Informationssicherheit)
MAC	Media Access Control
MFA	Authentisierung mit mehreren Faktoren
NIST	National Institute of Standards and Technology (USA)
OMB	Office of management and Budget (USA)
Policy	hier: Ein Regelsatz für die Zugriffssteuerung auf Ressourcen, der sich an den Anforderungen der Organisation orientiert (vgl. RFC3198 und RFC3060).
PDP	Policy Decision Point *Eine logische Entität, die Policy Entscheidungen für sich selbst oder weitere Entitäten, die eine Entscheidung anfragen, durchführt (vgl.* RFC3198 und *RFC2753*).
PEP	Policy Enforcement Point *Eine logische Entität, die die Entscheidung des Policy Decision Points erzwingt (vgl.* RFC3198 und *RFC2753*).
PE	Policy Engine
PA	Policy Administrator
RBAC	Role Based Access Control
SIEM	Security Information and Event Management
SSO	Single Sign On *Einmalanmeldung, ein Verfahren bei dem nach einer einmaligen zentralen Authentifizierung einer Identität, für einen definierten Zeitraum, auf Basis der durch die Authentifizierung verfügbaren abgeleiteten Anmeldeinformationen Zugriff auf weitere Ressourcen erteilt werden kann ohne, dass Entitäten erneut eine interaktive Authentifizierung durchführen müssen*.
SDP	Software Defined Perimeter
TPM	Trusted Platform Module
VPN	Virtual Private Network

Abkürzung	Bedeutung / Beschreibung
VSA	Verschlusssachenanweisung
VS	Verschlusssache
ZT	Zero Trust
ZTX	Zero Trust eXtended *Begriffsdefinition von Forrester Analyst Dr. Chase Cunningham, Der Begriff soll die Erweiterung des bis dahin Netz-zentrierten "Zero Trust" Forrester-Begriffs um Identitäts- und Zugriffsmanagement verdeutlichen.*

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang – Säulen des Zero Trust Integrationsmodells

Im Folgenden finden sich die fünf Säulen des Zero Trust Integrationsmodells inkl. aller identifizierten Funktionen und ihrer Ausprägung für alle drei Reifegrade.

A.1.1 Identität

Eine Identität repräsentiert eine bestimmte Kombination von Eigenschaften und Rollen eines Objekts (physisch, kontextuell, logisch), die mit einem eindeutigen Bezeichner benannt wird. Die einzelnen Rollen und Eigenschaften können die Art bestimmen, wie eine Identität agiert und interagiert.

Eine logische Identität ist eine Abbildung einer physischen Identität in einer nicht-realen Umgebung (bspw. einem Informationssystem) oder eine Abbildung einer kontextuellen Identität (Rolle). Diese logische Identität bezeichnet man manchmal auch als technische Identität. Sie wird in Informationssystemen in Form von Konten (engl. Accounts) verwaltet. Durch die Übernahme von Rollen kann eine Person (physische Identität) mehrere logische Identitäten besitzen. Diese logische Identität bildet - mit Fokus auf natürliche Personen als Identitätsträger - die Grundlage für die Maßnahmen in dieser Säule. Die Identitätsträger Gerät(e) und Anwendung(en) werden in den jeweiligen Säulen dediziert betrachtet.

A.1.1.1 Integrationsmöglichkeiten

Funktion	Klassisch	Fortschrittlich	Ideal
Authentisierung **(ID-01)**	Häufig ein Faktor (Kontoname/Passwort), gelegentlich zwei Faktoren für den Zugriff von hochprivilegierten Konten oder die initiale Anmeldung des Anwenders/der Anwenderin am Endgerät. Die abgeleiteten Anmeldeinformation werden heute vielfach ohne weitere Prüfung für die Authentisierung an vielen Diensten genutzt. **(ID-01-KL)**	Authentisierung mit mehreren Faktoren (MFA) für den Zugriff auf besonders schützenswerte Ressourcen. Dabei erfolgt die MFA an den einzelnen Anwendungen und nicht am unterliegenden Netzbereich (VPN). Für nicht MFA-kompatible Anwendungen kommen zusätzliche Verfahren wie z. B. Anwendungsreverseproxies zum Einsatz, die eine MFA ermöglichen. Die Nutzung der abgeleiteten Anmeldeinformation wird auf den für die einzelnen Anwendungen notwendigen Bereich und zeitlich eingeschränkt. **(ID-01-FO)**	Authentisierung mit MFA mit hohem Sicherheitsniveau, die für Zugriffe des Anwenders/der Anwenderin separat auf allen Anwendungen erfolgt und nicht am unterliegenden Netzbereich (VPN). Bei kontinuierlicher Prüfung kann bei Vertrauensverlust ein weiterer Faktor erneut eingefordert werden. Es erfolgt möglichst immer eine separate Authentisierung bei jeder einzelnen Anwendungssitzung. **(ID-01-ID)**

Funktion	Klassisch	Fortschrittlich	Ideal
Autorisierung **(ID-02)**	Rollenbasierte Zugriffskontrollen (role based access control, **RBAC**), die auf statischen vordefinierten Rollen basieren, die Identitäten – häufig manuell - zugewiesen werden. Die zugewiesenen Rollen bestimmen die Zugriffsrechte der Identität innerhalb der Organisation. **(ID-02-KL)**	Erste Integration von freigranularen und dynamisch definierten Zugriffsrechten, die auf Eigenschaften (engl. attributes) der Identität basieren (Attribute-based access control, **ABAC).** Die Identitätsattribute bilden dabei (neben bspw. dem verwendeten Gerät, dem genutzten Netzzugang oder den Attributen der Ressource) eine Quelle für die ABAC Zugriffsentscheidung bei einigen Anwendungen. **(ID-02-FO)**	Kombination aus ABAC (für die initiale Zugriffsentscheidung) und RBAC (für weitere detaillierte Autorisierungen). Die Identitätsattribute bilden dabei immer (neben bspw. dem verwendeten Gerät oder den Attributen der Ressource) eine Quelle für die ABAC Zugriffsentscheidung. **(ID-02-ID)**
Identitätsprovider **(ID-03)**	Die Organisation verwendet nur eigene lokale Identitätsprovider für die lokale/interne Nutzung lokaler/interner Identitäten. Der Zugriff auf Dienste von Dritten (bspw. dem ITZBund) muss daher über ein separates Identitätsmanagement erfolgen. **(ID-03-KL)**	Einige Identitäten der Organisation werden bedarfsgerecht mit Dritten föderiert. Anmeldungen an den wichtigsten Anwendungen der Organisation erfolgen mit den im Identitätsprovider zentral verwalteten Identitäten. Dieser kann auch von Dritten betrieben werden. **(ID-03-FO)**	Anmeldungen an den Anwendungen der Organisation erfolgen immer mit den im Identitätsprovider zentral verwalteten Identitäten. Dieser kann auch von Dritten betrieben werden. **(ID-03-ID)**
Identitätsver-waltung **(ID-04)**	Die Organisation verwaltet die Berechtigungen der Identitäten teilweise noch manuell, ggf. unter Zuhilfenahme von Ticketsystemen. Das Prinzip der minimalen Rechte ist nicht feingranular durchgesetzt. Teilweise werden Konten auch geteilt genutzt. Die Überprüfung der Berechtigungen erfolgt meistens anlassbezogenen,	Die Organisation verwaltet Berechtigungen größtenteils auf Grundlage von Sicherheitsrichtlinien auch ggf. über mehrere Identitätsprovider hinweg. Das Prinzip der minimalen Rechte ist feingranularer durchgesetzt. Die Überprüfung der Berechtigungen erfolgt anlassbezogen und regelmäßig in möglichst vielen	Die Organisation orchestriert den gesamten Identitätslebenszyklus. Gruppenzugehörigkeiten erfolgen dynamisch (bspw. in Abhängigkeit von dem genutzten Endgerät oder der Authentifizierungsstärke). Dafür wird das Prinzip Just-in-time zusätzlich für alle Identitäten umgesetzt. Das Prinzip der minimalen Rechte ist vollständig durchgesetzt. Die Organisation besitzt einen ganzheitlichen

Funktion	Klassisch	Fortschrittlich	Ideal
	z.B. bei der Einstellung und ggf. beim Verlassen der Organisation. **(ID-04-KL)**	der Identitätsprovider der Organisation. **(ID-04-FO)**	Überblick über alle ihre Identitäten inkl. der zugehörigen Verantwortungen und Befugnisse, sowohl lokal als auch föderiert. Die Überprüfung der Berechtigungen erfolgt anlassbezogen und regelmäßig in allen Identitätsprovidern. **(ID-04-ID)**
Detektion & Reaktion **(ID-DET)**	Die Organisation macht limitierte Abschätzungen bzgl. Identitätsrisiken und besitzt limitierte Detektionen. Die Risikoanalyse wird nicht oder nur bei einigen Authentifizierungs- und / oder Autorisierungsentscheidungen und meistens manuell berücksichtigt. **(ID-DET-KL)**	Die Organisation bestimmt Identitätsrisiken und die zugehörige Detektion basierend auf einfachen Analysen und statischen Regeln. Die Risikoanalyse wird bei vielen Authentifizierungs- und / oder Autorisierungsentscheidungen berücksichtigt. **(ID-DET-FO)**	Die Organisation zentralisiert die Sichtbarkeit der Anwendendenaktivitäten und analysiert Anwendendenverhalten in Echtzeit um Risiken zu bestimmen und durchgehenden Schutz zu gewährleisten. Die Risikoanalyse wird bei allen Autorisierungs-entscheidungen berücksichtigt. **(ID-DET-ID)**
Anforderungen an VS **(ID-VS)**	Die Organisation verlässt sich auf in den vorhandenen IT-Systemen implementierte Lösungen. Häufig erfolgt eine sehr weitreichende Rechtevergabe, die dem Grundsatz „Kenntnis, nur, wenn nötig“ entgegensteht. Der Perimeter Schutz eines Netzes übernimmt die VS konforme Kontrolle und Verwaltung von	Die Maßnahmen zur Authentisierung und Autorisierung ermöglichen eine feingranulare Zuweisung der Rechte auf einzelne Daten (VS). Die Behörde setzt eine feingranulare Zuweisung von Rechten um. Bei der Identität einer Person ist hinterlegt, ob diese auf den Zugang zu VS ermächtigt ist. Die VS Freigabe wird weiterhin über den Perimeter Schutz erreicht. Zero Trust Identitäten innerhalb	Zero Trust Identitäten sind so sicher aufgebaut, dass der Zugriff auf VS über sie abgesichert werden kann. Die zum Einsatz kommenden Produkte für die Authentisierung (ID-01-ID) und Autorisierung (ID-02-ID) verfügen über eine Zulassungsaussage des BSI. Die Zugriffsrechte auf einzelne VS werden grundsätzlich zuerst nur dem Ersteller erteilt. Erst im Rahmen einer expliziten Weitergabe der VS findet eine

Funktion	Klassisch	Fortschrittlich	Ideal
	Identitäten **(ID-VS-KL)**	eines Netzes werden jedoch verwendet, um das Need-to-Know (NtK) durchzusetzen. Dabei wird auch auf Funktionen der Komponenten des Perimeter Schutzes zurückgegriffen. **(ID-VS-FO)**	Anpassung der Berechtigung statt (§ 3 Abs. 1 VSA). **(ID-VS-ID)**

A.1.2 Gerät

Ein Gerät im Sinne dieses Konzepts ist eine physische oder virtualisierte Hardware-Komponente, die sich zu einem Netz verbinden kann (bspw. Internet of Things (IoT) Geräte, Smartphones, Laptops oder Server). Ein Gerät kann durch die Organisation verwaltet oder auch ein Gerät von Dritten sein. Ein Gerät subsummiert auch alle Anwendungen, die auf diesem betrieben werden.

Eine Organisation sollte alle durch sie verwalteten Geräte inventarisieren und absichern. Den Zugriff von unautorisierten Geräten auf Organisationsressourcen sollte sie unterbinden. Für den Zugriff sollte der Sicherheitszustand des Gerätes berücksichtigt werden. Dieser stellt eine Bewertung von mehreren Sicherheitsmerkmalen des Gerätes nach von der Organisation zu bestimmenden Regeln dar (bspw. der Patchstand des Gerätes, sicherheitsrelevante Konfigurationen).

A.1.2.1 Integrationsmöglichkeiten

Funktion	Klassisch	Fortschrittlich	Ideal
Compliance Monitoring **(GE-01)**	Die Organisation hat eine eingeschränkte Übersicht bzgl. des Compliance Status einzelner Geräte (bspw. nur Teilinformationen) sowie Geräte ohne ein Compliance Monitoring. **(GE-01-KL)**	Die Organisation hat eine einfache Übersicht bzgl. des Compliance-Status für die meisten Geräte. Die Ermittlung des Compliance Status basiert vorwiegend auf Lösungen von externen Herstellern, die den Sicherheitszustand auf Basis ihrer Richtlinien bewerten. Dabei können zum einen die Richtlinien des Herstellers von denen der Organisation abweichen. Zum anderen dokumentieren Hersteller ihre Richtlinien häufig nicht transparent, so dass der Sicherheitszustand für die Organisation nur eingeschränkt bewertbar ist. **(GE-01-FO)**	Die Organisation hat eine vollständige Übersicht bzgl. des Compliance Status aller Geräte. Der Compliance Status bildet den Sicherheitszustand auf Basis der von der Organisation vorgegebenen Sicherheitsrichtlinien ab. **(GE-01-ID)**
Compliance Durchsetzung **(GE-02)**	Die Organisation betreibt gelegentlich manuelle Compliance Durchsetzungsmechanismen für einzelne Geräte. **(GE-02-KL)**	Die Organisation betreibt größtenteils automatisierte Compliance Durchsetzungsmechanismen für die meisten Geräte. **(GE-02-FO)**	Die Organisation betreibt automatisierte Compliance Durchsetzungsmechanismen für alle Geräte. **(GE-02-ID)**

Funktion	Klassisch	Fortschrittlich	Ideal
Ressourcen-zugriff **(GE-03)**	Zugriff auf Ressourcen der Organisation ist nicht abhängig vom aktuellen Sicherheitszustand des Geräts, welches zum Zugriff auf die Ressourcen verwendet wird. **(GE-03-KL)**	Die Organisation berücksichtigt den aktuellen Sicherheitszustand aller Geräte beim initialen Zugriff auf besonders schützenswerte Ressourcen. **(GE-03-FO)**	Die Organisation berücksichtigt bei jedem Zugriff (z.B. Lesen, Schreiben, ...) auf jede beliebige Ressource den aktuellen Sicherheitszustand des Gerätes von dem aus der Zugriff erfolgt. **(GE-03-ID)**
Authentisierung **(GE-04)**	Bei einigen Geräten der Organisation erfolgt eine Authentisierung für einige Funktionen der zentralen Verwaltung mit einem einfachen Authentisierungsmerkmal (bspw. MAC Adresse). **(GE-04-KL)**	Bei einem Großteil der Geräte der Organisation erfolgt eine Authentisierung an den Ressourcen mit einem erweiterten Authentisierungsmerkmal (bspw. Zertifikat in Software) ausgestellt von einer zentralen Instanz. **(GE-04-FO)**	Bei den Geräten der Organisation erfolgt eine Authentisierung an den Ressourcen mit einem eindeutigen Authentisierungsmerkmal des Geräts, welches gegen Kopieren geschützt ist (bspw. vertrauenswürdiger hardwarebasierter Identitätsnachweis). **(GE-04-ID)**
Assetmanage-ment **(GE-05)**	Die Organisation hat ein einfaches und manuell gepflegtes Geräteinventar. **(GE-05-KL)**	Die Organisation verwendet automatisierte Methoden (Discovery), um mindestens alle selbstbetriebenen Geräte zu inventarisieren. **(GE-05-FO)**	Die Organisation integriert alle ihre Geräte automatisiert in das Assetmanagement. (inkl. selbstbetriebene und ausgelagerte Dienste).). **(GE-05-ID)**
Schwachstellen-management **(GE-06)**	Die Organisation führt ggf. gelegentlich manuell Schwachstellenanalysen durch. Zusätzlich werden periodische Netzscans durchgeführt, deren Reports manuell ausgewertet werden und manuelle Folgeaktivitäten auslösen. **(GE-06-KL)**	Die Organisation verwendet automatisierte Methoden um Schwachstellen zu identifizieren. Hierzu zählen auch regelmäßige, automatisierte Netzscans, auf Basis der Ergebnisse werden Folgeaktivitäten teilweise automatisiert ausgelöst. **(GE-06-FO)**	Die Organisation integriert das Schwachstellenmanagement in alle ihre Umgebungen (inkl. on-premise und ggf. ausgelagerte Dienste). Schwachstellen werden automatisch identifiziert, bewertet und es werden angemessene Folgeaktivtäten automatisch ausgelöst. **(GE-06-ID)**

Funktion	Klassisch	Fortschrittlich	Ideal
Sicherheits-funktionen **(GE-07)**	Die meisten Sicherheitsfunktionen (sichere Identifizierung, sicheren Speicher, Messen der Integrität) basieren auf softwarebasierten Implementierungen, die häufig über keine Aussage zur Vertrauenswürdigkeit oder Zuverlässigkeit verfügen **(GE-07-KL)**	Ein Großteil der Geräte bietet sicheren Speicher und sichere Funktionen hardwarebasiert an (bspw. TPM). Einige Sicherheitsfunktionen verfügen über Sicherheitsaussagen, die meistens allerdings nur die funktionalen Aspekte prüft. **(GE-07-FO)**	Alle Geräte bieten sicheren Speicher und hardwarebasierte Sicherheitsfunktionen an. Alle Sicherheitsfunktionen verfügen über eine Sicherheitsaussage (Zertifizierung oder Zulassung). **(GE-07-ID)**
Detektion & Reaktion **(GE-DET)**	Die Organisation führt Auswertungen von AV-Ereignissen des Geräts durch. Die Auswertung der Reports und die notwendigen Folgeaktivitäten erfolgen manuell. **(GE-DET-KL)**	Die Organisation führt eine zentralisierte Auswertung in einem SIEM[1] durch und isoliert teilweise automatisiert Geräte. **(GE-DET-FO)**	Die Organisation führt über die Compliancedurchsetzung hinausgehende Echtzeitanalysen bzgl. des Sicherheitszustands des Gerätes durch. Die Organisation zentralisiert die Sichtbarkeit der Geräteaktivitäten und analysiert Geräteverhalten in Echtzeit um Risiken zu bestimmen und durchgehenden Schutz zu gewährleisten. Die Risikoanalyse wird bei allen Zugriffsentscheidungen berücksichtigt. **(GE-DET-ID)**
Anforderungen an VS **(GE-VS)**	Geräte, welche eine IT-Sicherheitsfunktion nach VSA übernehmen, insbesondere am Perimeter, benötigen eine Zulassungsaussage. Innerhalb des Perimeters verortete Geräte benötigen	Neben der materiellen Absicherung der Endgeräte werden ergänzend zugelassene Endgeräte eingesetzt, um den Nutzer am Perimeter zu authentisieren. Wenn das Compliance Monitoring auch für Geräte	Ergänzend zu der materiellen Absicherung und der Authentisierung am zugelassenen Produkt werden IT-Sicherheitsfunktionen sowohl durch zugelassene Endgeräte als auch innerhalb der darauf betriebenen Software umgesetzt.

[1] Security Information and Event Management

Funktion	Klassisch	Fortschrittlich	Ideal
	i.d.R. keine Zulassungsaussage, da diese keine IT-Sicherheitsfunktionen zum Schutz der VS nach VSA übernehmen, wenn der Schutz durch materielle Maßnahmen oder den Perimeter sichergestellt wird. Die Überprüfung der Umsetzung der Geheimschutzmaßnahmen, worunter auch die Einhaltung der SecOps/EuBB fallen (vgl. GE-01-KL), erfolgt manuell durch den Geheimschutzbeauftragten, beispielsweise im Rahmen der VS-Freigaben oder nach geheimschutzrelevanten Änderungen. Die Geräte haben einen festen Einsatzzweck innerhalb der VS-IT. Die Compliance ist fest vorgegeben (vgl. GE-02-KL) und nur manuell veränderbar. Auch Ressourcenzugriffe auf VS sind nicht vom Sicherheitszustand des Gerätes abhängig (vgl. GE-03-KL). Eine Liste über diese Geräte, die zu einer VS-IT gehören, wird manuell vom Geheimschutzbeauftragten gepflegt (vgl. Nr. 2.2 Anlage II zur VSA	eingesetzt wird, mit denen VS verarbeitet werden, dann ist das Compliance Monitoring (GE-01-ID) und die Durchsetzung (GE-02-ID) für die meisten IT-Sicherheitsprodukte mit Zulassungsaussage, um die Überprüfung zur Einhaltung der SecOps/EuBB zu erweitern. Falls IT-Sicherheitsprodukte auch mit einem Authentisierungsmerkmal (GE-04-ID) ausgestattet werden sollen, ist dies bei der Zulassung zu berücksichtigen. Die meisten Geräte, die IT-Sicherheitsprodukte und Teil der betrachteten VS-IT sind, sind in ein halb automatisiertes Assetmanagement integriert. Geräte, die IT-Sicherheitsprodukte sind werden als solche gekennzeichnet. **(GE-VS-FO)**	Wenn das Compliance Monitoring auch für Geräte eingesetzt wird, mit denen VS verarbeitet werden, dann ist das Compliance Monitoring (GE-01-ID) und die Durchsetzung (GE-02-ID) für alle IT-Sicherheitsprodukte mit Zulassungsaussage, um die Überprüfung zur Einhaltung der SecOps/EuBB zu erweitern. Falls IT-Sicherheitsprodukte auch mit einem Authentisierungsmerkmal (GE-04-ID) ausgestattet werden sollen, ist dies bei der Zulassung zu berücksichtigen. Alle Geräte, die zusammen eine VS-IT darstellen, sind in ein automatisiertes Assetmanagement integriert (vgl. GE-05-ID) und gesondert zu kennzeichnen, wodurch der Geheimschutzbeauftragte und insb. Administratoren direkt erkennen kann, welche Geräte zur VS-IT gehören. **(GE-VS-ID)**

Funktion	Klassisch	Fortschrittlich	Ideal
	und GE-05-KL). **(GE-VS-KL)**		

A.1.3 Netz

Ein Netz im Sinne dieser Säule ist ein Kommunikationsmedium, welches für den Transport von Daten zwischen Geräten verwendet wird. Es existieren durch die Organisation verwaltete Netze und organisationsfremde Netze sowie Übergänge zwischen diesen. Die Gesamtheit der Übergänge von einem Netz zu anderen Netzen wird als Netzperimeter bezeichnet und umfasst alle Komponenten, die den Übergang herstellen. Meistens ist ein Netzperimeter speziell abgesichert (z.B. durch Firewalls oder ALGs). Ein Netzsegment ist ein Teil eines Netzes. Meist zeichnet sich ein Netzsegment durch eine charakteristische Eigenschaft aus, zum Beispiel eine Ethernet-Broadcastdomain, ein IP-Subnetz oder einen definierten Perimeter. Netzsegmente können einen unterschiedlichen Umfang haben. Anhand der Größe wird zwischen Makrosegmentierung (große Netzsegmente) und Mikrosegmentierung (kleine Netzsegmente) unterschieden.

A.1.3.1 Integrationsmöglichkeiten

Funktion	Klassisch	Fortschrittlich	Ideal
Netzseg-mentierung **(NET-01)**	Die Organisation definiert ihre Netzarchitektur indem sie das Netz sehr grob aufteilt, bspw. nur in ein internes Netz, eine DMZ[2] und ein externes Netz (Makrosegmentierung) **(NET-01-KL)**	Die Organisation definiert ihre Netzarchitektur indem sie die DMZ und das interne Netz zusätzlich aufteilt in weitere Netzsegmente, bspw. durch eine weitere Segmentierung des internen Netzes in Client- und Servernetze. **(NET-01-FO)**	Die Organisation definiert ihre Netzarchitektur indem sie die Netzsegmente möglichst feingranular aufteilt (Mikrosegmentierung), bspw. durch eine Aufteilung in Netzsegmente für einzelne Anwendungen. **(NET-01-ID)**
Perimeterschutz **(NET-02)**	Die Organisation verwendet meistens nur eine Paketfilterung an den zentralen Netzübergängen mit statischen, manuell konfigurierten Regeln. **(NET-02-KL)**	Die Organisation verwendet neben der Paketfilterung zusätzliche Schutzmaßnahmen bis hoch zur Applikationsschicht mit zum Teil dynamisch konfigurierten Filterregeln, welche auf dem aktuellen autorisierten Kommunikationsbedarf basieren. Die Schutzmaßnahmen werden in unterschiedlicher Qualität an den unterschiedlichen Netzübergängen angewendet. **(NET-02-FO)**	Die Paketfilterung und die zusätzlichen Schutzmechanismen der Organisation werden dynamisch konfiguriert basierend auf dem aktuellen autorisierten Kommunikationsbedarf und schützen auch die durch die Mikrosegmentierung gebildeten kleinen Netzsegmente. **(NET-02-ID)**

[2] Demilitarisierte Zone

Funktion	Klassisch	Fortschrittlich	Ideal
Intrusion Detection & Prevention Systeme (IDS/IPS) (Threat Protection) **(NET-03)**	Die IDP/IPS der Organisation basieren primär auf bekannten Bedrohungen und statischen Netzverkehr filtern. Die Netzsensoren werden dabei an den zentralen, neuralgischen Netzübergängen positioniert. **(NET-03-KL)**	Die IDP/IPS der Organisation integrieren zusätzliche Netzfilterungsmechanismen (bspw. zeitbasierte und sitzungsbasierte Netzfilterung) um komplexere Bedrohungen zu erkennen. Die Netzsensoren werden dabei an den feingranulareren Netzübergängen positioniert. **(NET-03-FO)**	Die IDS/IPS der Organisation integrieren einen ganzheitlichen, automatisierten Bedrohungsschutz und filtern Netzverkehr metadaten- und kontextbasiert (bspw. Protokollbefehle, Payloads, Datentagging), um auch Anomalien erkennen zu können. Die Netzsensoren werden dabei an den durch die Mikrosegmentierung gebildeten Netzsegmenten positioniert. **(NET-03-ID)**
Verschlüsselung **(NET-04)**	Die Organisation verschlüsselt nur einen Teil des externen und internen Netzverkehrs kontextbasiert und nach erfolgter Risikobetrachtung einen Teil metadatenbasiert. **(NET-04-KL)**	Die Organisation verschlüsselt sowohl jeden externen Netzverkehr als auch große Teil des internen Netzverkehrs. Dies wird für beide Szenarien kontextbasiert und nach erfolgter Risikobetrachtung auch große Teile metadatenbasiert umgesetzt. **(NET-04-FO)**	Die Organisation verschlüsselt jeden externen als auch internen Netzverkehr kontextbasiert und nach erfolgter Risikobetrachtung auch metadatenbasiert. **(NET-04-ID)**
Detektion & Reaktion **(NET-DET)**	Die Organisation stellt Sichtbarkeit am Perimeter mit einer zentralisierten Aggregation und Analyse sicher. **(NET-DET-KL)**	Die Organisation integriert Analysen über mehrere Sensortypen und Positionen im Netz mit manuell konfigurierten Policies und Triggern zur Alarmierung. **(NET-DET-FO)**	Die Organisation integriert Analysen über mehrere Sensortypen und Positionen im Netz mit automatisch konfigurierten Policies und Triggern zur Alarmierungen und Ausführung automatischer, vordefinierter Reaktionen. **(NET-DET-ID)**
Anforderungen an VS **(NET-VS)**	Sehr häufig wird der Schutz der VS über eine Perimeterabsicherung sichergestellt. Diese kann neben IT-spezifischen auch materielle Maßnahmen, bspw. Approved	Neben der Perimeterabsicherung wird der Schutz der VS grundsätzlich durch die Absicherung der Endgeräte und eine Verschlüsselung der Datenübertragung innerhalb des Perimeters erreicht.	Der Schutz der VS wird durch die Absicherung aller Geräte gewährleistet. Die Übertragung zwischen allen Geräten, welche VS verarbeiten, erfolgt zugelassen verschlüsselt (NET-04-ID).

Funktion	Klassisch	Fortschrittlich	Ideal
	Circuits[3], umfassen. Abweichend von NET-02-KL wird der Einsatz einer PAP-Struktur an den Netzübergängen vorausgesetzt. Die eingesetzten Firewalls benötigen eine Zulassungsaussage. Innerhalb des Perimeters werden keine weiteren Maßnahmen getroffen. Es findet keine zugelassene Verschlüsselung des internen Netzverkehrs (vgl. NET-04-KL) und keine Netzsegmentierung (vgl. NET-01-KL) statt. Es wird nur außerhalb der Perimetergrenzen mit zugelassenen IT-Sicherheitsprodukten verschlüsselt. Die Sicherheitsbeziehungen und kryptographischen Einstellungen sind statisch. **(NET-VS-KL)**	Mit Fokus auf die jeweiligen Arbeitsgruppen die in gemeinsamen Themenbereichen aktiv sind, wird das Netz segmentiert (NET-01-FO). Es wird innerhalb der Perimetergrenzen zusätzlich eine Verschlüsselung zur Trennung des Grundsatzes „Kenntnis nur, wenn nötig“ verwendet (NET-02-FO). Die Sicherheitsbeziehungen und kryptographischen Einstellungen sind statisch. **(NET-VS-FO)**	Die Segmentierung wird weiter fortgesetzt mit dem Ziel einer Mikrosegmentierung (NET-01-ID). Die Netztrennung wird durch zugelassene Produkte unterstützt. Es wird innerhalb und außerhalb des Perimeterschutzes mit zugelassenen IT-Sicherheitsprodukten verschlüsselt (NET-04-ID). **(NET-VS-ID)**

[3] Vgl. BSI Technische Leitlinie „BSI TL-01101-3“

A.1.4 Anwendung

Eine Anwendung im Sinne dieser Säule ist ein Computerprogramm oder ein Softwaredienst der Organisation, welche on-premise oder bei Dritten ausgeführt wird, um Daten zu verarbeiten. Die sichere Anwendungsbereitstellung durch die Administration wird in dieser Säule nicht betrachtet (vgl. Abgrenzung des ZTA-Fokus im Grundlagenkapitel).

A.1.4.1 Integrationsmöglichkeiten

Funktion	Klassisch	Fortschrittlich	Ideal
Zugriffsautorisierung **(AW-01)**	Die Zugriffsautorisierung der Anwendungen der Organisation erfolgt primär auf Basis von statischen Attributen (bspw. Gruppenzugehörigkeiten). Mit diesen statischen Attributen sind in der Anwendung feste Berechtigungen verbunden. **(AW-01-KL)**	Die Zugriffsautorisierung der Anwendungen der Organisation erfolgt bereits zusätzlich mit dynamischen Attributen. Das heißt, Zugriffe können abhängig von den dynamischen Attributen unterschiedliche Berechtigungen aufweisen. **(AW-01-FO)**	Die Zugriffsautorisierung der Anwendungen der Organisation erfolgt basierend auf Echtzeitrisikoanalysen. Die angefragten Berechtigungen können dabei auch Teil der Echtzeitrisikoanalysen sein. Aus dem Ergebnis der Echtzeitrisikoanalysen gehen dabei dann die Berechtigungen des Zugriffs in der Anwendung ein. **(AW-01-ID)**
Berechtigungssystem in der Anwendung **(AW-02)**	Die Organisation verwendet in ihrem Berechtigungssystem der Anwendung grobgranulare Berechtigungsgruppen. **(AW-02-KL)**	Die Organisation verwendet in ihrem Berechtigungssystem der Anwendung feingranularere und komplexere Berechtigungen. **(AW-02-FO)**	Die Organisation verwendet in ihrem Berechtigungssystem der Anwendung kleinstmögliche und hochkomplexe Berechtigungen. **(AW-02-ID)**
Authentisierung zwischen Anwendungen **(AW-03)**	Anwendung untereinander authentisieren sich teilweise nicht oder meistens nur schwach (bspw. mit Hilfe eines einfachen Passworts). **(AW-03-KL)**	Anwendungen untereinander authentisieren sich meistens unter Verwendung zeitlich befristeter Zugriffstokens. **(AW-03-FO)**	Anwendungen untereinander authentisieren sich immer stark, dabei wird mindestens bei der initialen Provisionierung ein unabhängiger zweiter Faktor genutzt. Bei der Prüfung der Authentisierung werden auch dynamische Attribute berücksichtigt. **(AW-03-ID)**

Funktion	Klassisch	Fortschrittlich	Ideal
Bedrohungs-schutz (Threat Protection) **(AW-04)**	Die Organisation integriert die Anwendungsabläufe minimal in den Bedrohungsschutz. Es werden allgemeingültige, (also nicht anwendungsspezifische) Schutzmaßnahmen für bekannte Bedrohungen verwendet. **(AW-04-KL)**	Die Organisation integriert die Anwendungsabläufe grundlegend in den Bedrohungsschutz für bekannte Bedrohungen mit einigen Anwendungsspezifischen Schutzmaßnahmen. **(AW-04-FO)**	Die Organisation integriert die Anwendungsabläufe vollständig in den Bedrohungsschutz. Dabei werden für alle Bedrohungen anwendungsspezifische Schutzmaßnahmen in der Infrastruktur getroffen. **(AW-04-ID)**
Zugriffsmöglich-keit (Accessability) **(AW-05)**	Auf einige wenige Anwendungen der Organisation können Anwendende der Organisation und ggf. Dritte aus einem organisationsfremden Netz zugreifen (extern exponiert). Auf alle weiteren Anwendungen kann über ein Virtual Private Network (VPN), welches das interne Netz der Organisation erweitert, zugegriffen werden. **(AW-05-KL)**	Auf einen Großteil der Anwendungen der Organisation können Anwendende der Organisation und ggf. Dritte aus einem organisationsfremden Netz zugreifen (extern exponiert). Hierzu zählen auch Anwendungen, die vorher nur über das zentrale VPN der Organisation zugreifbar waren. **(AW-05-FO)**	Alle Organisationsanwendungen sind direkt von einem organisationsfremden Netz erreichbar (in direkter Abhängigkeit von NET-04-ID). **(AW-05-ID)**
Anwendungs-sicherheit **(AW-06)**	Die Organisation hat häufig weder Anforderungen an die Anwendungssicherheit noch testet sie diese vor einem Deployment. Die Prüfung der Anwendung sind vorranging funktionaler Natur. **(AW-06-KL)**	Die Organisation hat Anforderungen an die Anwendungssicherheit von selbstentwickelten Anwendungen als auch bei Beschaffungen (bspw. die Unterstützung moderner Authentisierungsmechanismen durch die Anwendung). Sie berücksichtigt und priorisiert die Erfüllung der Anforderungen auch im Rahmen der Abnahme vor dem Deploymentprozess. **(AW-06-FO)**	Die Organisation hat erweiterte Anforderungen an die Anwendungssicherheit sowohl bei selbst entwickelten Anwendungen als auch bei Beschaffungen (bspw. spezifische Logging-Anforderungen für eine Anwendungsspezifische Detektion, feingranulares Berechtigungssystem). Sie prüft die Erfüllung der Anforderungen bei einer Beschaffung durch geeignete Nachweise (bspw. durch eine Zertifizierung).

Funktion	Klassisch	Fortschrittlich	Ideal
			(AW-06-ID)
Detektion & Reaktion **(AW-DET)**	Die Organisation führt keine bis kaum Auswertungen von Anwendungsspezifischen Logdateien durch. **(AW-DET-KL)**	Die Organisation führt Auswertungen von einigen anwendungsspezifischen Logdateien (abseits Betriebssystemlogs) durch. Die Organisation integriert Analysen über mehrere Ereignisquellen mit manuell konfigurierten Policies und Triggern zur Alarmierung. **(AW-DET-FO)**	Die Organisation führt Auswertungen für alle anwendungsspezifischen Logdateien aus. Die Organisation integriert Analysen über mehrere Ereignisquellen mit automatisch konfigurierten Policies und Triggern zur Alarmierungen und Ausführung automatischer, vordefinierter Reaktionen. **(AW-DET-ID)**
Anforderungen an VS **(AW-VS)**	An Anwendungen, welche VS verarbeiten, werden selten Anforderungen zur Absicherung der VS gestellt. Stattdessen wird häufig auf die Absicherung des Gerätes gesetzt. Für die Umsetzung des Need-to-know kommen ausschließlich Autorisierungsfunktionen zum Einsatz, die durch das Produkt mitgeliefert werden. **(AW-VS-KL)**	Soll die Zugriffsautorisierung (vgl. AW-01-FO) und das Berechtigungssystem (vgl. AW-02-FO) auf Anwendungsebene auch für den Schutz der VS eingesetzt werden, dann orientiert sich die Autorisierung zusätzlich einerseits an der Einstufung der VS und der Verpflichtung, bzw. Ermächtigung des Nutzers. Im Anwendungsdesign wurden Anforderungen berücksichtigt, die einen unbefugten Zugriffsversuch unterbinden. Die Software verfügt über Funktionen zur Validierung von Eingaben zum Schutz vor Schadcode, bzw. vor unberechtigter Nutzung. **(AW-VS-FO)**	Im Idealfall wird eine feingranulare Zugriffsautorisierung (vgl. AW-01-ID) und Berechtigungssystem (vgl. AW-02-ID) eingesetzt, welches zusätzlich auch überprüft ob der Nutzer auch das „Need to know“ hat, um eine entsprechende VS zu lesen. Sollte dies nicht der Fall sein, verweigert die Anwendung den Zugriff. Die Anwendung verwendet eine zugelassene Autorisierungsfunktion zur Durchsetzung des Need-to-know und ist nachweislich robust gegenüber Angriffen ausgelegt. Das Need-to-know wird sowohl gegenüber den Nutzern als auch gegenüber den Administratoren umgesetzt. **(AW-VS-ID)**

A.1.5 Daten

Daten im Sinne dieser Säule sind (maschinen-)lesbare und –bearbeitbare digitale Repräsentationen von Informationen. Diese Daten besitzen zusätzlich strukturierte Metadaten, die Informationen über die Daten enthalten (bspw. Erstellungszeitpunkt, Zeitpunkt der letzten Änderung). Zudem sind Verschlusssachen (VS) im öffentlichen Interesse geheimhaltungsbedürftige Daten. Unter Tagging im Sinne dieser Säule ist gemeint, dass Tags als Metadaten zu Daten hinzufügt werden können, um diese Tags dann in der Formulierung und Auswertung von Zugriffsrichtlinien verwenden zu können.

Ein einzelnes Datum ist, in dem hier betrachteten Kontext, keine in der Praxis relevante Einheit, mehrere Daten werden regelmäßig gemeinsam verarbeitet. Der Anwendungsbereich der u. g. Funktionen dieser Säule umfasst immer mehr als ein Datum, daher ist diese Säule mit „Daten“ statt „Datum“ bezeichnet.

A.1.5.1 Integrationsmöglichkeiten

Funktion	Klassisch	Fortschrittlich	Ideal
Dateninventarisierung ***(DA-01)***	Die Organisation inventarisiert Daten manuell und nicht einheitlich/vollständig. Die Datenkategorisierung erfolgt dabei ausschließlich manuell. Es erfolgt keine explizite Zuordnung der Daten zu Geschäftsprozessen der Organisation. **(DA-01-KL)**	Die Organisation inventarisiert Daten manuell mit einigen automatisierten Trackingmöglichkeiten. Die Organisation führt die Datenkategorisierung mit einer Kombination aus manuellen und statischen Analysemethoden durch. Es erfolgt eine technische Zuordnung der Daten zu kritischen Geschäftsprozessen der Organisation. **(DA-01-FO)**	Die Organisation kategorisiert und inventarisiert Daten kontinuierlich mit einem vertrauenswürdigen Tagging und Tracking. Es erfolgt immer eine technische Zuordnung der Daten zu den Geschäftsprozessen der Organisation. **(DA-01-ID)**
Zugriffsermittlung (Access Determination) ***(DA-02)***	Die Organisation regelt den Zugriff auf Daten basierend auf statischen Zugriffskontrollen. **(DA-02-KL)**	Die Organisation regelt den Zugriff auf Daten basierend auf statischen und teilweise dynamischen Zugriffskontrollen, die sowohl die zugreifende Identität als auch ggf. weitere Attribute berücksichtigen. Das „Least Privilege“ Prinzip wird größtenteils umgesetzt. **(DA-02-FO)**	Die Organisation regelt den Zugriff auf Daten dynamisch nach Least-Privilege-Prinzipien, ermöglicht „just-in-time“ Zugriffsberechtigungen und kontinuierliche risikobasierte Zugriffsentscheidungen. Dabei werden bei den Policies für die Zugriffsentscheidung ausreichend Metadaten

Funktion	Klassisch	Fortschrittlich	Ideal
			der angefragten Daten hinzugezogen. Insbesondere die Integrität des Taggings der Daten wird dabei ausgewertet. **(DA-02-ID)**
Verschlüsselung[4] ***(DA-03)***	Die Organisation verschlüsselt ihre Daten häufig nicht „at rest“[5]. Eine Verschlüsselung der Daten „in use[6]“ erfolgt nicht. **(DA-03-KL)**	Die Organisation verschlüsselt ihre Daten größtenteils „at rest“. Die Organisation verschlüsselt ihre Daten in einzelnen Fälle „in use“. **(DA-03-FO)**	Die Organisation verschlüsselt ihre Daten “in use” und “at rest”. **(DA-03-ID)**
Schadensausmaßanalyse ***(DA-SAA)***	Die Ermittlung des Schadensausmaßes erfolgt manuell und nur eingeschränkt möglich. Sie ist nur nachträglich mit viel Aufwand möglich. **(DA-SAA-KL)**	Die Ermittlung des Schadensausmaßes von kritischen Geschäftsprozessen der Organisation ist teilautomatisiert und kurzfristig nachträglich möglich. **(DA-SAA-FO)**	Die automatische Ermittlung des Schadenspotentials von Datenzugriffen auf Geschäftsprozessen ist möglich und kann bei der Risikoanalyse verwendet werden. **(DA-SAA-ID)**
Anforderungen an VS ***(DA-VS)***	VS sind entsprechend dem Geheimhaltungsgrad zu kennzeichnen. Dies erfolgt in den meisten Fällen durch organisatorische Maßnahmen. Es erfolgt für VS des Geheimhaltungsgrades VS-NfD kein Inventarmanagement (DA-01-KL). Der Zugriff auf VS muss nach dem Grundsatz „Kenntnis nur, wenn nötig“	Sollen VS auch vom Inventarmanagement erfasst werden (DA-01-FO), dann muss der Geheimhaltungsgrad der VS miterfasst werden. Zusätzlich sollte erfasst werden, welche(r) Personen(-kreis) ein berechtigtes Interesse am Zugriff hat, damit dies in der Zugriffsermittlung (DA-02-FO) miterfasst werden kann.	Wird ein kontinuierliches Inventarmanagement (DA-01-ID) und eine dynamische Zugriffsberechtigung (DA-02-ID) auch für VS angestrebt, dann entspricht dies grob der Funktionsweise einer elektronischen Registratur. Das wichtigste Kriterium für einen dynamischen Zugriff ist, ob die Person, die auf die Datei zugreifen will, verpflichtet, bzw.

[4] Für eine Verschlüsselung „in transit“ siehe NET-04

[5] Daten, die sich in persistenten/nicht flüchtigen Speichersystemen (bspw. der Festplatte eines Gerätes) befinden

[6] Daten, die sich in nicht persistenten/flüchtigen Speichersystemen (bspw. dem Arbeitsspeicher eines Gerätes) befinden

Funktion	Klassisch	Fortschrittlich	Ideal
	erfolgen. Nach der VSA dürfen nur verpflichtete Personen Zugriff auf VS erhalten, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis haben müssen. Der Zugriff erfolgt auf statischen Zugriffskontrollen (DA-02-KL). Falls der Schutz der VS durch eine Verschlüsselung erfolgen soll (vgl. DA-03-KL) und diese dadurch IT-Sicherheitsfunktionen nach VSA umsetzt, dann muss die dafür verwendete Software eine Zulassungsaussage besitzen. Die Zugriffsberechtigung wird auf Basis der Ordnerstruktur erteilt/verwaltet. **(DA-VS-KL)**	Erfüllt die Verschlüsselung (DA-03-FO) eine Sicherheitsfunktion zum Schutz von VS, muss durch ein Produkt mit positiver Zulassungsaussage erfolgen. VS, die nicht mit einem Produkt mit positiver Zulassungsaussage geschützt wird, muss durch materielle Maßnahmen gesichert werden. VS sind grundsätzlich nur durch den Ersteller veränderbar oder lesbar. Die Zugriffsberechtigung anderer Nutzer muss manuell erteilt werden. **(DA-VS-FO)**	ermächtigt ist und Kenntnis über die VS haben muss. Die Verschlüsselung (DA-03-ID) von VS muss durch ein Produkt mit positiver Zulassungsaussage erfolgen. **(DA-VS-ID)**