Silvia Knittl

Zero Trust: Die letzte Bastion für die IT-Sicherheit deutscher Behörden

Seit 2005 werden Cyberangriffe gegen Bundesbehörden, Politik und Wirtschaftsunternehmen registriert. Diese treten immer häufiger auf, auch im Zusammenhang mit Spionage. [1] Die Folgen: Datenverlust, Betriebsstörungen und finanzielle Schäden. Durch diese Cyber-Attacken kann die Sicherheit und Effektivität der behördlichen Arbeit beeinträchtigt werden, außerdem kann es zu Vertrauensverlusten auf der Seite der Öffentlichkeit und zu starken Reputationsschäden sowie politischen und nationalen Sicherheitsrisiken führen. In diesem Artikel wird das Zero-Trust-Prinzip als möglichen Lösungsansatz der Sicherheitsarchitektur für Behörden vorgestellt.

1 Einführung

Für Behörden ist es unumgänglich, auf dem neuesten Stand in Bezug auf Cyber-Sicherheitsstrategien zu sein, um den aktuellen Bedrohungen entgegenzuwirken. Neue und flexible Sicherheitsansätze können Organisationen dabei unterstützen, sich sowohl gegen bestehende als auch neuartige Cyber-Risiken zu schützen. Hierbei gewinnt die Implementierung einer Zero-Trust-Strategie immer mehr an Bedeutung. In diesem Artikel wird die Notwendigkeit von Zero Trust im öffentlichen Sektor erläutert, indem zunächst die aktuelle Lage in Bezug auf Cyberangriffe herausgearbeitet wird. Ein Vergleich zum aktuellen Sicherheitsstandard im Weißen Haus sowie das Vorhaben des BSI und des Innenministeriums verdeutlichen die Dringlichkeit der Implementierung einer Zero-Trust-Strategie. Anschließend wird im Detail auf die Umsetzung des Zero-Trust-Prinzips als Treiber einer Enterprise Security Architecture als nachhaltige Lösung eingegangen. Ein Beispiel aus Estland zeigt die Vorteile von Zero Trust in der Praxis.

1.1 Die Bedrohungslage bleibt verschärft: Bedeutung der IT-Sicherheit für deutsche Behörden

Ransomware gilt als eine der größten Bedrohungen der Cyberkriminalität. [2] In den Jahren 2020 bis 2021 verdoppelten sich die Fälle, in denen Daten aus Ransomware-Angriffen veröffentlicht wurden. Dienstleistungen für Kriminelle, wie Ransomware-as-a-Service und Access-as-a-Service, werden immer beliebter und vereinfachen die Zugänge und sorgen dadurch für ein starkes Wachstum bei Cyber-Bedrohungen. [3] Zusätzlich tritt auch die Erpressung und Sabotage durch Cyberkriminalität spürbar häufiger auf. [4] Es breiten sich immer mehr Methoden der Cyber-gestützten Erpressung aus, wie beispielsweise das "Big Game Hunting", bei dem umsatzstarke Unternehmen, Krankenhäuser, Banken und auch Behörden für Lösegeldzahlungen erpresst werden. [5]

Bei sogenannten Denial-of-Service-Attacken (DDoS-Attacken) werden die Server der Zielwebsite mit vielen Anfragen geflutet, sodass diese unter der Last zusammenbrechen und die Webseite lahmgelegt wird [6]. Im April 2023 wurden mehrere Landesregierungen und Behörden angegriffen und viele Internetseiten von öffentlichen Stellen waren nicht mehr erreichbar. Hacker versuchten zudem eine Plattform des Bundesentwicklungsministeriums für den Wiederaufbau der Ukraine zu stören [7].

IT-Dienstleister von Behörden oder Ministerien stehen ebenfalls im Visier der Hacker. Im Mai 2023 wurde bekannt, dass Cyberkriminelle drei IT-Dienstleister von Bundesministerien und Behörden angegriffen haben und wahrscheinlich eine Vielzahl an E-Mail-Daten abgreifen konnten. Zwei dieser Unternehmen bestätigten, dass Daten in den falschen Besitz kamen. Eines dieser Unternehmen wurde bereits im Mai 2022 attackiert, was erst ein Jahr später auffiel. [8]

1.2 Steigende Angriffe durch geopolitische Lage

Neben den aktuellen Trends haben die Covid-19-Pandemie und der Krieg in der Ukraine zu einer signifikanten Zunahme von Cyberangriffen geführt. Bereits drei Tage nach Beginn des Krieges wurde ein Anstieg von 196% der Cyberangriffe auf die ukrainische Regierung und das Militär festgestellt. Auch im weiteren Kriegsverlauf zwischen Februar und August 2022 nahmen die At-

Dr. Silvia Knittl

ist Direktorin im Bereich Cyber Security & Privacy bei PwC Deutschland und leitet dort EMEA-weit die Enterprise Security Architecture-Gruppe.

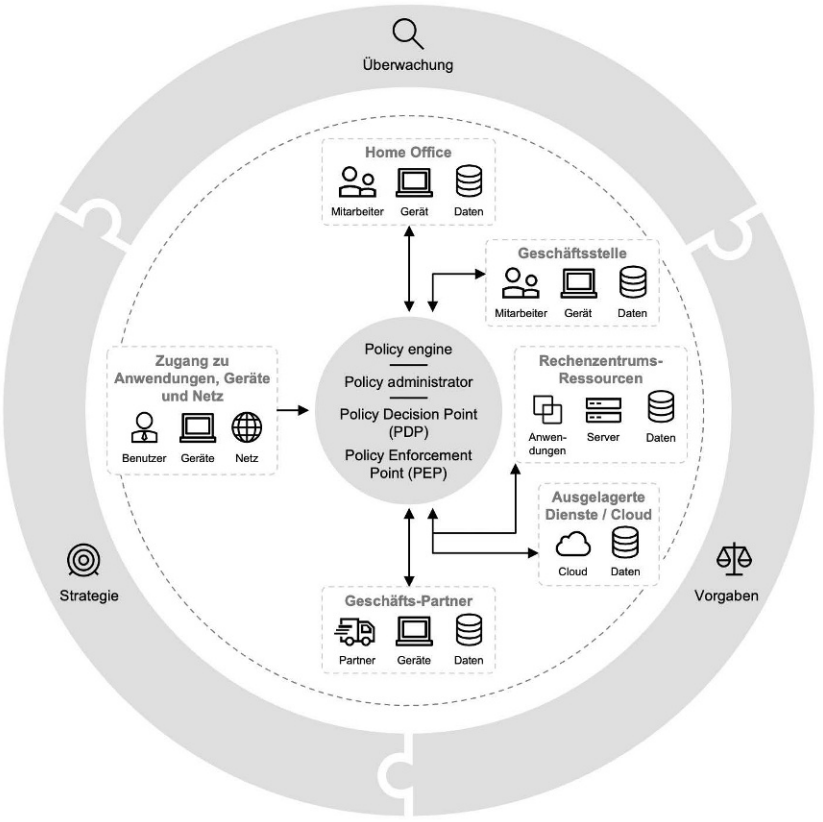
E-Mail: silvia.knittl@pwc.com

tacken um 112% zu. Das zeigt: Auch der virtuelle Krieg ist Bestandteil des Konfliktes. [9]

Zudem haben in Deutschland laut einer Studie von PwC 59% der Teilnehmenden angegeben, einen Anstieg seit dem Beginn des Ukraine-Krieges festgestellt zu haben. In den letzten zwölf Monaten waren die meisten Organisationen bis zu zehn kritischen Cyberangriffen ausgesetzt, während bei 30% der Teilnehmenden sogar mehr als zehn Angriffe verzeichnet wurden. Um der steigenden Cyber-Bedrohungslage entgegenzuwirken, fehlt es insbesondere im öffentlichen Sektor oft an IT-Sicherheitsexperten. [10]

Hinzu kommt, dass die Grenzen zwischen sogenannten „Hacktivisten" und staatlich gelenkten Hackern immer mehr verschwimmen. Cyberkriminelle haben ihre Vorgehensweise verändert und arbeiten teils über Ländergrenzen hinweg zusammen. Im Untergrund hat sich eine leistungsfähige kriminelle Dienstleistungswirtschaft entwickelt, in der Schadprogramme, Daten oder Ähnliches zum Kauf angeboten werden. [11]

Abbildung 1 | Zero Trust Bestandteile



2 Paradigmenwechsel und Zero Trust als Lösungsansatz

Der drastische Anstieg von Cyber-Bedrohungen und Datenschutzverletzungen verbunden mit einer steigenden Komplexität der digitalen Infrastruktur, verbunden mit dem Aufkommen fortschrittlicher Angriffsmethoden, stellt herkömmliche Sicherheitsansätze vor große Herausforderungen, sodass diese den Bedrohungen der heutigen vernetzten Welt nicht mehr standhalten können. Bisherige Sicherheitslösungen müssen überdacht werden, insbesondere im öffentlichen Sektor, wo die technischen Schulden aufgrund zurückhaltender Digitalisierung der vergangenen Jahre hoch sind und der Schutz kritischer Systeme und Daten im Vordergrund steht. [12] Zero Trust gewinnt als innovative Lösung zunehmend an Bedeutung.

2.1 Definition und Grundprinzipien von Zero Trust

In herkömmlichen, traditionellen Umgebungen wird davon ausgegangen, dass innerhalb eines – i. d. R. des eigenen – Netzes ein gewisses Vertrauensniveau implizit vorhanden ist und Bedrohungen oder Angriffe eher von außen zu erwarten sind. Diese Sicherheitsstrategien fokussieren sich lediglich auf die Sicherheit am Perimeter, d. h. Übergang zwischen dem öffentlichen und internen Netz, wodurch sie keinen ausreichenden Schutz gegen die heutigen Sicherheitsbedrohungen garantieren. [13] Zero Trust geht von der Annahme aus, dass alle Instanzen, sowohl innerhalb als auch außerhalb des Netzes, standardmäßig als nicht vertrauenswürdig erachtet werden. Dies trägt der modernen Arbeitsweise Rechnung, vereinfacht dargestellt in Abbildung 1. Mitarbeitende, Dienstleister und Bürger:innen greifen auf verschiedene digitale Dienste zu. Sie nutzen dazu eigene Geräte oder von der Behörde zur Verfügung gestellte. Die Anwendungen können sowohl innerhalb des eigenen Rechenzentrums oder ausgelagert beim Dienstleister oder in der Cloud betrieben werden.

Das National Institute of Standards and Technology (NIST) definiert Zero Trust als „*ein Cybersicherheitsparadigma, das sich auf den Schutz von Ressourcen und die Prämisse konzentriert, dass Vertrauen niemals implizit gewährt wird, sondern kontinuierlich evaluiert werden muss*". Das erfordert auch einen Kulturwandel, der die traditionellen Annahmen in Frage stellt. Folglich umfasst der Zero-Trust-Ansatz nicht nur technische Maßnahmen, sondern bedarf eine ganzheitliche Sicherheits-Mentalität. [14]

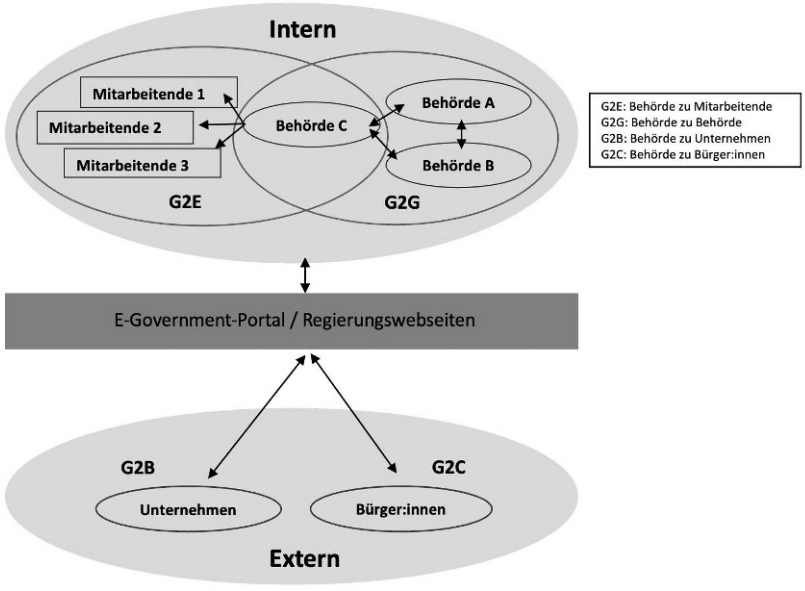
Mehrere Sicherheitsprinzipien bilden die Grundlage für Zero Trust und tragen der Vertrauenswürdigkeit von digitalen Ökosystemen bei. Das Prinzip „Never trust, always verify." oder auch „*Vertrauen ist gut, Kontrolle ist besser.*" ist ein grundlegendes Prinzip des Zero-Trust-Modells und betont die Notwendigkeit einer konsequenten Sicherheitsstrategie, die auf Kontrolle, Überprüfung und ständiger Wachsamkeit basiert. Das Prinzip beruht auf dem Verständnis, dass angemessene Verifikations- und Authenifizierungsmechanismen implementiert werden müssen. Durch die strikte Umsetzung dieses Prinzips wird das Risiko von unbefugtem Zugriff, Datenverlust oder Kompromittierung erheblich reduziert. Daneben beschränkt das Prinzip „Just enough Access" die Zugriffsberechtigungen auf die unmittelbar notwendigen Daten und Ressourcen. Das Prinzip gibt an, dass Nutzende nur die für ihre Tätigkeit benötigten Berechtigungen erhalten, um so den Schutz sensibler Daten zu gewährleisten. Just enough Access basiert somit auf dem Prinzip des „Least Privilege", in-

dem sichergestellt wird, dass Benutzer:innen nur die notwendigen Zugriffsrechte erhalten und keine übermäßigen Privilegien besitzen. Indem der Zugriff auf privilegierte Funktionen oder sensible Daten eingeschränkt wird, wird das Risiko von Fehlverhalten, Fehlkonfigurationen oder böswilligem Missbrauch reduziert. [15] Komplexe Cyber-Vorfälle treten derzeit häufig auf, wenn Angreifende Anmeldedaten nutzen, um Zugriffsberechtigungen zu erlangen, die über ihre eigenen Benutzerrechte hinausgehen. Somit wird durch dieses Prinzip die Angriffsfläche verringert.

Zusätzlich begrenzt das Prinzip „Just in Time" die Zugriffsrechte auf den bestimmten Zeitraum, der für eine Tätigkeit vorgesehen ist.

Um das Konzept von Zero Trust effektiv umzusetzen, bedarf es einer integrierten Lösung, bei der verschiedene Komponenten zusammenarbeiten und ein umfassendes Zero-Trust-Ökosystem schaffen (vgl. Abbildung 1). Ausgehend von der Strategie und Leitlinie wird abgeleitet, welche expliziten Vertrauenslevel notwendig sind bzw. wie hoch der Risikoappetit einer Organisation ist. Zudem muss festgelegt werden, welche Akteure adressiert werden.

Abbildung 2 | Behördenakteure nach [18]



Die technischen Komponenten "Policy Engine", "Policy Decision Point" (PDP) und "Policy Enforcement Point" (PEP) setzen die notwendigen Vertrauensstufen um, die für die verschiedenen Akteure notwendig sind. [16] Dabei fungiert die Policy Engine als zentrales Steuerelement und verantwortet die Verwaltung und Umsetzung der Sicherheitsrichtlinien im Zero-Trust-Modell. Der PDP bereitet Entscheidungen für eine Nutzungsanfrage vor. Damit werden die Sicherheitsrichtlinien analysiert und anhand von verschiedenen Faktoren die Entscheidung darüber getroffen, ob der Zugriff auf eine Ressource erlaubt oder verweigert wird. Beim PEP wird die getroffene Entscheidung dann automatisiert umgesetzt [17]. Die Einführung einer Policy Engine, eines PDPs und eines PEPs im Kontext von Zero Trust ermöglichen einen höheren Grad der Automatisierung.

Eine umfassende Strategie umfasst alle Akteure, mit denen eine Behörde interagiert, d. h. Mitarbeitender, Dienstleister, Bürger:innen oder Zugriffe- sowie Datenaustausche zwischen den Behörden (Abbildung 2). Diese Vorgaben beinhalten an den Risikoappetit angepasste Zugriffskontrollen, Authentifizierungsverfahren, Verschlüsselung, Berechtigungsstufen und weitere Sicherheitsmaßnahmen, die als Leitfaden für die Implementierung und den Betrieb des Zero-Trust-Konzepts dienen. Dadurch wird eine einheitliche Vorgehensweise der Komponenten des Ökosystems sichergestellt.

Des Weiteren wird durch das integrierte Monitoring eine kontinuierliche Überwachung des Netzverkehrs, der Benutzeraktivitäten und der Sicherheitsereignisse sichergestellt, wodurch verdächtige Aktivitäten oder Anomalien erkannt und entsprechende Maßnahmen frühzeitig ergriffen werden können.

Der vorgestellte Ansatz basiert auf globalen Standards. Das Zero-Trust-Modell von CISA bildet eine wichtige Grundlage und enthält die folgenden fünf komplementären Handlungsbereiche: Identität, Geräte, Netze, Anwendungen und Workloads und Daten mit den jeweils drei übergreifenden Themen: Sichtbarkeit und Analyse, Automatisierung und Orchestrierung sowie Governance.

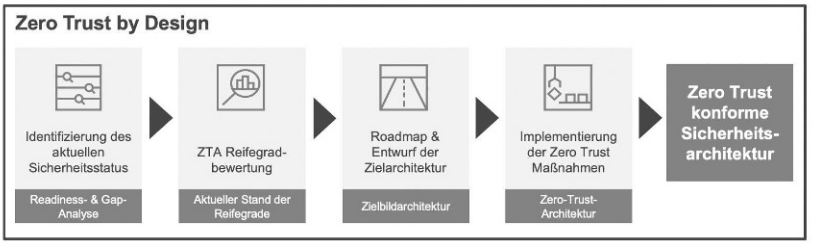
Innerhalb jedes Bereichs bietet das Modell spezifische Beispiele, um die eigene Reife einzuschätzen. [19] Die vorher vorgestellten technischen Komponenten können verschiedene Ausprägungen in den jeweiligen Handlungsbereichen haben und müssen aufeinander abgestimmt werden, um das volle Automatisierungspotenzial auszuschöpfen.

3 Enterprise Security Architecture (ESA) als Methodik zur Implementierung von Zero Trust

Die Umsetzung von Zero Trust im öffentlichen Sektor erfordert eine ganzheitliche Methode, um die Komplexität zu bewältigen und die Sicherheit auf allen Ebenen der Organisation zu gewährleisten. Eine Enterprise Security Architecture (ESA) (vgl. [20]) trägt mit bewährten Methoden dazu bei, die Entwicklung, Implementierung und Verwaltung einer umfassenden Sicherheitsstrategie basierend auf den Prinzipien von Zero Trust in einen strukturieren Rahmen zu fassen. Im Kontext von Zero Trust kann ESA im öffentlichen Sektor dabei unterstützen, ein Sicherheitsmodell zu implementieren, das anpassungsfähig, proaktiv und risikobewusst ist. Der ganzheitliche Ansatz von ESA ermöglicht eine umfassende Analyse, Messung und Überwachung der aktuellen Sicherheitslage, indem ein Rahmen zur Bewertung der Wirksamkeit von Sicherheitskontrollen, Überwachung von Sicherheitsvorfällen, Richtlinienverstößen und Compliance-Problemen in Echtzeit geschaffen wird. Zudem schafft ESA die Identifizierung von kritischen und schutzbedürftigen Assets, bewertet die damit verbundenen Risiken und unterstützt die Implementierung der erforderlichen Maßnahmen.

Die Implementierung einer Zero-Trust-Architektur von der Analyse bis zum strukturierten Lagebild sowie abgestimmter Roadmap kann mithilfe von ESA wie folgt durchgeführt werden (Abbildung 3): Zunächst erfolgt die Identifizierung der relevanten Cyber-Fähigkeiten und bereits eingesetzten IT-Systeme mit Sicherheitsbezug in Form eines Lagebilds, welches anhand von Reifegraden bewertet wird. Das Lagebild bildet die Grundlage für die Entwicklung der Zielbild-Architektur. Aus diesem werden strategische Empfehlungen abgeleitet, die sich an den geschäftlichen und technischen Anforderungen des Unternehmens orientieren und priorisiert eine Zero-Trust-Roadmap darstellen. Anhand der Roadmap erfolgt im letzten Schritt die Umsetzung der definierten Maßnahmen, die Implementierung der neu definierten Prozesse sowie eine kontinuierliche Verbesserung der neu implementierten Prozesse und Technologien.

Abbildung 3: Zero Trust by Design Ansatz



Die Vorgehensweise zur Anwendung von ESA wird beispielsweise von PwCs Enterprise-Security-Framework unterstützt, welches einen Fähigkeitenkatalog von über 300 in der Praxis erprobten und vorkonfektionierten Cyber-Fähigkeiten umfasst, mit denen eine auf die individuelle Bedrohungslage des Unternehmens angepasste Sicherheitsarchitektur entwickelt und bewertet werden kann (siehe exemplarisch in [20]). Cyber-Fähigkeiten beschreiben dabei die für die Ausgestaltung einer Fähigkeit relevante Zusammenarbeit von Menschen, Prozessen und Technologien (siehe auch Fähigkeiten (engl. Capabilities) gem. TOGAF in [21]). Diese vordefinierten Fähigkeiten dienen damit als Muster für Blaupausen der Sicherheitsarchitektur und ermöglichen eine effiziente und beschleunigte Umsetzung einer Zero Trust konformen Sicherheitsarchitektur.

3.1 Estland zeigt die Vorteile der ganzheitlichen Umsetzung von Zero Trust

Eine Zero-Trust-Architektur im öffentlichen Sektor zu implementieren ist komplex, aber nachhaltig. Es ist von wesentlicher Bedeutung zu erkennen, dass Zero Trust nicht impliziert, sämtliche Komponenten gänzlich neu zu konzipieren. Vielmehr besteht die Zielsetzung darin, auf vorhandenen Initiativen aufzubauen (vgl. auch [16]). Ein exemplarisches Vorgehen hierfür ist die Integration des BSI-Grundschutzes als Ausgangspunkt. Demnach gilt es, beispielsweise bei der Bewertung von Assets zu ermitteln, welches Schutzniveau präzise erforderlich ist. In diesem Kontext umfasst Zero Trust ebenso die Beantwortung der Fragestellung, welches Schutzniveau beziehungsweise Vertrauenslevel notwendig ist.

Dabei ist entscheidend, dass Bürger:innen in den Umsetzungsprozess der Cybersicherheitsstrategie mit einbezogen werden. Das Beispiel Estland verdeutlicht, wie Zero Trust ganzheitlich als notwendiger Schutzmechanismus in Zeiten steigender Cyberangriffe dienen kann und gleichzeitig eine vertrauenswürdige und effiziente staatliche Digitalisierung ermöglicht. Laut einer Umfrage von e-estonia, der staatlichen Digitalisierungsinitiative Estlands, sind 99% der Dienstleistungen online und 64% der Bürger:innen nutzen ihren elektronischen Ausweis regelmäßig. Es wird deutlich, dass die estnische Gesellschaft Vertrauen in die Digitalisierung hat, dadurch, dass die Behörden durch Zero Trust Datensicherheit und Datenschutz ernst nehmen. Das Vertrauen in die Digitalisierung entsteht, da die Bürger:innen jederzeit einsehen können, wer die eigenen Daten wann und wie abruft oder nutzt, wodurch sie ihre „Data Ownership" behalten.

Auch für die estländischen Behörden wird die Handhabung der eID bei Sicherheitsvorfällen bedeutend leichter. Beispielsweise konnten so 2017 über 600.000 fehlerhafte digitale Ausweise aus der Ferne nachgebessert werden, so entstand eine enorme Zeitersparnis. [22]

Am Beispiel Estland wird somit deutlich, dass Digitalisierung vertrauensvoll gestaltet und jede Zero-Trust-Transformation individuell betrachtet und implementiert werden muss, um langfristig erfolgreich zu sein. Die individuellen Bedürfnisse und Anforderungen der jeweiligen Bürger:innen und Mitarbeitenden müssen in den Umsetzungsprozess mit einbezogen werden. Dafür wurden bei der Einführung des estnischen digitalen Identitätssystems e-Estonia Befragungen durchgeführt, um die Bedürfnisse der Bürger:innen zu berücksichtigen. Zudem halfen Schulungen und Sensibilisierungsmaßnahmen von rund 30.000 Menschen im Rahmen des Schulungsprojekt „eCitizen's Training Network" dabei, diese im Alltag zu begleiten und den Mehrwert der neuen Cyber-Sicherheitsstrategie zu verdeutlichen. Die Weiterentwicklung der eID-Software erfolgt basierend auf dem Feedback der Benutzer, wodurch die Bürger:innen ein aktiver Teil des Weiterentwicklungsprozesses sind. [23]

3.2 Innenministerium fordert schrittweise Implementierung einer Zero-Trust-Architektur

Das Innenministerium plädiert für eine schrittweise Implementierung einer Zero-Trust-Architektur als Reaktion auf die zunehmend kritische Cyber-Sicherheitslage. Dies forderte beispielsweise Andreas Könen, Leiter der Abteilung Cyber- und IT-Sicherheit im Bundesinnenministerium (BMI) auf der Jahreskonferenz des Verbands Teletrust in Berlin. [24] Könen erwartet, dass sich der Bund „schrittweise in Richtung Zero Trust" aufstellt. [25] Laut Könen erhofft so der Bund von vornherein zu verhindern, dass Angriffsmittel (wie Schadsoftware) in IT-Systemen installiert werden können. [26] In der praktischen Umsetzung erfordert dies sichere und skalierbare Vertrauensdienste und lenkt auch die Aufmerksamkeit auf das Thema digitale Souveränität. [24]

An dieser Stelle kann die eIDAS-Verordnung als ein wichtiger Baustein für den Übergang zu einer vertrauensvollen Zero-Trust-Infrastruktur dienen, der die formellen Anforderungen als Grundstein legt. Die eIDAS-Verordnung bietet zunächst einen rechtlichen Rahmen für elektronische Identifizierung und Vertrauensdienste in der Europäischen Union und trägt dazu bei, das Vertrauen in elektronische Transaktionen zu stärken. [27] Die

Ermöglichung vertrauenswürdiger Verbindungen und Transaktionen zwischen verschiedenen Parteien stellt gleichzeitig eine grundlegende Voraussetzung für eine Zero-Trust-Architektur dar. Durch die Implementierung der eIDAS-Verordnung werden vertrauenswürdige Dienste und Mechanismen für Identitätsüberprüfung und Authentifizierung bereitgestellt, die den Prinzipien des Zero-Trust-Ansatzes entsprechen und verschiedene Anwendungsfälle ermöglichen (vgl. [28], [29], [30]).

Insbesondere in der eIDAS-Verordnung (EU 910/2014) wird explizit die Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierung dargestellt mit Verweis auf die Norm ISO/IEC 29115 „Information technology – Security techniques – Entity authentication assurance framework". Das stellt eine wichtige Handreichung dar, an der sich Behörden orientieren können [31].

3.3 Vorreiter: US-Regierung

Während in Deutschland und anderen Teilen Europas kein konkreter Plan vorliegt, steigt zumindest das Bewusstsein für die Notwendigkeit und die Umsetzung von Zero Trust. Im Gegensatz dazu herrscht in den USA bereits formaler Druck auf Behörden und Unternehmen. [32] Die US-Regierung strebt eine bundesweite Modernisierung ihrer Sicherheitskonzepte an. Dabei setzen sie als oberste Prämisse auf die Zero-Trust-Architektur als neue Strategie.

Im Mai 2021 veranlasste Präsident Joe Biden die Executive Order (EO) 14028 zur Verbesserung der Cybersicherheit der Nation. Ziel ist in erster Linie, die Sicherstellung grundlegender Sicherheitspraktiken, um die US-Regierung zu einer Zero-Trust-Architektur zu migrieren. Abschnitt 3 fordert die Bundesbehörden und ihre Lieferanten ausdrücklich dazu auf, *„[ihren] Ansatz zur Cybersicherheit zu modernisieren*", indem sie den Wechsel zu sicheren Cloud-Diensten beschleunigen und eine Zero-Trust-Architektur implementieren. So sollen unter anderem auch die Sicherheitsvorteile einer Cloud-basierten Infrastruktur genutzt und gleichzeitig Risiken vermindert werden.

Um Unsicherheiten für Behörden zu reduzieren und einen gemeinsamen Weg zur Umsetzung der Order zu skizzieren, wurde eine Federal Zero Trust Architecture (ZTA)-Strategie festgelegt, die die Behörden verpflichtet, bis Ende des Geschäftsjahres 2024 bestimmte Cyber-Sicherheitsstandards und -Ziele zu erfüllen. Die Umsetzung umfasst unter anderem [12]:

- die Konsolidierung der Identitätssysteme der Agenturen
- die Bekämpfung von Phishing durch starke Multifaktor-Authentifizierung
- die Behandlung interner Netze als nicht vertrauenswürdig
- die Verschlüsselung des Datenverkehrs
- die Verlagerung des Schutzes näher an die Daten durch Stärkung der Anwendungssicherheit

So sollen in den USA bis 2024 die meisten Behördensysteme auf eine ZTA umgestellt sein. Gemäß einem Bericht setzen über 70% der US-Bundesbehörden konsequent auf das Zero-Trust-Konzept, während weitere 26% es selektiv anwenden. [33]

Neben dem Weißen Haus arbeiteten ebenfalls das National Cyber Security Center (NCSC) aus Großbritannien und das National Institute of Standards and Technology (NIST) an Leitlinien und Schlüsselprinzipien für die Implementierung einer ZTA. [34]

4 Fazit und Ausblick

Insgesamt lässt sich festhalten, dass die Implementierung von Zero Trust für Behörden eine wirksame Möglichkeit darstellt, ihre Sicherheitsmaßnahmen zu verbessern und potenzielle Bedrohungen frühzeitig zu erkennen und abzuwehren. Sowohl das Bundesamt für Sicherheit in der Informationstechnik als auch das deutsche Innenministerium erkennen die Notwendigkeit einer Zero-Trust-Implementierung und planen eine schrittweise Umsetzung.

Die Bestrebungen der USA können als vorbildhaftes Beispiel dienen und zeigen, dass die Umsetzung mit einer Modernisierung einhergehen kann. Die estnischen Digitalisierungsinitiativen verdeutlichen, dass eine aktive Kommunikations- und Informationspolitik ein kritischer Erfolgsfaktor für die Akzeptanz der Bürger:innen ist.

Es ist festzuhalten, dass auch deutsche Behörden aufholen und fortschrittliche Sicherheitskonzepte einführen wollen, um ihre Sicherheitsmaßnahmen zu stärken und sich frühzeitig gegen potenzielle Bedrohungen zu wappnen. Durch die Anwendung moderner Sicherheitskonzepte wie Zero Trust können sie ihre Systeme effizient schützen und das Vertrauen in ihre Dienstleistungen stärken.

Literatur

[1] BMI, „Mehr Angriffe auf Politik, Behörden & Wirtschaft durch Cyber-Spionace," 2023. [Online]. [Zugriff am 20 06 2023].

[2] BSI, „Ransomware – Fakten und Abwerhstrategien," [Online]. [Zugriff am 20 06 2023].

[3] PwC, „Cyber Threats 2021: A Year in a Retrospect," 2022. [Online]. [Zugriff am 20 06 2023].

[4] Crowdstrike, „Geschichte der Ransomware," [Online]. [Zugriff am 20 06 2023].

[5] Crowdstrike, „Big Game Hunting durch Cyberangreifer," 02 11 2022. [Online]. Available: https://www.crowdstrike.de/cybersecurity-101/cyber-big-game-hunting/. [Zugriff am 20 06 2023].

[6] Tagesschau, „Bundesregierung bestätigt Hacker-Angriffe," 09 05 2022. [Online]. [Zugriff am 20 06 2023].

[7] „Bundesweite Cyberattacken auf Ministerien und Behörden," 04 04 2023. [Online]. [Zugriff am 20 06 2023].

[8] C. Grükov, A. Meyer-Fünffinger und M. Zierer, *IT-Dienstleister des Bundes im Visier,* 2023.

[9] H. Wieler, „Wie Cyberkriminalität als Waffe im Ukraine-Krieg eingesetzt wird," 26 09 2022. [Online]. Available: https://www.infopoint-security.de/wie-cyberkriminalitaet-als-waffe-im-ukraine-krieg-eingesetzt-wird/a32283/. [Zugriff am 20 06 2023].

[10] PwC, „Cyber Security in Germany," [Online]. Available: https://www.strategyand.pwc.com/de/en/industries/public-sector/cyber-security-in-germany.html. [Zugriff am 27 06 2023].

[11] M. Hein, „Mehr Cybercrime durch Krieg in der Ukraine," DW, 09 05 2022. [Online]. Available: https://www.dw.com/de/wie-der-krieg-in-der-ukraine-mit-cybercrime-zusammenh%C3%A4ngt/a-61739052. [Zugriff am 20 06 2023].

[12] Executive Office of the President, „Memorandum for the Heads of Executive Departments and Agencies," Whitehouse Gov, 2022.

[13] PwC, „Zero Trust Assessment & Architecture," 2023. [Online]. Available: https://www.pwc.de/de/im-fokus/cyber-security/enterprise-security-architecture/zero-trust-assessment-and-architecture.html. [Zugriff am 20 06 2023].

[14] S. Rose, O. Borchert, S. Mitchell und S. Connelly, „Zero Trust Architecture," NIST, 2023.

[15] NIST, „An Introduction to Information Security," NIST, 2023.

[16] C. Buck, T. Eymann und D. Jelito, „Cyber-Sicherheit für kritische Energieinfrastrukturen – Handlungsempfehlungen zur Umsetzung einer Zero-Trust-Architektur," *HMFD,* Bd. 60, p. 494–509, 2023.

[17] C. Buck, C. Olenberger, A. Schweizer, F. Völter und T. Eymann, „Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-trust," in *Computers & Security*, 2021.
[18] A. R. Alsoud, *Towards a Life-Event Oriented Governement-to-Citizen E-Service Provision in Jordan: The NoBLE Framework,* 2012.
[19] CISA, „Zero Trust Maturity Model," Cybersecurity & Infrastructure Security Agency, 2023.
[20] K. Ismailji, C. Mosler und S. Knittl, „Anwendbarkeit von Enterprise Security Assessments sowie Enterprise Architecture Tools für KMU," in *35. AKWI-Jahrestagung*, 2022.
[21] T. O. Group, „TOGAF Definitions," The Open Group, [Online]. Available: https://pubs.opengroup.org/architecture/togaf91-doc/arch/chap03.html.
[22] e-Estonia, „Facts & Figures".
[23] „Estonian eID card: entering the contactless world," 14 June 2017. [Online]. Available: https://e-estonia.com/estonian-eid-card-entering-the-contactless-world/. [Zugriff am 12 July 2023].
[24] Bare.ID, „Bund forciert Zero-Trust Architektur," 2022. [Online]. Available: https://www.bare.id/ressourcen/blog/zerotrust-bund/. [Zugriff am 06 2023].
[25] S. Scheuer, „Zero Trust: Diese Technologie verändert Sicherheit – und die Arbeitswelt," Handelsblatt, 13 08 2022. [Online]. Available: https://www.handelsblatt.com/technik/cybersecurity/insight-innovation-zero-trust-diese-technologie-veraendert-cybersicherheit-und-die-arbeitswelt/28569546.html. [Zugriff am 12 07 2023].
[26] S. Krempl, „Zero Trust: Bund will bei IT-Sicherheit niemanden mehr vertrauen," *heise online,* 28 06 2022.
[27] ENISA, „Building Trust in the Digital Era: ENISA boosts the uptake of the eIDAS regulation," 11 03 2021. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/building-trust-in-the-digital-era-enisa-boosts-the-uptake-of-the-eidas-regulation. [Zugriff am 20 06 2023].
[28] H. Strack, S. Karius, M. Gollnick, M. Lips, S. Wefel und R. Altschaffel, „Preservation of (higher) Trustworthiness in IAM for distributed workflows and systems based on eIDAS," in *Open Identiy Summit*, 2022.
[29] M. M. Roca, *New Innovations in eIDAS-compliant Trust Services: Anomaly detection on log data,* Universitat Politècnica de Catalunya, 2020.
[30] D. G. Berbecaru, A. Lioy und C. Cameroni, „Providing Login and Wi-Fi Access Services With the eIDAS Network: A Practical Approach," *IEEE ACCESS,* pp. 126186-126200, 2020.
[31] EUROPEAN COMMISSION, „IMPLEMENTING REGULATION (EU) 2015/1502," *Official Journal of the European Union,* 08 09 2015.
[32] J. Jung, „Effektive Zero-Trust Initiativen," zdnet, 02 08 2022. [Online]. Available: https://www.zdnet.de/88402689/effektive-zero-trust-initiativen/. [Zugriff am 20 06 2023].
[33] S. Scheuer, „Zero Trust: Diese Technologie verändert Cybersicherheit – und die Arbeitswelt," *Handelsblatt,* 13 08 2022.
[34] Merlin, „More than 90 Percent of Federal Cybersecurity Decision Makers Have Increased Confidence in Implementing Zero Trust following Government Mandates," 25 01 2022. [Online]. Available: https://www.businesswire.com/news/home/20220125005864/en/More-than-90-Percent-of-Federal-Cybersecurity-Decision-Makers-Have-Increased-Confidence-in-Implementing-Zero-Trust-following-Government-Mandates. [Zugriff am 20 06 2023].