Fraunhofer SIT

Zero-Trust für Kommunen

Handreichung zur Umsetzung von Zero-Trust in Kommunen

Matthias Enzmann, Daniel Trick, Ruben Wolf

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

HESSEN
Hessisches Ministerium
des Innern, für Sicherheit
und Heimatschutz

Liebe Leserin, lieber Leser,

Die Lage der Cyberbedrohungen in Deutschland bleibt angespannt. Kommunen, Landkreise, Unternehmen und öffentliche Einrichtungen sind täglich Ziel von Cyberangriffen. Cyberangriffe auf Kommunen legen mitunter über Wochen hinweg Abläufe still. In der Folge fallen Bürgerdienste aus, Anträge bleiben liegen und Termine platzen. Die Auswirkungen betreffen den Alltag der Menschen direkt. Der Schaden geht über die Technik hinaus, denn das Vertrauen der Bürger schwindet oft schneller, als es wieder aufgebaut werden kann. Es gibt keine absolute Sicherheit, auch nicht mit erheblichem Mitteleinsatz. Keine einzelne Kommune kann Angriffe vollständig abwehren. Es ist jedoch möglich, den Aufwand für Angreifer spürbar zu erhöhen und Schäden zu begrenzen. Genau an diesem Punkt setzt Zero-Trust an.

Das Zero-Trust-Motto „Never trust, always verify“ beschreibt die nüchterne Lage: In digital vernetzten Verwaltungsstrukturen ist implizites Vertrauen fehl am Platz. Geräte, Konten und Netzwerkverbindungen stehen allesamt unter einem Vertrauensvorbehalt. Vertrauen muss immer neu „verdient“ werden. Zugriffsberechtigungen entstehen nicht durch angenommenes Vertrauen, sondern durch stetige Prüfung. Und diese Prüfung endet nicht mit der Anmeldung am System. Hier setzt diese Handreichung des Fraunhofer-Instituts für Sichere Informationstechnologie SIT an. Sie wurde gemeinsam mit engagierten Kommunalvertretern und dem Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz erarbeitet. Die Handreichung ist praxisnah und unabhängig von der Größe der Kommune oder dem Reifegrad der IT anwendbar. Anhand von fünf thematischen Feldern werden konkrete Maßnahmen zur Einführung von Zero-Trust in Kommunen und Landkreisen dargestellt. Viele Maßnahmen sind miteinander verzahnt, aber bereits einzelne Schritte führen zur Verbesserung der Cybersicherheit. Es geht nicht darum, alles sofort auf den Kopf zu stellen. Vielmehr wollen wir mit Augenmaß und dem notwendigen Nachdruck schrittweise vorangehen.

Das Land Hessen begleitet seine Kommunen mit konkreten Unterstützungsangeboten. Mit dem Aktionsprogramm Kommunale Cybersicherheit haben wir zusätzliche Angebote geschaffen. Dabei geht das Angebot von Pentests über Notfallplanung bis hin zu eLearning-Modulen für kommunale Beschäftigte. Über 350 hessische Kommunen haben diese Angebote bereits genutzt. Cybersicherheit erfordert die enge Zusammenarbeit von Bund, Ländern und Kommunen, aber auch die Eigenverantwortung jeder einzelnen Organisation. Diese Handreichung ist ein Beitrag dazu, diese Eigenverantwortung mit konkretem Wissen zu unterlegen. Ich danke dem Fraunhofer SIT sowie allen Beteiligten, die durch ihre Expertise und Offenheit das Gelingen dieses Projekts ermöglicht haben. Nehmen Sie bitte die Angebote des Landes in Anspruch und gehen Sie die nächsten Schritte. Denn bei der Cybersicherheit gilt: Wer wartet, verliert.

Prof. Dr. Roman Poseck
Hessischer Minister des Innern, für Sicherheit und Heimatschutz

Executive Summary

Die Einführung von Zero-Trust-Maßnahmen kann die Resilienz hessischer Kommunen gegenüber Cyberangriffen nachhaltig stärken. Erfolgreiche Angriffe werden hierdurch erschwert und selbst wenn sie gelingen, wird das Schadensausmaß deutlich begrenzt. Einer der Leitsätze von Zero-Trust besagt, dass stets der Fall eines erfolgreichen Angriffs berücksichtigt werden soll („Assume Breach“) und für diesen Maßnahmen zur Eindämmung vorzusehen sind. Die Umsetzung von Zero-Trust-Maßnahmen ist allerdings fordernd, sowohl was den technischen als auch den zeitlichen Hintergrund betrifft. Die Einführung von Zero-Trust benötigt vielfach Jahre und sollte deshalb in evolutionären Schritten erfolgen. In der vorliegenden Handreichung werden für fünf technische Säulen einer Zero-Trust-Architektur – Identität, Geräte, Netzwerk, Workload & Apps, Daten – erste Schritte in allgemeiner Form beschrieben, die einen unmittelbaren Sicherheitsgewinn bieten. Identitäten von Nutzungskonten sollen im ersten Schritt mittels Multi-Faktor-Authentifizierung abgesichert, Berechtigungen dieser Konten nach dem Least-Privilege-Prinzip vergeben und administrative Konten von Nutzungskonten strikt getrennt werden. Geräte sollten zentral inventarisiert, für denselben Einsatzzweck (bspw. selbes Fachamt) einheitlich konfiguriert und kontinuierlich im laufenden Betrieb mittels EDR-Agenten überwacht werden, bspw. im Hinblick auf Schadsoftware und ungewöhnliches Verhalten im Netzwerk. Als fortgeschrittene Maßnahme empfiehlt sich Comply-to-Connect, das Geräten erst nach eingehender Prüfung im Hinblick auf die Einhaltung der kommunalen Sicherheitsrichtlinie (Compliance) Zugang zum kommunalen Netzwerk gewährt. Im kommunalen Netzwerk sollte Netzwerksegmentierung genutzt werden, um verschiedene funktionale oder fachliche Bereiche voneinander zu trennen, sodass diese nur über dedizierte Übergangspunkte zugänglich sind. Die Trennung kann initial grob über VLANs und Firewalls realisiert und im nächsten Schritt mittels Software-Defined-Networks, das größere Flexibilität und einfachere Verwaltung ermöglicht, verfeinert werden (Mikrosegmentierung). Daneben sollte der Netzwerkzugang von Geräten mittels zertifikatsbasierter Netzwerkzugangskontrolle (NAC) reglementiert werden. Für die kontinuierliche Überwachung des Netzwerks sollten Intrusion-Detection-/Intrusion-Prevention-Systeme genutzt werden, um Cyberangriffe schneller erkennen und ggf. darauf reagieren zu können. Als initialer Schritt im Bereich Workload & Apps sollte ein zentrales Software-Inventar erstellt werden, das u. a. einen Überblick darüber gibt, welche Anwendungen in der Kommune genutzt werden, deren aktuelle Versionsstände, existierende Schwachstellen sowie Geräte, auf denen die Software installiert ist. Sämtliche Server-Anwendungen sollten durch Zugriffskontrollmaßnahmen abgesichert werden und ihre Nutzungsprotokolle (Logs) durch ein SIEM-System überwacht werden. Im Bereich Daten sollte ein strukturiertes Dateninventar in Verbindung mit einer Analyse zentraler Datenflüsse die Grundlage für die Ableitung differenzierter Schutzbedarfe bilden, aus denen sich geeignete Maßnahmen für Zugriffskontrolle, Verschlüsselung sowie Backup- und Wiederherstellungsverfahren ableiten lassen. Die Einführung einer Zero-Trust-Architektur bedeutet für Kommunen und Landkreise eine langfristige Weiterentwicklung der Sicherheit ihrer kommunalen IT-Infrastruktur. Einzelne Maßnahmen können jedoch auch zeitnah die Resilienz und Widerstandsfähigkeit maßgeblich erhöhen – eine Liste der hier betrachteten Maßnahmen findet sich in Anhang A.

Danksagung

Im Rahmen der Erarbeitung dieser Handreichung wurden fünf qualitative Experteninterviews mit Verantwortlichen aus den Bereichen kommunale Informationstechnologie und Informationssicherheit in hessischen Kommunalverwaltungen geführt, die Einblicke in organisatorische, technische sowie prozessuale Strukturen der jeweiligen IT-Organisation ermöglichten. An den Gesprächen beteiligten sich Vertreterinnen und Vertreter der folgenden Kommunen und Landkreise:

- Kreis Bergstraße,
- Stadt Gießen,
- Stadt Kassel,
- Landkreis Marburg-Biedenkopf,
- Landeshauptstadt Wiesbaden.

Insbesondere bedanken wir uns bei

- Herrn Dr. Johannes Bunsch,
- Herrn Michael Dittmar,
- Herrn Olaf Kirsch,
- Herrn Jens Lange,
- Herrn Benjamin Pfister,
- Herrn Martin Sautner und
- Herrn Michael Tönnesmann.

Die Interviews lieferten Einblicke in bestehende IT-Governance-Strukturen, organisatorische Zuständigkeiten sowie in eingesetzte technische Infrastrukturen und Sicherheitsmaßnahmen und wurden durch Einschätzungen zu praktischen Herausforderungen bei der Einführung einer Zero-Trust-Infrastruktur ergänzt. Wir danken den beteiligten Kommunen und Landkreisen ausdrücklich für ihre Bereitschaft zur Teilnahme an den Experteninterviews sowie für die bereitgestellten Einblicke und das fachliche Feedback, das wesentlich zum Gelingen des Projekts beigetragen hat.

Inhaltsverzeichnis

Vorwort 3

Executive Summary 5

Danksagung 7

Inhaltsverzeichnis 9

1 Einleitung 13

2 Zero-Trust 17
- 2.1 Zentrale Prinzipien von Zero-Trust . . . 18
- 2.2 Zero-Trust-Einführung als Transformationsprozess . . . 18
- 2.3 Gemeinsame säulenübergreifende konzeptionelle Ziele . . . 19

3 Kommunale IT-Rahmenbedingungen 21
- 3.1 IT-Infrastruktur . . . 21
- 3.2 Fachanwendungen . . . 22
- 3.3 Rolle externer IT-Dienstleister . . . 22
- 3.4 Heterogene Endgeräte- und Gerätelandschaften . . . 23
- 3.5 Organisation und Ressourcen . . . 23
- 3.6 Arbeitsweise und organisatorische Prozesse . . . 24

4 Initiale Umsetzungsschritte in der Säule Identität 25
- 4.1 Identitäten und Authentifizierung . . . 28
  - 4.1.1 Benutzerinventar . . . 29
  - 4.1.2 Multi-Faktor-Authentifizierung (MFA) . . . 31
  - 4.1.3 Single-Sign-On (SSO) . . . 33
- 4.2 Berechtigungen und Zugriffskontrolle . . . 36
  - 4.2.1 Management von Berechtigungen und Least-Privilege . . . 36
  - 4.2.2 Zugriffsmanagement für privilegierte Accounts . . . 38
- 4.3 Fortgeschrittene Maßnahmen . . . 40

5 Initiale Umsetzungsschritte in der Säule Geräte 41
- 5.1 Inventarisierung . . . 41
  - 5.1.1 IT-Asset-Management . . . 42
  - 5.1.2 Onboarding . . . 42
  - 5.1.3 Offboarding . . . 43
- 5.2 Überprüfung, Monitoring und Kontrolle . . . 44
  - 5.2.1 Endgeräte-Schutz . . . 44
  - 5.2.2 Schutz mobiler Endgeräte . . . 45
- 5.3 Fortgeschrittene Maßnahmen . . . 46

6 Initiale Umsetzungsschritte in der Säule Netzwerk 47
- 6.1 Segmentierung . . . 48

6.1.1 Makrosegmentierung . . . 48
6.1.2 Software Defined Networks (SDN) . . . 49
6.1.3 Software Defined Perimeters (SDP) . . . 50
6.2 Intrusion Detection & Prevention (IDS/IPS) . . . 51
6.2.1 Statische und dynamische Filterregeln . . . 51
6.2.2 Nutzung von Machine-Learning-Methoden . . . 51
6.3 Netzwerkzugangskontrolle . . . 52
6.3.1 Lokale Zugangskontrolle . . . 52
6.3.2 Sicherer Fernzugriff . . . 53
6.4 Fortgeschrittene Maßnahmen . . . 54

7 Initiale Umsetzungsschritte in der Säule Workload & Apps 57
7.1 Software-Verwaltung und Software-Sicherheit . . . 57
7.1.1 Inventarisierung und Verteilung von Software . . . 57
7.1.2 Wartung von Software . . . 58
7.1.3 Lieferkettensicherheit . . . 59
7.2 Zugriffskontrolle bei Netzwerk-Diensten . . . 60
7.2.1 Agent-Gateway . . . 61
7.2.2 Enclave-Gateway . . . 62
7.2.3 Interne vs. externe Dienste . . . 62
7.3 Protokollierung und Auswertung . . . 63
7.4 Fortgeschrittene Maßnahmen . . . 63

8 Initiale Umsetzungsschritte in der Säule Daten 65
8.1 Aufbau eines Dateninventars mit klarer Datenverantwortung . . . 68
8.1.1 Erstellung eines Dateninventars . . . 68
8.1.2 Zuordnung der fachlichen und technischen Datenverantwortung . . . 69
8.2 Einheitliche Datenklassifizierung und Schutzniveaus . . . 69
8.2.1 Schutzklassen und Mindestanforderungen an Sicherheitsmaßnahmen 70
8.2.2 Metadaten . . . 70
8.2.3 Technische Umsetzung der Datenklassifikation . . . 71
8.3 Analyse und Absicherung kritischer Datenflüsse . . . 72
8.3.1 Erfassung der Datenflüsse . . . 72
8.3.2 Festlegung sicherer Datenflüsse . . . 73
8.4 Ausrichtung von Verschlüsselungsmaßnahmen am Schutzbedarf . . . 73
8.4.1 Erhebung der Ausgangslage . . . 74
8.4.2 Festlegung schutzbedarfsbezogener Mindeststandards . . . 74
8.4.3 Risikobasierte Behandlung von Legacy-Systemen . . . 74
8.4.4 Klar geregeltes Schlüsselmanagement . . . 75
8.4.5 Priorisierte Umsetzung . . . 75
8.5 Einsatz einer resilienten Backup-Strategie . . . 76
8.5.1 Analyse der bestehenden Backup-Landschaft . . . 76
8.5.2 Aufbau einer widerstandsfähigen Backup-Architektur . . . 76
8.5.3 Ausrichtung von Backup-Strategien am Schutzbedarf . . . 77
8.6 Verankerung von Wiederherstellungstests . . . 77
8.6.1 Fachliche und technische Festlegung der Wiederherstellungsziele . . . 78
8.6.2 Definition von Wiederherstellungsprozessen . . . 78
8.6.3 Durchführung regelmäßiger praktischer Wiederherstellungstests . . . 78

8.7 Fortgeschrittene Maßnahmen 79

9 Zusammenfassung **81**
9.1 Rahmenbedingungen kommunaler IT-Landschaften 82
9.2 Überblick über die Umsetzungsschritte in den fünf technischen Säulen . . 83
9.3 Gemeinsame konzeptionelle Ziele der Umsetzungsschritte 84
9.4 Umsetzung der vorgeschlagenen Maßnahmen 84
9.5 Bedeutung für zukünftige IT-Modernisierung 85
9.6 Fazit 85

10 Abkürzungen **87**

Literatur **91**

A Anhang A: Verzeichnis vorgeschlagener Umsetzungsschritte **95**

Impressum **99**

1
Einleitung

Das Funktionieren der öffentlichen Verwaltung muss sichergestellt sein, da viele Menschen auf deren Leistungen zurückgreifen oder gar darauf angewiesen sind. Um die wachsenden Aufgaben effizient und bürgernah durchführen zu können, werden viele Leistungen durch oder mit Hilfe von Informationstechnik (IT) bereitgestellt. Die hierfür notwendige Digitalisierung der Verwaltung hat spätestens mit der Verabschiedung des Onlinezugangsgesetzes (OZG) im Jahr 2017 begonnen. Dies ist ein andauernder Prozess, der stetig erweitert und verbessert wird. Die Digitalisierung der Verwaltung und der damit einhergehenden Vernetzung der verschiedenen IT-Systeme innerhalb einer Kommune oder eines Landkreises[1] sowie die Anbindung von externen IT-Dienstleistern oder dem Angebot und Betrieb eigener Dienste (einschließlich digitaler Bürgerdienste) erfordert eine Anbindung an das globale Internet. Hierdurch eröffnen sich viele Möglichkeiten, wie bspw. die orts- und zeitunabhängige Nutzung von Serviceleistungen für Bürgerinnen und Bürger. Den Vorteilen stehen jedoch auch Risiken gegenüber, die sich erst durch die Öffnung der kommunalen Verwaltungen ergeben haben. Eines dieser Risiken sind Cyberangriffe, die über das Internet ausgeführt werden, und die bei einem Erfolg großen Schaden in der IT einer Kommune anrichten und damit den Betrieb nachhaltig stören oder gar zum Erliegen bringen können.

Die Bereitstellung von Informationstechnik (Infrastruktur, Betrieb, Software) fällt in den Bereich der Kommunalhoheit. Die kommunale IT-Landschaft in Hessen weist hierbei eine große Heterogenität auf. Bei der Aufgabenerfüllung bedienen sich die derzeit mehr als 440 hessischen Kommunen sowohl eigener Organisationseinheiten, als auch teilweise oder vollständig externer Dienstleister. Die Aufgabenstellungen der Kommunen gleichen sich zwar, die Umsetzung erfolgt aber mit Hilfe unterschiedlichster Fachanwendungen oder Betriebssysteme. Der sichere Betrieb der IT bedingt bei allen Kommunen einen entsprechenden Einsatz von finanziellen Ressourcen. Mit der Abnahme der Größe einer Kommune steigt jedoch insbesondere die Herausforderung, die Erfordernisse der Informationssicherheit fachlich und personell in der gebotenen Weise leisten zu können [Elf23]. Nach öffentlichen Zahlen waren 2024 durchschnittlich jeden Monat mehr als eine hessische Kommune von einem Cybervorfall betroffen.[2] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt in seinem Lagebericht 2025 gar fest, dass „[d]ie öffentliche Verwaltung [..] ein Hauptziel von Cyberspionage [war]“[3].

1 Zum Zwecke der besseren Lesbarkeit wird im weiteren Verlauf an vielen Stellen lediglich von „Kommunen“ gesprochen, wobei stets „Kommunen und Landkreise“ gemeint sind, sofern keine explizite Differenzierung erfolgt.

2 https://hessen.de/presse/cybersicherheit-in-hessen-gefaehrdungslage-2024-weiterhin-hoch, zuletzt abgerufen am 01.06.2026

3 https://medien.bsi.bund.de/lagebericht/de/cyberspionage-und-cybersabotage/, zuletzt abgerufen am 01.06.2026

Es liegt nicht in der Hand einer Kommune, Cyberangriffe zu verhindern – Angreifer agieren weltweit und können zu jedem Zeitpunkt zuschlagen. Was eine Kommune jedoch tun kann, ist den Preis für einen erfolgreichen Angriff für Angreifer in die Höhe zu treiben. Angreifer handeln i. d. R. ökonomisch und nutzen den Weg des geringsten Widerstands, um ihr Ziel zu erreichen. Mit anderen Worten werden aus der Masse der möglichen Ziele jene mit den größten oder meisten Schwachstellen in der IT-Sicherheit ausgewählt, sodass der Aufwand des Angreifers hinsichtlich der eingesetzten Ressourcen *pro Angriffsziel* möglichst klein bleibt und er mit seinen gegebenen Ressourcen möglichst viele Ziele treffen kann. Dies folgt der Erwartung, dass sich in der Masse der Ziele schon ein oder mehr Opfer finden werden. Steigt der Aufwand des Angreifers für einen Erfolg aus solchen Massenangriffen, wird er i. d. R. nicht gewohnheitsmäßig versuchen, mehr Angriffs-Ressourcen in ein Ziel zu investieren, da er diese – dem ökonomischen Gedanken folgend – eher für schlechter gesicherte Ziele einsetzen wird, um dort vermeintlich leichter zum Erfolg zu kommen.

Ein Cyberangriff kann trotz aller Sorgfalt und der eingesetzten Sicherheitsmechanismen erfolgreich sein. Es gilt deshalb auch für diesen Fall Vorkehrungen zu treffen, sodass der Schadensumfang begrenzt und der kommunale Betrieb nicht gänzlich zum Erliegen kommt. Eine Herangehensweise, um zum einen, die Hürden für einen erfolgreichen Angriff zu erhöhen, und zum anderen, dafür zu sorgen, dass sich der Schaden eines erfolgreichen Angriffs auf ein System innerhalb eines Fachamtes oder einer Fachabteilung nicht auf weitere Systeme oder Ämter einer Kommune ausweitet, ist die Umsetzung einer sogenannten Zero-Trust-Architektur (ZTA), welche die Netzwerksicherheit einer Kommune deutlich verbessern kann. In diesem Zusammenhang sollten sich Verantwortliche deshalb zuerst die Frage stellen, wie gut sie ihre IT-Landschaft kennen und ob sie einen Überblick über sämtliche Nutzungskonten, aktiven Geräte, Netzwerk- und Anwendungszugänge, etc. haben. Werden alle diese Komponenten während des Betriebs kontinuierlich im Hinblick auf IT-Sicherheit überprüft? Können Sicherheitsmaßnahmen einheitlich und zeitnah umgesetzt werden? Gibt es eine zentrale Stelle an der alle wichtigen Informationen zusammenlaufen und überwacht werden können? Für diese und weitere Fragen im Zusammenhang mit IT-Sicherheit und Cyberresilienz sollen am Ende des Übergangs hin zu einer ZTA positive Antworten gegeben werden.

Eine ZTA ist eine äußert wirkungsvolle Sicherheitsvorkehrung, führt jedoch ein neues Paradigma ein, das in „klassischen“ IT-Infrastrukturen in dieser Tiefe in der Regel nicht verfolgt wird. Viele aktuell verbaute IT-Komponenten und -Dienste sind zudem faktisch nicht oder nur bedingt tauglich für Zero-Trust und der Übergang zu einer ZTA bedeutet regelmäßig den kompletten Umbau eines IT-Netzwerks, seiner Zugänge und der (Sicherheits-)Interaktion mit den Nutzerinnen und Nutzern. Zum letzten Punkt ist zudem zu beachten, dass die Umsetzung einer ZTA eine Beachtung der Themen Gebrauchstauglichkeit und Nutzerakzeptanz erfordert. Eine Umstellung auf eine ZTA benötigt deshalb Zeit und Ressourcen, die gerade in Kommunen häufig rar sind. Aus diesem Grund brauchen Kommunen einen Übergang zu einer ZTA, der ihren Bedarfen und Gegebenheiten Rechnung trägt. In den über 440 Kommunen in Hessen gibt es eine große Spannbreite hinsichtlich ihrer IT-Personalausstattung, IT-Infrastrukturen sowie eingesetzten Anwendungen. Diese Heterogenität gilt es für einen Übergang hin zu einer ZTA zu berücksichtigen.

Die vorliegende Handreichung soll hessischen Kommunen bei der Verbesserung der Sicherheit ihrer IT-Infrastruktur nachhaltig und mit konkreten Handlungsempfehlungen unterstützen, um so ihre Resilienz gegenüber Cyberangriffen zu stärken. Hierfür wird eine ZTA in fünf Säulen eingeteilt: Identität, Geräte, Netzwerk, Workload & Apps sowie Daten. Für jede Säule werden erste mögliche Umsetzungsschritte beschrieben, welche zur Verbesserung der Cybersicherheit beitragen sollen. Diese Schritte sind sowohl organisatorischer als auch technischer Natur, wenngleich sie „technikneutral“ beschrieben werden, d. h. es werden keine Empfehlungen gegeben oder Konfigurationen vorgestellt für konkrete Produkte eines Hard- oder Software-Herstellers. Die Beschreibungen sind deshalb bewusst allgemein gehalten, sodass sie auf verschiedene Lösungen anwendbar sind. Diese Allgemeinheit setzt jedoch ein gewisses Maß an technischem Vorwissen – insbesondere im Bereich der IT-Sicherheit – voraus, um die Schritte konkret umsetzen zu können. Kleinere Kommunen, die u. U. viele Dienste von einem externen Dienstleister beziehen, können genauso von den hier vorgestellten Maßnahmen profitieren wie mittlere oder große Kommunen, wenngleich sich ihr praktischer Nutzen womöglich nicht über alle fünf vorgestellten Säulen gleichermaßen erstreckt.

Die nachfolgenden Abschnitte dieser Handreichung gliedern sich wie folgt: Zunächst werden die konzeptionellen Grundlagen von Zero-Trust dargestellt (Abschnitt 2), gefolgt von einer Analyse der spezifischen Rahmenbedingungen kommunaler IT-Landschaften (Abschnitt 3). Darauf aufbauend beschreiben die Abschnitte 4 bis 8 die initialen Umsetzungsschritte einer Zero-Trust-Architektur entlang der fünf technischen Säulen – Identität, Geräte, Netzwerk, Workload & Apps und Daten. Abschnitt 9 fasst die wesentlichen Ergebnisse zusammen und ordnet diese in einen übergreifenden Kontext ein. Im Anhang A werden die betrachteten initialen und fortgeschrittenen Maßnahmen zur Umsetzung einer Zero-Trust-Architektur nochmals zusammenfassend als Liste dargestellt.

2
Zero-Trust

Der Begriff „Zero-Trust“ beschreibt einen Sicherheitsansatz, der den Umgang mit Vertrauen innerhalb von IT-Infrastrukturen neu bewertet. Häufig wird er mit der Formel „Never trust, always verify!“ zusammengefasst. Hierbei werden alle Zugriffe auf Systeme, Anwendungen oder Daten grundsätzlich überprüft und ausschließlich explizit gewährt. Vertrauen wird nicht dauerhaft vorausgesetzt, sondern wird stets kontextabhängig bewertet und muss bei jeder Interaktion erneut verdient werden. Der Zero-Trust-Ansatz wurde vor dem Hintergrund sich verändernder IT-Strukturen entwickelt. Klassische Sicherheitsarchitekturen orientieren sich meist an einem klar abgegrenzten Netzwerkperimeter. Innerhalb dieses Perimeters gelten Systeme und Benutzer häufig als vertrauenswürdig und haben relativ weitreichenden Zugriff auf interne Systeme, während externe Zugriffe stärker kontrolliert werden. Technisch wurden diese klassischen Architekturen durch Firewalls, Netzwerkzonen und VPN-Zugänge umgesetzt.

Die Rahmenbedingungen bei der heutigen IT-Nutzung haben sich jedoch verändert. Anwendungen liegen zunehmend außerhalb der eigenen Infrastruktur, mobile Geräte wechseln regelmäßig ihre Umgebung, und Benutzer greifen aus unterschiedlichen Kontexten auf Dienste zu. Sicherheitsvorfälle zeigen zugleich, dass Angriffe nicht ausschließlich über den äußeren Netzrand erfolgen. Kompromittierte Benutzerkonten, manipulierte Endgeräte oder bereits infiltrierte Systeme spielen häufig eine Rolle. Eine Zero-Trust-Architektur (ZTA) setzt genau an dieser Stelle an. Jeder Zugriff wird unabhängig vom Netzwerkstandort bewertet. Die Unterscheidung zwischen internem und externem Zugriff verliert an Bedeutung. Mehrere Prüfschichten ersetzen die einmalige Sicherheitsprüfung am Netzwerkperimeter. Identität, Gerätezustand, Kontext und Berechtigungen fließen fortlaufend in die Autorisierung einzelner Zugriffe ein. Viele Organisationen sprechen in diesem Zusammenhang von einem Paradigmenwechsel in der IT-Sicherheit. Vertrauen wird nicht mehr primär über Netzwerkgrenzen definiert, sondern über überprüfbare Eigenschaften – etwa die Identität eines Nutzers oder den Sicherheitszustand eines Geräts.

Der Zero-Trust-Ansatz wurde in den vergangenen Jahren von verschiedenen, vor allem US-amerikanischen Organisationen vorangetrieben. Als zentrale Referenz gilt die „NIST Special Publication 800-207 Zero Trust Architecture“ [NIS20]. Das Dokument beschreibt grundlegende Architekturprinzipien sowie typische Implementierungsmodelle einer ZTA. Weitere Leitlinien stammen unter anderem vom US Department of Defense (DoD) [DoD22b][DoD22a] sowie von der Cybersecurity and Infrastructure Security Agency (CISA) [CIS23]. In Deutschland ordnet das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Konzept in seinem Positionspapier zu Zero-Trust [BSI23e] ein. Auch Untersuchungen zur kommunalen IT-Praxis greifen das Thema auf. Eine Studie zu Zero-Trust der Initiative-K [Elf23] zeigt, dass viele Kommunen bereits einzelne Sicherheitsmaßnahmen umsetzen (etwa Multi-Faktor-Authentifizierung), häufig fehlt jedoch ein übergreifendes Konzept, das diese Maßnahmen in ein konsistentes Sicherheitsmodell integriert.

2.1
Zentrale Prinzipien von Zero-Trust

Trotz unterschiedlicher Implementierungen lassen sich mehrere zentrale Grundprinzipien von Zero-Trust identifizieren, die in nahezu allen Zero-Trust-Architekturen auftreten.

Assume Breach. Zero-Trust geht davon aus, dass Sicherheitsvorfälle jederzeit möglich sind. Systeme werden daher so gestaltet, dass ein erfolgreicher Angriff nicht automatisch zur vollständigen Kompromittierung der IT-Infrastruktur führt. Ziel ist eine möglichst frühe Erkennung und eine Begrenzung potenzieller Schäden.

Starke Identitäten. Identitäten bilden eine zentrale Grundlage für Zugriffsentscheidungen. Benutzer, Dienste und Geräte müssen eindeutig identifizierbar sein. Verfahren wie Multi-Faktor-Authentifizierung reduzieren das Risiko kompromittierter Konten.

Least-Privilege und kontextbasierter Zugriff. Zugriffsrechte werden restriktiv vergeben. Nutzer erhalten nur die Berechtigungen, die für ihre aktuelle Aufgabe erforderlich sind. Kontextinformationen – etwa Zugriffszeitpunkt, Gerätezustand, Standort oder Risikoeinschätzungen – fließen zusätzlich in die Entscheidung ein.

Mikrosegmentierung. Netzwerke und Anwendungen werden stärker segmentiert als in traditionellen Architekturen. Systeme können nur mit den Komponenten kommunizieren, die für ihre jeweilige Funktion notwendig sind. Dies verkleinert den Aktionsradius eines Angreifers innerhalb der IT-Infrastruktur (*lateral movement*).

Kontinuierliche Verifizierung. Autorisierungsentscheidungen erfolgen nicht einmalig. Systeme überwachen fortlaufend Benutzerverhalten, Gerätezustände und Systemaktivitäten. Auffälligkeiten können so früher erkannt werden.

2.2
Zero-Trust-Einführung als Transformationsprozess

Die Einführung einer ZTA erfolgt selten als einmalige technische Umstellung. In der Praxis handelt es sich meist um einen langfristigen Transformationsprozess.
IT-Sicherheitsmechanismen werden schrittweise angepasst, ergänzt und stärker miteinander verbunden. Zahlreiche Organisationen, die eine ZTA einführen möchten, verfügen bereits über einzelne Komponenten oder Systeme zur Umsetzung von IT-Sicherheitsmaßnahmen, die später Ausgangsbasis einer ZTA werden können, wie etwa Multi-Faktor-Authentifizierung, Netzwerksegmentierung oder zentrale Monitoring-Systeme.
Die Einführung einer ZTA betrifft viele Aspekte und Bereiche der IT-Organisation. Hierzu zählen insbesondere Identitäts- und Berechtigungsmanagement, Gerätemanagement, Netzwerkarchitekturen, Anwendungen sowie der Schutz und die Klassifikation von Daten. Entsprechend strukturieren viele Referenzmodelle und Leitlinien zu Zero-Trust diese Themenfelder entlang von fünf technischen Säulen (*pillars*): Identität, Geräte, Netzwerke, Workload & Apps sowie Daten (siehe Abbildung 2.1, vgl. [CIS23]).

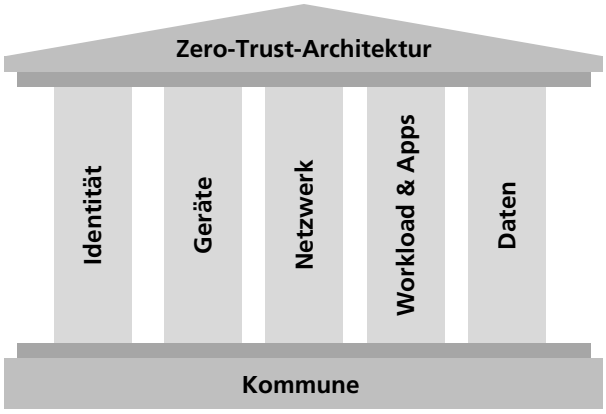

Abb. 2.1:
Fünf technische Säulen von Zero-Trust (in Anlehnung an [CIS23])

Innerhalb dieser Säulen werden jeweils die technischen und organisatorischen Maßnahmen beschrieben, die für eine schrittweise Einführung einer ZTA erforderlich sind. Jede Säule adressiert dabei einen zentralen Bereich der ZTA und bündelt die zugehörigen Kontrollen, Prozesse und technischen Mechanismen. Zusammen bilden diese fünf Säulen den konzeptionellen Rahmen, innerhalb dessen Zero-Trust-Maßnahmen geplant und umgesetzt werden können.

2.3 Gemeinsame säulenübergreifende konzeptionelle Ziele

Die in den einzelnen Säulen beschriebenen Umsetzungsschritte weisen trotz unterschiedlicher fachlicher Schwerpunkte eine Reihe gemeinsamer konzeptioneller Ziele auf. Diese Ziele lassen sich säulenübergreifend beobachten und bilden einen wiederkehrenden Ordnungsrahmen für die schrittweise Einführung einer ZTA (s. Abbildung 2.2). Diese im Folgenden genannten übergeordneten Ziele sollten bei der Umsetzung jeglicher Maßnahmen – der hier beschriebenen sowie ggf. auch weiterer – stets im Blick behalten werden. Wird eine neue Maßnahme zur Unterstützung von Zero-Trust geplant, sollte man sich im Vorfeld stets fragen, ob diese auf mindestens eine der genannten Ziele hinwirkt und damit einen Beitrag zu Zero-Trust liefern kann.

Sichtbarkeit. Am Anfang steht regelmäßig die Herstellung von Sichtbarkeit. In allen Säulen zeigt sich, dass belastbare Informationen über vorhandene Identitäten, Geräte, Netzstrukturen, Anwendungen oder Datenbestände eine zentrale Voraussetzung für weitergehende Maßnahmen darstellen. Ohne eine solche Transparenz bleiben Sicherheitsentscheidungen punktuell und wenig belastbar.

Konsolidierung. Darauf aufbauend folgt häufig eine Phase der Konsolidierung. Historisch gewachsene und oft heterogene Strukturen werden schrittweise vereinheitlicht. Dies betrifft sowohl technische Komponenten als auch organisatorische Zuständigkeiten. Ziel ist es, Komplexität zu reduzieren und die Grundlage für konsistente Sicherheitsmechanismen zu schaffen.

Abb. 2.2: Säulenübergreifende konzeptionelle Ziele

Zentralisierung. Eng damit verbunden ist der Trend zur Zentralisierung. Steuerungs- und Verwaltungsfunktionen werden zunehmend gebündelt, etwa im Bereich des Identitäts- und Berechtigungsmanagements oder beim Management von Endgeräten und Netzwerken. Zentrale Instanzen ermöglichen es, sicherheitsrelevante Entscheidungen einheitlich zu treffen und übergreifend durchzusetzen.

Durchsetzung. Ein weiterer wiederkehrender Aspekt ist die konsequente Durchsetzung von Sicherheitsrichtlinien. Zugriffsentscheidungen werden nicht nur definiert, sondern technisch umgesetzt und dynamisch angewendet. Regelwerke wie Least Privilege oder kontextbasierte Zugriffskontrollen werden dabei systematisch genutzt, um Zugriffe situationsabhängig zu steuern.

Monitoring. Parallel dazu gewinnt das kontinuierliche Monitoring an Bedeutung. Sicherheitsrelevante Ereignisse werden fortlaufend erfasst und ausgewertet, um Auffälligkeiten frühzeitig zu erkennen. Die Protokollierung bildet zugleich die Grundlage für Analyse, Reaktion auf Vorfälle und die Bewertung bestehender Sicherheitsmaßnahmen.

Resilienz. In vielen Bereichen tritt schließlich der Aspekt der Resilienz in den Vordergrund. Maßnahmen werden so gestaltet, dass sie nicht nur Angriffe erschweren, sondern auch deren Auswirkungen begrenzen. Isolationsmechanismen, segmentierte Strukturen sowie Wiederherstellungsprozesse tragen dazu bei, die Funktionsfähigkeit der IT auch im Störungsfall möglichst schnell wiederherzustellen.

Diese sechs Ziele – Sichtbarkeit, Konsolidierung, Zentralisierung, Durchsetzung, Monitoring und Resilienz – treten in unterschiedlicher Ausprägung in allen fünf technischen Säulen auf und verdeutlichen, dass die Einführung von Zero-Trust nicht aus isolierten Einzelmaßnahmen besteht, sondern einem übergreifenden konzeptionellen Ansatz folgt.

3
Kommunale IT-Rahmenbedingungen

In diesem Abschnitt werden zentrale Rahmenbedingungen und wiederkehrende Herausforderungen kommunaler IT-Strukturen dargestellt. Die Darstellung basiert auf einer qualitativen Analyse der Ausgangssituation in hessischen Kommunen und Landkreisen. Grundlage der Analyse bildeten strukturierte Experteninterviews mit Vertretern aus fünf Kommunen und Landkreisen, die Einblicke in organisatorische, technische und prozessuale Aspekte kommunaler IT-Umgebungen ermöglichten. Die dabei gewonnenen Beobachtungen wurden durch zusätzliche Literatur- und Quellenrecherchen ergänzt.

Die dargestellten Rahmenbedingungen sind nicht als einheitliche Beschreibung aller kommunalen IT-Strukturen zu verstehen. Vielmehr spiegeln sie typische Merkmale und wiederkehrende Herausforderungen wider, die im Rahmen der Analyse identifiziert wurden und in kommunalen IT-Landschaften in unterschiedlicher Ausprägung auftreten können. Ziel der Darstellung ist es, die Bandbreite möglicher struktureller Ausgangsbedingungen sichtbar zu machen, die bei der Planung und Umsetzung einer Zero-Trust-Architektur (ZTA) berücksichtigt werden sollten. Im Folgenden werden zentrale Themenfelder beschrieben, die im Kontext der Einführung einer ZTA besondere Relevanz aufweisen können.

3.1
IT-Infrastruktur

Die IT-Infrastruktur kommunaler Verwaltungen ist in vielen Fällen durch eine erhebliche strukturelle Vielfalt gekennzeichnet. Diese Vielfalt lässt sich häufig auf historisch gewachsene Systemlandschaften zurückführen, in denen über einen längeren Zeitraum hinweg unterschiedliche IT-Systeme, Fachverfahren und technische Plattformen eingeführt wurden. In zahlreichen Verwaltungen sind in diesem Zusammenhang auch Systeme älteren Ursprungs weiterhin im Einsatz, deren technische Architektur oder begrenzte Integrationsmöglichkeiten die Einbindung neuer Sicherheitsmechanismen teilweise erschweren können.

Hinzu kommt, dass für den Betrieb und die Verwaltung der verschiedenen Infrastrukturkomponenten oftmals unterschiedliche Administrations- und Managementwerkzeuge genutzt werden. Diese Werkzeuge sind in der Regel auf bestimmte Systembereiche oder Gerätekategorien zugeschnitten, sodass eine vollständig einheitliche und zentralisierte Verwaltung aller Systeme nicht in jeder Umgebung realisiert ist. Änderungen an administrativen Abläufen – beispielsweise im Zusammenhang mit dem Eintritt oder Ausscheiden von Beschäftigten – können daher Anpassungen in mehreren Systemen erforderlich machen. Dies erhöht mitunter den organisatorischen Aufwand und kann die Nachvollziehbarkeit einzelner Prozessschritte erschweren.

3.2 Fachanwendungen

In kommunalen Verwaltungen besteht häufig eine erhebliche Vielfalt an eingesetzten Fachanwendungen. Umfang und Zusammensetzung dieser Anwendungslandschaften können sich zwischen einzelnen Kommunen und Landkreisen deutlich unterscheiden. Insbesondere in größeren Verwaltungen kommt es vor, dass eine hohe Zahl unterschiedlicher Fachverfahren parallel betrieben wird. Diese Anwendungen weisen oftmals Unterschiede hinsichtlich ihrer technischen Architektur, der Gestaltung ihrer Benutzeroberflächen, ihrer Integrationsmöglichkeiten sowie ihrer Authentifizierungs- und Berechtigungskonzepte auf.

Darüber hinaus variieren auch die Betriebsmodelle der eingesetzten Fachanwendungen. Während ein Teil der Fachanwendungen (z. B. ältere und nicht leicht ersetzbare Fachanwendungen) weiterhin innerhalb der kommunalen IT-Infrastruktur betrieben wird, erfolgt der Betrieb anderer Fachanwendungen (zunehmend) über kommunale Dienstleister oder über externe Cloud-Anbieter. Diese unterschiedlichen Bereitstellungsformen haben Auswirkungen auf technische Schnittstellen, Authentifizierungsverfahren sowie auf organisatorische Abläufe im Betrieb und in der Wartung.

3.3 Rolle externer IT-Dienstleister

In vielen kommunalen IT-Umgebungen übernehmen externe IT-Dienstleister zentrale Aufgaben, etwa beim Betrieb von Fachanwendungen oder bei der Bereitstellung und Wartung von Infrastrukturkomponenten. Umfang und Ausgestaltung dieser Zusammenarbeit unterscheiden sich jedoch zwischen einzelnen Kommunen erheblich, da einige Verwaltungen große Teile ihrer IT selbst betreiben, während andere bestimmte Dienste oder Anwendungen stärker auslagern.

In solchen Konstellationen haben kommunale IT-Abteilungen häufig nur begrenzten Einfluss darauf, wie technische oder organisatorische Prozesse beim Dienstleister umgesetzt werden, welche Schnittstellen bereitgestellt werden oder wie administrative Abläufe ausgestaltet sind. Dies betrifft insbesondere Prozesse im Identitäts- und Berechtigungsmanagement, bei denen Änderungen teilweise über Ticketsysteme oder andere manuelle Verfahren abgewickelt werden. Zudem liegen bestimmte sicherheitsrelevante Maßnahmen innerhalb der Infrastruktur externer Anbieter außerhalb des direkten Einflussbereichs der Kommunen. Dadurch können bei der Einführung einer Zero-Trust-Architektur zusätzliche Abstimmungen erforderlich werden, etwa bei Schnittstellen, Authentifizierungsmechanismen oder Sicherheitsrichtlinien über Organisationsgrenzen hinweg.

3.4 Heterogene Endgeräte- und Gerätelandschaften

Die Vielfalt eingesetzter Endgeräte stellt in vielen kommunalen IT-Umgebungen einen zusätzlichen Komplexitätsfaktor dar. Neben klassischen Arbeitsplatzrechnern kommen häufig mobile Geräte wie Laptops, Tablets oder Smartphones sowie infrastrukturelle Komponenten wie Netzwerkgeräte, Drucker oder spezialisierte Fachhardware zum Einsatz. Unterschiedliche Hersteller, Betriebssysteme und Firmware-Versionen führen dabei oftmals zu heterogenen Verwaltungs- und Updateprozessen, wodurch ein einheitliches und zentral gesteuertes Gerätemanagement erschwert werden kann. Hinzu kommen besondere Nutzungsmuster einzelner Geräte. So werden beispielsweise Präsentations- oder Reservegeräte teilweise nur sporadisch eingesetzt und verbleiben über längere Zeiträume außerhalb des regulären Betriebs, wodurch sicherheitsrelevante Updates oder Konfigurationsanpassungen verzögert erfolgen können.

Schließlich existieren in manchen Umgebungen Systeme, für die aufgrund ihres Alters oder aus technischen beziehungsweise regulatorischen Gründen keine regelmäßigen Sicherheitsupdates mehr bereitgestellt werden. In solchen Fällen kann es erforderlich sein, verbleibenden Risiken durch ergänzende infrastrukturelle Maßnahmen zu begegnen.

3.5 Organisation und Ressourcen

Die organisatorischen und personellen Rahmenbedingungen kommunaler IT unterscheiden sich teilweise erheblich zwischen einzelnen Kommunen und Landkreisen. Während größere kommunale Verwaltungen häufig über spezialisierte IT-Abteilungen mit unterschiedlichen Fachrollen verfügen, arbeiten kleinere Kommunen teilweise mit deutlich begrenzteren personellen Ressourcen. Diese Unterschiede können Auswirkungen auf die Planung und Umsetzung umfangreicher IT-Sicherheitsmaßnahmen haben. Insbesondere Projekte zur Einführung neuer Sicherheitsarchitekturen erfordern häufig sowohl technische Expertise als auch organisatorische Koordinationsprozesse, die in ressourcenbegrenzten Umgebungen zusätzliche Herausforderungen darstellen können.

Gleichzeitig verfügen viele kommunale Verwaltungen bereits über etablierte Sicherheitsmaßnahmen oder organisatorische Strukturen im Bereich der IT-Sicherheit. Diese bestehenden Maßnahmen können im Rahmen einer Weiterentwicklung hin zu einer Zero-Trust-Architektur als Ausgangspunkt dienen und schrittweise erweitert oder angepasst werden.

3.6
Arbeitsweise und organisatorische Prozesse

Ein weiterer relevanter Kontextfaktor ergibt sich aus der organisatorischen Struktur kommunaler Verwaltungen. Viele Kommunen sind durch eine dezentrale Organisation mit verschiedenen Fachämtern, Außenstellen oder Verwaltungsstandorten geprägt, die jeweils spezifische Anforderungen an IT-Systeme und Fachanwendungen stellen können. Diese organisatorische Struktur kann sich auch in den zugrunde liegenden IT-Prozessen widerspiegeln. So können beispielsweise unterschiedliche Verfahren für Onboarding- und Offboarding-Prozesse, Rollenwechsel oder Berechtigungsvergaben existieren, die teilweise über mehrere Systeme hinweg umgesetzt werden müssen. In einigen Fällen sind diese Prozesse zudem mit externen Dienstleistern abgestimmt oder von deren technischen Plattformen abhängig.

Darüber hinaus erfolgt die Einführung neuer Sicherheitsmaßnahmen in der Regel im laufenden Verwaltungsbetrieb. Kritische Fachanwendungen und Verwaltungsdienste müssen daher weiterhin verfügbar bleiben, wodurch technische Änderungen häufig schrittweise umgesetzt werden müssen. Gleichzeitig ist zu berücksichtigen, dass technische Sicherheitsmaßnahmen regelmäßig Auswirkungen auf bestehende Arbeitsabläufe sowie auf administrative Tätigkeiten haben können. Vor diesem Hintergrund kommt der frühzeitigen Einbindung zentraler Nutzergruppen – sowohl der kommunalen Beschäftigten als auch der IT-Administratoren – eine wichtige Bedeutung zu, um organisatorische Akzeptanz sowie eine praktikable Integration neuer Sicherheitsmechanismen in bestehende Arbeitsprozesse zu gewährleisten.

Zusammenfassend verdeutlicht die Analyse der kommunalen IT-Rahmenbedingungen, dass kommunale IT-Landschaften häufig durch eine Kombination aus struktureller Heterogenität, einer Vielzahl eingesetzter Fachanwendungen, unterschiedlichen Organisationsmodellen im IT-Betrieb sowie teilweise begrenzten personellen und finanziellen Ressourcen geprägt sind. Hinzu kommen in vielen Fällen Abhängigkeiten von externen IT-Dienstleistern sowie historisch gewachsene Systemstrukturen, die technische Integrations- und Modernisierungsprozesse beeinflussen können. Diese Rahmenbedingungen beschreiben somit ein Spektrum möglicher organisatorischer und technischer Konstellationen innerhalb kommunaler IT-Umgebungen.

4
Initiale Umsetzungsschritte in der Säule Identität

Im Zentrum der Zero-Trust-Architektur (ZTA) steht das Prinzip, keinem Benutzer, keinem Gerät und keinem Dienst automatisch zu vertrauen, unabhängig davon, ob sie sich innerhalb oder außerhalb des eigenen Netzwerks befinden. Identitäten bilden hierbei das Fundament, auf dem alle weiteren Sicherheitsentscheidungen aufbauen. Jede Zugriffsentscheidung, jede Autorisierung und jede Sicherheitsrichtlinie hängt letztlich von der korrekten und verlässlichen Identifizierung der beteiligten Entitäten ab. Eine digitale Identität[1] bezeichnet die eindeutige Zuordnung einer Entität – sei es eine natürliche Person oder ein Gerät – zu einer Menge charakteristischer Merkmale oder Attribute. Eine Identität hat einen eindeutigen Bezeichner. Eine Identität dient als Grundlage, um Rechte und Pflichten, Rollen und Verantwortlichkeiten eindeutig zuzuordnen. In einer Zero-Trust-Architektur sind Identitäten das zentrale Bindeglied zwischen dem Benutzer bzw. Gerät und den Ressourcen, auf die zugegriffen wird. Nur wenn eine Identität eindeutig und vertrauenswürdig festgestellt wurde, können Richtlinien greifen, die den Zugriff erlauben, einschränken oder verweigern. Benutzer innerhalb einer Organisation, wie bspw. einer Kommune oder eines Landkreises, benötigen Identitäten, um auf Anwendungen, Daten und Dienste zugreifen zu können. Eine Identität repräsentiert dabei die Person in der IT-Infrastruktur und ermöglicht eine überprüfbare Zuordnung von Aktionen und Berechtigungen. Oft besitzen Benutzer mehrere Identitäten, insbesondere bei einer über einen längeren Zeitraum gewachsenen IT-Infrastruktur, die aus vielen unterschiedlichen Anwendungen und Legacy-Systemen besteht. Häufig werden statt des Begriffs Identität auch die Begriffe *Konto* oder *Account* verwendet, insbesondere im Zusammenhang mit der Nutzung von Anwendungen und Diensten.

Identitäten bestehen aus einer Menge von Attributen, die eine Entität eindeutig beschreiben und sie innerhalb der IT-Umgebung identifizierbar machen. Sie setzen sich aus verschiedenen technischen und organisatorischen Informationen zusammen, die die Identität einer Person oder eines Geräts abbilden. Die (digitale) Identität einer natürlichen Person (z. B. Mitarbeiter oder externer Benutzer) setzt sich in der Regel aus folgenden Bestandteilen zusammen:

- Eindeutiger Bezeichner wie Benutzername, E-Mail-Adresse oder Mitarbeiter-ID.
- Authentifizierungsinformationen wie Nachweise zur Identitätsprüfung, etwa Passwörter, PINs, Kryptoschlüssel, Smartcards, Hardware- oder Software-Token oder biometrische Merkmale.
- Attribute und Metadaten, insbesondere Informationen wie Name, Organisationseinheit, Position, Funktionsrolle, Kontaktinformationen, Zugehörigkeit zu Gruppen oder Projekten.
- Rollen und Berechtigungen wie zugeordnete Zugriffsrechte, Rollen oder Profile, die festlegen, auf welche Systeme und Daten der Benutzer zugreifen darf.
- Lebenszyklus-Informationen wie zeitliche Gültigkeit, Erstellungs- und Ablaufdaten, Status (aktiv, gesperrt, deaktiviert), sowie Audit-Informationen über Änderungen.

1 Teilweise auch *logische* Identität genannt [BSI23e]. Vereinfachend wird der Begriff *Identität* verwendet, sofern nicht explizit darauf hingewiesen wird.

Geräte-Identitäten

Nicht nur Personen, sondern auch Geräte wie Arbeitsplatzrechner, mobile Endgeräte, Netzwerk-Router oder Server benötigen eindeutige Identitäten. Nur so kann sichergestellt werden, dass die Geräte authentisch sind und autorisiert auf andere Komponenten innerhalb des zugehörigen Netzwerks zugreifen dürfen. In der Regel werden Geräteidentitäten durch zentrale Systemkomponenten wie ein Mobile-Device-Management (MDM), Endpoint-Management oder eine Public-Key-Infrastruktur (PKI) erstellt, verwaltet und regelmäßig überprüft. Während digitale Identitäten von Personen primär der Abbildung organisatorischer Zugehörigkeit und individueller Zugriffsrechte dienen, stehen bei digitalen Identitäten von Geräten technische Merkmale und Vertrauensnachweise im Vordergrund. Die Identität eines Geräts besteht in der Regel aus folgenden Bestandteilen:

- Einem eindeutigem Geräteidentifikator, z. B. Seriennummer, Hostname, MAC-Adresse, Geräte-ID oder UUID.
- Kryptografische Nachweise wie Zertifikate, Schlüsselpaare oder Token, die das Gerät eindeutig authentifizieren und eine vertrauenswürdige Kommunikation ermöglichen.
- Geräteattribute und -informationen wie Gerätetyp, Betriebssystem, Patch-Level, Standort, Eigentümer oder Zugehörigkeit zu einer Organisationseinheit.
- Registrierungsstatus und Vertrauensstufe, z. B. Angabe, ob das Gerät registriert, verwaltet und als „vertrauenswürdig“ eingestuft ist (z. B. durch MDM- oder Endpoint-Management-Systeme).
- Nutzungs- und Gültigkeitsinformationen wie Aktivierungszeitpunkt, Ablaufdatum von Zertifikaten und Gerätestatus (aktiv, außer Betrieb, kompromittiert).

Authentifizierung

Bei der Authentifizierung weist eine Entität (Person oder Gerät) ihre Identität nach. Sie stellt sicher, dass die Entität, die auf eine Ressource im Netzwerk zugreifen möchte, tatsächlich die angegebene Identität besitzt. Authentifizierung kann auf verschiedenen Faktoren basieren – Wissen (z. B. mittels Passwort), Besitz (z. B. mittels Token, Smartcard) oder Inhärenz (z. B. biometrische Merkmale wie ein Fingerabdruck). Innerhalb einer Zero-Trust-Architektur wird festgelegt, welche Identitäten sich an welchen Systemen anmelden dürfen bzw. welche Komponenten mit anderen Komponenten im Netzwerk kommunizieren dürfen und welches Authentifizierungsverfahren hierfür zulässig sind. Unter Umständen ist auch eine mehrstufige Authentifizierung erforderlich, bei der mehrere Faktoren zum Einsatz kommen, bspw. eine Smartcard und eine PIN bzw. ein Passwort und ein zusätzliches aktuelles Einmalpasswort. In diesem Fall spricht man von einer Zwei-Faktor-Authentifizierung (2FA) oder im allgemeinen Fall von einer Mehr-Faktor-Authentifizierung (MFA).

Autorisierung und Zugriffskontrolle

Nach erfolgreicher Authentifizierung folgt die Autorisierung, also die Entscheidung, ob eine nachgewiesene Identität auf eine bestimmte Ressource (z. B. ein Netzwerklaufwerk, eine Fachanwendung, eine Datenbank oder einen Server) zugreifen darf. Berechtigungen legen fest, welche Aktionen erlaubt sind. Diese können direkt einer Identität zugewiesen oder über Rollen vermittelt werden (rollenbasierte Zugriffskontrolle, RBAC [ANS04]). Grundlage jeder Autorisierung ist die zuvor geprüfte Authentizität der Identität.

Die Umsetzung der Zugriffskontrolle in einer Zero-Trust-Architektur erfolgt über verschiedene funktionale Komponenten, welche das Rückgrat der Zugriffssteuerung bilden. Der Policy-Decision-Point (PDP) bewertet Zugriffsanfragen, die von einem Policy-Enforcement (PEP) geschickt werden, und trifft die Entscheidung, ob ein Zugriff gewährt oder verweigert wird. Der PEP setzt die getroffene Entscheidung des PDP am eigentlichen Zugriffspunkt um und erlaubt bzw. verweigert den Zugriff. Die Zugriffsentscheidung basiert auf einer festgelegten Menge von Zugriffsregeln, der sogenannten Zugriffsrichtlinie bzw. Zugriffs-Policy. Im Falle einer kontextabhängigen oder dynamischen Zugriffskontrolle werden zusätzlich weitere Meta-Informationen der zugreifenden Identität oder der Umgebung (z. B. Uhrzeit, Wochentag, etc.) einbezogen, die von einem optionalen Policy-Information-Point (PIP) bereitgestellt werden. Je nach Netzwerkstruktur und Anbindung der einzelnen Systemkomponenten und Fachanwendungen kann es eine oder mehrere Instanzen der jeweiligen funktionalen Komponente innerhalb der Netzwerkinfrastruktur geben. Idealerweise können die Zugriffsanfragen mehrerer PEPs von einem zentralen PDP verarbeitet werden und die Administration der Zugriffsregeln erfolgt zentral in einem Policy-Administration-Point.

Management von Identäten und Berechtigungen

Das Identitätsmanagement umfasst die Erstellung, Verwaltung, Änderung und Löschung digitaler Identitäten. Es stellt sicher, dass diese konsistent, aktuell und sicher verwaltet werden. Dazu gehören auch die entsprechenden Anmeldeinformationen wie Passwörter, kryptografische Schlüssel oder Token bzw. daraus abgeleitete Informationen für die Validierung der Anmeldeinformationen. Verwaltungssysteme für Identitäten ermöglichen die zentrale Kontrolle und Nachvollziehbarkeit von Benutzer- und Geräteidentitäten. In einem gewachsenen System mit einer Vielzahl von Benutzern, Geräten, Systemkomponenten und Legacy-Anwendungen kann es vorkommen, dass unterschiedliche Verwaltungssysteme für das Management der verschiedenen digitalen Identitäten existieren. Dieses Vielzahl der Verwaltungssysteme erhöhen die Komplexität und sollten idealerweise über standardisierte Schnittstellen miteinander abgeglichen werden. Gleiches gilt auch für das Management von Berechtigungen. Das Berechtigungsmanagement befasst sich mit der Zuweisung und Verwaltung von Zugriffsrechten. Da in komplexen Infrastrukturen oft mehrere Systeme parallel existieren – etwa für Geräte, Fachanwendungen oder VPN-Zugriffe – müssen Berechtigungen in allen relevanten Systemen konsistent verwaltet werden. Dies erfordert idealerweise abgestimmte Prozesse und zentrale Verwaltungslösungen. Zur Umsetzung und Integration dieser Funktionen werden Identity-and-Access-Management-Systeme (IAM) eingesetzt. Diese bündeln das Identitäts- und Berechtigungsmanagement in einer zentralen Plattform und ermöglichen konsistente Richtlinien, automatisierte Provisionierung und eine einheitliche Sicht auf Identitäten und Zugriffe innerhalb der gesamten Organisation. IAM-Systeme sind somit eine wesentliche Voraussetzung für den Aufbau und Betrieb einer Zero-Trust-Architektur.

Übergang zur Umsetzung einer ZTA

Die schrittweise Einführung einer Zero-Trust-Architektur (ZTA) orientiert sich an den zuvor genannten fünf technischen Säulen einer ZTA ([KNS25]). Im Folgenden werden mögliche initiale Umsetzungsschritte innerhalb der Säule Identität beschrieben. Die Themen rund um digitale Identitäten bilden hierbei die Grundlage für viele weitere Aspekte und Komponenten einer ZTA. Eine verlässliche Identitätsverwaltung ist Voraussetzung und Enabler für zahlreiche Maßnahmen in den übrigen Säulen, die in den späteren Abschnitten behandelt werden. Die nachstehenden Empfehlungen für mögliche initiale Umsetzungsschritte berücksichtigen die besonderen technischen und organisatorischen Rahmenbedingungen in Kommunen und Landkreisen. Sie basieren auf Erkenntnissen aus durchgeführten Experteninterviews und weiteren Recherchen und sind auf die spezifischen Anforderungen öffentlicher Verwaltungen zugeschnitten.

4.1 Identitäten und Authentifizierung

In der Säule Identität zählt zu den wichtigsten Zielen bei der Implementierung einer ZTA ein aktuelles Benutzerinventar. Im Rahmen einer Identitätsinventur werden sämtliche digitalen Identitäten – sowohl von Benutzern als auch von Geräten – in der eigenen Infrastruktur sowie bei kommunalen oder externen Dienstleistern erfasst. Gerade in einer kommunalen Verwaltung liegen bedingt durch die Heterogenität und der Einsatz zahlreicher Legacy-Systeme Informationen über die bestehenden Identitäten verstreut in einer Vielzahl von Managementsystemen. Nach dem Zusammentragen und im Zuge der anschließenden Bereinigung und Konsolidierung entsteht ein Benutzerinventar, welches alle aktuellen digitalen Benutzeridentitäten enthält und als Ausgangspunkt für viele weitere Maßnahmen bei der Einführung von Zero-Trust dient. Weiteres Ziel in der Anfangsphase der Einführung einer ZTA ist die konsequente Trennung von Standard- und Administrationskonten, um überprivilegierte Alltagskonten zu vermeiden. Hierdurch werden Verantwortlichkeiten klar abgegrenzt und die Sicherheit der Systeme deutlich erhöht. Gleichzeitig verbessert diese Maßnahme die Nachvollziehbarkeit von Administrationsaktivitäten, reduziert das Risiko von Fehlkonfigurationen und erleichtert die Einhaltung von Compliance- und Auditvorgaben. Die Einführung eines einheitlichen Mindestniveaus für Multi-Faktor-Authentifizierung (MFA) ist ein weiteres Ziel, um die Basissicherheit unmittelbar zu erhöhen. Besonders für Administratorenkonten trägt MFA wesentlich zum Schutz der kommunalen IT-Infrastruktur bei, da privilegierte Zugänge und Berechtigungen gezielt abgesichert werden. Anschließend sollten sukzessiv weitere Zugänge (bspw. zu Netzwerkzugängen über VPN oder Zugänge zu Fachanwendungen) an die MFA gekoppelt werden. Zusätzlich sollte Single-Sign-On (SSO) eingeführt werden, das möglichst viele moderne Anwendungen über einen zentralen oder wenige verteilte (und verbundene) Identity-Provider integriert. Hierdurch werden die Anzahl unterschiedlicher Accounts und Passwörter in der IT-Infrastruktur und den genutzten Fachanwendungen reduziert, der Onboarding-Prozess vereinfacht und die tägliche Nutzung für Mitarbeitende verbessert werden. Im Verlauf sollte angestrebt werden, immer mehr Fachanwendungen an SSO anzubinden.

Ein fortgeschrittenes Ziel ist die Umsetzung phishing-resistenter MFA-Verfahren zertifikatsbasierter oder tokenbasierte Authentifizierung. Diese Verfahren eliminieren gängige Angriffsvektoren und beschleunigen für viele Benutzer die Anmeldung und sind oft schneller nutzbar als passwort-basierte Varianten. Darauf aufbauend sollte kontextbasierte Authentifizierung eingeführt werden, bei der Zugriffe abhängig von Gerätezustand, Standort oder Risikomustern bewertet werden. Für Benutzer bedeutet dies weniger unnötige MFA-Anfragen im Low-Risk-Kontext und gleichzeitig höhere Sicherheit im High-Risk-Kontext. Im nächsten Schritt wird die Föderation von Identitäten auf externe Dienstleister, kommunale IT-Dienstleister und moderne Fachanwendungen ausgeweitet. Hierdurch sinkt die Anzahl der separat gepflegten Konten, Passwörter und Anmeldewege deutlich, was sowohl Sicherheit als auch Benutzbarkeit steigert.

Die nachfolgend beschriebenen Umsetzungschritte sollen dabei helfen, die initialen Ziele im Bereich Identitäten und Authentifizierung umzusetzen. Weitere mögliche Umsetzungsschritte für die fortgeschrittenen Ziele werden im Anschluss in Abschnitt 4.3 skizziert.

4.1.1 Benutzerinventar

Ein Benutzerinventar ist ein zentraler Baustein jeder Zero-Trust-Architektur und bildet die Grundlage für alle identitätsbezogenen Sicherheitsentscheidungen. Zero-Trust beruht auf dem Prinzip, dass keine Identität – unabhängig von Netzwerkstandort oder Gerät – als vertrauenswürdig vorausgesetzt wird. Jede Zugriffsentscheidung basiert auf überprüfbaren und aktuellen Informationen über die jeweilige digitale Identität. Genau hier setzt das Benutzerinventar an. Es liefert eine strukturierte, konsolidierte und belegbare Übersicht über alle digitalen Benutzerkonten, die in einer kommunalen Verwaltung existieren. Ohne ein solches Inventar sind weder die Einführung starker Authentisierungsverfahren noch die Umsetzung eines Least-Privilege-Prinzips möglich. Behörden, die kein vollständiges Bild ihrer Benutzerkonten haben, sind dauerhaft einem unkalkulierbaren Risiko ausgesetzt. Das Benutzerinventar schafft Transparenz in einer historisch gewachsenen, häufig stark fragmentierten IT-Landschaft und ermöglicht es, identitätsbezogene Risiken systematisch zu reduzieren.

Abgrenzung und Inhalte. Ein Benutzerinventar umfasst ausschließlich die digitalen Identitäten von Personen. Dazu gehören Standardkonten, administrative Konten, externe Gastkonten für die Kooperation mit Externen (sowie gegebenenfalls technische Konten, sofern sie einer Person oder einem Verantwortungsbereich zugeordnet werden können). Geräteidentitäten werden dagegen in einem eigenständigen Geräteinventar verwaltet, da sie anderen Sicherheitsanforderungen unterliegen und separat bewertet werden müssen (siehe Abschnitt 5.1). Im Zero-Trust-Kontext ist diese Abgrenzung wichtig, da Entscheidungen über Zugriffe auf der Kombination aus Benutzeridentität, Gerätestatus, Anwendungssensitivität und Kontext beruhen. Nur wenn die Benutzeridentität sauber dokumentiert und nachweisbar aktuell ist, lässt sich ihr Risiko korrekt bewerten. Ein Benutzerinventar bildet

somit die Grundlage für kontextabhängige Zugriffsregeln, starke Authentifizierung, Rollen- und Rechtemanagement sowie für Protokollierung und Audits. Ein vollständiges Benutzerinventar enthält (Referenzen auf) alle für die Zero-Trust-Entscheidungen relevanten Informationen. Hierzu gehören:

- Personenstammdaten wie Name, Organisationseinheit, Funktion oder Fachamt
- Zugehörige digitale Konten über alle Systeme hinweg
- Statusinformationen zu digitalen Konten, bspw. aktiv, deaktiviert oder in Prüfung
- Rollen und Berechtigungen innerhalb der Fachanwendungen
- Zugehörigkeit zu Fachabteilungen und Verantwortungsbereichen
- Informationen zu zu administrativen Verantwortlichkeiten und zugehörigen administrativen Konten

Gerade in kommunalen Verwaltungen, in denen häufig mehrere hundert Fachanwendungen zum Einsatz kommen, ist eine saubere und nachvollziehbare Zuordnung entscheidend. Die Erfahrung zeigt, dass ohne ein konsolidiertes Benutzerinventar veraltete, doppelte oder verwaiste Konten regelmäßig unentdeckt bleiben. Diese Konten bergen ein erhebliches Sicherheitsrisiko, da sie oft schwache Passwörter, veraltete Rollen oder unnötig weitreichende Berechtigungen aufweisen.

Erstellung des Benutzerinventars. Die Erstellung eines Benutzerinventars ist ein mehrstufiger Prozess, der einen systematischen Ansatz erfordert. Kommunale IT-Umgebungen sind sehr heterogen: Es gibt lokale Active-Directories (ADs), Entra-ID-Tenants, Systeme der kommunalen IT-Dienstleister und zahlreiche Fachanwendungen mit eigenen Benutzerverwaltungen. Daher beginnt der Prozess mit der Identifikation aller relevanten Identitätsquellen. Die zentrale Herausforderung besteht darin, die Informationen aus diesen unterschiedlichen Quellen zusammenzuführen. Erst durch die Kombination aus personenbezogener und systembezogener Sicht entsteht ein verlässliches Inventar. Die personenbezogene Sicht analysiert, welche Konten einer bestimmten Person gehören. Die systembezogene Sicht bewertet, welche Konten in den Fachanwendungen existieren und ob sie einer aktiven Person zugeordnet werden können.

Sicherstellung der Aktualität. Ein Benutzerinventar verliert sofort an Wert, wenn es nicht aktuell gehalten wird. In kommunalen Verwaltungen verändern sich Identitäten kontinuierlich. Es werden neue Mitarbeitende eingestellt, andere wechseln innerhalb der Organisation oder verlassen sie. Viele Sicherheitslücken entstehen dadurch, dass Offboarding-Prozesse nicht sauber umgesetzt werden und die Konten ehemaliger Mitarbeitender bestehen bleiben. Ein aktuelles Benutzerinventar hilft dabei, solche Risiken gezielt zu identifizieren und auszuräumen. Die Aktualisierung sollte daher weitgehend automatisiert erfolgen. Dazu gehören das regelmäßige Abfragen der angeschlossenen Systeme, die API-basierte Synchronisation und der Einsatz von Crawlern, die Konten und Statusinformationen erfassen. Ein automatisierter Prozess stellt sicher, dass Konten konsistent angelegt, aktualisiert und deaktiviert werden.

Exkurs: Keycloak als Brückentechnologie. In vielen Kommunen existiert keine einheitliche Identity-Management-Plattform. Stattdessen findet sich eine Vielzahl unabhängiger Benutzerverwaltungen. Eine praktikable Lösung besteht darin, eine Brückentechnologie einzusetzen, die diese Systeme schrittweise verbindet. Die Open-Source-Software Keycloak[2] eignet sich hierfür besonders gut, weil es unterschiedliche Identitätsquellen anbinden und vereinheitlichen kann. Keycloak kann als Aggregator eingesetzt werden, der regelmäßig Benutzerkonten aus Active-Directory (AD), Entra-ID, Fachanwendungen oder Diensten der kommunalen IT-Dienstleister ausliest. Die dabei gewonnenen Daten lassen sich normalisieren und in ein konsolidiertes Benutzerinventar überführen. Zudem kann Keycloak Attribute transformieren, Rollen abgleichen und unterschiedliche Account-Strukturen miteinander verknüpfen. In einem späteren Projektstadium kann Keycloak von einer Adapterlösung zu einem zentralen Identity-Provider ausgebaut werden, der Authentifizierung und Single-Sign-On für die gesamte Verwaltung übernimmt. Dann können Fachanwendungen schrittweise auf föderierte Identitäten umgestellt werden, sodass gesonderte Benutzerkonten für lokale Anwendungen oder Anwendungen eines Dienstleisters vollständig entfallen. Dieser Übergang ist für Kommunen besonders attraktiv, weil er eine behutsame Modernisierung erlaubt, ohne bestehende Systeme sofort ablösen zu müssen.

Sukzessive Entwicklung hin zu einem zentralen IAM. Das langfristige Ziel besteht darin, das Benutzerinventar als Fundament eines zentralen Identity- und Access-Managements (IAM) zu etablieren. Ein solches IAM übernimmt alle Aufgaben entlang des Lebenszyklus einer Identität, steuert die Berechtigungen für alle Fachanwendungen und sorgt für konsistente Sicherheitsrichtlinien. Ein zentrales IAM ist unerlässlich, um Zero-Trust vollständig umzusetzen, da jede Zugriffsentscheidung vom Zustand der Identität abhängig ist. Durch die schrittweise Konsolidierung der Benutzerkonten und deren Integration in einheitliche Prozesse entsteht eine robuste Grundlage für weitere Maßnahmen wie starke Multi-Faktor-Authentifizierung (MFA) oder feingranulare Zugriffsrichtlinien.

4.1.2 Multi-Faktor-Authentifizierung (MFA)

Die Multi-Faktor-Authentifizierung ist eine Kernvoraussetzung, um Identitäten in einer Zero-Trust-Architektur zuverlässig zu verifizieren. Zero-Trust geht davon aus, dass ein Passwort für die Authentifizierung grundsätzlich nicht ausreicht, um einer Identität zu vertrauen [KNS25][BSI23e][CIS23]. Erst die Kombination mehrerer unabhängiger Faktoren ermöglicht eine belastbare Aussage darüber, ob eine Person tatsächlich die ist, für die sie sich ausgibt. Zahlreiche nationale und internationale Leitfäden zu Zero-Trust (u. a. [DoD22a][NIS20][BSI23e][CIS23]) stufen MFA als notwendige Basiskontrolle ein, insbesondere für privilegierte, externe und besonders sensible Zugänge. In kommunalen Umgebungen mit vielen historisch gewachsenen, eigenständigen Fachanwendungen ist MFA deshalb ein schnell wirksamer Baustein für den Einstieg in Zero-Trust. Der IT-Grundschutz beschreibt im Baustein ORP.4 „Identitäts- und Berechtigungsmanagement“ [BSI23a] die Notwendigkeit einer starken Authentisierung bei erhöhtem Schutzbedarf und empfiehlt explizit Verfahren mit kryptografischem Besitzfaktor, etwa Zertifikate, Smartcards oder dedizierte Token. Die WiBA-Vorgehensweise des BSI [BSI23f] überträgt diese Grundsätze auf

2 https://www.keycloak.org/

die Realität kommunaler Verwaltungen und machen MFA zu einer zentralen Mindestanforderung für das Rollen- und Berechtigungsmanagement, die sichere externe Arbeit und den administrativen Zugriff. Beide Rahmenwerke betonen, dass selbst im Basisabsicherungs-Niveau ein Passwort allein nicht mehr genügt, sobald Daten oder Prozesse einen höheren Schutzbedarf besitzen oder Zugriffspfade aus dem Internet möglich sind.

Einführung von MFA für privilegierte Konten. Als erster Umsetzungsschritt eignet sich die Einführung von MFA für administrative Konten. Diese Konten bergen in jeder Organisation das höchste Angriffspotenzial dar, da ihre Kontenbesitzer tief in Systeme eingreifen, Konfigurationen verändern und auf zentrale Daten zugreifen können. In kommunalen IT-Landschaften ist sich diese Bedeutung noch größer, weil häufig ein kleiner Kreis von Administratoren mehrere Fachanwendungen, Infrastrukturkomponenten und zentrale Dienste betreut. Damit kann ein kompromittiertes Administrationskonto zu einem vollständigen Kontrollverlust über wesentliche Teile der kommunalen IT führen. Der Einstieg über die Zielgruppe der Administratoren bietet einen deutlichen Sicherheitsgewinn bei vergleichsweise geringem organisatorischem Aufwand. Die Anzahl privilegierter Konten ist überschaubar, die Zielgruppe ist technisch kompetent, und die Einführung verursacht kaum Reibungen bei der breiten Belegschaft. Dieser Schritt stellt einen klaren „Zero-Trust-Quick-Win“ dar: Das Risiko sinkt sofort, während die operative Belastung gering bleibt. Gleichzeitig entsteht ein Testfeld, um Prozesse, Support und Identity-Provider-Konfigurationen stabil einzuführen, bevor die Maßnahme auf weitere Nutzergruppen ausgeweitet wird.

MFA für externe Zugriffe und mobile Arbeit. Ein zweiter naheliegender Anwendungsbereich ist der Zugriff aus dem Home-Office, von mobilen Arbeitsplätzen oder über das Internet. Kommunale Verwaltungen betreiben heute häufig hybride Infrastrukturen, Cloud-Dienste und externe Zugänge zu Fachanwendungen. Da der Netzwerkperimeter in diesen Anwendungsbereichen zunehmend weniger Schutz bietet, gilt MFA in vielen Leitfäden als zwingende Voraussetzung, bevor ein externer Zugriff zugelassen wird. Für die kommunale IT-Praxis bedeutet dies, dass VPN-Zugänge, Webportale und E-Mail- oder Kollaborationslösungen nicht mehr ohne MFA erreichbar sein sollten.

Auswahl geeigneter MFA-Verfahren unter Berücksichtigung kommunaler Besonderheiten. Aus technischer Sicht stehen verschiedene Verfahren zur Verfügung: Authenticator-Apps, Hardware-Token, Smartcards, FIDO2-Schlüssel oder zertifikatsbasierte Verfahren. Laut internationalen Best Practices sollten phishing-resistente Verfahren wie FIDO2/WebAuthn oder PKI-Authentisierung priorisiert werden, da sie im Gegensatz zu SMS-TAN oder einfachen Push-Verfahren deutlich widerstandsfähiger gegen moderne Social-Engineering-Angriffe wie Phishing- und MFA-Ermüdungsangriffe (*MFA Fatigue*) sind. In der kommunalen Praxis müssen jedoch auch Akzeptanz, Arbeitsrealität und Datenschutz berücksichtigt werden. Viele Beschäftigte wollen oder dürfen ihr privates Smartphone nicht für dienstliche Zwecke einsetzen. Ein Arbeitgeber kann dies nicht erzwingen. Deshalb müssen Alternativen angeboten werden. Geeignete Ersatzmethoden sind Hardware-Token, OTP-Generatoren, dienstliche Smartphones oder Smartcards, die ggf. bereits für andere Anwendungsfelder (z. B. qualifizierte elektronische Signaturen oder Verwaltungsportale) genutzt werden. Zudem ist zu erwarten, dass in Teilen der Mitarbeiterschaft Vorbehalte gegenüber biometrischen Merkmalen bestehen. Diese müssen datenschutzrechtlich

sorgfältig behandelt werden und nicht-biometrische Alternativen müssen jederzeit verfügbar bleiben. Für Außenstellen, Schulen, Bauhöfe und kommunale Betriebe sind robuste und einfach bedienbare Hardware-Token möglicherweise praktikabler als app-basierte Lösungen. Die Auswahl des Verfahrens sollte daher sowohl den Sicherheitsgrad als auch die technische und organisatorische Realität in den verschiedenen Fachämtern berücksichtigen.

4.1.3 Single-Sign-On (SSO)

Ausgangslage in Kommunen. Kommunale IT-Landschaften sind stark durch historisch gewachsene Strukturen geprägt. Zwar dient Microsoft Active-Directory nahezu überall als zentrale Identitätsquelle, jedoch existieren parallel dazu zahlreiche weitere Benutzerkonten in hochgradig unterschiedlichen Fachanwendungen. Viele dieser Systeme basieren auf einer eigenen Benutzerverwaltung, proprietären Authentifizierungsmechanismen oder alten Schnittstellen, die moderne SSO-Standards nicht unterstützen. Hierdurch entsteht eine fragmentierte Identitätslandschaft, in der ein vollständiger und konsistenter Überblick über aktive Konten, Berechtigungen und Rollen kaum möglich ist. Die teilweise bestehende enge Abhängigkeit von kommunalen IT-Dienstleistern erschwert zusätzlich die Etablierung eines einheitlichen Identitäts- und Authentifizierungsmodells. Die Dienstleister entscheiden oft selbst, welche technischen Integrationsoptionen bereitstehen. Während sich manche Fachanwendungen problemlos anbinden lassen, wird bei anderen der Einsatz moderner Authentifzierungsverfahren nicht unterstützt. Für Kommunen ist diese Situation problematisch, da Zero-Trust auf verlässliche, exakt definierte und zentral kontrollierbare Identitäten angewiesen ist. Ein fragmentiertes Identitätsbild verhindert jedoch das Zero-Trust-Ziel der „Continuous Verification“, also die stetige Überprüfung der Berechtigungslage eines Zugriffs, die im Zero-Trust-Modell grundlegend ist.

Um diesen Herausforderungen zu begegnen, ist ein zentraler Identity-Provider das strategische Zielbild. Ob dieser innerhalb der kommunalen IT selbst betrieben oder vom kommunalen Dienstleister bereitgestellt wird, hängt davon ab, wie stark die Kommune von extern betriebenen Fachanwendungen abhängig ist. Entscheidend ist, dass alle Authentifizierungsprozesse auf einen gemeinsamen Ursprung zurückgreifen und über standardisierte Verfahren abgewickelt werden. Zentrales SSO basiert auf modernen Protokollen wie SAML oder OpenID-Connect. Diese Standards erlauben es, Benutzer über ein einziges, sicheres Authentifizierungsverfahren in unterschiedlichste Anwendungen zu bringen – unabhängig davon, wo diese betrieben werden. In einer heterogenen Umgebung wie einer Kommune ist das von großem Vorteil, da viele der bisherigen Insellösungen ersetzt oder zumindest konsolidiert werden können. Ein weiterer entscheidender Punkt ist, dass Multi-Faktor-Authentifizierung nicht nur eine sinnvolle Ergänzung zu SSO ist, sondern eine zwingende Voraussetzung. Da SSO die Anzahl der erforderlichen Anmeldungen reduziert, steigt der Sicherheitswert jeder einzelnen Authentifizierung. Zero-Trust verlangt, dass Benutzeridentitäten zuverlässig und manipulationsresistent überprüft werden. Ohne MFA wäre SSO zu riskant, da erfolgreiches Passwort-Phishing sofort Zugriff auf alle angebundenen Fachanwendungen erlauben würde. Schließlich sollten normalen Benutzerkonten und Administrationskonten strikt getrennt werden.

Vorbereitende Maßnahmen zur Einführung von SSO. Zunächst ist eine Bestandsaufnahme der existierenden Identitäten (siehe Benutzerinventar), Fachanwendungen und Authentifizierungsverfahren erforderlich. Bevor SSO implementiert werden kann, muss die Kommune ihre tatsächliche Identitätslandschaft vollständig erfassen. Dies beginnt mit einer umfassenden Inventarisierung aller Benutzerkonten einschließlich der Konten in von Dienstleistern betriebenen Fachanwendungen sowie technischer Konten. Dabei ist es wichtig zu verstehen, welche Verfahren zum Einsatz kommen und ob diese für SSO geeignet sind oder welche Anpassungen nötig wären. Einige Fachanwendungen werden SAML oder OpenID-Connect bereits unterstützen, andere können mit vertretbarem Aufwand über technische Adapter angebunden werden, während eine dritte Gruppe technisch so alt oder proprietär ist, dass eine Integration nur langfristig oder gar nicht möglich ist. Ein weiterer wesentlicher Aspekt ist die Definition und Implementierung eines präzisen Identity-Lifecycle-Prozesses. Zero-Trust setzt voraus, dass Identitäten vom Eintritt über Rollenwechsel bis zum Austritt eines Mitarbeiters zuverlässig gesteuert werden können. Parallel zur Bestandsaufnahme müssen technische und organisatorische Grundlagen geschaffen werden. Hierzu gehört insbesondere die Modernisierung und Härtung der Identitätsinfrastruktur, also des Active-Directory oder einer möglichen cloudbasierten Erweiterung. Schwache Passwort-Richtlinien, unklare Rollenzuweisungen oder unzureichende Härtung privilegierter Konten müssen beseitigt werden, bevor SSO produktiv genutzt wird. MFA muss zum Standard werden – und zwar nicht nur für Administratoren, sondern für alle Benutzer. Außerdem muss verbindlich festgelegt werden, dass neue oder zu beschaffende Fachanwendungen moderne Authentifizierungsverfahren unterstützen müssen. Nur so lässt sich verhindern, dass Kommunen weiterhin Systeme anschaffen, die modernisierte Sicherheitsstrategien blockieren. Schließlich müssen Richtlinien für SSO definiert werden, z. B. hinsichtlich der Stärke der Authentifizierung, der Gültigkeitsdauer von Sessions, der Häufigkeit von Reauthentifizierungen und der technischen Trennung von administrativen und regulären Konten.

SSO-Integration in Fachanwendungen. Grundsätzlich lassen sich drei Hauptmodelle unterscheiden: lokal betriebene Fachanwendungen innerhalb des kommunalen Netzwerks, Anwendungen, die von einem kommunalen IT-Dienstleister betrieben werden, sowie Cloud-Anwendungen externer Anbieter. Zusätzlich besitzen Fachanwendungen unterschiedliche Arten von Benutzungsschnittstelle (z. B. lokal installierte Anwendung (*Fat-Client*) vs. webbasierte Benutzungsschnittstelle). Jedes Modell bringt eigene Herausforderungen mit sich. So sind lokale Anwendungen oft technisch veraltet und benötigen zusätzliche Adapter oder Proxy-Lösungen. Anwendungen beim Dienstleister erfordern abgestimmte Schnittstellen und gemeinsame Prozesse für das Identitätsmanagement. Cloud-Anwendungen sind dagegen meist technologisch modern und lassen sich schnell über standardisierte Föderationsmechanismen anbinden. Diese Unterscheidung dient in erster Linie dazu, eine realistische SSO-Roadmap zu erstellen. Zunächst werden die Anwendungen integriert, bei denen dies am schnellsten und mit geringem Aufwand möglich ist. Komplexere Altverfahren folgen anschließend (s. auch Abschnitt 7 Initiale Umsetzungsschritte in der Säule Workload & Apps).

SSO für Normalnutzer und Administrationskonten. SSO bietet für reguläre Benutzerkonten erhebliche Vorteile. Die Anzahl der benötigten Passwörter sinkt, die Zahl der erforderlichen Anmeldungen reduziert sich deutlich und somit werden sowohl die Benutzerfreundlichkeit als auch die Produktivität erhöht. Gleichzeitig entlastet dies den

Support, da viele Passwortprobleme gar nicht mehr auftreten. Das Risiko liegt vor allem in der Zentralisierung: Wenn ein Angreifer ein Benutzerkonto übernimmt, erhält er potenziell Zugriff auf alle angebundenen Anwendungen. Dieses Risiko wird durch MFA und ein gutes Session-Management jedoch weitgehend gemindert. Bei Administratoren ist die Lage deutlich sensibler. Auch hier kann SSO zu einer erheblichen Entlastung führen, da Administrationsaufgaben typischerweise viele verschiedene Systeme umfassen. Gleichzeitig ist der Schaden bei einer Kompromittierung eines Admin-SSO-Tokens um ein Vielfaches größer. Ein einziger erfolgreicher Angriff könnte eine gesamte Fachanwendungen, Fachämter oder Netzwerksegmente kompromittieren. Daher sind erhöhte Sicherheitsmaßnahmen zwingend erforderlich. Administrationskonten benötigen streng segmentierte Arbeitsumgebungen, separate Admin-Workstations, klar voneinander getrennte Authentifizierungswege und deutlich kürzere Session-Laufzeiten. MFA ist in diesem Bereich nicht optional, sondern zwingend erforderlich. Die gesamte Architektur muss so konstruiert sein, dass administrative Zugriffe stets eine höhere Vertrauensanforderung erfüllen als reguläre Benutzerzugriffe.

Authentifizierungs-Adapter in heterogener kommunaler IT. Viele Kommunen sehen sich mit der Herausforderung konfrontiert, dass ein erheblicher Teil ihrer Fachanwendungen keine modernen Authentifizierungsstandards unterstützt und auch nicht kurzfristig modernisiert werden kann. In solchen Fällen kann ein System wie Keycloak (wie auch schon zuvor bei der Erstellung des Benutzerinventars) als flexible Brücke dienen. Es kann als zentraler Vermittler auftreten, der verschiedene Protokolle unterstützt und somit alte und neue Systeme miteinander verbindet. Keycloak kann bspw. eine Legacy-Anwendung mit klassischem Login so einbinden, dass sich die Benutzer zentral authentifizieren und Keycloak die Anmeldedaten intern weiterreicht. Ebenso kann Keycloak zwischen Kommunen und kommunalen Dienstleistern vermitteln, indem es unterschiedlich strukturierte Rollenmodelle oder Protokolle übersetzt. Keycloak ist besonders wertvoll für die Anbindung von veralteten Legacy-Fachanwendungen an ein einheitliches SSO-Ökosystem, da diese sofort mit modernen Protokollen wie OIDC verbunden werden können.

Praktische Empfehlungen zur Einführung von SSO. Kommunen sollten SSO konsequent als sicherheitssteigernde Maßnahme betrachten. Dazu gehört, MFA flächendeckend einzuführen und SSO niemals allein als Komfortfunktion zu verstehen. Die BSI-Grundschutzempfehlungen [BSI23d][BSI23a] betonen die Bedeutung einer zentralen Benutzerverwaltung, einer strikten Rollentrennung und sicherer Authentifizierungsmechanismen. Diese Prinzipien gelten auch für die WiBA-Empfehlungen [BSI23f], die ebenfalls auf klare organisatorische und technische Mindeststandards abzielen. Wichtig ist auch, den Identity-Provider als kritische Infrastruktur zu behandeln. Das bedeutet konsequente Härtung, redundanter Aufbau, durchgehendes Monitoring und revisionssichere Protokollierung. Ebenso sollte die Integration der Fachanwendungen schrittweise erfolgen. Zunächst sollten Anwendungen angebunden werden, die moderne Standards unterstützen, da sie schnelle Erfolge liefern. Die Integration von Fachanwendungen, die von einem Dienstleister gehostet werden, sollte in enger Abstimmung erfolgen [Sch25], während komplexe Altverfahren zu einem späteren Zeitpunkt folgen. Darüber hinaus müssen die Beschaffungsprozesse angepasst werden. Jede neue Anwendung sollte zwingend moderne Authentifizierungsverfahren wie SAML oder OIDC unterstützen. Nur so lässt sich langfristig verhindern, dass technisch unintegrierbare

Insellösungen entstehen. SSO bietet Kommunen einen klaren Mehrwert, da es die Komplexität reduziert, die Sicherheit steigert und die Grundlage für alle weiteren Zero-Trust-Maßnahmen in der Säule Identität schafft. Des Weiteren stärkt SSO die Governance einer Kommune, weil es Identitäten konsolidiert, konsistente Identitätsprüfungen über alle Systeme hinweg erlaubt, Prozesse strukturiert und die Nachvollziehbarkeit und Auditierbarkeit von Anmeldeprozessen erlaubt.

4.2
Berechtigungen und Zugriffskontrolle

Ein wichtiges Ziel ist der Aufbau einer klar definierten und konsistenten Definition von Rollen- und Berechtigungen als Grundlage für ein strukturiertes Zugriffsmanagement. Auf Basis von Rollen, Zuständigkeiten und organisatorischen Aufgabenbereichen sollen eindeutige Zugriffsrichtlinien entwickelt werden, die eine nachvollziehbare und überprüfbare Vergabe von Berechtigungen ermöglichen. Weiteres Ziel ist der Aufbau eines rollenbasierten Zugriffskonzepts (RBAC), das Benutzerzugriffe auf vordefinierte Rollen und Gruppen beschränkt. Durch gezieltes Role-Engineering und die systematische Zuordnung von Berechtigungen zu diesen Rollen wird die Verwaltung vereinfacht, Fehlerquellen reduziert, Sonderfälle für Berechtigungszuweisungen minimiert und die Transparenz im Umgang mit Berechtigungen erhöht. Weiteres Ziel ist es, dass künftig feingranulare Zugriffsentscheidungen auf Basis definierter Attribute wie Abteilung, Standort oder Gerätetyp getroffen werden. Ein weiteres Ziel ist die konsequente Umsetzung des Least-Privilege-Prinzips, beginnend mit privilegierten Konten. Hierdurch wird sichergestellt, dass nur tatsächlich erforderliche Berechtigungen vergeben werden. So werden Angriffsflächen verringert, die IT-Sicherheit gestärkt und gleichzeitig die Funktionsfähigkeit der Nutzer erhalten. Weiteres Ziel ist die Einführung eines Zugriffsmanagements für privilegierte Accounts zum Schutz und zur Steuerung von Administrationskonten.

4.2.1
Management von Berechtigungen und Least-Privilege

Im Zero-Trust-Modell bilden Identitäten und deren Berechtigungen die zentrale Grundlage jeder Zugriffsentscheidung. Für kommunale Verwaltungen bedeutet das: Nicht mehr das Netzwerk oder der Standort entscheidet über den Zugriff, sondern ausschließlich die Identität der Person, ihre Rolle und die zusätzlichen Nebenbedingungen, die erfüllt sein müssen. Kernprinzipien sind das Least-Privilege-Prinzip und die Deny-by-Default-Richtlinie.

Leitprinzipien für das Berechtigungsmanagement von Zero-Trust. Der wichtigste Grundsatz ist das Least-Privilege-Prinzip: Jeder Nutzer erhält ausschließlich die Berechtigungen, die er wirklich benötigt. Als technische Basis eignet sich eine rollenbasierte Zugriffskontrolle (RBAC). Hierbei werden Berechtigungen nicht direkt einzelnen Benutzern zugewiesen, sondern an vordefinierte Rollen gebunden. Nutzer erhalten Rollen, die zu ihren Aufgaben passen, und erben so die benötigten Berechtigungen. Diese orientieren sich an Aufgaben, Fachämtern, Fachbereichen und Funktionsrollen. In Microsoft Active-Directory-Umgebungen wird RBAC typischerweise über AD-Gruppen umgesetzt. Um Rollen nicht unnötig breit zu definieren, sollten ergänzend statische Kontextattribute wie Fachamt, Organisationseinheit oder Standort berücksichtigt werden.

Priorisierung von administrativen Berechtigungen. Da der Sicherheitsgewinn hier am größten ist und normale Mitarbeitende nicht betroffen sind, sollte die Umsetzung mit privilegierten Konten beginnen. Zunächst werden alle Administrationskonten und -gruppen identifiziert und anschließend bereinigt, d. h., überflüssige Mitgliedschaften werden entfernt, Benutzer- und Admininistrationskonten werden getrennt und es werden klare Vergabe- und Freigabeverfahren etabliert.

Sukzessive Erweiterung auf erste Fachämter und Fachbereiche. Der nächste Schritt ist die gemeinsame Abstimmung eines Rollenmodells zwischen der IT-Verwaltung und einigen ausgewählten Fachämtern bzw.-bereichen. Grundlage hierfür ist eine einfache Rollenbeschreibung: Welche Rollen gibt es und welche Berechtigungen werden dafür benötigt? Diese Rollen werden anschließend technisch umgesetzt (z. B. als AD-Gruppen). Nutzer erhalten ihre Rechte ausschließlich über ihre Rollen- bzw. Gruppenmitgliedschaften. Wo Fachanwendungen AD-Gruppen nicht direkt nutzen können, dienen die Rollen dennoch als Leitplanke für die lokale Berechtigungsverwaltung. In heterogenen Landschaften könnte die Kombination eines Microsoft Active-Directory als Master für interne Identitäten mit der Open-Source-Software Keycloak als zentralem Authentifizierungs- und Autorisierungslayer ein praktikabler Ansatz sein. Keycloak liest Benutzer, Gruppen und Attribute aus dem AD aus und stellt sie Anwendungen bereit, die OIDC oder SAML unterstützen. Dadurch können Berechtigungen zunehmend zentral gesteuert werden, ohne dass die Fachanwendungen tiefgreifend umgebaut werden müssen.

Statischer Kontextattribute für Zugriffsentscheidungen. Statische Kontextattribute sind zusätzliche Informationen einer digitalen Identität, die sich nur selten ändern. Dazu zählen Metadaten wie das zugehörige Fachamt, der Fachbereich, die Organisationseinheit, der Dienstort oder der organisatorische Verantwortungsbereich. Diese Attribute existieren innerhalb des zuvor aufgebauten Benutzerinventars, werden aber bislang kaum systematisch für Zugriffsentscheidungen genutzt. Statische Kontexte (*static contraints* bei RBAC [ANS04] bzw. *subject attributes* bei Attributbasierter Zugriffskontrolle (ABAC) [NIS21][DoD22b]) ergänzen die Zugriffskontrolle als zweite Entscheidungsebene. Eine Rolle beschreibt, welche Berechtigungen grundsätzlich erlaubt wären. Der statische Kontext grenzt Berechtigungen weiter ein, indem geprüft wird, ob die Identität die dafür vorgesehenen organisatorischen Eigenschaften besitzt. Ein Zugriff wird nur gewährt, wenn die Rolle stimmt und alle relevanten Kontextattribute passen.

Best Practices zum Berechtigungsmanagement für Zero-Trust. Für den langfristigen Erfolg ist eine klare, aber schlanke Governance unerlässlich. Rollen, Rechte und Verantwortlichkeiten müssen einheitlich definiert und nachvollziehbar umgesetzt werden. Durch die zunehmende zentrale Steuerung werden Vergabe, Änderung und Entzug von Berechtigungen konsistent, prüfbar und revisionssicher, was Fehlberechtigungen und Schattenstrukturen reduziert. Ein einfaches Berechtigungskonzept genügt, solange es verbindlich umgesetzt wird. Onboarding-, Offboarding- und Wechselprozesse sollten an die Personalmanagement-Prozesse gekoppelt sein. Kritische Rollen und administrative Zugänge müssen regelmäßig überprüft werden. Zu Beginn sollten Logging und Reporting pragmatisch erfolgen, etwa über einfache Reports aus AD oder Keycloak. Vertretungsregeln sollten sauber modelliert werden, um Ad-hoc-Freischaltungen zu vermeiden und die Integrität des Berechtigungsmodells zu wahren.

4.2.2
Zugriffsmanagement für privilegierte Accounts

Privilegierte Konten zählen zu den wichtigsten Angriffszielen, da sie eine systemübergreifende Kontrolle ermöglichen. Schon ein einziges kompromittiertes Administrationskonto kann ausreichen, um große Teile der IT-Infrastruktur zu übernehmen – inklusive Fachanwendungen, zentraler Komponenten der IT-Infrastruktur (wie Firewalls, Switches und Server) sowie zentraler Identitätsdienste. Zero-Trust fordert deshalb minimale, notwendige Rechte, eine klare Aufgabentrennung und die kontinuierliche Überprüfung aller administrativen Aktionen. Dies ist besonders für Kommunen relevant, da sowohl interne Systeme als auch Fachanwendungen lokal betrieben oder bei Dienstleistern verwaltet werden können und es unterschiedliche Admin-Ebenen gibt. In kommunalen IT-Landschaften existieren viele unterschiedliche Arten von Administrationskonten, wie Domänen-, Server-, M365- und Fachanwendungs-Administratoren sowie adminbezogene Dienstleisterkonten. Die Trennung von Benutzer- und Administrationskonten ist zwar üblich, jedoch nicht immer konsequent in allen Systemen und Fachanwendungen umgesetzt. Die Kombination aus heterogener Systemlandschaft, Aufgabenteilung mit kommunalen Rechenzentren und unterschiedlichen Sicherheitsniveaus führt zu komplexen Risiken: Ein kompromittiertes Administrator-Konto einer Fachanwendung oder eines Dienstleisters kann direkten Zugriff auf kritische Daten ermöglichen.

Die folgenden Maßnahmen bilden den grundlegenden Kern für die Absicherung privilegierter Konten. Sie reduzieren die Angriffsfläche unmittelbar, unterbinden typische Angriffsvektoren wie *Credential-Theft* und *Lateral-Movement* und schaffen die Grundlage für weitere Zero-Trust-Ausbaustufen.

Überprüfung der Trennung von Benutzer- und Administrationskonten. Die Trennung ist in vielen Kommunen und Landkreisen bereits Standard, sollte aber für alle Systeme und Fachanwendungen konsequent überprüft werden. Administrationskonten dürfen ausschließlich für Verwaltungsaufgaben genutzt werden. Sie sollten technisch daran gehindert werden, normale Tätigkeiten ohne Administrationsbezug auszuführen, bspw. E-Mails abzurufen, klassische Office-Tätigkeiten auszuführen oder im Internet zu surfen. Hierdurch wird verhindert, dass administrative Konten durch Alltagsrisiken wie Phishing oder Drive-by-Downloads kompromittiert werden.

Einführung bzw. Absicherung eines Admin-Rollenmodells. Ein klar definiertes Admin-Rollenmodell stellt sicher, dass administrative Aufgaben sauber voneinander getrennt werden und jede Rolle nur die Rechte erhält, die sie tatsächlich benötigt. Das Microsoft-Tiering-Modell [Mic25] bietet hierfür eine praxistaugliche Orientierung, indem es administrative Tätigkeiten in Sicherheitsstufen (Tier 0, Tier 1, Tier 2) gliedert und somit unnötige Rechteüberschneidungen verhindert. In kommunalen Umgebungen ist diese Struktur besonders hilfreich, um die Domänenadministration, den Serverbetrieb und die Fachanwendungsadministration voneinander abzugrenzen. Auf dieser Basis können Administrationskonten technisch und organisatorisch sauber zugeordnet, kontrolliert und überwacht werden.

Geschützte und kontrollierte Zugangswege. Administrationszugriffe sollten nur über speziell gesicherte Wege erfolgen. Dazu gehören dedizierte VPN-Verbindungen für Administrationszwecke, die Nutzung von *Jump-Hosts* oder *Terminalservern* als zentrale Einstiegspunkte sowie optional *Privileged-Access-Workstations (PAWs)*. Bei diesen PAWs ist das Gerät vollständig für sichere Verwaltungstätigkeiten gehärtet. PAWs dienen als hochsicheres „Schutzschild" für kritische Zugriffe, indem sie administrative Aufgaben strikt von alltäglichen Sicherheitsrisiken wie E-Mails oder Web-Surfen trennen. Hierdurch werden die verbreitete Angriffsversuche nicht direkt an kritischen Systemen ausgeführt und alle administrativen Zugriffe sind besser kontrollierbar.

Härtung der Authentifizierung und sichere SSO-Strategie Für privilegierte Konten gelten erhöhte Anforderungen an die Authentifizierung. Dazu gehören längere Passwörter, strengere Richtlinien sowie eine verpflichtende Multi-Faktor-Authentifizierung, idealerweise in einer phishing-resistenten Form wie FIDO2. SSO erleichtert Administratoren die Arbeit erheblich und reduziert die Nutzung von Passwörtern. Gleichzeitig besteht das Risiko, dass ein kompromittiertes SSO-Token weitreichende Zugriffe ermöglicht. Um dieses Risiko zu reduzieren, sollten besonders sensible administrative Aktionen eine zusätzliche MFA-Abfrage unmittelbar vor der Ausführung verlangen. Ein einmaliges vorheriges Login reicht damit nicht aus, um weitreichende Änderungen vorzunehmen. Ergänzend sollten die Gültigkeitsdauer der Token verkürzt und Komfortfunktionen wie „Remember-Me" für Administratoren deaktiviert werden. Zudem ist es sinnvoll, SSO-Sitzungen privilegierter Konten strikt an definierte Geräte, z. B. Admin-Arbeitsplätze oder spezielle Terminalserver, zu binden. Schließlich sollten Administrationskonten strengere SSO-Richtlinien erhalten, bspw. durch einen separaten Sicherheitslevel oder einen eigenen Satz von IdP-Policies. Das Spannungsfeld zwischen IT-Sicherheit und Usability ist bei Administrationskonten besonders ausgeprägt. Einerseits müssen administrative Zugriffe maximal geschützt werden, andererseits dürfen Sicherheitsmaßnahmen die Arbeit der Administratoren nicht unnötig behindern. Zu strenge oder umständliche Prozesse führen erfahrungsgemäß dazu, dass Benutzer Workarounds entwickeln, wodurch neue Sicherheitsrisiken entstehen können. Gleichzeitig profitieren gerade Administratoren von guter Usability, da konsistente und gut integrierte Sicherheitsmechanismen ihre tägliche Arbeit effizienter und weniger fehleranfällig machen.

Logging, regelmäßige Überprüfung und Auditierung. Alle administrativen Anmeldungen, Rollenänderungen und kritischen Operationen sollten mindestens im Active-Directory, in IT-Infrastruktur-Komponenten, in Cloud-Systemen und in Fachanwendungen protokolliert werden. Darüber hinaus sollten Admin-Berechtigungen regelmäßig überprüft werden. So können Missbrauchsversuche frühzeitig erkannt, die Transparenz verstärkt und eine Verbesserung der Governance durch Nachvollziehbarkeit und Auditierbarkeit erreicht werden.

4.3
Fortgeschrittene Maßnahmen

Nachdem grundlegende Identitäts- und Berechtigungsmechanismen etabliert wurden, stehen weitere, fortgeschrittene Maßnahmen zur Umsetzung einer ZTA im Fokus. Diese bauen auf den zuvor beschriebenen Grundlagen auf und führen zu einer höheren Reife der Identitäts- und Zugriffsinfrastruktur.

Zentrales und integriertes Identitäts- und Berechtigungsmanagement: Ermöglichung eines durchgängigen Lifecycle-Managements von Identitäten und Rechten von der Erstellung bis zur Löschung. Automatisierung und Integration von Onboarding- und Offboarding-Prozessen, Einbindung kommunaler Dienstleister in Verwaltungsprozesse von Identitäten und Berechtigungen, Vereinheitlichung der Verwaltung von Identitäten und Berechtigungen.

Übergreifende ZTA-Berechtigungsarchitektur: Umsetzung eines Berechtigungsmanagements innerhalb der ZTA, das aus verschiedenen Policy-Enforcement-Points (PEPs), wenigen Policy-Decision-Points (PDPs) und wenigen Policy-Administration-Points (PAPs) besteht,

Kontinuierliche Authentifizierung: Von einer einmaligen Authentifizierung über eine periodische Authentifizierung hin zu einer kontinuierlichen Authentifizierung und Re-Authentifizierung mit und ohne Nutzerinteraktion.

Dynamische Kontexte: Eine dynamische, kontextabhängige Zugriffskontrollen sorgt für mehr Sicherheit und Anpassungsfähigkeit. Zugriffsentscheidungen werden abhängig von Kriterien wie Metadaten der Identität oder Informationen der Umgebung (z. B. Login-Ort, IP-Adresse, Uhrzeit und Gerätetyp, Benutzer- und Gerätestatus).

Identitätsanbieter und föderierte Identitäten: Aufbau und Integration kommunaler Public-Key-Infrastrukturen (PKIs) und kommunaler Identitätsanbieter (Identity-Provider, IdP), Möglichkeiten zur Anbindung kommunenübergreifender oder externer IdPs.

Privileged-Access-Management (PAM): Einführung eines Privileged-Access-Management-Systems, das Admin-Passwörter zentral verwaltet, Berechtigungen bei Bedarf temporär vergibt und administrative Sitzungen nachvollziehbar macht.

5
Initiale Umsetzungsschritte in der Säule Geräte

Ein Gerät stellt im Rahmen dieser Studie ein Anlagegut (*Asset*) dar, bestehend aus Hard- und Software, Firmware, etc., das sich mit einem Netzwerk verbinden kann. Dies schließt Server, Desktop-Rechner (PCs), Laptops, Drucker, Smartphones, Netzwerkgeräte (bspw. Router) und ähnliches ein. Geräte können Eigentum der Kommune, deren Mitarbeitenden oder von Dritten (bspw. Gäste) sein. Kommuneneigene Geräte bilden das Gros der Geräte, welche für die IT-gestützten Arbeiten innerhalb der Kommune genutzt werden. Daneben könnten private Geräte von Mitarbeitenden (*Bring-Your-Own-Device*, BYOD) zum Einsatz kommen, um auf interne Dienste der Kommune zugreifen zu können oder um die Funktionalität kommuneneigener Geräte zu ergänzen, bspw. private Smartphones mit Authenticator-Apps zur Multi-Faktor-Authentifizierung (MFA). Gäste werden i. d. R. keinen Zugriff auf interne Ressourcen haben, könnten jedoch über ein Drahtlosnetzwerk (WLAN) speziell für Gäste Internetzugriff erhalten.

Die Verwaltung und Sichtbarkeit von Geräten im kommuneneigenen Netzwerk, insbesondere solcher Geräte die Zugriff auf interne Ressourcen haben, spielt eine zentrale Rolle in einer Zero-Trust-Architektur (ZTA). Jedes Gerät das im kommuneneigenen Netzwerk, im Folgenden meist nur noch als Netzwerk bezeichnet, in irgendeiner Form aktiv wird, muss zentral erfasst werden können, sodass es keine „blinden Flecken“ gibt, die von Angreifern ausgenutzt werden können. Dies ist der erste Schritt, um Sichtbarkeit von Geräten zu erreichen.

Generell sollten Geräte keinen Zugriff auf kommuneninterne Ressourcen erhalten, die nicht im Vorfeld – d. h. vor dem Zugriff – geprüft und zugelassen wurden. Die Prüfung stellt, nach der Herstellung von Sichtbarkeit, den zweiten Schritt dar, um zu gewährleisten, dass auf Geräten keine veraltete Software, die ggf. ausnutzbare Schwachstellen enthält, oder unbekannte Software installiert ist, die ggf. ein Schadprogramm (*Malware*) ist bzw. enthält. Weiterhin ist wichtig, dass die Prüfung regelmäßig erfolgt, d. h. nicht nur einmalig, wenn das Gerät in Betrieb genommen wird. Die Bestandteile der Prüfung müssen im Vorfeld festgelegt werden und dienen dazu, die innerhalb der Kommune festgelegte Sicherheitsrichtlinie (*security policy*) praktisch umzusetzen bzw. deren Einhaltung zu prüfen. Eine bestandene Prüfung ist ein Beitrag zur Einhaltung der Sicherheitsrichtlinie der Kommune, im Folgenden auch mit dem englischen *Compliance* bezeichnet.

In den folgenden Abschnitten wird es darum gehen, welche Maßnahmen zur Gewährleistung von Sichtbarkeit und Compliance von Geräten innerhalb der kommunalen IT ergriffen werden können.

5.1
Inventarisierung

Einer der ersten Schritte, um Sichtbarkeit von Geräten im Sinne von Zero-Trust zu unterstützen, ist Inventarisierung. Darunter wird im Folgenden die systematische Erfassung von netzwerkfähigen Geräten innerhalb der kommuneneigenen IT-Landschaft verstanden. Die zu erfassenden Geräte werden im Folgenden auch als *Assets* bezeichnet.

Geräte, die nicht im Besitz der Kommune sind, wie bspw. private Smartphones von Mitarbeitenden, werden im Regelfall nicht im Rahmen der Inventarisierung erfasst, u. a. weil sie nicht unter der Kontrolle der Kommune stehen und deshalb kaum sicherheitsrelevante „Zustandsinformationen“ über sie verfügbar sind bzw. diese nicht verlässlich von den Geräten bezogen werden können. BYOD zur Nutzung von kommuneninternen Ressourcen zu erlauben, stellt mangels Informationen und Kontrollmöglichkeiten ein IT-Sicherheitsrisiko dar. Privatgeräte von Mitarbeitenden sollten deshalb wie Geräte von Dritten behandelt werden, einschließlich Geräte, die aus dem Internet zugreifen. Aus diesen Gründen werden im Folgenden private Endgeräte im Sinne von BYOD nicht weiter behandelt.

5.1.1 IT-Asset-Management

Im IT-Asset-Management (im Folgenden nur Asset-Management) sollen identifizierende Merkmale der kommuneneigenen Geräte, sowohl von Hardware, bspw. MAC-Adressen von verbauten Netzwerkkarten oder Geräteseriennummern, als auch andere „hinzugefügte“ Identitätsdaten wie kryptografische Zertifikate/Schlüssel erfasst und über den gesamten Lebenszyklus des Geräts verwaltet werden. Daneben können ggf. zusätzlich weitere Hardware-Informationen wie Hersteller, Modelltyp, CPU, Festplattengröße, etc. für das jeweilige Asset ergänzt werden. Es sollte deshalb eine entsprechende Software genutzt werden, über die diese Informationen *zentral* verwaltet werden können.

Ziel ist es, mit diesen Informationen jedes aktive Gerät im kommuneninternen Netzwerk identifizieren zu können.

5.1.2 Onboarding

Unter dem Begriff „Onboarding“ wird im Folgenden der Prozess der Registrierung sowie der Konfiguration eines Asset verstanden. Die Registrierung besteht in diesem Zusammenhang aus zwei Aspekten. Zum einen dem verwaltungsmäßigen Aspekt, der den Eintrag ins Asset-Management betrifft, und zum anderen Eintragungen in Komponenten der technischen Infrastruktur, bspw. Zugriffsregeln in Firewalls, MAC-Adressen in DHCP-Server, Computer-Identitäten in Microsoft Active-Directory (AD).

Abhängig von der Art (bspw. Laptop, Desktop-PC, Rack-Server, Netzwerk-Appliance, Netzwerk-Router, Netzwerk-Drucker) oder der Funktion (bspw. Arbeitsplatzrechner, Server, Netzwerk-Management) des jeweiligen Asset, werden hierfür unterschiedliche Einstellungen benötigt. Es sollten deshalb, je nach Art und Funktion des Asset, wiederkehrende Arbeitsschritte für dessen Eingliederung in die kommunale IT-Landschaft in einem Prozess definiert werden und nach Möglichkeit vorgefertigte Profile/Templates für unterschiedliche Konfigurationen erstellt werden. Dies soll einheitliche Ausgangszustände nach Abschluss eines (Teil-)Prozesses sicherstellen, sodass mögliche anschließende Prozesse verlässlich auf diesen Ausgangszuständen aufbauen können.

Für einen Arbeitsplatzrechner könnte ein Prozess dafür festgelegt werden, wie ein Betriebssystem, bspw. Microsoft Windows, auf einen neuen Laptop aufgebracht werden soll. Dies kann kann lokal und manuell über entsprechende Installationsmedien (DVD,USB-Stick,etc.), über Festplatten-Images (mit „vorgefertigter“ Windows-Installation) oder über das Netzwerk mit Hilfe von PXE-Boot erfolgen. Nachdem das Betriebssystem installiert ist, kann in einem anschließenden Prozess eine Software zur *Software-Verteilung* genutzt werden, um die benötigten Fachanwendungen für einen Arbeitsplatzrechner eines Amts auf den Rechner aufzuspielen. Idealerweise kommen hierfür prototypische Anwender-Profile zum Einsatz, welche die benötigten Fachanwendungen amts- oder funktionsspezifisch gruppieren, sodass initial alle Arbeitsplatzrechner eines Fachamts dieselbe Software-Ausstattung bekommen und diese im Inventar der Software-Verteilungssoftware *gerätefein* hinterlegt ist. Zusätzliche, individuell erforderliche Software kann dann im Nachgang ebenfalls über die Software-Verteilung auf dem Gerät installiert werden, sodass auch diese im Inventar vermerkt wird. Im Anschluss kann im Folgeprozess die technische Eingliederung in die IT-Infrastruktur erfolgen, bspw. die Erstellung des Computer-/Maschinenkontos im AD.

Der Beitrag des Onboarding zu Zero-Trust besteht darin, einheitliche Zugriffsregeln in der IT-Infrastruktur für gleichartige Geräte umzusetzen und gleichzeitig über eine zentrale Software-Verteilung einen Überblick über die auf den Endgeräten installierte Software zu ermöglichen, was die Grundlage für das anschließende Monitoring des Gerätezustands ist (s. Abschnitt 5.2 Überprüfung, Monitoring und Kontrolle).

5.1.3 Offboarding

Unter dem Begriff „Offboarding“ wird im Folgenden die Außer-Dienst-Stellung eines Asset verstanden. Gründe hierfür sind bspw. defekte Geräte, die Rückgabe von geleasten Geräten oder wegen Alters ausgemusterte Geräte. Analog zum Onboarding müssen Konfigurationen innerhalb der IT-Landschaft angepasst werden, hier bspw. gerätespezifische Einträge entfernt werden, und im Asset-Management das Gerät als „außer Dienst“ markiert werden, sodass auch dem Gerät möglicherweise zugewiesene Software-Lizenzen zurückgezogen und neu vergeben werden können. Hierdurch soll verhindert werden, dass bspw. ein ausgemustertes, einmal zugelassenes Gerät ohne Zutun des administrativen Personals erneut Zugriff auf interne, kommunale Ressourcen erhält. Durch die Markierung, anstatt der Löschung des Asset-Eintrags, wird sichergestellt, dass ein neues Gerät nicht eine Identität/Kennzeichnung eines alten Geräts erhält. Dies kann wichtig werden, wenn bspw. durch Fehler im Ablauf des Offboarding eines Altgeräts dessen Zugriffsrechte nicht vollständig aus Konfigurationen ausgetragen wurden und dann womöglich das neue Gerät die „alten“ Zugriffsrechte „erben“ würde. Der zweite Schritt im Offboarding besteht in der vollständigen und sicheren Löschung sämtlicher auf dem Gerät befindlicher Daten, bspw. durch Überschreiben des Speichermediums mit zufälligen Daten oder, sofern das Medium nach dem Stand der Technik verschlüsselt ist, durch sicheres Löschen des Entschlüsselungsschlüssels (s. CON.6, [BSI23c]).

5.2
Überprüfung, Monitoring und Kontrolle

Sichtbarkeit von Geräten im kommunalen Netzwerk ist für eine Zero-Trust-Architektur unerlässlich, da nur bekannten und geprüften Geräten der Zugriff auf Netzwerk-Ressourcen erlaubt werden soll. Alle übrigen Geräte müssen ebenfalls erkannt werden, aber nur zu dem Zweck, sie aus dem Netzwerk auszuschließen oder sie wenigstens in einem Subnetz zu isolieren. Um diesen Zustand zu erreichen, müssen sowohl Netzwerk-Ressourcen als auch Endgeräte regelmäßig und automatisch überprüft werden sowie ihr Netzwerkverhalten kontinuierlich überwacht werden, da von jedem Endgerät potenziell ein Cyberangriff ausgehen kann.

Im Folgenden werden Maßnahmen beschrieben, die dazu beitragen sollen, Angriffe im Bestfall zu verhindern oder zumindest deutlich zu erschweren. Indem Geräteinformationen und Geräteverhalten zentral gesammelt und ausgewertet werden, kann die Einhaltung von Sicherheitsrichtlinien zentral überwacht und dezentral auf Endgeräten umgesetzt werden.

5.2.1
Endgeräte-Schutz

Für den Schutz eines Endgeräts bietet sich eine auf dem Endgerät lokal installierte Software an, die oft als *Agent* bezeichnet wird. Der Agent überwacht und protokolliert den Zustand des Endgeräts sowie lokale Aktivitäten, prüft diese im Hinblick auf mögliche Sicherheitsgefährdungen bzw. Verstöße gegen zentral festgelegte Sicherheitsrichtlinien und übermittelt typischerweise regelmäßig ein Gerätezustandsprotokoll an einen zentralen Überwachungsserver. Bei festgestellten Gefährdungen oder Verstößen reagiert der Agent entsprechend, bspw. durch Echtzeitmeldung an den zentralen Überwachungsserver und/oder durch Unterbinden der verdächtigen Aktivität. Diese Art der Geräteüberwachung und -kontrolle wird im Englischen oft als *Endpoint Detection and Response* (EDR) bezeichnet.

Prüfungen des Agenten können die Erkennung von Schadsoftware (*Malware*), Veränderungen an Systemeinstellungen, verdächtige Netzwerkaktivitäten (vom oder zum Endgerät) u. ä. beinhalten sowie das Ergreifen von Gegenmaßnahmen auf erkannte Bedrohungen, wie In-Quarantäne-nehmen von Schadsoftware, Wiederherstellen von Systemeinstellungen und Unterbinden von Netzwerkverbindungen. Entsprechende Reaktionen des EDR-Agenten tragen somit dazu bei, die Sicherheitsrichtlinie (*security policy*) der Kommune unmittelbar auf dem Gerät und mittelbar im Netzwerk durchzusetzen, im Sinne eines Policy-Enforcement-Point (PEP), vgl. Abschnitt 4.

Durch den Einsatz eines EDR-Agenten – in Verbindung mit einem zentralen Überwachungsserver – wird die Sichtbarkeit von Geräten im kommunalen Netzwerk verbessert und zugleich eine kontinuierliche Kontrolle des Endgeräts ermöglicht. Verdächtiges Verhalten eines Endgeräts innerhalb des kommunalen Netzwerks kann so – mittels des Überwachungsserver – schneller identifiziert und ggf. isoliert werden, um das

beobachtete Verhalten zu klären und möglichem Schaden vorzubeugen. Das vom Agenten übermittelte Gerätezustandsprotokoll kann zudem darüber Aufschluss geben, ob und inwieweit das jeweilige Endgerät aktuell die Sicherheitsrichtlinie der Kommune einhält und liefert somit auch eine Beitrag zur Überwachung der Compliance.

Eine auf einem Endgerät installierte Antiviren-Software kann als rudimentäre Variante eines EDR-Agenten verstanden werden, deckt jedoch nur den Bereich der Erkennung von Schadsoftware und der Reaktion darauf ab. Eine auf dem Endgerät aktivierte und zentral verwaltete Firewall kann u. U. ebenfalls einen Teil der EDR-Funktion übernehmen, dadurch dass nur erlaubte ein- und ausgehende Netzwerkverbindungen über entsprechende Regeln konfiguriert werden. Beide Maßnahmen können in Ermangelung einer EDR-Komponente, wie zuvor beschrieben, einen Beitrag zur Sicherheit leisten. Jedoch ist eine zentrale Überwachung in diesen und ähnlichen Ansätzen oft nicht möglich, da die Komponenten lokal und unabhängig voneinander arbeiten und zudem Gerätezustände nicht an eine zentrale Stelle in der Kommune (oder an einen entsprechenden Dienstleister) zur weiteren Auswertung gemeldet werden. Aus diesem Grund werden mögliche Zusammenhänge von lokal festgestellten Ereignissen nur schwer „global“ erkennbar sein und das angestrebte Ziel, hin zu mehr (zentraler) Sichtbarkeit von sicherheitsrelevanten Ereignissen im kommunalen Netzwerk, kaum erreicht werden können.

5.2.2 Schutz mobiler Endgeräte

Grundsätzlich gilt der vorherige Abschnitt sowohl für stationäre (Desktop-PCs, Server) als auch für mobile Endgeräte (Laptops, Smartphones, Tablets, u. a.). Mobile Endgeräte, die mit einem auf Android basierenden Betriebssystem oder mit iOS/iPadOS ausgestattet sind, wie Smartphones oder Tablets, sollten jedoch anders behandelt werden als Laptops – Laptops werden im Folgenden nicht weiter als mobile Endgeräte geführt, sondern mit Desktops und Servern als PCs zusammengefasst.

Mobile Endgeräte lassen sich im Allgemeinen und speziell mit Blick auf den Endgeräteschutz (s. Abschnitt 5.2.1 Endgeräte-Schutz) weniger gut kontrollieren/überwachen als PCs. Dies mag einer der Gründe dafür sein, dass mobilen Endgeräten der direkte Zugriff auf interne Netze und Anwendungen im Regelfall nicht erlaubt wird. Dennoch können sie eine wichtige Rolle spielen, um Außendienstmitarbeitende vor Ort zu unterstützen, bspw. wenn Sachverhalte mit Hilfe eines Smartphones durch Fotos oder Videos dokumentiert und zentral gespeichert werden sollen. Wenn mobile Endgeräte für dienstliche Zwecke genutzt werden, sollten diese mit Hilfe einer Software zum *Mobile-Device-Management* (MDM) verwaltet werden. Ein MDM arbeitet ähnlich wie eine Software zur Software-Verwaltung für PCs. Neben der Verwaltung der auf dem mobilen Endgerät installierten Anwendungen (*Apps*) lassen sich darüber auch Systemeinstellungen verwalten, wie bspw. das Sperren des Geräts nach Inaktivität, das Erzwingen von PIN-Eingaben zum Entsperren, eine VPN-Verbindung zu einem dedizierten Subnetz für mobile Endgeräte konfigurieren, die Nutzung bzw. Installation von Apps einschränken oder das Gerät aus der Ferne sperren und ggf. Daten löschen. Da mobile Endgeräte leicht gestohlen oder verloren gehen können, sollte darüber hinaus eine *unkontrollierte* Nutzung mobiler Endgeräte für dienstliche Zwecke vermieden werden. Spezifische Gefährdungen für mobile Endgeräten sowie Sicherheitsanforderungen für deren Nutzung finden sich bspw. in [BSI23c], Abschnitt SYS.3.2.1.

5.3 Fortgeschrittene Maßnahmen

Die zentrale Kontrolle und Überwachung von Endgeräten sind die wesentlichen Ziele, die mit der Säule Geräte erreicht werden sollen, um letztlich eine einheitliche Umsetzung der kommunalen Sicherheitsrichtlinie (*security policy*) auf allen Geräten zu gewährleisten. Mit anderen Worten sollen Geräte konform (*compliant*) zur Sicherheitsrichtlinie sein, damit sie auf interne kommunale Ressourcen zugreifen dürfen. In diesem Zusammenhang wird oft der Begriff bzw. das Sicherheitskonzept *Comply-to-Connect* (C2C) verwendet. Im Umkehrschluss bedeutet dies, dass Geräte, welche nicht *compliant* sind, idealerweise überhaupt keinen Zugriff auf das kommunale Netzwerk erhalten.

Um Compliance festzustellen, muss notwendigerweise das Zugriff anfragende Gerät inspiziert werden, wofür eine Netzwerkverbindung zum Gerät hergestellt werden muss. Diese Verbindung darf jedoch *nicht* derart sein, dass das Gerät vor Abschluss der Inspektion bereits Zugriff auf „beliebige“ Netzwerkressourcen erhält. Es muss deshalb sichergestellt werden, dass zunächst nur Verbindungen zu Diensten erlaubt werden, die für die Compliance-Prüfung notwendig sind, bspw. die Kommunikation eines EDR-Agenten mit dem Überwachungsserver oder die des Update-Agenten mit dem zentralen Software-Verteilungsserver. Erst nach Abschluss der Prüfung und festgestellter Compliance, wird dem Gerät der Vollzugriff ermöglicht – im Rahmen der ihm zugewiesenen Zugriffsrechte. In Abschnitt 6.4 Fortgeschrittene Maßnahmen wird die Umsetzung von C2C auf Netzwerkebene weiter ausgeführt.

In der Praxis ist es häufig jedoch so, dass ein inventarisiertes Gerät sich in irgendeiner Form identifiziert bzw. authentifiziert und nachdem dies erfolgt ist, das Gerät unmittelbar Vollzugriff im Rahmen des ihm zugewiesenen Subnetzes erhält. Erst wenn diese Verbindung etabliert ist, starten typischerweise Compliance-Prüfungen, wie oben skizziert. Für ein nicht konformes Gerät, das bspw. nicht auf dem aktuellen Versionsstand hinsichtlich seiner Software ist, können dann Updates eingespielt werden. Da das Gerät bereits Vollzugriff hat, ist es allerdings denkbar, dass ein kompromittiertes Gerät die Compliance-Prüfung sabotiert und noch während diese läuft einen Cyberangriff startet oder Informationen dafür sammelt und ausleitet. Ob und inwieweit ein solcher Angriff erfolgreich sein kann, wird maßgeblich von weiteren Maßnahmen beeinflusst, wie bspw. der Netzwerksegmentierung (s. Abschnitt 6.1 Segmentierung) oder ob Maßnahmen zum Endgeräte-Schutz etabliert wurden und wirken (s. Abschnitt 5.2.1 Endgeräte-Schutz).

6
Initiale Umsetzungsschritte in der Säule Netzwerk

Das Netzwerk im Rahmen dieser Studie umfasst sämtliche Kommunikationskanäle, welche für den Datenaustausch zwischen den Endpunkten einer Kommune (Clients, Server, IoT-Geräte, u. s. w.) genutzt werden, sowie die Steuerungsmechanismen, die deren Interaktion und Zugriff regeln. Hierbei unterscheidet man zwischen dem „internen“ Netzwerk, d. h. dem Teil der Netzwerkinfrastruktur, der von der Kommune selbst verwaltet wird, und dem „externen“ Netzwerk, welches das öffentliche Internet bzw. Mobilfunknetz aber auch Netze anderer Behörden sowie Rechenzentrumsnetze externer Dienstleister umfasst.

Der Übergang zwischen dem internen und dem externen Netzwerk wird als Netzwerkperimeter bezeichnet. Traditionell wird im Bereich der Netzwerkssicherheit vor allem die Kommunikation in der sogenannten „Nord-Süd“-Richtung betrachtet, d. h. der Datenaustausch, der zwischen Endpunkten im internen Netzwerk und Endpunkten außerhalb dieses Netzwerks stattfindet. Dementsprechend erfolgen Sicherungs- bzw. Überwachungsmaßnahmen bisher in erste Linie am Netzwerkperimeter, etwa durch den Einsatz von Firewalls oder VPNs. Dies lässt jedoch nur eine relativ grobe Kontrolle der Datenflüsse zu. bspw. erhalten Mitarbeiter per VPN zumeist Zugriff auf das gesamte interne Netzwerk, und Firewalls kontrollieren i. d. R. nur den Netzwerkverkehr am Übergang zwischen dem internen und dem externen Netzwerk.

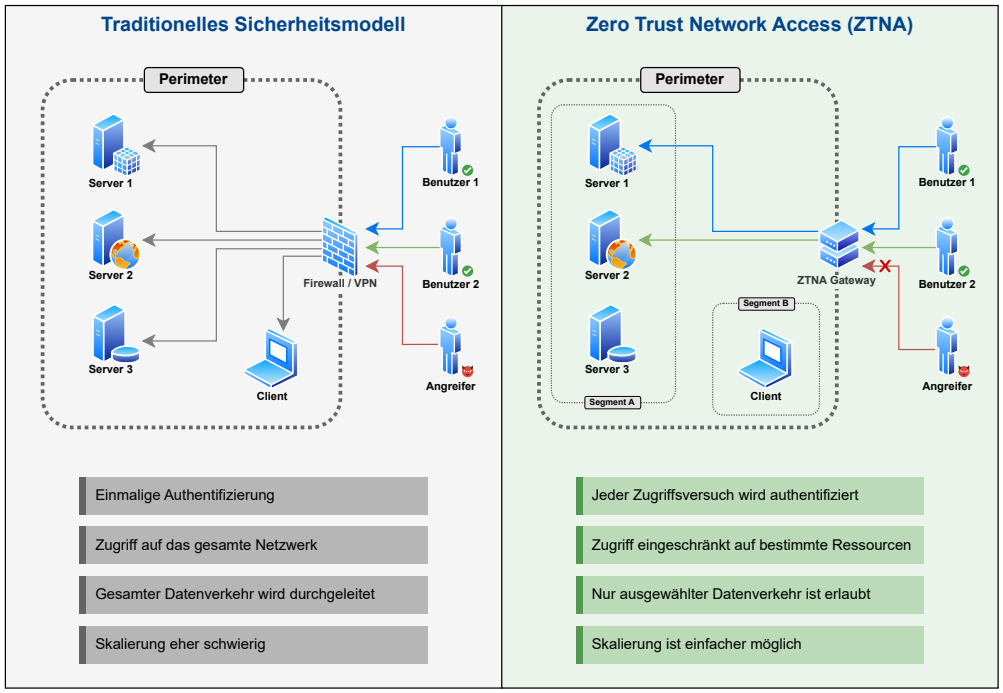

Abb. 6.1:
Traditionelles Sicherheitsmodell vs. Zero Trust Network Access

Im Sinne einer Zero-Trust-Architektur (ZTA) rückt jedoch in zunehmendem Maße auch die Kommunikation in der sogenannten „Ost-West“-Richtung in den Fokus, d. h. die Kommunikation zwischen den verschiedenen Endpunkten *innerhalb* des kommunalen Netzwerks. Dabei wird die klare Trennung zwischen internem und externem Netzwerk bei den Sicherheitsmaßnahmen immer weiter aufgeweicht. Stattdessen setzt eine ZTA vermehrt auf feingranulare und kontextbasierte Netz-Zugriffskontrollen (siehe Abbildung 6.1). Dabei gilt das Prinzip, dass *kein* Rechner, egal ob außerhalb oder innerhalb des internen Netzwerks, implizit als „vertrauenswürdig“ eingestuft wird, sondern Benutzer oder Gerät erst nach einer expliziten Authentifizierung Zugriff auf bestimmte Netzwerk-Ressourcen erhalten. Darüber hinaus erhalten Benutzer stets nur den minimal benötigten Netzwerk-Zugriff, um ihre jeweilige Aufgabe erledigen zu können.

In den folgenden Abschnitten werden Maßnahmen beschrieben, um ein existierendes kommunales Netzwerk schrittweise in eine solche Zero-Trust-Netzwerk-Architektur (ZTNA) zu überführen.

6.1 Segmentierung

Mittels Segmentierung wird das interne Netzwerk in mehrere Unterbereiche (Segmente) aufgeteilt, die weitestgehend gegeneinander abgeschottet sind, und zwischen denen ein Datenaustausch, wenn überhaupt, nur eingeschränkt auf die unbedingt erforderlichen Kommunikationspfade möglich ist. Ziel hierbei ist es den potenziellen Schaden, der durch mögliche Angriffe entstehen kann, auf einzelne Segmente einzudämmen. In einem „flachen“, d. h. nicht segmentierten, Netzwerk könnte der Angreifer bereits nach der Kompromittierung eines einzelnen Geräts im internen Netzwerk von dort aus Zugriff auf viele weitere interne Geräte erlangen und sich somit im ungünstigsten Fall schnell auf das komplette interne Netzwerk ausbreiten. Eine Segmentierung des Netzwerks hingegen sorgt dafür, dass sich der Angreifer nicht mehr „lateral“ von einem kompromittierten Netzwerksegment hin zu weiteren Segmenten fortbewegen kann, wodurch der mögliche Schaden eines erfolgreichen Angriffs erheblich gemindert wird.

6.1.1 Makrosegmentierung

Um eine Segmentierung des internen Netzwerks im Sinne einer ZTNA einzuführen, kann zunächst mit einer initialen *Makrosegmentierung* begonnen werden. Hierbei werden etwa einzelne Ämter bzw. Standorte als eigenen Netzwerk-Segmente voneinander getrennt. Ebenso sollte eine Unterteilung in separate Client- und Server-Netzwerksegmente erfolgen. Für Server, die von außerhalb des internen Netzwerks erreichbar sein müssen, wie z. B. Web- oder Mailserver, wird dabei die Einrichtung einer gesonderten und besonders abgesicherten „demilitarisierten Zone“ (DMZ) empfohlen, wohingegen alle übrigen Server ausschließlich aus dem internen Netzwerk bzw. aus den entsprechenden Client-Zonen heraus erreichbar sein sollten. Dies schafft die Grundlage für eine zukünftige, sukzessive Verfeinerung der Netzwerk-Segmentierung.

Die initiale Segmentierung des Netzwerks kann mit Firewalls und **Virtual Local Area Networks (VLAN)** erreicht werden. Dabei trennt ein VLAN-fähiger Switch die einzelnen Netzwerksegmente „logisch“ voneinander, ohne dass dafür eine „physikalische“ Trennung mittels separater Leitungen bzw. Switches erforderlich ist. Gleichzeitig wird der Datenverkehr zwischen den verschiedenen VLANs sowie nach außen hin an den Übergangspunkten mit einer Firewall absichert und kontrolliert, wobei i. d. R. *Zugriffskontrolllisten (ACL)* zum Einsatz kommen, um die benötigten Datenflüsse zu erlauben und alle anderen Datenflüsse zu unterbinden. Die Zuordnung von Rechnern zu den entsprechenden VLANs erfolgt in dieser Ausbaustufe i. d. R. auf der Ebene der Netzwerk-Ports und muss manuell konfiguriert werden.

Ist eine initiale Makrosegmentierung bereits erfolgt, kann die Netzwerk-Segmentierung weiter verfeinert werden, indem zusätzlich auch innerhalb der einzelnen Ämter bzw. Standorte verschiedene Benutzergruppen in eigene, separate Netzwerk-Segmente isoliert werden, etwa getrennt nach Abteilungen oder Fachbereichen, die jeweils nur Zugriff auf die tatsächlich benötigen Dienste bzw. Netzwerk-Ressourcen erhalten. Die Zuordnung der Clients zu den Netzwerk-Segmenten kann hierbei automatisch über die Geräte-Identität (Abschnitt 4) erfolgen. Darüber hinaus kann auch das Server-Netz weiter in kleinere Segmente unterteilt werden, bspw. auf Basis der Zugehörigkeit der Server zu den jeweiligen Fachanwendungen.

6.1.2 Software Defined Networks (SDN)

Das finale Ziel einer ZTNA in Bezug auf die Netzwerk-Segmentierung stellt die *Mikrosegmentierung* dar, wobei letztendlich jeder einzelne Client und jeder einzelne Server nun als separates Netzwerk-Segment betrachten wird. In dieser Ausbaustufe erfolgt die Regulierung der Netzwerk-Zugriffe nicht mehr auf der Basis statischer Netzwerk-Segmente, sondern dynamisch mit Sicherheitsrichtlinien auf der Ebene einzelner Anwendungen, Benutzer und Geräte. Da einfache technische Ansätze wie VLANs bei fortschreitender Verfeinerung der Netzwerk-Segmentierung jedoch bald an ihre Grenzen geraten, insbesondere im Hinblick auf den Verwaltungsaufwand bei regelmäßigen Änderungen, bietet sich ab einem gewissen Punkt der Einsatz dynamischer Ansätze zur Netzwerk-Verwaltung mittels **Software Defined Networks (SDN)** an.

Ein SDN sieht die Trennung zwischen der *Steuerungsebene*, welche alle Entscheidungen über den Datenverkehr in einem Netzwerk trifft, und der *Datenebene*, welche für die eigentliche Weiterleitung der Daten in dem Netzwerk zuständig ist, vor. Steuerungsentscheidungen werden daher nicht mehr verteilt auf den einzelnen Netzwerkinfrastruktur-Komponenten (Switches, Router, etc.) getroffen, sondern zentral auf dem SDN-Controller. Um die Entscheidungen des SDN-Controllers an die SDN-fähigen Netzwerkinfrastruktur-Komponenten zu kommunizieren, werden im Rahmen von SDN standardisierte Protokolle wie *OpenFlow* eingesetzt. Hierdurch wird das Netzwerk gewissermaßen „programmierbar“ und kann dadurch sehr viel einfacher jederzeit dynamisch an neue Anforderungen angepasst werden.

Somit bilden SDNs eine wichtige technische Grundlage zur Umsetzung einer ZTNA, da mit ihrer Hilfe eine zentralisierte Datenflusskontrolle auf der Netzwerk-Ebene sowie eine dynamische Segmentierung des Netzwerks bis hin zur Mikrosegmentierung erst sinnvoll möglich bzw. handhabbar wird. Im Sinne einer Zero-Trust-Architektur stellt der SDN-Controller den Policy Decision Point (PDP) dar, und die SDN-fähigen Netzwerkinfrastruktur-Komponenten bilden die Policy Enforcement Points (PEP). Zusätzlich können in einem SDN Netzwerk-Monitoring-Werkzeuge als Policy Information Point (PIP) eingebunden werden.

6.1.3 Software Defined Perimeters (SDP)

Eine weitere Möglichkeit Mikrosegmentierung zu erreichen ist mit **Software Defined Perimeters (SDP)**[1] gegeben. Dabei handelt es sich um ein Overlay-Netzwerk, das den Zugriff auf Netzwerk-Ressourcen in einem potenziell unsicheren Netzwerk schützt. Die grundlegende Idee besteht darin, dass alle relevanten Netzwerk-Ressourcen vor unautorisierten Teilnehmern „versteckt“ werden. Der Zugriff auf eine bestimmte Ressource durch einen bestimmten Teilnehmer wird erst dann freigegeben, wenn die Identität und die Vertrauenswürdigkeit dieses Teilnehmers bestätigt wurden, und wenn darüber hinaus sichergestellt wurde, dass der betreffende Teilnehmer dazu berechtigt ist, mit dem jeweiligen Ziel zu kommunizieren.

Der Zugriff auf einen „versteckten“ Dienst erfolgt bei SDP immer über den entsprechenden *Accepting-Host (AH)*, welcher direkt in dem jeweiligen Dienst bzw. Server integriert oder als separates, vorgeschaltetes Gateway ausgeführt sein kann. Bevor ein bestimmter *Initiating-Host (IH)*, d. h. ein Benutzer oder ein Gerät, auf einen bestimmten Dienst resp. AH zugreifen kann, muss dieser sich immer zunächst beim zentralen SDP-Controller authentifizieren. Der SDP-Controller liefert dem IH daraufhin eine Liste der für ihn freigegebenen AHs und instruiert gleichzeitig diese AHs eingehende Verbindungen von dem authorisierten IH zu akzeptieren. Der IH kann schließlich eine gesicherte Verbindung zu dem AH mittels *SPA (Single Packet Authentication)* und unter Verwendung von *mTLS*, d. h. wechselseitig authentifiziertem TLS, herstellen.

Bei SPA handelt es sich um eine Weiterentwicklung der „Port Knocking“ Technik, welche die gesamte Authentifizierungs-Information in einem einzigen IP-Datenpaket kapselt. SPA wird insbesondere im Kontext von SDP dazu verwendet, um „versteckte“ Netzwerkdienste gegen Port-Scanning und Denial-of-Service (DoS) Angriffe abzusichern. Dabei gilt, dass die Firewall am AH grundsätzlich *alle* eingehenden Pakete sofort verwirft, sodass keine „offenen“ Ports sichtbar sind. Gleichzeitig überwacht der SPA-Dienst fortlaufend die eingehenden Pakete. Erst wenn ein SPA-Paket mit der gültigen Authentifizierung eines berechtigten IH erkannt wird, richtet der SPA-Dienst eine *temporäre* Firewall-Ausnahmeregel für den betreffenden IH ein, um diesem eingehende Netzwerk-Verbindungen zum AH zu ermöglichen.

1 https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2

6.2 Intrusion Detection & Prevention (IDS/IPS)

Für eine ZTNA stellt der Einsatz eines Intrusion-Detection-Systems (IDS) oder Intrusion-Prevention-Systems (IPS) einen zentralen Baustein dar. Ein IDS überwacht kontinuierlich den Netzwerkverkehr, um Anomalien, d. h. signifikante Abweichungen vom normalen Verhalten, zu erkennen. Solche Anomalien, etwa ein auffällig hoher Datenverkehr von einem bestimmten Gerät oder eine auffällig hohe Anzahl von Verbindungsversuchen zu verschiedenen Ports innerhalb kurzer Zeit, können auf einen laufenden Angriff im Netzwerk hindeuten. Indem ein IDS derartige Anomalien an die Netzwerkadministratoren meldet, können diese zeitnah die Ursache analysieren und ggf. *manuell* geeignete Gegenmaßnahmen ergreifen. Ein IPS ist darüber hinaus dazu in der Lage *automatisch* Gegenmaßnahmen einzuleiten, etwa indem „verdächtige“ Geräte oder Netzwerksegmente sofort vom restlichen Netzwerk isoliert werden. Somit kann ein IPS mögliche Angriffe noch schneller eindämmen als dies mit einem reinen IDS möglich wäre, gleichzeitig erhöht sich dadurch allerdings auch die Gefahr von Netzwerkausfällen durch Fehlalarme.

6.2.1 Statische und dynamische Filterregeln

In einem ersten Schritt kann eine Kommune ein IDS oder IPS einführen, um den Netzwerkverkehr an den neuralgischen Netzübergängen nach *statischen* Regeln zu filtern und so bekannte Bedrohungen zu erkennen. Insbesondere wenn in der Kommune bereits erste Maßnahmen zur Netzwerk-Segmentierung umgesetzt wurden, kann die Überwachung des Netzwerkverkehrs mittels IDS/IPS nicht nur am Netzwerkperimeter, sondern zusätzlich auch an den Übergängen zwischen den verschiedenen Netzwerksegmenten erfolgen, um ein vollständigeres Bild über die Datenflüsse im Netzwerk zu erhalten. Auf dieser Grundlage können später ggf. fortgeschrittene IDS/IPS Lösungen ergänzt werden.

Zu einer fortgeschrittenen IDS/IPS-Lösung gehören neben der Paketfilterung an den Übergangspunkten zusätzliche Schutzmaßnahmen, die in Form sogenannter „Agenten“ den Datenverkehr auch direkt auf den einzelnen Endgeräten bzw. Servern überwachen. Dabei kann u. a. Deep Packet Inspection (DPI) genutzt werden, um die Datenpakete bis hinab zur Applikationsschicht zu überwachen, anstatt lediglich deren Header-Daten zu analysieren. Die *dynamisch* konfigurierten Filterregeln basieren in dieser Ausbaustufe stets auf dem aktuell autorisierten Kommunikationsbedarf. Somit ist es möglich, bspw. mit Hilfe von zeit- oder sitzungsbasierten Netzwerk-Filtern, auch „komplexe“ Bedrohungen zu erkennen.

6.2.2 Nutzung von Machine-Learning-Methoden

Ansätze aus dem Bereich des „Machine Learning“ (ML) können insbesondere im Zusammenhang mit SDN zur verhaltensbasierten Erkennung von Bedrohungen im Netzwerk eingesetzt werden. Auf diese Weise können bisher unbekannte Bedrohungen erkannt werden, welche mit den „klassischen“ Methoden kaum zu erfassen sind. Das ML-Modul

dockt an das Management-Interface des SDN-Controllers an und nutzt sowohl dessen Monitoring-Fähigkeiten, um Informationen über sämtliche Datenflüsse im Netzwerk in Echtzeit zu erhalten, als auch die Möglichkeit, dynamisch neue Datenflussregeln anzulegen bzw. jederzeit existierende Datenflussregeln wieder deaktivieren zu können.

Bei diesem Ansatz wird zwischen der „Trainingsphase“ und der „Durchsetzungsphase“ unterschieden: In der *Trainingsphase* analysiert das ML-Modul das Verhalten des Netzwerks unter normalen Bedingungen, d. h. wenn keine Angriffe vorliegen. Hierbei erlernt das ML-Modul die minimal benötigten Netzwerk-Zugriffe, die für einen normalen Betrieb erforderlich sind, und erlernt die Datenflussregeln, welche die erforderlichen Datenflüsse im Netzwerk ermöglichen. In der *Durchsetzungsphase* überwacht das ML-Modul dann kontinuierlich die Datenflüsse im Netzwerk. Bei neuen Verbindungsanfragen entscheidet das ML-Modul jeweils anhand des zuvor erlernten Modells, ob dieser Netzwerk-Zugriff erlaubt werden soll, und aktiviert ggf. die dafür notwendigen Datenflussregeln im SDN-Controller. Für alle aktiven Datenflüsse werden darüber hinaus die Echtzeit-Datenflussstatistiken überwacht. Bei signifikanten Abweichungen vom zuvor erlernten Kommunikationsverhalten kann das ML-Modul den „verdächtigen“ Datenfluss sofort unterbrechen, indem die entsprechende Datenflussregel im SDN-Controller wieder deaktiviert wird.

6.3 Netzwerkzugangskontrolle

Ein weiterer wesentlicher Aspekt einer ZTNA ist die Netzwerkzugangskontrolle, auch **Network Access Control (NAC)** genannt. Das Ziel von NAC besteht darin, dass ausschließlich berechtigte Geräte nach einer erfolgreichen Authentifizierung Zugriff auf das Netzwerk erhalten, wohingegen unbekannte bzw. (noch) nicht authentifizierte Geräte grundsätzlich zu blockieren sind. Außerdem sollte in einer ZTNA der Netzwerk-Zugriff, den ein bestimmtes Gerät oder ein bestimmter Benutzer erhält, so weit wie möglich auf die tatsächlich benötigten Netzwerk-Ressourcen eingeschränkt werden. Dies gilt sowohl für lokale Geräte, die drahtgebunden per Ethernet oder drahtlos per WLAN auf das Netzwerk zugreifen möchten, als auch für entfernte Geräte, die sich bspw. per VPN oder SSH-Tunnel mit dem Netzwerk zu verbinden versuchen.

6.3.1 Lokale Zugangskontrolle

Um den Netzwerk-Zugang lokaler Geräte einzuschränken und zu kontrollieren, kann eine Kommune als ersten Schritt die obligatorische Authentifizierung mittels des Standards **IEEE 802.1X** einführen. Dieser heute weithin gebräuchliche Standard beschreibt Methoden zur Authentifizierung von Geräten in Netzwerken. Kommt IEEE 802.1X zum Einsatz, muss sich jedes Gerät, welches sich mit dem Netzwerk verbinden möchte – hier „Supplicant“ (Bittsteller) genannt – immer zunächst gegenüber dem jeweiligen „Authenticator“ authentifizieren, der den Zugang zum Netzwerk schützt. Die Rolle des Authenticators wird dabei typischerweise von einem 802.1X-fähigen Switch bzw. Router oder von einem entsprechenden WLAN-Access-Point wahrgenommen. Die Authentifizierung der Geräte kann u. a. auf Basis von Zertifikaten erfolgen, welche typischerweise bei der Ersteinrichtung auf

allen berechtigten Geräten installiert werden. Zur Validierung der Zugangsdaten bzw. Zertifikate greift der Authenticator auf den zentralen Authentifizierungs-Server der Kommune zurück, der etwa in Form eines **RADIUS** (Remote Authentication Dial-In User Service) Servers umgesetzt sein kann, und der verschiedene Backends wie z. B. LDAP (Lightweight Directory Access Protocol) oder Microsoft Active-Directory (AD) nutzen kann. Darüber hinaus kann ein Gerät nach erfolgreicher 802.1X-Authentifizierung seiner Identität entsprechend dem passenden VLAN bzw. Netzwerk-Segment zugewiesen werden, um dessen Zugang geeignet einzuschränken.

Falls in einer Kommune noch Geräte zum Einsatz kommen (müssen), die eine moderne Authentifizierung mittels IEEE 802.1X *nicht* unterstützen, kann alternativ MAC Authentication Bypass (MAB) genutzt werden, um solchen Geräten dennoch einen kontrollierten Zugang zum Netzwerk zu ermöglichen. Dabei verwirft der MAB-fähige Switch zunächst alle Netzwerkpakete, die an dem betreffenden Port von dem angeschlossenen Gerät eingehen, extrahiert jedoch die MAC-Adresse aus dem ersten empfangenen Paket. Sobald die MAC-Adresse ermittelt wurde, authentifiziert der Switch das Gerät automatisch beim zentralen Authentifizierungs-Server und gibt ggf. den Zugriff auf das Netzwerk bzw. das festgelegte VLAN frei. Es ist zu beachten, dass MAB nur eingeschränkte Authentifizierungs-Entscheidungen ermöglicht, da lediglich die MAC-Adresse des Geräts zur Verfügung steht. Es handelt sich bei MAB auch ausdrücklich *nicht* um eine sichere Authentifizierung, denn MAC-Adressen können leicht, bspw. mittels *Spoofing*, manipuliert werden. Deshalb sollten derart authentifizierte Geräte höchstens einen eingeschränkten Netzwerk-Zugriff erhalten.

6.3.2 Sicherer Fernzugriff

Sofern die Kommune ihren Mitarbeitern auch aus dem externen Netzwerk einen Zugang zu internen Netzwerk-Ressourcen, wie z. B. Anwendungs-Servern, ermöglicht – etwa zwecks Home-Office oder für Außendienst-Mitarbeiter – müssen diese Zugänge ebenfalls im Sinne einer ZTNA abgesichert werden. Werden die Zugänge für Mitarbeiter aus dem externen Netzwerk noch mit Hilfe eines klassischen VPN (virtuelles privates Netzwerk) bereitgestellt, müssen diese VPN-Zugänge für die betreffenden Benutzer bzw. Geräte mit individuellen Zugangsdaten oder vorzugsweise durch Anbindung des zentralen Authentifizierungs-Servers abgesichert werden. Gleichzeitig sollten speziell angepasste VPN-Profile zum Einsatz kommen, um den Netzwerk-Zugang per VPN so weit wie möglich auf die von den Benutzern minimal benötigten Netzwerk-Ressourcen einzugrenzen, anstatt den VPN-Benutzern uneingeschränkten Zugriff zu gestatten. Auch hier zahlt sich eine geeignete Segmentierung des internen Netzwerks aus.

Eine Alternative zu Netzwerk-Zugängen per VPN oder entsprechenden Technologien stellt die Nutzung eines „Jump-Server“ bzw. „Remote-Desktop-Gateway“ dar. Dabei greifen die externen Benutzer per Remote Desktop Protocol (RDP) bzw. über ein entsprechendes Web-Interface auf einen speziellen Jump-Server zu, welcher *indirekt* und erst nach einer geeigneten Authentifizierung den Zugriff auf die benötigten internen Dienste über eine virtuelle Desktop-Umgebung bereitstellt. Die Verbindung zum Jump-Server sollte hierbei unbedingt mittels TLS-Verschlüsselung abgesichert werden. Bei diesem Ansatz müssen lediglich die speziell zu diesem Zweck bereitgestellten Jump-Server für einen Zugriff aus

dem externen Netzwerk freigegeben werden, während direkte Zugänge zum internen Netzwerk durch externe Benutzer vollständig vermieden werden. Darüber hinaus können die Interaktionsmöglichkeiten mit den internen Diensten, die den externen Benutzer über den Remote-Desktop zur Verfügung stehen, stark eingeschränkt werden (etwa durch die Deaktivierung von „Copy & Paste“), wodurch die Angriffsoberfläche weiter reduziert wird.

Unabhängig von der Umsetzung des Fernzugriffs sollten alle Benutzer zuvor mittels einer Mehr-Faktor-Authentifizierung (MFA) sicher authentifziert werden.

6.4 Fortgeschrittene Maßnahmen

Comply-to-Connect (C2C)

Comply-to-Connect (C2C) ist ein Sicherheitskonzept, das die Zero-Trust-Prinzipien im Netzwerk durchsetzt, indem sich ausschließlich vertrauenswürdige Geräte, welche alle notwendigen Sicherheitsrichtlinien erfüllen, mit dem Netzwerk verbinden dürfen. C2C wurde vom US-Verteidigungsministerium (Department of Defense, DoD) gefördert und umfasst verschiedene Aspekte, welche i. d. R. durch Kombination verschiedener Produkte von unterschiedlichen Herstellern umgesetzt werden.

Das Grundprinzip von C2C besteht darin, dass jedes Gerät, das versucht sich mit dem Netzwerk zu verbinden, zunächst einmal *erkannt* und sowohl anhand verschiedener Merkmale des Geräts selbst (Hersteller, Betriebssystem, etc.) als auch anhand der Eigenschaften des Netzwerkzugangs (z. B. dem zum Zugang genutzter Port) *klassifiziert* wird. Auf diese Weise können die verbundenen Geräte in einem Netzwerk sichtbar gemacht und verschiedenen Gruppen bzw. Kategorien zugeordnet werden. Nach der Erkennung bzw. Klassifizierung müssen sich alle erkannten Geräte, die Zugang zum Netzwerk erhalten möchten, zwingend *authentifizieren*. Damit wird sichergestellt, dass ausschließlich die in der Organisation bekannten Geräte bzw. Benutzer einen Zugang zum Netzwerk erhalten. Abhängig von der Geräte-Klasse und der Benutzer-Rolle wird dann ggf. der Zugriff auf die entsprechenden Netzwerk-Segmente *autorisiert*. Die Authentifizierung bzw. Autorisierung erfolgt hierbei z. B. mittels IEEE 802.1X oder auch mittels MAB.

Darüber hinaus werden bei C2C alle Geräte hinsichtlich ihrer *Regelkonformität (Compliance)* überprüft, d. h. es wird bei jedem Verbindungsversuch sichergestellt, dass das Gerät aktuell den festgelegten Sicherheitsrichtlinien entspricht, bevor der Zugriff auf das interne Netzwerk tatsächlich freigegeben wird – etwa indem die Geräte nach der initialen Authentifizierung so lange in einem eingeschränkten „Quarantäne“-Netzwerkbereich isoliert werden, bis alle notwendigen Sicherheitsprüfungen erfolgreich abgeschlossen sind. Im Rahmen dieser Prüfungen kann u. a. ermittelt werden, ob auf dem Gerät wichtige Updates/Patches fehlen oder ob dort unautorisierte Software vorhanden ist. Die Überprüfung erfolgt typischerweise durch einen „Agenten“ der eingesetzten Endgerätesicherheits-Lösung (Endpoint Security), welcher als notwendige Voraussetzung für den Netzwerk-Zugang auf dem Gerät aktiv sein muss.

Auch bereits mit dem internen Netzwerk verbundene Geräte werden im Rahmen von C2C *fortlaufend überwacht*, um sicherzustellen, dass diese sich weiterhin in einem regelkonformen Zustand befinden. Wird ein Regelverstoß festgestellt, können entsprechende Gegenmaßnahmen (semi-)automatisch eingeleitet werden. So kann bspw. der Netzwerk-Zugriff eines Gerätes temporär eingeschränkt werden, wenn festgestellt wird, dass ein erforderlicher Schwachstellen-Scan zu lange nicht durchgeführt wurde oder dass von dem Gerät eine „verdächtige“ Netzwerkaktivität ausgeht, die auf einen möglichen Angrifft hindeutet (vgl. Abschnitt 5.3).

7
Initiale Umsetzungsschritte in der Säule Workload & Apps

Aus Sicht der meisten Nutzenden stellen Anwendungen (*apps*) das Herzstück ihrer täglichen Arbeit dar. Anwendungen, einschließlich Fachanwendungen der Kommune, laufen heutzutage nicht nur lokal auf den PCs der Nutzenden, sondern nutzen auch Dienste im Netzwerk oder sind sogar nur noch Clients, die die Arbeit (*workload*) gänzlich an Server- oder Cloud-Dienste auslagern. Mit anderen Worten sind Anwendungen oft Teil einer vernetzten Anwendungsinfrastruktur, in der Anwendungen über Netzwerke zugänglich gemacht und durch ein Client-Server-Modell umgesetzt werden. In den vorangegangenen Abschnitten wurde die Absicherung und die Verwaltung von Endgeräten betrachtet (s. Abschnitt 5 Initiale Umsetzungsschritte in der Säule Geräte), auf denen die Client-Komponente der Anwendung letztlich laufen, sowie die Absicherung von Computer-Netzwerken (s. Abschnitt 6 Initiale Umsetzungsschritte in der Säule Netzwerk), über die Clients mit ihren Servern kommunizieren. In der Säule „Workload & Apps“ geht es nunmehr um die Verwaltung von Anwendungen und um die Absicherung von Server-Komponenten.

In der Vergangenheit wurde die Absicherung von Server-Anwendungen, im Folgenden auch Dienste genannt, oft alleine durch Zugangsbeschränkungen des Netzwerks umgesetzt, in dem der Server logisch verortet ist. Im Sinne von Zero-Trust soll dieser grobe Schutz gewissermaßen näher an die Server-Anwendung heranrücken. Darunter ist zu verstehen, dass die Anwendung nicht nur durch ihre Netzwerkumgebung abgesichert ist, sondern idealerweise selbst Sicherheitsvorkehrungen trifft oder zusätzliche Sicherheitsmaßnahmen speziell für die Anwendung umgesetzt werden.

7.1
Software-Verwaltung und Software-Sicherheit

Software (inkl. Firmware) wird im Laufe ihres Lebenszykluses auf Grund von Programmfehlern oder Schwachstellen i. d. R. mehrfach vom Hersteller aktualisiert. Um einen einheitlichen Versionsstand einer gegebenen Software innerhalb einer Kommune zu realisieren, ist es notwendig, dass alle Geräte, auf denen die Software aktuell installiert ist, nach Möglichkeit die aktuellste Version erhalten. Dies erfordert zum einen Wissen darüber, auf welchen Geräten die betroffene Software installiert ist und zum anderen einen Prozess, in dem geregelt ist, wann und wie die aktualisierte Version der Software (das *Update*) auf betroffene Rechner aufgespielt werden sollen.

7.1.1
Inventarisierung und Verteilung von Software

Ein Software-Inventar stellt eine Wissensbasis dar, die sämtliche in der kommunalen Infrastruktur genutzte Software bzw. alle Anwendungen erfasst, einschließlich ihrer Versionen und ggf. weiterer Informationen wie bspw. vorhandene Software-Lizenzen. Für den Aufbau bzw. die Verwaltung eines Software-Inventars wird darüber hinaus Wissen benötigt, auf welchen Geräten die Software installiert ist. Dieses Wissen kann manuell erfasst oder mittels Software-Agenten zusammengetragen werden, die lokal auf Endgeräten

installiert sind – ähnlich wie EDR-Agenten, die auf Endgeräten zu deren Schutz installiert sind (s. Abschnitt 5.2.1 Endgeräte-Schutz). Ein Software-Agent katalogisiert die auf einem Endgerät bereits installierte Software (einschließlich Versionsnummern) und meldet diese an ein zentrales Software-Inventar zurück. Am Ende entsteht auf diese Weise ein vollständiges Lagebild über die in der Kommune eingesetzte Software. Dies erlaubt es, an zentraler Stelle eine globale Sicht der auf kommunalen Endgeräten installierten Software zu erhalten und zugleich die Information, ob diese auf dem aktuellsten Versionsstand ist.

Die Nutzung von Software-Agenten ist vorteilhaft, da sie die regelmäßige Aktualisierung der erfassten Informationen zum Gerätezustand erleichtert und automatisiert erfolgen kann. Dies ist umso wichtiger, wenn sich erfasste Informationen häufig ändern, wie bspw. nach Software-Updates, und eine große Anzahl an Endgeräten verwaltet wird.

Server-Software für Netzwerk-Dienste und andere Netzwerk-Ressourcen sollten, ähnlich wie Anwendungen auf Nutzer-Endgeräten, zentral verwaltet werden. Die Fehlerfreiheit und Betriebssicherheit von Server-Software spielt eine noch größere Rolle als bei Software auf Endgeräten, da sie Schnittstellen zum Zugriff auf Verarbeitungskapazitäten sowie Daten bereitstellt und deshalb – prinzipbedingt – eine größere Angriffsfläche bietet als lokale Anwendungen. Schwachstellen in Server-Software können deshalb einen erfolgreichen Cyberangriff begünstigen oder gar erst ermöglichen. Aus diesem Grund gilt es, ähnlich wie bei Software auf Endgeräten von Nutzern, diese auf dem aktuellen Sicherheitsstand zu halten.

7.1.2 Wartung von Software

Aus IT-Sicherheitssicht ist, neben dem Versionsstand und der Information, ob der Hersteller aktuell ein Update seiner Software bereitstellt, wichtig zu wissen, ob installierte Software eine Schwachstelle enthält und wie hoch deren Gefährdungspotenzial für die kommunale IT-Infrastruktur einzuschätzen ist. Wie genau das Gefährdungspotenzial eines Geräts bestimmt werden kann, würde den Rahmen der Betrachtung hier sprengen, da hierfür eine Vielzahl von Faktoren berücksichtigt werden können, die i. d. R. auch von den lokalen Begebenheiten abhängen. Als mögliche Faktoren zur Bestimmung des Gefährdungspotenzials sollen deshalb hier nur einige Beispiele genannt werden, wie die verfügbaren Informationen zu Schwachstellen (bspw. über CVE[1]) und deren Schwere (bspw. über CVSS[2]) von auf dem Gerät installierten Soft- oder Firmware, die Verfügbarkeit von Patches und der Zeithorizont für deren Installation sowie die Kritikalität der Verfügbarkeit des Geräts bzw. der darauf laufenden Software für die Kommune. Die Einschätzung des Gefährdungspotenzials kann (teil-)automatisiert durch entsprechende Software erfolgen oder nach menschlichem Ermessen – einschlägige Erfahrung vorausgesetzt. Maßnahmen zur Verbesserung des IT-Sicherheitszustands sollten entsprechend des Gefährdungspotenzials priorisiert und umgesetzt werden. Grundsätzlich birgt Software, die auf externe Ressourcen/Diensten zugreift, wie bspw. ein Web-Browser, ein E-Mail-Client oder eine Cloud-Anwendung, bzw. selbst einen Dienst umsetzt, ein höheres Gefährdungspotenzial als Software, die ausschließlich als nicht vernetzte, lokale

1 https://www.cve.org/

2 https://www.first.org/cvss/

Anwendung auf dem Gerät ausgeführt wird und sollte deshalb bei der Behebung von Schwachstellen i. d. R. priorisiert werden. Einige am Markt verfügbare Lösungen zur Software-Verteilung bzw. zum Software-Management liefern neben der Information zur Verfügbarkeit von Updates auch Hinweise im Hinblick auf Schwachstellen der Software, wie bspw. den CVE-Eintrag und/oder den CVSS-Score.

Priorisierung. Eine Priorisierung kann notwendig sein, wenn verschiedene Anwendungen Updates erhalten haben, die nicht alle gleichzeitig aufgespielt werden können oder sollen. Zum Beispiel könnten generell Sicherheitsupdates (*Patches*) vor Funktionsupdates eingespielt werden oder Patches nur dann priorisiert werden, wenn diese eine „schwerwiegende“ Schwachstelle beheben oder organisationskritische Anwendungen immer zuerst Updates erhalten. Die Festlegung von Prioritäten kann auch situativ erfolgen, d. h. dass von der üblichen Abfolge in begründeten Einzelfällen abgewichen werden kann. Jedoch sollte dies die Ausnahme sein, da ansonsten der Update-Prozess keinen einheitlichen Ablauf gewährleisten kann und Optimierungen in einem sich ständig ändernden Prozess schwierig umzusetzen sind. In Fällen, wo die Ausnahme zur Regel wird, sollte der Update-Prozess überarbeitet werden, um die häufigsten Ausnahmen, die sich in der Praxis bewährt haben, in den Prozess zu integrieren. In jedem Fall, sollte eine Priorisierung im Update-Prozess beschrieben werden, um einen geordneten Ablauf des Update-Prozesses auch in Zeiten erhöhter Arbeitslast sicherzustellen.

Server-Software. Im Unterschied zum Update von Software auf Endgeräten kann das Abschalten einer Server-Anwendung für Wartungszwecke eine Vielzahl von Nutzern betreffen und somit Betriebsabläufe in größerem Umfang stören, da neben unmittelbar betroffenen Primärnutzenden auch Sekundärnutzende betroffen sein können, die auf Zuarbeiten der Primärnutzenden angewiesen sind. Gleichzeitig muss aber der Schutz einer Server-Anwendung gewährleistet werden, da er zum einen durch die notwendige Erreichbarkeit über Netzwerke eine größere Angriffsoberfläche besitzt als lokale Anwendungen oder Client-Software und zum anderen würde ein erfolgreicher Angriff Nutzende ähnlich treffen und womöglich eine längere Ausfallzeit nach sich ziehen als eine Wartung.

Für die Wartung der Server-Anwendungen sollten deshalb regelmäßige Zeitfenster eingeplant werden, die ggf. außerhalb der üblichen Service-/Dienstzeiten der Kommune liegen, abhängig von der Kritikalität der Anwendung für die Aufrechterhaltung des Betriebs, um eine längere Störung des Betriebs zu vermeiden, gerade wenn Updates länger dauern können oder unvorhergesehene Seiteneffekte haben könnten, bspw. wenn von der Server-Anwendung weitere Dienste abhängen.

7.1.3 Lieferkettensicherheit

Praktisch jede Anwendung nutzt heutzutage Programmbibliotheken, sei es direkt oder über eine Laufzeitumgebung (*runtime environment*) wie Java oder .NET. Für eine Server-Anwendung spielen diese Bibliotheken aus Sicherheitssicht eine bedeutende Rolle, da sie Teil der Lieferkette der Server-Anwendung sind. Auch wenn der Anwendungshersteller die Bibliotheken nicht selbst entwickelt, sind sie doch Teil seiner Entwicklung und können Schwachstellen oder Schadcode enthalten, bspw. wenn veraltete Bibliotheksversionen

verwendet oder die Bibliotheken aus kompromittierten Quellen bezogen wurden. Ein bekanntes Beispiel für eine Schwachstelle in einer verwundbaren Java-Bibliothek ist „Log4Shell“ [BSI21], die in der Bibliothek Log4J zu finden war und häufig in der Protokollierung von auf Java basierenden Server-Anwendungen genutzt wird.

Anwendungshersteller stellen normalerweise Updates im Hinblick auf die Funktionalität oder die Sicherheit ihrer Anwendungen über den gesamten Software-Lebenszyklus hinweg bereit. Dies schließt jedoch nicht notwendigerweise (Sicherheits-)Updates der durch die Anwendung verwendeten Bibliotheken bzw. Laufzeitumgebungen ein, etwa weil der Hersteller diese nur im Hinblick auf funktionale Änderungen überwacht, die unmittelbare Folgen für die eigene Software haben.

Bibliotheken. Stützt sich eine Anwendung ausschließlich auf Bibliotheken, die vom Betriebssystemhersteller bereitgestellt werden (verbreitet etwa auf Linux-basierten Systemen), sollten diese im Rahmen der regelmäßigen Betriebssystem-Updates auf dem aktuellen Sicherheitsstand gehalten werden. Andere Bibliotheken von Dritten sollten grundsätzlich vom Hersteller im Hinblick auf Schwachstellen überwacht werden und im Rahmen von Anwendungs-Updates aktualisiert werden, ggf. auch als alleiniges Update für eine eingebundene Bibliothek mit einer Schwachstelle.

Laufzeitumgebungen. Bei Laufzeitumgebungen kann es sein, dass der Hersteller auf eine bei Endnutzenden installierte, systemweit verfügbare Version zurückgreift. Es kann sogar sein, dass die Laufzeitumgebung initial vom Anwendungshersteller bei der Erstinstallation der Anwendung installiert wurde. Wartet oder prüft der Anwendungshersteller die von seiner Software benötigte Laufzeitumgebung auf dem System seines Kunden nicht, fällt diese Aufgabe dem Kunden zu. Laufzeitumgebungen sollten deshalb genauso überwacht und aktualisiert wie andere Softwarekomponenten, da darin vorhandene Schwachstellen ähnlich ausgenutzt werden können, wie solche in der „eigentlichen“ Anwendung. Insbesondere bei Server-Anwendungen ist dies ein großes Problem, da Angreifer durch präparierte Server-Anfragen u. U. eine solche Schwachstelle aus der Ferne ausnutzen könnten.

7.2 Zugriffskontrolle bei Netzwerk-Diensten

Für die Absicherung von Diensten, die über ein Computer-Netzwerk zur Verfügung gestellt werden, hängen die Handlungsspielräume der Kommune davon ab, ob der Dienst im Eigenbetrieb (intern) zur Verfügung gestellt wird oder durch einen externen Anbieter, bspw. durch einen kommunalen Dienstleister oder einen Cloud-Dienstanbieter, einschließlich Software-as-a-Service (SaaS). Ist der Dienst von Haus aus mit einem Zugriffsschutz ausgestattet, ist zunächst eine Basisabsicherung gegeben, vorausgesetzt dass diese dem Stand der Sicherheitstechnik entspricht, vgl. Abschnitt 4.1 Identitäten und Authentifizierung. Im Sinne des Ziels einer Zero-Trust-Architektur, eine einheitliche und zentral gesteuerte Zugriffsverwaltung zu etablieren, ist weiterhin zu unterscheiden, ob ein Dienst Schnittstellen

anbietet, die es der Kommune erlaubt ihre eigene Lösung zur Identitäts- und Zugriffsverwaltung (*Identity and Access Management*, IAM) einzusetzen, bspw. mittels Single-Sign-On (SSO), oder ob die Anwendung ein eigenes oder womöglich auch kein IAM bietet.

7.2.1 Agent-Gateway

Für die Absicherung von Netzwerk-Ressourcen und -diensten beschreibt das US-amerikanische National Institute of Standards and Technology (NIST) in seiner Veröffentlichung zu Zero-Trust-Architekturen [NIS20] verschiedene Umsetzungsmodelle. Das darin beschriebene Agent-Gateway-Modell ist in Abbildung 7.1 zu sehen. In der Abbildung sind die in Abschnitt 4 bereits beschriebenen Komponenten PDP (Policy Decision Point) und PEP (Policy Enforcement Point) zu finden, die zur Autorisierung und Zugriffskontrolle zum Einsatz kommen. Der Agent auf Seite der Nutzenden stellt eine Client-Anwendung dar, die auf einen Dienst/Server oder eine andere in einem Netzwerk bereitgestellte Ressource zugreifen möchte. Dem Dienst vorangestellt ist der PEP (alternativ kann der PEP auch in den Dienst integriert sein), der den Zugriff darauf überwacht und erst erlaubt, wenn der Agent die notwendige Autorisierung durch den PDP erhalten hat.

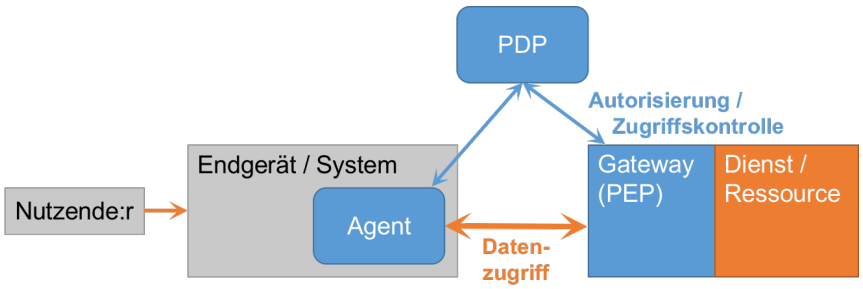

Abb. 7.1: Agent-Gateway-Modell (nach [NIS20])

In einem praktischen Anwendungsfall kann der Agent ein Browser sein, der auf eine Web-Anwendung (die Ressource) zugreifen möchte. Der Gateway kann als Teil der Web-Anwendung realisiert sein oder für sich stehen, bspw. in Form eines Web-Proxy. Würde für die Autorisierung bspw. das SSO-Protokoll OpenID-Connect genutzt, würde der Gateway den Agenten zunächst an den PDP weiterleiten, der Nutzende würde sich gegenüber dem PDP authentifizieren, der PDP bei Erfolg den Zugriff autorisieren und den Agenten zusammen mit den Autorisierungsinformationen wieder an den PEP zurückleiten. Nach Prüfung der Autorisierungsinformationen würde der PEP schließlich den Zugriff auf die Web-Anwendung freigeben. Alle folgenden Zugriffe des Agenten auf die Web-Anwendung würden vom PEP ebenfalls freigegeben, ohne Umweg über den PDP, solange die Autorisierung gültig ist.

7.2.2
Enclave-Gateway

In einer Variante des Agent-Gateway-Modells beschreibt das NIST das Enclave-Gateway-Modell bei dem der Gateway weder Teil eines Dienstes noch diesem vorangestellt ist, sondern als separate Komponente existiert, die den Zugriff auf *mehrere* Dienste/Ressourcen kontrolliert, s. Abbildung 7.2. Die Enclave wird in diesem Modell vom Gateway zusammen mit den kontrollierten Diensten gebildet. Dieses Modell kann bspw. dann zum Einsatz kommen, wenn eine Web-Anwendung aus verschiedenen Diensten zusammengesetzt ist. Durch die Nutzung eines Gateway für mehrere Dienste geht jedoch die Einzelabsicherung, wie im Agent-Gateway-Model, verloren und wird durch eine Kollektivabsicherung ersetzt. Dies kann dazu führen, dass Nutzende, die für den Zugriff auf einen der Dienste autorisiert wurden, u. U. Dienste sehen können für die sie keine Autorisierung haben.

Kommen verschiedene PDP-Instanzen zum Einsatz, bspw. für unterschiedliche Umsetzungsmodelle, ist es wichtig, dass diese zentral gesteuert/konfiguriert werden können, um eine *einheitliche Umsetzung* der kommunalen Sicherheitsrichtlinie für jeden Dienst zu gewährleisten.

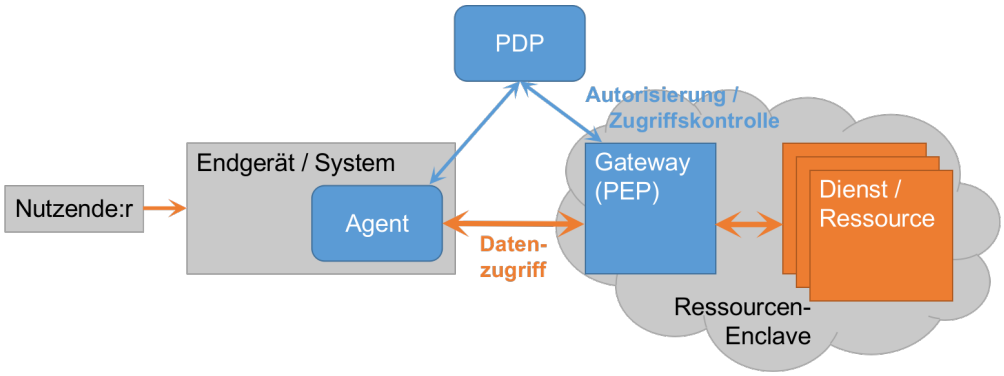

Abb. 7.2:
Enclave-Gateway-Modell (nach [NIS20])

7.2.3
Interne vs. externe Dienste

Sowohl das Agent-Gateway-Modell als auch das Enclave-Gateway-Modell können für Dienste innerhalb der kommunalen Infrastruktur als auch bei externen Diensten zum Einsatz kommen. In letzterem Fall würde der PEP, genauso wie der Dienst, beim externen Anbieter verortet sein, während der PDP von der Kommune betrieben würde, bspw. als eigenständiger Identity-Provider (4.1 Identitäten und Authentifizierung).

Für *innerhalb* der kommunalen Infrastruktur bereitgestellte Dienste, die keine IAM-Anbindung und kein eigenes IAM bieten, kann ebenfalls das Agent-Gateway-Modell bzw. das Enclave-Gateway-Modell für mehr Sicherheit sorgen. Wird einem solchen Dienst ein PEP vorangestellt, verhindert dieser, dass unautorisierte Personen Zugriff auf den Dienst erhalten. Beispiele für solche Dienste sind interne Web- oder Druck-Server.

Dienste ohne IAM, die von einem Dritten *außerhalb* der kommunalen Infrastruktur bereitgestellt werden, sollten hingegen nicht für die Verarbeitung interner Daten eingesetzt werden. Zugriffe auf einen solchen Dienst können offensichtlich nicht auf berechtigte kommunale Mitarbeitende wirksam beschränkt werden, sodass die Gefahr unberechtigter Zugriffe durch Dritte stets gegeben ist.[3]

7.3 Protokollierung und Auswertung

Praktisch alle Server-Anwendungen erlauben eine Protokollierung von Zugriffen in Log-Dateien (kurz: Logs). In diesen Logs werden im Regelfall u. a. potenziell sicherheitskritische Ereignisse festgehalten, wie bspw. wiederholte Falscheingaben von Anmeldedaten, aber auch andere Ereignisse wie der Absturz einer Anwendung, der ggf. durch einen Cyberangriff herbeigeführt wurde. Jedes Log für sich genommen kann u. U. bereits Aufschluss über derartige Probleme, Unregelmäßigkeiten oder (Vorbereitungen für) die Ausführung von Cyberangriffe liefern. In allen Server-Anwendungen sollte deshalb die Protokollierung aktiviert werden, falls sie nicht per Default schon aktiv ist.

Eine manuelle Durchsicht aller Logs aus den verschiedenen Server-Anwendungen ist i. d. R. auf Grund der Anzahl und des Umfangs von Log-Dateien nicht mehr sinnvoll möglich. Zudem ist es bei einer manuellen Auswertung schwierig, Korrelationen von Ereignissen aus verschiedenen Logs zu erkennen, die in ihrer Kombination womöglich die Vorbereitung oder die Ausführung eines Cyberangriffs aufzeigen könnten. Dennoch sollten einzelne Logs von kritischen Anwendungen, wie ausgewählte Server-Dienste, Firewalls und zentralen Gateways, die Subnetzübergänge ermöglichen, regelmäßig auf Fehler und unerlaubte Zugriffe bzw. Zugriffsversuche hin untersucht werden, um ein mögliches Sicherheitsproblem identifizieren zu können.

7.4 Fortgeschrittene Maßnahmen

Security Information and Event Management (SIEM). Der Einsatz eines SIEM-Systems (*Security Information and Event Management*) erlaubt es, sicherheitsrelevante Ereignisse von Anwendungen – insbesondere Server-Anwendungen – automatisch zu analysieren und zu korrelieren, indem es u. a. Logs verschiedener Anwendungen *zentral* und Log-übergreifend verarbeitet. Bei Erkennung eines verdächtigen Ereignisses setzt das SIEM dann entsprechende Warnmeldungen ab, um IT-Sicherheitspersonal darauf aufmerksam zu machen. Hierdurch wird gleichzeitig die Sichtbarkeit von im Netzwerk aktiven Geräten erhöht, da unbekannte Geräte, die versuchen auf Netzwerk-Ressourcen bzw. Server zuzugreifen, in den jeweiligen Logs auftauchen werden und so mittels des SIEM-Systems erkannt werden können. In diesem Sinne kann ein SIEM-System auch die beiden Zero-Trust-Säulen Geräte (Abschnitt 5) und Netzwerk (Abschnitt 6) unterstützen.

3 Zugriffe auf den Dienst aus dem kommunalen Netzwerk heraus könnten zwar beschränkt werden, Beschränkungen von Zugriffen aus externen Netzwerken jedoch nur durch den Dienstbetreiber selbst.

In der Praxis kann der Betrieb eines SIEM-Systems, neben zusätzlichen Personalressourcen, auch eine kontinuierliche Feinabstimmung erforderlich machen, um zum einen fälschlich ausgelöste Warnmeldungen (*False-Positives*) zu reduzieren, als auch fälschlicherweise übersehene, sicherheitsrelevante Ereignisse (*False-Negatives*) zukünftig zu melden. Ohne SIEM-System muss zwischen dem Aufwand für manuelle Überprüfungen und der Gewährleistung der Dienstsicherheit stärker abgewogen werden.

Automatische Auswertung von SBOMs für Lieferkettensicherheit. Software-Stücklisten (*software bill of materials*, SBOM) sind Teil der Entwicklungsdokumentation eines Software-Herstellers und enthalten u. a. Angaben über Art (bspw. Bibliothek, Laufzeitumgebung, Versionsnummer) und Herkunft (bspw. Hersteller, Open-Source-Projekt) von Drittkomponenten, also Komponenten, die der Hersteller für sein Produkt verwendet, jedoch nicht selbst entwickelt hat. Hierdurch soll ein Überblick geschaffen werden, im Hinblick auf die verwendeten Komponenten. Hersteller von Server-Software sind durch den EU Cyber-Resilience-Act (CRA) dazu verpflichtet, eine SBOM zu ihrem Produkt zu führen. Sie sind jedoch nicht verpflichtet, diese zu veröffentlichen, weshalb womöglich nicht jeder Hersteller dies pauschal tun wird.

SBOMs können einen wichtigen Beitrag zur Lieferkettensicherheit leisten, da hierdurch die Herkunft von Teilkomponenten einer Anwendung für Endnutzende transparent gemacht wird und anhand ihrer Versionsnummern geprüft werden kann, ob eine aktuelle bzw. eine schwachstellenfreie Version ausgeliefert wurde. Falls keine SBOM veröffentlicht und ggf. auch auf Nachfrage beim Hersteller nicht herausgegeben wird, kann u. U. ein Blick in die Liste der Fremdlizenzen helfen. Wird Software von Dritten vom Hersteller in seine Anwendung eingebunden, so müssen die Lizenzbedingungen der eingebundenen Software beachtet und typischerweise auch mitgeliefert werden. In der Fremdlizenzliste sollte sich dann zumindest ein Teil der verwendeten Komponenten finden lassen, da diese ihren jeweiligen Lizenzen zugeordnet werden müssen. Eine weitere Möglichkeit besteht darin, spezielle Scanner-Software zu nutzen, die eine SBOM für eine gegebene Anwendungsinstallation erstellt.

Idealerweise liegt die SBOM in einem maschinenlesbaren Format wie SPDX oder CycloneDX vor, s. dazu auch [BSI25]. Hierdurch können Anwendungskomponenten mit Hilfe einer entsprechenden Monitoring-/Management-Software im Hinblick auf ihre Aktualität bzw. ihren Sicherheitsstand leichter überwacht werden, ähnlich wie Anwendungen aus der Software-Verteilung auf Updates geprüft werden (s. Abschnitt 7.1.2 Wartung von Software). Wird eine Komponente mit einer Schwachstelle in einer kommunalen Anwendung identifiziert, können Sicherheitsverantwortliche zeitnah das Risiko für einen erfolgreichen Cyberangriff abwägen. Dies kann insbesondere für Server-Anwendungen, die auch über das Internet erreichbar sind, entscheidend sein, um rechtzeitig Maßnahmen zur Reduktion des Risikos ergreifen zu können, bspw. durch Abschottung der Anwendung vom Internet, bis eine aktualisierte, schwachstellenfreie Version der Komponente verfügbar ist bzw. installiert wurde.

8
Initiale Umsetzungsschritte in der Säule Daten

Die technische Säule Daten innerhalb des Zero-Trust-Modells stellt das eigentliche Schutzgut der Informationsverarbeitung, die in einer Organisation verarbeiteten Datenbestände, in den Mittelpunkt der sicherheitstechnischen Betrachtung. Maßgebliche Referenzmodelle, darunter insbesondere die „NIST Special Publication 800-207 (Zero Trust Architecture)“ [NIS20], das „CISA Zero Trust Maturity Model v2.0“ [CIS23] sowie die „DoD Zero Trust Reference Architecture v2.0“ [DoD22b], definieren Daten explizit als eigenständige Ressource, für die Zugriffsentscheidungen risikobasiert sowie kontextabhängig zu treffen sind. Daraus ergibt sich die grundlegende Anforderung, dass Schutzmaßnahmen nicht ausschließlich an Infrastrukturkomponenten oder Netzwerkgrenzen ausgerichtet werden, sondern unmittelbar am Datenobjekt selbst ansetzen.

Für Kommunen und Landkreise besitzt diese Perspektive eine besondere Relevanz, da öffentliche Verwaltungen regelmäßig große Mengen sensibler oder personenbezogener Daten verarbeiten. Hierzu zählen unter anderem Datenbestände aus dem Meldewesen, aus Sozialleistungsverfahren, aus der Jugendhilfe, aus Bau- und Planungsverfahren sowie aus der Schulverwaltung. Diese Daten unterliegen regelmäßig erhöhten gesetzlichen Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit. Gleichzeitig ist die IT-Landschaft kommunaler Verwaltungen typischerweise durch eine hohe strukturelle Heterogenität gekennzeichnet. Die Infrastruktur ist häufig historisch gewachsen, verteilt sich über mehrere organisatorische Standorte sowie technische Betriebsumgebungen und wird teilweise durch kommunale IT-Dienstleister betrieben. Datenbestände befinden sich daher nicht selten verteilt über mehrere Rechenzentren, Fachanwendungen, Dateispeicherstrukturen oder Cloud-Dienste. Ohne eine systematische und organisationsweite Sicht auf diese Datenbestände bleibt jede Sicherheitsstrategie zwangsläufig unvollständig.

Sichtbarkeit und Strukturierung von Datenbeständen

Vor diesem Hintergrund liegt der zentrale Fokus der Daten-Säule auf der Herstellung von Transparenz über vorhandene Datenbestände sowie deren strukturelle Einordnung. In diesem Zusammenhang sind insbesondere folgende Fragestellungen zu adressieren: Welche Daten existieren innerhalb der Organisation, wo befinden sich diese Datenbestände, welche organisatorischen Stellen tragen die fachliche Verantwortung und welche Schutzanforderungen ergeben sich aus rechtlichen, organisatorischen oder technischen Rahmenbedingungen?

Als methodischer Ansatz dient hierbei die systematische Datenklassifikation, bei der Datenbestände nach ihrer Vertraulichkeitsstufe sowie nach weiteren relevanten Eigenschaften kategorisiert werden. Ergänzend erfolgt eine Anreicherung mit Metadaten, etwa zur organisatorischen Zuständigkeit (z. B. Fachamt), zur Art der Daten oder zum jeweiligen Schutzbedarf. Diese Informationen bilden die Grundlage für eine technisch nutzbare Steuerung sicherheitsrelevanter Maßnahmen.

Die Umsetzungsschritte innerhalb der Daten-Säule verfolgen im Kern drei miteinander verknüpfte Zielsetzungen:

1. Sichtbarmachung und Strukturierung von Datenbeständen: Hierzu zählt insbesondere der Aufbau eines belastbaren Dateninventars sowie die Herstellung von Transparenz über zentrale Datenflüsse innerhalb der Organisation.
2. Operationalisierung von Schutzanforderungen: In diesem Zusammenhang erfolgt die Einführung einer technisch nutzbaren Datenklassifikation, die mit klar definierten Mindestanforderungen an Schutzmaßnahmen verbunden ist.
3. Dynamische Durchsetzung und Resilienz: Aufbauend auf der Klassifikation werden Schutzmaßnahmen – etwa Verschlüsselung, Monitoring, Backup oder Recovery – systematisch und schutzbedarfsorientiert umgesetzt.

Durch die systematische Betrachtung der verarbeiteten Daten innerhalb einer Zero-Trust-Architektur kann die Angriffsfläche einer Organisation in mehrfacher Hinsicht reduziert werden. So ermöglicht die strukturierte Analyse von Datenbeständen beispielsweise die Identifikation und Beseitigung unnötiger Datenkopien, redundanter Exporte oder verwaister Datenablagen. Darüber hinaus können Sicherheitsmaßnahmen – etwa die Verschlüsselung von Daten während der Speicherung oder der Übertragung – gezielt dort implementiert werden, wo aufgrund des Schutzbedarfs der größte Sicherheitsgewinn zu erwarten ist. Schließlich trägt die Daten-Säule auch zur Erhöhung der organisatorischen Resilienz bei, da durch geeignete Backup- und Recovery-Mechanismen die Wiederherstellungsfähigkeit kritischer Datenbestände sichergestellt wird und gleichzeitig durch Monitoring-Mechanismen potenzielle Datenabflüsse frühzeitig erkannt werden können.

Wechselwirkungen mit anderen technischen Säulen

Die Daten-Säule ist nicht isoliert zu betrachten, sondern fungiert als strukturierendes Element der gesamten Zero-Trust-Architektur. Sie stellt die inhaltliche Grundlage bereit, auf deren Basis die übrigen technischen Säulen operieren können. Ihre Wirksamkeit entfaltet sich daher erst im Zusammenspiel mit den Säulen Identität, Geräte, Netzwerk sowie Workloads & Apps.

Im Fokus der Säule Identität (vgl. Abschnitt 4) stehen digitale Identitäten, Authentifizierungsmechanismen, Attributverwaltung sowie die Definition von Zugriffsrechten im Vordergrund. Die Daten-Säule liefert hierfür die fachliche Grundlage in Form von Datenklassifikationen und zugehörigen Metadaten, etwa hinsichtlich Vertraulichkeitsstufen, organisatorischer Zuständigkeiten oder Datenarten. Erst die Kombination aus Identitätsattributen und Daten-Metadaten ermöglicht kontext- und risikobasierte Zugriffsentscheidungen. Ohne belastbare Identitätsattribute bleibt eine Datenklassifikation praktisch wirkungslos, während umgekehrt ein Identitätsmodell ohne Bezug zu klassifizierten Daten keinen fachlichen Kontext für Zugriffsbewertungen besitzt.

Die Säule Geräte (vgl. Abschnitt 5) adressiert den Sicherheitszustand von Endgeräten und Servern. Diese Informationen liefern einen zusätzlichen Kontext für Zugriffsentscheidungen. Je höher der Schutzbedarf eines Datenbestandes ist, desto höher fallen in der Regel die Anforderungen an den Sicherheitszustand des zugreifenden Geräts aus. Darüber hinaus können geräteseitige Schutzmaßnahmen (wie etwa Festplattenverschlüsselung) gezielt anhand der zuvor definierten Datenklassifikation umgesetzt werden.

Die Säule Netzwerk (vgl. Abschnitt 6) ergänzt diese Perspektive um netzwerkbezogene Kontextinformationen, beispielsweise hinsichtlich Standort, Netzwerksegment oder Zugangsart. Während die Daten-Säule die Schutzwürdigkeit von Datenbeständen definiert und kritische Datenflüsse identifiziert, stellt die Netzwerk-Säule Mechanismen zur Absicherung der entsprechenden Kommunikationsbeziehungen bereit, etwa durch Segmentierung oder kontrollierte Verbindungen zwischen Systemen. In diesem Zusammenspiel definiert die Daten-Säule den Schutzbedarf des Inhalts, während die Netzwerk-Säule den Transportpfad absichert.

Die Säule Workloads & Apps (vgl. Abschnitt 7) bezieht sich auf Fachanwendungen, die in kommunalen IT-Landschaften die primären Orte der Datenverarbeitung darstellen. Anwendungen übernehmen dabei eine zentrale Rolle bei der Erzeugung, Verarbeitung und Verwaltung von Daten-Metadaten. Fachverfahren werden mittels einem oder mehreren Fachanwendungen umgesetzt. Sofern die Fachanwendungen keine Klassifikation unterstützen oder keine geeigneten Metadaten bereitstellen, kann die Daten-Säule ihre Steuerungsfunktion nur eingeschränkt erfüllen. Umgekehrt profitieren modernisierte Anwendungsarchitekturen – etwa containerisierte oder cloudbasierte Dienste – von technischen Konzepten wie softwaredefinierten Speicherarchitekturen (Software-Defined Storage, SDS) sowie automatisierten Richtlinien für Verschlüsselung, Replikation und Datensicherung.

In der Datensäule zeigt sich, dass zahlreiche Umsetzungsschritte ohne die inhaltliche Zuarbeit der Fachämter nur eingeschränkt umsetzbar sind. Die Fachämter verfügen über die notwendige Kenntnis der Daten – insbesondere hinsichtlich ihrer fachlichen Bedeutung, ihrer Semantik, möglicher Risiken sowie des daraus abzuleitenden Schutzbedarfs – und übernehmen damit die Aufgabe, diese Aspekte systematisch zu ermitteln, zu klassifizieren und zu dokumentieren. Auf dieser Grundlage werden geeignete Sicherheitsmaßnahmen, etwa hinsichtlich Verschlüsselung, Zugriffskontrolle oder Datensicherung, überwiegend durch die IT abgeleitet und technisch umgesetzt. Im Verlauf ist dabei regelmäßig eine Abstimmung mit den Fachämtern erforderlich, um sicherzustellen, dass die gewählten Sicherheitsmaßnahmen den fachlichen Anforderungen und dem tatsächlichen Schutzbedarf der Daten entsprechen. Ohne diese Verzahnung bleiben Sicherheitsmaßnahmen häufig zu pauschal und adressieren die spezifischen Risiken nur unzureichend.

8.1
Aufbau eines Dateninventars mit klarer Datenverantwortung

Ein belastbares Dateninventar stellt eine zentrale Voraussetzung für die Umsetzung einer ZTA dar. Das CISA Zero Trust Maturity Model [CIS23] fordert in der Daten-Säule ausdrücklich Transparenz (im Sinne von Sichtbarkeit) über Datenbestände, Speicherorte und Verantwortlichkeiten verlangt. Ohne eine solche Transparenz bleiben Maßnahmen wie Datenklassifikation, Zugriffskontrolle, Monitoring oder Verschlüsselung nur eingeschränkt umsetzbar. Ziel dieses Umsetzungsschrittes ist der Aufbau einer strukturierten und priorisierten Datenlandkarte.

8.1.1
Erstellung eines Dateninventars

Der Einstieg erfolgt pragmatisch und konzentriert sich zunächst auf besonders kritische Verfahren, etwa im Meldewesen, in Sozialleistungsverfahren, im Finanz- und Kassenwesen, in der Schulverwaltung oder in zentralen Fileserver-Strukturen.

Für diese Verfahren werden systematisch zentrale Informationen erfasst, insbesondere Datenarten (z. B. Stamm-, Leistungs- oder Zahlungsdaten sowie besondere Kategorien personenbezogener Daten), der Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit, relevante Speicherorte (etwa lokale Systeme, kommunale Rechenzentren oder Cloud-Dienste), bestehende Schnittstellen und Datenexporte sowie die fachliche und technische Verantwortung innerhalb der Organisation oder bei externen Dienstleistern.

Beispiel 1. Für ein Sozialhilfe-Fachverfahren wird dokumentiert, dass besonders schutzbedürftige Sozialdaten im Rechenzentrum eines kommunalen IT-Dienstleisters verarbeitet werden, regelmäßige Datenübermittlungen an die Kämmerei erfolgen und zusätzlich lokale Auswertungsdateien in einem gemeinsamen Netzlaufwerk abgelegt werden. Erst diese Transparenz ermöglicht eine gezielte Ableitung von Klassifikationsregeln sowie technischen Maßnahmen, etwa im Bereich Verschlüsselung oder Data-Loss-Prevention.

Beispiel 2. Ein Fileserver enthält sowohl veröffentlichte Pressemitteilungen als auch interne vertrauliche Dokumente. Ohne Differenzierung werden beide Datenarten identisch behandelt, etwa im Rahmen von Backup- oder Verschlüsselungsmaßnahmen. Das Dateninventar macht jedoch sichtbar, dass unterschiedliche Schutzanforderungen bestehen und daher eine differenzierte technische Absicherung erforderlich ist.

Weiterführende Informationen liefern u. a. das BSI mit dem Projekt „Weg in die Basis-Absicherung“ (WiBA) [BSI23f], bspw. mit der „Checkliste: Umgang mit Informationen“, sowie die Arbeitsgruppe Kommunale Basis-Absicherung (AG KOBA) mit ihrem „IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung“ [BSI23d]. Beispiele und mögliche Parameter zur Klassifizierung verschiedener Datenarten liefert u. a. das Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) mit ihrer Veröffentlichung „Datenstrategien in Kommunen“ [BBS23].

8.1.2
Zuordnung der fachlichen und technischen Datenverantwortung

Parallel zur technischen Bestandsaufnahme ist die Klärung der Datenverantwortung erforderlich. Für jedes wesentliche Datenverfahren sind sowohl eine fachliche Datenverantwortung – in der Regel auf Ebene der zuständigen Fachamts – als auch eine eindeutig definierte technische Betriebsverantwortung festzulegen. Erst auf dieser Grundlage können Schutzbedarfe, Klassifikationen, Aufbewahrungsfristen sowie Löschkonzepte verbindlich bestimmt werden.

Der Anspruch dieses Umsetzungsschrittes ist dabei bewusst pragmatisch zu halten. Ziel ist nicht die vollständige Erfassung einzelner Datensätze, sondern die Herstellung belastbarer Transparenz bzw. Übersicht über zentrale Datenbestände und wesentliche Datenflüsse. In der Praxis erfolgt dies typischerweise iterativ. Zunächst werden besonders kritische Verfahren erfasst, anschließend wird die Datenübersicht schrittweise erweitert. Das Ergebnis ist eine konsolidierte Datenübersicht, die als Referenz für weitere Maßnahmen der Daten-Säule dient, insbesondere für Klassifikation, Verschlüsselung, Backup-Strategien und Monitoring.

8.2
Einheitliche Datenklassifizierung und Schutzniveaus

Eine datenzentrierte Zero-Trust-Architektur setzt voraus, dass Datenbestände nicht ausschließlich technisch verwaltet, sondern auch hinsichtlich ihrer Sensitivität und Kritikalität bewertet werden. Referenzmodelle von CISA, NIST und DoD betonen in diesem Zusammenhang, dass der Schutzbedarf von Daten in strukturierter Form vorliegen muss, damit Zugriffskontrollsysteme, Data-Loss-Prevention-Mechanismen oder Monitoring-Systeme belastbare Entscheidungen treffen können. Datenklassifikation fungiert damit als zentraler technischer Steuerungsmechanismus innerhalb der Daten-Säule.

In kommunalen Verwaltungen existieren häufig bereits Schutzbedarfsbewertungen, etwa im Rahmen von Informationssicherheitsmanagementsystemen (ISMS) oder im Kontext der Datenschutz-Grundverordnung (DSGVO), beispielsweise durch Datenschutz-Folgenabschätzungen oder Verzeichnisse von Verarbeitungstätigkeiten. Diese Bewertungen können grundsätzlich als Ausgangspunkt für eine Datenklassifikation genutzt werden. In vielen Fällen sind sie jedoch nicht ausreichend präzise oder nicht in einer technisch nutzbaren Form dokumentiert, sodass eine direkte Verwendung in Zugriffskontrollen, Verschlüsselungsrichtlinien, Backup-Strategien oder Monitoring-Maßnahmen nur eingeschränkt möglich ist. Der Zweck dieses Umsetzungsschrittes besteht daher darin, bestehende Schutzbedarfsbewertungen in ein konsistentes und technisch nutzbares Klassifikationsmodell zu überführen.

8.2.1
Schutzklassen und Mindestanforderungen an Sicherheitsmaßnahmen

Für Kommunen empfiehlt sich ein pragmatisches Klassifikationsmodell mit wenigen klar definierten Schutzklassen. Häufig wird ein vierstufiges Modell verwendet, das sich beispielsweise wie folgt strukturieren lässt:

- Öffentlich: Daten, die zur Veröffentlichung bestimmt sind oder bereits veröffentlicht wurden.
- Intern: Verwaltungsinterne Informationen ohne besondere Sensibilität.
- Vertraulich: Personenbezogene oder fachlich sensible Daten.
- Streng vertraulich: Besonders schutzbedürftige personenbezogene oder sicherheitsrelevante Daten.

Entscheidend ist weniger die Anzahl der Schutzklassen als deren eindeutige Definition und technische Nutzbarkeit. Ausgehend vom jeweiligen Schutzbedarf – der insbesondere mögliche Schäden bei Verletzung von Vertraulichkeit, Integrität oder Verfügbarkeit berücksichtigt – werden konkrete Sicherheitsmaßnahmen abgeleitet. Jede Schutzklasse ist daher mit verbindlichen Mindestanforderungen zu verknüpfen.

Beispiel 3. Veröffentlichte Satzungen oder Haushaltspläne könnten bspw. der Schutzklasse „öffentlich“ zugeordnet werden, bei denen vor allem Integritätsschutz relevant ist. Interne Protokolle oder Entwürfe von Verwaltungsvorlagen fallen typischerweise in die Schutzklasse „intern“ und erfordern eine Zugriffsbeschränkung auf Mitarbeitende. Daten der Schutzklasse „vertraulich“, etwa Meldedaten einzelner Bürger, Vertragsunterlagen oder Zahlungsinformationen, erfordern in der Regel Transport- und Speicherverschlüsselung sowie eingeschränkte Exportmöglichkeiten. Für Daten der Schutzklasse „streng vertraulich“, etwa Sozial- oder Gesundheitsdaten, kommen zusätzlich erweiterte Protokollierung, verstärktes Monitoring und restriktive Weitergaberegeln hinzu.

In einem ersten Schritt erfolgt die grobe Zuordnung der im Dateninventar identifizierten Fachverfahren zu diesen Schutzklassen, zunächst auf Ebene der Verfahren. So könnten beispielsweise Fachverfahren des Sozialamtes grundsätzlich der Schutzklasse „streng vertraulich“ zugeordnet werden. Anschließend werden die verschiedenen Datenbestände der jeweiligen Fachverfahren genauer betrachtet und sukzessive den entsprechenden Schutzklassen zugeordnet.

8.2.2
Metadaten

Im Rahmen der Datenklassifizierung ist zu berücksichtigen, dass einzelne Fachverfahren häufig mehrere Schutzklassen enthalten können. Ein Bauantragsverfahren umfasst beispielsweise personenbezogene Angaben des Antragstellers, Lagepläne und Bauzeichnungen, Informationen zu Grundstücken und Eigentumsverhältnissen, interne Stellungnahmen beteiligter Fachämter sowie behördeninterne Prüfvermerke. Während die veröffentlichte Baugenehmigung nach Abschluss des Verfahrens – sofern kein sensibler Personenbezug mehr besteht – teilweise als öffentlich oder zumindest intern eingeordnet

werden kann, bleiben die vollständigen Antragsunterlagen mit personenbezogenen Angaben und internen Bewertungen regelmäßig mindestens der Schutzklasse „vertraulich“ zuzuordnen; in besonderen Konstellationen, etwa bei sicherheitsrelevanter Infrastruktur, kann auch eine Einstufung als streng vertraulich erforderlich sein.

Dieses Beispiel verdeutlicht zwei zentrale Aspekte der Datenklassifizierung. Erstens können innerhalb eines einzelnen Fachverfahrens unterschiedliche Schutzklassen auftreten, sodass eine pauschale Einstufung häufig nicht ausreicht und eine Differenzierung auf Dokument- oder Datenartebene erforderlich sein kann. Zweitens kann sich der Schutzbedarf im Verlauf des Datenlebenszyklus verändern. Dokumente, die während der Bearbeitung eines Verfahrens einem hohen Schutzbedarf unterliegen, können nach Abschluss teilweise veröffentlicht oder archiviert werden.

Für die technische Umsetzung folgt daraus, dass neben der eigentlichen Schutzklasse auch ergänzende Metadaten berücksichtigt werden sollten, etwa zur Verfahrensart, zum Bearbeitungsstatus oder zum Dokumenttyp. Auf dieser Grundlage können sicherheitsrelevante Maßnahmen – beispielsweise Zugriffsbeschränkungen, Exportregeln, Verschlüsselungsanforderungen oder Monitoring – kontextabhängig angewendet werden.

8.2.3 Technische Umsetzung der Datenklassifikation

Zentral ist die technische Abbildung der Datenklassifikation, da sie ihre Wirkung nur entfalten kann, wenn sie nicht ausschließlich in Richtlinien dokumentiert bleibt. In der Praxis bieten bestehende Systeme häufig erste Ansatzpunkte für eine Umsetzung. Kollaborationsplattformen unterstützen beispielsweise Sensitivity-Labels, über die automatisiert Verschlüsselung, Weiterleitungsbeschränkungen oder Regeln für Data-Loss-Prevention-Regeln (DLP) ausgelöst werden können. DLP bezeichnet hierbei Sicherheitsmaßnahmen und -technologien, die darauf abzielen, den unbefugten Abfluss sensibler Daten zu verhindern, indem Datenflüsse überwacht, klassifiziert und bei Bedarf blockiert oder kontrolliert werden. Auch in Dateisystemen lassen sich Schutzklassen an Ablagestrukturen oder Dateiverzeichnisse koppeln. Fachanwendungen ermöglichen teilweise die Nutzung zusätzlicher Metadaten, etwa über Mandanten, Fallarten oder definierte Datenfelder.

Höhere ZTA-Reifegrade setzen in der Daten-Säule strukturierte Metadaten und Klassifikationskennzeichnungen an Datenobjekten voraus, damit diese in Monitoring- und DLP-Mechanismen einbezogen werden können. Erst wenn Klassifikationsinformationen in technisch auswertbarer Form vorliegen, lassen sie sich in dynamische Zugriffsentscheidungen sowie in Verschlüsselungs-, Backup- oder Monitoring-Richtlinien integrieren.

Ein weiterer Effekt der Datenklassifikation liegt in der Priorisierung von Sicherheitsmaßnahmen. Maßnahmen wie Verschlüsselung, Monitoring oder Backup können gezielt auf Daten mit hohem Schutzbedarf konzentriert werden. Gleichzeitig lassen sich differenzierte Aufbewahrungs- und Löschkonzepte entwickeln, da nicht alle Daten denselben regulatorischen oder fachlichen Anforderungen unterliegen. Außerdem können die abgeleiteten Schutzmaßnahmen auch für die Definition verbindlicher Anforderungen gegenüber externen Dienstleistern dienen.

8.3 Analyse und Absicherung kritischer Datenflüsse

Im Zero-Trust-Modell stehen nicht nur gespeicherte Daten im Fokus, sondern auch deren Bewegung innerhalb und außerhalb einer Organisation. Traditionelle Sicherheitsmaßnahmen konzentrieren sich häufig auf Datenbanken, Fileserver oder Archive. In der Praxis entstehen jedoch zahlreiche Risiken entlang der Kommunikations- und Austauschprozesse zwischen Systemen, Fachanwendungen, Organisationseinheiten und externen Stellen. Die betrachteten Zero-Trust-Referenzmodelle und Spezifikationen weisen daher ausdrücklich darauf hin, dass Datenbewegungen – etwa über APIs, Dateiübertragungen, Datenexporte oder Systemreplikationen – zentrale Angriffs- und Exfiltrationspfade darstellen und innerhalb der Daten-Säule gezielt adressiert werden müssen [CIS23][NIS20]. Analysen von ENISA zeigen zudem, dass Angriffe auf öffentliche Verwaltungen häufig auf Datenabfluss und anschließende Erpressung abzielen [ENI25].

Für Kommunen und Landkreise ist dieser Aspekt besonders relevant, da viele Verwaltungsprozesse organisationsübergreifend ablaufen. Daten werden regelmäßig zwischen Fachämtern ausgetauscht, an kommunale IT-Dienstleister übertragen oder an Behörden auf Landes- und Bundesebene weitergeleitet. Gleichzeitig bestehen vielfach historisch gewachsene Austauschmechanismen, die nur teilweise dokumentiert sind.

8.3.1 Erfassung der Datenflüsse

Der erste Schritt besteht darin, zentrale fachliche Szenarien als Datenflüsse zu erfassen und zu dokumentieren. Dabei wird nicht die gesamte IT-Landschaft im Detail modelliert, sondern zunächst auf besonders sensible oder kritische Prozesse fokussiert. Typische Beispiele sind etwa der Austausch von Sozialdaten zwischen Sozialamt, Jugendamt, Jobcenter und externen Trägern, die Übermittlung von Meldedaten an Landesbehörden, der Datenaustausch zwischen Fachanwendungen und zentralen Finanzsystemen sowie Datenübertragungen zu kommunalen IT-Dienstleistern. Für diese Szenarien wird der Datenfluss Ende-zu-Ende dokumentiert, einschließlich Ursprungssystem, Zwischenstationen, Transportmechanismen (z. B. TLS-gesicherte Webdienste, VPN-Verbindungen oder Dateiübertragungen), temporärer Ablagen und Zielsysteme. Auch mögliche Weiterleitungen oder Zwischenspeicherungen – etwa Exportdateien in Arbeitsverzeichnissen oder Datenkopien in Analyseumgebungen – sind zu berücksichtigen.

Diese Transparenz macht häufig bislang wenig beachtete Schwachstellen sichtbar, beispielsweise unverschlüsselte Dateiübertragungen, gemeinsam genutzte Ablageordner ohne klare Zugriffsregelung, manuelle Datenexporte aus Fachanwendungen oder nicht standardisierte Übertragungswege zu Dienstleistern.

8.3.2
Festlegung sicherer Datenflüsse

Auf Grundlage der Analyse lassen sich standardisierte Muster für sichere Datenübertragungen definieren. Hierzu zählen insbesondere die verpflichtende Nutzung zentraler Transferlösungen, klar definierte Schnittstellen für die Kommunikation zwischen Fachanwendungen und Diensten sowie eine bewusste Reduktion der übertragenen Daten und Attribute. Ergänzend werden Vorgaben für temporäre Speicherung und anschließende Löschung festgelegt. Ziel dieser Maßnahmen ist es, informelle oder historisch gewachsene Austauschmechanismen schrittweise durch nachvollziehbare und kontrollierte Übertragungsverfahren zu ersetzen. Die systematische Analyse kritischer Datenflüsse bildet eine wichtige Grundlage für weitere nachfolgende Umsetzungsschritte in der Daten-Säule, wie das Monitorig zur Entdeckung von auffälligen Ereignissen (z. B. ungewöhnlich große Datenexporte, wiederholte Übertragungen sensibler Datensätze oder unerwartete Kommunikationsbeziehungen zwischen Fachanwendungen und Diensten).

8.4
Ausrichtung von Verschlüsselungsmaßnahmen am Schutzbedarf

Verschlüsselung stellt innerhalb einer ZTA keine optionale Sicherheitsmaßnahme dar, sondern dient dem Schutz sensibler Informationen auch in Szenarien, in denen andere Schutzmechanismen bereits umgangen wurden (vgl. „Assume-Breach-Ansatz“ von Zero-Trust). Die eingangs genannten ZT-Referenzmodelle von CISA , DoD und NIST gehen grundsätzlich davon aus, dass Angreifer interne Systeme erreichen können. Daraus folgt die Anforderung, Daten mit erhöhtem Schutzbedarf unabhängig vom Standort oder Netzwerksegment abzusichern, sowohl bei der Übertragung als auch bei der Speicherung. Das DoD hebt in diesem Zusammenhang insbesondere die Bedeutung eines strukturierten Schlüsselmanagements hervor, um Risiken durch Insider oder privilegierte Administratoren zu begrenzen.

Die Ausgangssituation in kommunalen IT-Umgebungen ist häufig heterogen. Transportverschlüsselung über TLS ist in vielen Bereichen vorhanden, jedoch nicht immer nach einheitlichen Konfigurationsstandards umgesetzt. Während Endgeräte häufig über Festplattenverschlüsselung verfügen, werden zentrale Fileserver teilweise weiterhin ohne Speicherverschlüsselung betrieben. Ältere Fachanwendungen unterstützen zudem nicht immer moderne kryptographische Verfahren oder nutzen veraltete Protokolle. Bei ausgelagerten Fachanwendungen und Speicherdiensten ist darüber hinaus häufig unklar, welche Verschlüsselungsmechanismen tatsächlich eingesetzt werden, da entsprechende Details beim Dienstleister liegen. Gleichzeitig sind Zuständigkeiten für kryptographische Verfahren und Schlüsselverwaltung zwischen interner IT, Fachämtern und externen Dienstleistern nicht immer eindeutig geregelt.

8.4.1
Erhebung der Ausgangslage

Der erste Schritt besteht in einer strukturierten Bestandsaufnahme aller Fachanwendungen und Dienste, die Daten höherer Schutzklassen – etwa vertraulich oder streng vertraulich – verarbeiten. Ziel dieser Analyse ist es, einen belastbaren Überblick über die tatsächlich eingesetzten kryptographischen Verfahren zu erhalten. Dabei werden insbesondere Transportmechanismen (z. B. verwendete TLS-Versionen, Zertifikatslaufzeiten oder API-Schnittstellen), Verfahren zur Verschlüsselung von Netzlaufwerken, Datenbanken, Speichersystemen und Endgeräten sowie die kryptographischen Funktionen der eingesetzten Fachanwendungen betrachtet. Ebenso ist zu prüfen, ob einzelne Fachanwendungen oder Dienste veraltete Protokolle oder proprietäre Verfahren einsetzen oder bisher keine zeitgemäße Verschlüsselung unterstützen. Ein weiterer Bestandteil der Analyse betrifft ausgelagerte Fachanwendungen und Dienste, bei denen zu klären ist, wie Daten während der Übertragung und Speicherung beim Dienstleister abgesichert werden.

Diese Transparenz ist erforderlich, da in gewachsenen kommunalen IT-Landschaften einzelne Komponenten häufig gut abgesichert sind, während angrenzende Systeme geringere Sicherheitsstandards aufweisen. Ohne eine konsolidierte Bestandsaufnahme besteht daher das Risiko, Sicherheitsmaßnahmen an ungeeigneter Stelle zu priorisieren oder kritische Bereiche unberücksichtigt zu lassen.

8.4.2
Festlegung schutzbedarfsbezogener Mindeststandards

Auf Grundlage dieser Analyse werden verbindliche Mindestanforderungen für die jeweiligen Schutzklassen definiert. Maßgeblich ist dabei die zuvor eingeführte Datenklassifikation. Für Systeme, die vertrauliche Daten verarbeiten, werden Anforderungen an Transport- und Speicherverschlüsselung sowie an abgesicherte Schnittstellen festgelegt. Für streng vertrauliche Daten können zusätzliche Maßnahmen erforderlich sein, etwa verpflichtende Verschlüsselung von Datenbanken und Speichersystemen oder restriktive Regelungen für portable Datenträger.

Die Anforderungen sind dabei möglichst eindeutig und technisch überprüfbar zu formulieren. Anstelle allgemeiner Vorgaben sollten konkrete Festlegungen zu zulässigen Protokollversionen, Cipher-Suites, Zertifikatsmanagement und unterstützten kryptographischen Verfahren erfolgen. Zur dauerhaften Umsetzung werden diese Vorgaben in Architekturleitlinien, Beschaffungsrichtlinien und Dienstleisterverträgen integriert, sodass neue bzw. modernisierte Fachanwendungen und Dienste von Beginn an den definierten Kryptostandards entsprechen.

8.4.3
Risikobasierte Behandlung von Legacy-Systemen

In kommunalen IT-Landschaften stellen Legacy-Systeme häufig einen festen Bestandteil der Infrastruktur dar, sodass eine kurzfristige Umstellung auf aktuelle kryptographische Standards nicht immer möglich ist. In solchen Fällen ist ein risikobasierter Umgang erforderlich. Wenn eine unmittelbare Modernisierung technisch oder organisatorisch nicht

realisierbar ist, werden Kompensationsmaßnahmen eingesetzt, etwa vorgeschaltete TLS-Absicherung über Reverse-Proxys, restriktive Netzsegmentierung, reduzierte Benutzerkreise oder verstärktes Monitoring. Parallel sollte geprüft werden, ob mittelfristig eine Migration oder Ablösung der betroffenen Fachanwendungen und Diensten möglich ist.

8.4.4
Klar geregeltes Schlüsselmanagement

Die Wirksamkeit kryptographischer Verfahren hängt wesentlich vom zugrunde liegenden Schlüsselmanagement ab. In der Praxis sind kryptographische Schlüssel jedoch häufig unzureichend organisiert, etwa durch zentrale Ablagen, unklare Verantwortlichkeiten oder weitreichende Zugriffsrechte für Administratoren. Dadurch können Insider- oder Administrationsrisiken entstehen, selbst wenn technisch aktuelle Verschlüsselungsverfahren eingesetzt werden.

Vor diesem Hintergrund sind klare Zuständigkeiten und Prozesse für das Schlüsselmanagement festzulegen. Für alle Fachanwendungen und Dienste, die Verschlüsselung einsetzen, muss nachvollziehbar geregelt sein, wer Schlüssel erzeugt, verwaltet, speichert und löscht sowie unter welchen Bedingungen ein Zugriff erfolgt. Ergänzend sind verbindliche Regelungen für Rotation, Widerruf und Ersatz kompromittierter Schlüssel zu definieren. Ein zentrales Prinzip besteht in der organisatorischen Trennung von Systemadministration und Schlüsselverwaltung.

Zugriffe auf Schlüsselmaterial sollten regelmäßig überprüft werden. Die sichere Ablage kann beispielsweise über dedizierte Schlüsselmanagementsysteme erfolgen. Besondere Aufmerksamkeit erfordern ausgelagerte Fachanwendungen und Dienste. Hier ist zu klären, wer die kryptographische Kontrolle besitzt und ob der Dienstleister theoretisch oder praktisch Zugriff auf die Schlüssel des Auftraggebers hat. Entsprechende Verantwortlichkeiten und Regelungen sind daher vertraglich eindeutig festzulegen.

8.4.5
Priorisierte Umsetzung

Die Einführung einer schutzbedarfsorientierten Strategie für Verschlüsselung und Schlüsselmananagement erfolgt in der Regel schrittweise. Da eine gleichzeitige Anpassung aller Fachanwendungen und Dienste organisatorisch und technisch kaum realisierbar ist, sollte der Schwerpunkt zunächst auf besonders kritischen Fachanwendungen und Diensten mit hohem Schutzbedarf liegen. Auf dieser Grundlage können übergreifende Standards entwickelt und anschließend sukzessive auf weitere Fachanwendungen und Dienste übertragen werden. Neue IT-Projekte, Beschaffungen und Modernisierungen sollten die definierten Kryptovorgaben von Beginn an berücksichtigen. Dieses Vorgehen trägt der heterogenen und häufig dienstleistergeprägten Struktur kommunaler IT-Landschaften Rechnung und unterstützt eine konsistente Umsetzung kryptographischer Schutzmaßnahmen im Sinne einer datenzentrierten ZTA.

8.5
Einsatz einer resilienten Backup-Strategie

Backups bilden einen zentralen Bestandteil der Resilienz innerhalb der Daten-Säule. Zero-Trust-Referenzmodelle gehen davon aus, dass Systeme kompromittiert werden können und Organisationen daher über belastbare Wiederherstellungsmechanismen verfügen müssen. Für kommunale Verwaltungen ist diese Fähigkeit besonders relevant, da zahlreiche Verwaltungsleistungen – etwa im Meldewesen, in Sozialverfahren oder im Finanzwesen – unmittelbar von der Verfügbarkeit der zugrunde liegenden Daten abhängen.

8.5.1
Analyse der bestehenden Backup-Landschaft

Der Ausgangspunkt für eine resiliente Backup-Strategie ist eine strukturierte Analyse der vorhandenen Sicherungsmechanismen. Ziel ist ein realistisches Gesamtbild darüber, welche Daten tatsächlich gesichert werden, wie Wiederherstellungen erfolgen und welche technischen oder organisatorischen Abhängigkeiten bestehen. In kommunalen IT-Landschaften umfassen diese Sicherungsprozesse häufig verschiedene Fachanwendungen und Dienste mit unterschiedlichen Backup-Lösungen und heterogenen Backup-Konfigurationen. Einige Fachanwendungen verfügen über eigene Sicherungsmechanismen, während bei ausgelagerten Fachanwendungen und Diensten häufig der kommunale IT-Dienstleister die Datensicherung übernimmt. Parallel existieren zentrale Backup-Systeme für Server, Netzlaufwerke, Datenbanken oder virtuelle Infrastrukturen, wodurch eine komplexe Sicherungslandschaft entsteht. Die Situation wird zusätzlich durch Legacy-Systeme erschwert, die teilweise keine modernen Backup-Schnittstellen unterstützen oder sich nur eingeschränkt in zentrale Sicherungssysteme integrieren lassen. In solchen Fällen entstehen häufig individuelle Lösungen, etwa datenbankspezifische Sicherungen oder durch Dienstleister bereitgestellte Backup-Prozesse. Ohne eine systematische Betrachtung kann daher der Eindruck entstehen, dass Daten gesichert sind, obwohl sie außerhalb der zentralen Backup-Strategie liegen.

Die Analyse sollte daher klären, welche Fachanwendungen, Dienste und Datenspeicher tatsächlich in Sicherungsprozesse einbezogen sind und wie diese umgesetzt werden. Dazu gehören auch Informationen zu Aufbewahrungsfristen, Speicherorten, Zugriffskontrollen sowie zu möglichen Abhängigkeiten von Administrationskonten oder zentralen Infrastrukturen. Diese Bestandsaufnahme bildet die Grundlage für den Aufbau einer konsistenten und resilienten Backup-Strategie.

8.5.2
Aufbau einer widerstandsfähigen Backup-Architektur

Auf Basis der vorherigen Analyse wird eine abgestufte Backup-Architektur entwickelt, deren Ziel darin besteht, Sicherungen möglichst unabhängig vom Sicherheitsstatus der Produktivumgebung zu betreiben. Ein zentrales Prinzip ist die logische und organisatorische Trennung von Backup-Infrastruktur und operativem Betrieb. Zugriffsrechte auf Backup-Systeme sollten stark eingeschränkt und getrennt verwaltet werden, um Manipulation oder Missbrauch zu erschweren. Darüber hinaus empfiehlt sich der Einsatz

mehrerer Sicherungsebenen. Neben lokalen Sicherungen können Offsite- oder cloudbasierte Backups eingesetzt werden, um auch bei infrastrukturellen Ausfällen eine Wiederherstellung zu ermöglichen. Für besonders kritische Datenbestände sind unveränderbare Speicherlösungen (sog. *Immutable-Backups*) geeignet, da sie verhindern, dass Sicherungen nachträglich verändert oder gelöscht werden können und insbesondere bei Ransomware-Angriffen eine zusätzliche Schutzschicht darstellen.

Bei ausgelagerten Fachanwendungen, Diensten oder Backup-Diensten sollten entsprechende Anforderungen vertraglich abgesichert werden. Dazu gehören klar definierte Backup-Mechanismen, nachvollziehbare Nachweise erfolgreicher Sicherungen sowie definierte Wiederherstellungsziele und Service-Level-Vereinbarungen.

8.5.3
Ausrichtung von Backup-Strategien am Schutzbedarf

Die zuvor eingeführte Datenklassifikation kann zur gezielten Ausgestaltung von Backup-Strategien genutzt werden. Auf dieser Grundlage lassen sich Backup-Frequenz, Aufbewahrungsdauer und Speichertechnologien am Schutzbedarf der jeweiligen Daten ausrichten. Fachanwendungen mit besonders sensiblen Datenbeständen, etwa im Sozial-, Melde- oder Finanzbereich, erfordern in der Regel kürzere Sicherungsintervalle und zusätzliche Sicherungsebenen, während weniger kritische Daten mit längeren Intervallen gesichert werden können.

Metadaten wie Datenklassifikation, Herkunft oder die Unterscheidung zwischen primären Datenbeständen und Arbeitskopien unterstützen zudem eine effizientere Sicherungsstrategie. Wenn klar definiert ist, welches System die maßgebliche Datenquelle darstellt, müssen identische Inhalte nicht mehrfach vollständig gesichert werden. Darüber hinaus erleichtert die Klassifikation die Abgrenzung zwischen Backup- und Archivierungszwecken sowie die Priorisierung von Wiederherstellungsmaßnahmen im Störungsfall. Der Aufbau einer resilienten Backup-Strategie hilft maßgeblich dabei, die Wiederanlauffähigkeit kommunaler IT-Infrastrukturen sicherzustellen.

8.6
Verankerung von Wiederherstellungstests

Neben der Erstellung von Backups stellt die Fähigkeit zur Wiederherstellung von Daten, Fachanwendungen und Diensten einen zentralen Bestandteil der Resilienz einer ZTA. CISA und DoD betonen in der Daten-Säule, dass klar definierte Wiederherstellungsziele und regelmäßig getestete Recovery-Verfahren ein wichtiges Reifegradmerkmal darstellen [CIS23][DoD22b].

Auch wenn Wiederherstellung eng mit dem Thema Backup verbunden ist, erfordert ihre praktische Bedeutung eine eigenständige Betrachtung. Backups allein garantieren noch keine funktionierende Wiederherstellung. Erst wenn klar ist, wie Daten, Fachanwendungen und Dienste im Ernstfall tatsächlich zurückgeführt werden, kann von einer belastbaren Resilienzstrategie gesprochen werden. Für Kommunen und Landkreise ist eine verlässliche Wiederanlauffähigkeit besonders relevant, da zahlreiche Fachverfahren unmittelbar mit gesetzlichen Aufgaben und Bürgerleistungen verbunden sind.

8.6.1 Fachliche und technische Festlegung der Wiederherstellungsziele

Ein erster Schritt besteht darin, für priorisierte Fachanwendungen und zentrale Datenbestände verbindliche Wiederherstellungsziele festzulegen. Hierzu gehören insbesondere Recovery-Time-Objectives (RTO) und Recovery-Point-Objectives (RPO) (vgl. [BSI23b]), also die maximal tolerierbare Wiederanlaufzeit sowie der maximal akzeptable Datenverlust.

Diese Ziele sollten nicht ausschließlich technisch definiert werden, sondern in Abstimmung mit den zuständigen Fachämtern erfolgen. In der Praxis zeigt sich häufig, dass fachliche Erwartungen an Wiederherstellungszeiten von den vorhandenen technischen Möglichkeiten abweichen. Der Abgleich zwischen fachlicher Kritikalität und realen Infrastruktur- und Backup-Kapazitäten ist daher ein wichtiger Schritt zur Definition belastbarer Wiederherstellungsziele.

8.6.2 Definition von Wiederherstellungsprozessen

Auf dieser Grundlage werden konkrete Wiederherstellungsprozesse definiert und dokumentiert. Dazu gehört die Festlegung, wer im Schadensfall über eine Wiederherstellung entscheidet, welche Datenstände bevorzugt genutzt werden und wie verhindert wird, dass bereits kompromittierte Daten – etwa nach einem Ransomware-Angriff – wiederhergestellt werden. Recovery-Prozesse müssen zudem mit bestehenden Incident-Response- und Notfallprozessen abgestimmt werden. Bei Cyberangriffen können zunächst forensische Analysen erforderlich sein, während gleichzeitig ein hoher Druck besteht, zentrale Fachanwendungen und deren Daten möglichst schnell wieder verfügbar zu machen. Bei der Wiederherstellung der Fachanwendungen und Dienste ist inbesondere zu berücksichtigen, auf welcher IT-Infrastruktur eine Wiederherstellung erfolgen soll, abhängig von der Art des Vorfalls (z. B. Hardware-Ausfall oder Cyberangriff).

8.6.3 Durchführung regelmäßiger praktischer Wiederherstellungstests

Ein wesentlicher Bestandteil einer belastbaren Recovery-Strategie sind regelmäßige Wiederherstellungsübungen. Erst praktische Tests zeigen, ob Backup-Daten nutzbar sind, Wiederherstellungsprozesse funktionieren und organisatorische Abläufe ausreichend klar definiert sind. Solche Übungen sollten sich zunächst auf besonders kritische Fachanwendungen konzentrieren und sowohl technische als auch organisatorische Aspekte einbeziehen. Regelmäßige Tests helfen, Schwachstellen frühzeitig zu erkennen und Prozesse

kontinuierlich zu verbessern. Sie tragen zudem dazu bei, dass Verantwortliche im Ernstfall mit den Abläufen vertraut sind und Entscheidungen schneller getroffen werden können. Eine resiliente Backup-Strategie entfaltet ihren Nutzen daher erst dann vollständig, wenn auch die Wiederherstellung systematisch geplant, dokumentiert und regelmäßig getestet wird.

8.7 Fortgeschrittene Maßnahmen

Aufbauend auf den zuvor dargestellten initialen Umsetzungsschritten sollten fortgeschrittene Maßnahmen erfolgen, die auf einen höheren Reifegrad der Daten-Säule innerhalb einer ZTA abzielen.

Data-Security-Monitoring und Data-Loss-Prevention. Mit zunehmendem Reifegrad wird eine kontinuierliche Überwachung von Datenzugriffen und Datenbewegungen erforderlich. Ziel ist die frühzeitige Erkennung ungewöhnlicher Nutzungsaktivitäten oder potenzieller Datenabflüsse, etwa durch unzulässige externe Weitergaben, massenhafte Modifikationen von Daten, Massendownloads sensibler Daten oder Uploads in nicht freigegebene Cloud-Dienste. Ein pragmatischer Einstieg konzentriert sich auf zentrale Kommunikationskanäle wie E-Mail, Dateispeicher-Dienste, Kollaborationsplattformen sowie definierte Exportpfade und Kommunikationsschnittstellen von Fachanwendungen und Diensten. Auf Basis der Datenklassifikation können Regeln eingerichtet werden, die risikobehaftete Aktionen erkennen oder blockieren. Technisch erfolgt dies typischerweise über DLP-Funktionen vorhandener Plattformen sowie über SIEM-Systeme zur Auswertung entsprechender Ereignisse.

Software-Defined Storages. Mit zunehmendem Reifegrade sollte auch die Speicherarchitektur stärker an Zero-Trust-Prinzipien ausgerichtet werden. Software-Defined Storage (SDS) ermöglicht eine zentrale und policybasierte Steuerung von Speicherpools, Verschlüsselung und Backup-Mechanismen. Anforderungen aus der Datenklassifikation können hierdurch automatisiert umgesetzt werden. Die Einführung erfolgt typischerweise schrittweise, etwa durch Konsolidierung bestehender Speicherlösungen, Integration mit Identitäts- und Klassifikationssystemen sowie die Definition standardisierter Speicherprofile. SDS kann die technische Durchsetzung von Speicher-Policies unterstützen, ersetzt jedoch keine übergeordnete Data-Governance.

Data-Governance-Modell mit Dienstleistern und Fachämtern. Für eine nachhaltige Umsetzung der Daten-Säule sind klare Governance-Strukturen erforderlich. Zuständigkeiten zwischen Fachämtern, interner IT und kommunalen Dienstleistern müssen verbindlich geregelt sein, damit technische Maßnahmen organisatorisch wirksam werden. Ein entsprechendes Data-Governance-Modell legt fest, wer für Schutzbedarfsbewertungen, Datenklassifikation, Aufbewahrungsfristen, Datenexporte und Entscheidungen im Sicherheitsvorfall verantwortlich ist. Anforderungen an Verschlüsselung, Logging, Backup/Recovery und Monitoring können anschließend schrittweise in Verträge, Leistungsbeschreibungen und Service-Level-Agreements integriert werden, um deren Umsetzung auch im laufenden Betrieb nachvollziehbar sicherzustellen.

Daten in Test- und Analyseumgebungen. Test- und Analyseumgebungen können ein erhöhtes Risiko darstellen, wenn dort Produktivdaten verwendet werden. Ziel ist daher eine möglichst weitgehende Vermeidung sensibler Daten in solchen Umgebungen. Entsprechende Szenarien entstehen in kommunalen IT-Landschaften beispielsweise bei Updates von Fachanwendungen, Migrationen oder Fehleranalysen. Produktivdaten sollten nur in begründeten Ausnahmefällen eingesetzt werden, während in der Regel maskierte, pseudonymisierte oder synthetische Daten verwendet werden. Auch kommunale IT-Dienstleister sollten Test- und Migrationsumgebungen grundsätzlich mit anonymisierten Daten betreiben. Ausnahmen sind zu begründen und zeitlich zu begrenzen.

9
Zusammenfassung

Kommunale Verwaltungen stehen seit einigen Jahren verstärkt im Fokus von Cyberangriffen. Ransomware-Kampagnen und gezielte Angriffe auf öffentliche Einrichtungen gehören inzwischen zum Alltag. Gleichzeitig entstehen – unter anderem getrieben durch Digitalisierung, mobile Arbeitsformen und die Einbindung kommunaler IT-Dienstleister – immer mehr Möglichkeiten für Angreifer, in die IT-Systeme einzudringen. IT-Systeme werden offener und vernetzter, wodurch es schwieriger wird, den Überblick zu behalten und Sicherheitsmaßnahmen konsistent umzusetzen. Hinzu kommen oftmals begrenzte personelle Kapazitäten und enge Haushaltsrahmen.

Vor diesem Hintergrund gewinnt der Zero-Trust-Ansatz als Weiterentwicklung klassischer Sicherheitsmodelle zunehmend an Relevanz. Dabei handelt es sich nicht um ein einzelnes Sicherheitsfeature, sondern um ein grundlegendes Sicherheitsparadigma. Während klassische Modelle oft davon ausgehen, dass innerhalb des eigenen Netzwerks ein gewisses Vertrauen besteht, stellt Zero-Trust genau diese Annahme infrage. Vertrauen wird nicht vorausgesetzt, sondern muss bei jedem Zugriff erneut verdient werden. Dies lässt sich anschaulich mit einem Gebäude vergleichen: In traditionellen Modellen genügt eine Zugangskontrolle am Eingang. Wer diese passiert hat, kann sich im Inneren meist frei bewegen. Zero-Trust funktioniert anders. Jede Tür bleibt gesichert. Für jeden Raum wird erneut geprüft, ob ein Zutritt zulässig ist – abhängig von Identität, Aufgabe, Situation und Kontext. Übertragen auf die IT bedeutet das: Anwendungen liegen heute häufig außerhalb der eigenen Infrastruktur, Benutzer greifen aus unterschiedlichen Umgebungen auf Systeme zu und Geräte wechseln regelmäßig ihren Einsatzort. Angriffe erfolgen dabei oft nicht über den äußeren Netzrand, sondern über kompromittierte Konten oder bereits vorhandene Zugänge. Genau hier setzt Zero-Trust an. Jeder Zugriff wird einzeln bewertet, es gibt mehrere Prüfschichten, die ineinandergreifen, und Faktoren wie Identität, Gerätezustand und Nutzungskontext werden fortlaufend berücksichtigt.

Der Nutzen von Zero-Trust zeigt sich unmittelbar in der Resilienz gegenüber Cyberangriffen. Zero-Trust-Maßnahmen erschweren erfolgreiche Angriffe und begrenzen gleichzeitig deren Auswirkungen. Zero-Trust folgt bewusst dem Prinzip „Assume Breach“ – ein erfolgreicher Angriff wird einkalkuliert. IT-Infrastrukturen werden durch die Einführung von Zero-Trust resilienter und so gestaltet, dass sich Angreifer möglichst wenig ausbreiten können und kritische Bereiche geschützt bleiben. Die Einführung von Zero-Trust kann dazu beitragen, die Resilienz kommunaler IT-Infrastrukturen gegenüber Cyberangriffen deutlich zu erhöhen. Die gesteigerte Resilienz führt wiederum dazu, dass Angriffe seltener erfolgreich sind, sich deren Auswirkungen weniger stark ausbreiten und Ausfallzeiten verkürzt werden können. Im Ernstfall kann genau dies den Unterschied machen: Sind nur einzelne kommunale Fachverfahren kurzfristig eingeschränkt oder fallen zentrale Verwaltungsprozesse über Tage oder Wochen aus?

Die vorliegende Handreichung greift den Zero-Trust-Ansatz auf und überträgt ihn in die kommunale Praxis. Sie beschreibt die Einführung einer Zero-Trust-Architektur (ZTA) anhand konkreter Umsetzungsschritte mit denen bestehende IT-Sicherheitsstrukturen schrittweise weiterentwickelt werden können. Die Darstellung versteht sich als praxisorientierte Guideline. Sie bündelt zentrale Handlungsfelder und skizziert erste Maßnahmen für einen Transformationsprozess, der in der Praxis meist über mehrere Jahre verläuft, aber bereits mit einzelnen Maßnahmen spürbare Verbesserungen der Resilienz erreichen kann.

Die Einschätzungen in dieser Handreichung stützen sich unter anderem auf fünf Experteninterviews mit Vertretern aus hessischen Kommunen und Landkreisen. Ergänzend wurden einschlägige Fachpublikationen sowie technische Leitlinien ausgewertet. Adressiert werden vor allem IT-Leitungen und IT-Sicherheitsverantwortliche kommunaler Verwaltungen. Die inhaltliche Orientierung folgt etablierten Referenzmodellen internationaler Organisationen – insbesondere NIST, CISA, DoD und das BSI. Deren grundlegende Prinzipien werden auf die organisatorischen und technischen Rahmenbedingungen kommunaler IT-Strukturen übertragen. Zu diesem Zweck werden praktikable, technikneutrale Einstiegsschritte vorgeschlagen. Wie diese konkret umgesetzt werden, hängt zwangsläufig von den jeweiligen organisatorischen und technischen Gegebenheiten einer Kommune ab.

9.1 Rahmenbedingungen kommunaler IT-Landschaften

Kommunale IT-Strukturen zeigen ein wiederkehrendes Muster: hohe Heterogenität. Die Ursachen liegen meist weit zurück. Systeme wurden über Jahre ergänzt, Fachverfahren sukzessive eingeführt, ältere Fachanwendungen selten vollständig abgelöst. Daraus entstehen Systemlandschaften, die aus unterschiedlichsten Technologien bestehen, von modernen Webanwendungen bis zu langjährig betriebenen Legacy-Systemen.

Auch die Zusammensetzung der Fachanwendungen variiert erheblich. Zwei benachbarte Kommunen können völlig unterschiedliche Softwareportfolios betreiben. Viele Kommunen sind zudem eng mit kommunalen IT-Dienstleistern oder externen Anbietern verflochten. Diese betreiben Teile der Infrastruktur oder stellen zentrale Fachanwendungen bereit. Daraus entstehen zusätzliche technische und organisatorische Abstimmungsprozesse. IT-Verwaltungsprozesse wirken häufig fragmentiert. Besonders sichtbar wird das im Identitäts- und Berechtigungsmanagement. Benutzerkonten entstehen in mehreren Systemen parallel, Onboarding- und Offboarding-Prozesse verlaufen nicht immer konsistent. Das erhöht den administrativen Aufwand und erschwert eine einheitliche Umsetzung von Sicherheitsrichtlinien.

Kleinere Kommunen stehen zusätzlich vor einer nüchternen Realität: begrenztes Personal, begrenzte Budgets. Der Aufbau moderner Sicherheitsarchitekturen wie einer ZTA konkurriert dort mit zahlreichen anderen IT-Aufgaben. Ein weiterer Faktor wird in technischen Konzeptpapieren oft unterschätzt: die Nutzer. Veränderungen an

Sicherheitsarchitekturen greifen unmittelbar in Arbeitsabläufe ein. Beschäftigte in der Verwaltung und IT-Administratoren müssen mit neuen Authentifizierungsverfahren, geänderten Zugriffswegen oder zusätzlichen Kontrollmechanismen arbeiten. Ohne ihre Einbindung entstehen schnell Akzeptanzprobleme.

Diese strukturellen Rahmenbedingungen sind kein Randaspekt. Sie definieren den Ausgangspunkt jeder realistischen Zero-Trust-Transformation im kommunalen Umfeld.

9.2 Überblick über die Umsetzungsschritte in den fünf technischen Säulen

Die vorgeschlagenen Maßnahmen orientieren sich an fünf technischen Säulen einer Zero-Trust-Architektur: Identitäten, Geräte, Netzwerke, Workloads & Apps sowie Daten. Für jede Säule werden erste Umsetzungsschritte beschrieben, die sich als Einstieg in eine schrittweise ZTA-Einführung eignen.

In der Säule Identität beginnt der Prozess mit Transparenz. Zunächst muss klar sein, welche digitalen Identitäten überhaupt existieren. Dazu gehört ein konsolidiertes Benutzerinventar, das alle Benutzerkonten. Auf dieser Grundlage folgen Maßnahmen zur Stärkung der Authentifizierung. Multi-Faktor-Authentifizierung und Single-Sign-On gehören hier zu den zentralen Bausteinen. Parallel dazu rückt das Berechtigungsmanagement in den Fokus – etwa durch konsequente Anwendung des Least-Privilege-Prinzips und durch einen kontrollierten Umgang mit privilegierten Konten. Die Geräte-Säule richtet den Blick auf die vorhandenen Endgeräte. Ohne vollständige Inventarisierung bleibt jede Sicherheitsstrategie lückenhaft. Erst wenn bekannt ist, welche Geräte im Netzwerk aktiv sind, lassen sich strukturierte Onboarding- und Offboarding-Prozesse etablieren. Darauf bauen weitere Maßnahmen auf: Endpoint-Schutz, Protokollierung sicherheitsrelevanter Ereignisse, regelmäßige Updates und ein kontinuierliches Schwachstellenmanagement. In der Netzwerk-Säule stehen Segmentierung und Überwachung im Mittelpunkt. Klassische Netzwerksegmentierung bildet häufig den Einstieg. Moderne Ansätze – etwa softwarebasierte Netzwerksteuerung oder Mikrosegmentierung – erweitern diese Konzepte. Ergänzt wird dies durch Mechanismen zur Netzwerküberwachung sowie durch Netzwerkzugangskontrollen. Die Säule Workloads & Apps adressiert vor allem die Absicherung eingesetzter Fachverfahren und Dienste. Zugriffskontrollen auf Anwendungsebene spielen hier eine zentrale Rolle. Hinzu kommen Protokollierungsmechanismen sowie organisatorische und technische Maßnahmen für Wartung, Updates und Lieferkettensicherheit. Die Daten-Säule beginnt ebenfalls mit Transparenz. Ein belastbares Dateninventar schafft Überblick über vorhandene Datenbestände. Darauf aufbauend lassen sich Datenflüsse analysieren, Schutzbedarfe definieren und geeignete Verschlüsselungsmechanismen festlegen. Ebenso wichtig sind belastbare Backup- und Wiederherstellungsprozesse.

In allen fünf Säulen werden neben diesen initialen Maßnahmen auch weiterführende Schritte skizziert. Sie bauen auf den beschriebenen Grundlagen auf und ermöglichen eine schrittweise Weiterentwicklung der Sicherheitsarchitektur.

9.3 Gemeinsame konzeptionelle Ziele der Umsetzungsschritte

Ein Blick über alle fünf Säulen hinweg zeigt wiederkehrende Strukturen. Der erste Schritt ist immer eine Bestandsaufnahme. Ohne belastbare Übersicht über Identitäten, Geräte, Netzwerke, Anwendungen oder Daten bleibt jede Sicherheitsstrategie fragmentarisch. Sichtbarkeit bildet die Grundlage jeder ZTA. Darauf folgt häufig eine Phase der Konsolidierung. Strukturen, die über Jahre fragmentiert gewachsen sind, werden vereinheitlicht. Beispiele finden sich in nahezu allen Bereichen: zentrale Identitätsverwaltung, standardisierte Geräteverwaltung, strukturierte Netzwerksegmentierung oder konsistente Datenklassifikation.

Weitere wiederkehrende Ziele betreffen die Zentralisierung sowie die konsistente Durchsetzung definierter Sicherheitsrichtlinien. In vielen Umsetzungsschritten zeigt sich, dass Managementfunktionen, Zugriffsentscheidungen und Monitoring zunehmend zentral gebündelt werden – etwa durch ein zentrales Identitäts- und Berechtigungsmanagement (IAM) sowie durch übergreifende Lösungen für Netzwerk- und Gerätemanagement. Ziel ist es, Zuständigkeiten zu vereinheitlichen und sicherheitsrelevante Entscheidungen nachvollziehbar und konsistent zu treffen.

Eng damit verknüpft ist die regelbasierte Durchsetzung von Sicherheitsanforderungen. Zugriffsregeln werden zentral definiert und dynamisch angewendet, wobei Prinzipien wie Least Privilege, Netzwerkzugangskontrollen oder compliance-basierte Entscheidungslogiken eine zentrale Rolle einnehmen. Sicherheitsrichtlinien werden damit nicht nur festgelegt, sondern technisch und kontinuierlich überprüft. Monitoring und Protokollierung ergänzen diese Ansätze. Die kontinuierliche Beobachtung sicherheitsrelevanter Ereignisse ermöglicht es, Auffälligkeiten frühzeitig zu erkennen, während die systematische Protokollierung die Grundlage für Incident-Response-Maßnahmen sowie für die Bewertung der Wirksamkeit bestehender Sicherheitskontrollen schafft.

Schließlich tritt in vielen Säulen der Aspekt Resilienz deutlich hervor. In der Daten-Säule durch robuste Backup-Architekturen, klar definierte Wiederherstellungsprozesse und regelmäßige Wiederherstellungstests. In den Säulen Workload & Apps, Netzwerk und Geräte liefern die dort verankerten Isolierungsmechanismen im Schadfall einen wesentlichen Beitrag zur Resilienz.

9.4 Umsetzung der vorgeschlagenen Maßnahmen

Die in dieser Handreichung beschriebenen Maßnahmen folgen bewusst einem schrittweisen Ansatz. Eine ZTA entsteht nicht durch ein einzelnes Projekt. Sie entwickelt sich über mehrere Iterationen hinweg – technisch, organisatorisch und oft auch kulturell. Gerade deshalb besitzen kleinere Schritte einen realen Effekt. Verbesserungen bei

Authentifizierungsverfahren, erste Netzwerksegmentierungen oder eine konsolidierte Geräteverwaltung können das Sicherheitsniveau bereits spürbar erhöhen. Der schrittweise Ansatz reduziert außerdem operative Risiken. Veränderungen lassen sich kontrolliert einführen und an bestehende Betriebsprozesse anpassen.

Gleichzeitig bleibt eine Einschränkung unvermeidlich. Die beschriebenen Maßnahmen lassen sich selten unverändert übernehmen. Kommunale IT-Umgebungen unterscheiden sich erheblich – in ihrer technischen Infrastruktur, ihren organisatorischen Strukturen und im Reifegrad vorhandener Sicherheitsmaßnahmen. Die dargestellten Umsetzungsschritte sind daher bewusst technikneutral formuliert. Sie liefern Orientierungspunkte. Die konkrete Ausgestaltung erfolgt vor Ort – mit geeigneten Produkten, Diensten oder betrieblichen Verfahren.

Viele Kommunen verfügen bereits über etablierte Sicherheitsmechanismen. Authentifizierungssysteme, segmentierte Netzwerke oder Backup-Strategien existieren häufig auch schon. In solchen Fällen liegt der pragmatische Weg nicht im vollständigen Neubau der Sicherheitsarchitektur, sondern in der Weiterentwicklung vorhandener Strukturen.

9.5 Bedeutung für zukünftige IT-Modernisierung

Die beschriebenen Maßnahmen betreffen nicht nur bestehende Infrastrukturen. Sie liefern auch einen Referenzrahmen für zukünftige Modernisierungs- und Beschaffungsentscheidungen. Typische Situationen sind der Ersatz älterer Systeme, Migrationen von lokal betriebenen Fachverfahren zu Diensten kommunaler IT-Dienstleister oder die Erneuerung zentraler Infrastrukturkomponenten wie Firewalls, Router Netzwerkmanagementlösungen oder Identitätsmanagementsysteme.

Neuanschaffungen sollten daraufhin geprüft werden, ob sie die Umsetzung von Zero-Trust-Prinzipien und die vorgeschlagenen Umsetzungsschritte unterstützen. Hier wirken die vorgeschlagenen Umsetzungsschritte wie ein Filter. Neue Technologien und potentielle Dienste externe Dienstleister lassen sich daran messen, ob sie zentrale Anforderungen einer ZTA unterstützen: starke Authentifizierung, feingranulare Zugriffskontrollen, Netzwerksegmentierung, belastbares Monitoring oder strukturierte Datenklassifikation. Produkte und Dienste, die diese Prinzipien bereits technisch unterstützen, erleichtern spätere Entwicklungsschritte erheblich.

9.6 Fazit

Die Einführung einer Zero-Trust-Architektur bedeutet für Kommunen und Landkreise eine langfristige Weiterentwicklung ihrer Sicherheitsstrukturen. Parallel zur Digitalisierung kommunaler Verwaltungsprozesse wächst auch die Angriffsfläche. Öffentliche Verwaltungen stehen längst im Fokus organisierter Cyberangriffe wie Ransomware-Kampagnen.

Die in dieser Handreichung beschriebenen Umsetzungsschritte liefern einen strukturierten Einstieg. Entlang der fünf technischen Säulen lassen sich bestehende Sicherheitsmechanismen gezielt weiterentwickeln und neue Kontrollmechanismen schrittweise integrieren. Der Transformationsprozess ist jedoch langwierig. Einzelne Maßnahmen können dennoch bereits spürbare Effekte erzeugen – insbesondere bei Authentifizierung, Netzwerksegmentierung, Geräteverwaltung und Datensicherung. Genau dort entscheidet sich oft, wie widerstandsfähig eine kommunale IT-Infrastruktur im Ernstfall tatsächlich ist.

10
Abkürzungen

2FA	Zwei-Faktor-Authentifizierung
ABAC	Attribute-based Access Control
ACL	Access Control List
AD	Active Directory
AH	Accepting Host
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
C2C	Comply-to-Connect
CISA	U.S. Cybersecurity & Infrastructure Security Agency
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DMZ	Demilitarized Zone
DoD	U.S. Department of Defense
DoS	Denial of Service
DLP	Data Loss Prevention
DPI	Deep Packet Inspection
DSGVO	Datenschutz-Grundverordnung
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
FIDO2	Fast Identity Online 2
IAM	Identity and Access Management
ID	Identität bzw. Identifikator

IdP	Identity Provider
IDS	Intrusion Detection System
IH	Initiating Host
IKZ	Interkommunale Zusammenarbeit
IPS	Intrusion Prevention System
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik bzw.-technologie
LDAP	Lightweight Directory Access Protocol
M365	Microsoft 365
MAB	MAC Authentication Bypass
MAC	Media Access Control
MDM	Mobile Device Management
MFA	Multi-Faktor-Authentifzierung
ML	Machine Learning
mTLS	Mutual Transport Layer Security
NAC	Network Access Control
NIST	U.S. National Institute of Standards and Technology
OIDC	OpenID Connect
OTP	One-Time Password
PAM	Privileged Access Management
PAP	Policy Administration Point
PAW	Privileged Access Workstation
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIN	Personal Identification Number
PIP	Policy Information Point

PKI	Public Key Infrastructure
PXE	Preboot Execution Environment
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-based Access Control
RDP	Remote Desktop Protocol
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SaaS	Software-as-a-Service
SAML	Security Assertion Markup Language
SDN	Software Defined Networking
SDP	Software Defines Perimeter
SIEM	Security Information and Event Management
SMS	Short Message Service
SPA	Single Packet Authentication
SSO	Single Sign On
TAN	Transaktionsnummer
TLS	Transport Layer Security
UUID	Universally Unique Identifier
VPN	Virtuelles privates Netzwerk
WiBA	Weg in die Basis-Absicherung
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
ZT	Zero-Trust
ZTA	Zero-Trust-Architektur
ZTNA	Zero Trust Network Access

Literatur

[ANS04] American National Standard for Information Technology ANSI. *ANSI INCITS 359-2004 – Role Based Access Control*. Information Technology Industry Council, Feb. 2004.

[BBS23] Bundesinstitut für Bau-, Stadt- und Raumforschung BBSR. *Datenstrategien in Kommunen: Handlungsempfehlungen zur praktischen Umsetzung*. ISBN 978-3-98655-043-1, https://www.smart-city-dialog.de/system/files/media/1191/1707898632/SmartCities_BBSR_Fachpublikation_Datenstrategien_final.pdf (Abgerufen: 02.07.2026). Juli 2023.

[BSI21] Bundesamt für Sicherheit in der Informationstechnik BSI. *Kritische Schwachstelle in Java-Bibliothek Log4j*. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Schwachstelle-log4Shell-Java-Bibliothek/log4j-schwachstelle/log4j_node.html (Abgerufen: 02.07.2026). 2021.

[BSI23a] Bundesamt für Sicherheit in der Informationstechnik BSI. *Baustein ORP.4 Identitäts- und Berechtigungsmanagement, IT-Grundschutz, Edition 2023*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2023.html (Abgerufen: 02.07.2026). Feb. 2023.

[BSI23b] Bundesamt für Sicherheit in der Informationstechnik BSI. *BSI-Standard 200-4: Business Continuity Management, Version 1.0*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf (Abgerufen: 02.07.2026). Juni 2023.

[BSI23c] Bundesamt für Sicherheit in der Informationstechnik BSI. *IT-Grundschutz-Kompendium*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (Abgerufen: 02.07.2026). Feb. 2023.

[BSI23d] Bundesamt für Sicherheit in der Informationstechnik BSI. *IT-Grundschutz-Profil – Basis-Absicherung Kommunalverwaltung*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html (Abgerufen: 02.07.2026). Nov. 2023.

[BSI23e] Bundesamt für Sicherheit in der Informationstechnik BSI. *Positionspapier Zero Trust 2023*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.pdf?__blob=publicationFile&v=4 (Abgerufen: 02.07.2026). Juni 2023.

[BSI23f] Bundesamt für Sicherheit in der Informationstechnik BSI. *Weg in die Basisabsicherung (WiBA) – Vorgehensweise*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/WIBA/Weg_in_die_Basis_Absicherung_WiBA_node.html (Abgerufen: 02.07.2026). 2023.

[BSI25] Bundesamt für Sicherheit in der Informationstechnik BSI. *Technical Guideline BSI TR-03183: Cyber Resilience Requirements for Manufacturers and Products — Part 2: Software Bill of Materials (SBOM)*. 2025.

[CIS23] Cybersecurity and Infrastructure Security Agency CISA. *Zero Trust Maturity Model, Version 2.0*. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf (Abgerufen: 02.07.2026). Apr. 2023.

[DoD22a] Department of Defense DoD. *DoD Zero Trust Strategy*. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf (Abgerufen: 02.07.2026). Okt. 2022.

[DoD22b] Department of Defense DoD. *Zero Trust Reference Architecture, Version 2.0*. https://dodcio.defense.gov/Portals/0/Documents/Library/%28U%29ZT_RA_v2.0%28U%29_Sep22.pdf (Abgerufen: 02.07.2026). Juli 2022.

[Elf23] Elfnullelf GmbH. *Initiative K: Studie zur Rolle von Zero Trust in deutschen Kommunen*. https://initiative-k.org/ergebnisse-zero-trust-studie-in-kommunen/ (Abgerufen: 02.07.2026). Feb. 2023.

[ENI25] European Union Agency for Cybersecurity ENISA. *ENISA Threat Landscape 2025*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (Abgerufen: 02.07.2026). Okt. 2025.

[KNS25] Michael Kreutzer, Javor Nikolov und Kirstin Scheel. *Zero Trust Roadmap Hessen, Reifegradhärtung des Landes Hessen durch (stufenweise) Einführung einer Zero Trust Architektur*. Feb. 2025.

[Mic25] Microsoft. *Privileged Access: Enterprise-Zugriffsmodell, Version vom 27.3.2025*. https://learn.microsoft.com/de-de/security/privileged-access-workstations/privileged-access-access-model (Abgerufen: 02.07.2026). März 2025.

[NIS20] National Institute of Standards and Technology NIST. *NIST Special Publication 800-207: Zero Trust Architecture*. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf (Abgerufen: 02.07.2026). Aug. 2020.

[NIS21] National Institute of Standards and Technology NIST. *NIST Special Publication 800-204B: Attribute-based Access Control for Microservices-based Applications Using a Service Mesh*. https://doi.org/10.6028/NIST.SP.800-204B (Abgerufen: 02.07.2026). Aug. 2021.

[Sch25] Alexander Schaeff. *ekom21 – Vom IT-Dienstleister zum Integrator*. Kommune 21, https://www.kommune21.de/k21-meldungen/vom-it-dienstleister-zum-integrator/ (Abgerufen: 02.07.2026). Okt. 2025.

A
Anhang A:
Verzeichnis vorgeschlagener Umsetzungsschritte

In diesem Anhang sind alle vorgeschlagenen initialen Umsetzungsschritte und fortgeschrittenen Maßnahmen jeder Säule in Listenform inklusive Referenzen zu den Abschnitten, in denen die jeweiligen Umsetzungsschritte beschrieben wurden, aufgeführt.

A.1
Säule Identität

Initiale Umsetzungsschritte: Thema Identitäten und Authentifizierung (Abschnitt 4.1)

- Benutzerinventar (Abschnitt 4.1.1)
- Multi-Faktor-Authentifizierung (MFA) (Abschnitt 4.1.2)
- Single-Sign-On (SSO) (Abschnitt 4.1.3)

Initiale Umsetzungsschritte: Thema Berechtigungen und Zugriffskontrolle (Abschnitt 4.2)

- Management von Berechtigungen und Least-Privilege (Abschnitt 4.2.1)
- Zugriffsmanagement für privilegierte Accounts (Abschnitt 4.2.2)

Fortgeschrittene Maßnahmen (Abschnitt 4.3)

- Zentrales und integriertes Identitäts- und Berechtigungsmanagement
- Übergreifende ZTA-Berechtigungsarchitektur
- Kontinuierliche Authentifizierung
- Dynamische Kontexte
- Identitätsanbieter und föderierte Identitäten
- Privileged-Access-Management (PAM)

A.2
Säule Geräte

Initiale Umsetzungsschritte: Thema Inventarisierung (Abschnitt 5.1)

- IT-Asset-Management (Abschnitt 5.1.1)
- Onboarding (Abschnitt 5.1.2)
- Offboarding (Abschnitt 5.1.3)

Initiale Umsetzungsschritte: Thema Überprüfung, Monitoring und Kontrolle (Abschnitt 5.2)

- Endgeräte-Schutz (Abschnitt 5.2.1)
- Schutz mobiler Endgeräte (Abschnitt 5.2.2)

Fortgeschrittene Maßnahmen (Abschnitt 5.3)

- Comply-to-Connect (C2C) auf Geräteebene mit EDR-Agenten

A.3 Säule Netzwerk

Initiale Umsetzungsschritte: Thema Segmentierung (Abschnitt 6.1)

- Makrosegmentierung (Abschnitt 6.1.1)
- Software Defined Networks (SDN) (Abschnitt 6.1.2)
- Software Defined Perimeters (SDP) (Abschnitt 6.1.3)

Initiale Umsetzungsschritte: Thema Intrusion Detection & Prevention (IDS/IPS) (Abschnitt 6.2)

- Statische und dynamische Filterregeln (Abschnitt 6.2.1)
- Nutzung von Machine-Learning-Methoden (Abschnitt 6.2.2)

Initiale Umsetzungsschritte: Thema Netzwerkzugangskontrolle (Abschnitt 6.3)

- Lokale Zugangskontrolle (Abschnitt 6.3.1)
- Sicherer Fernzugriff (Abschnitt 6.3.2)

Fortgeschrittene Maßnahmen (Abschnitt 6.4)

- Comply-to-Connect (C2C) auf Netzwerkebene

A.4 Säule Workload & Apps

Initiale Umsetzungsschritte: Thema Software-Verwaltung und Software-Sicherheit (Abschnitt 7.1)

- Inventarisierung und Verteilung von Software (Abschnitt 7.1.1)
- Wartung von Software: Priorisierung, Server-Software (Abschnitt 7.1.2)
- Lieferkettensicherheit: Monitoring von Bibliotheken und Laufzeitumgebungen (Abschnitt 7.1.3)

Initiale Umsetzungsschritte: Thema Zugriffskontrolle bei Netzwerk-Diensten (Abschnitt 7.2)

- Agent-Gateway (Abschnitt 7.2.1)
- Enclave-Gateway (Abschnitt 7.2.2)
- Interne vs. externe Dienste (Abschnitt 7.2.3)

Initiale Umsetzungsschritte: Thema Protokollierung und Auswertung (Abschnitt 7.3)

- Protokollierung (Logging) von kritischen Anwendungen aktivieren
- Regelmäßige Prüfung von Logs auf sicherheitskritische oder verdächtige Ereignisse

Fortgeschrittene Maßnahmen (Abschnitt 7.4)

- Einsatz eines SIEM-Systems (Security Information and Event Management)
- Automatische Auswertung von SBOMs für Lieferkettensicherheit

A.5 Säule Daten

Initiale Umsetzungsschritte: Thema Aufbau eines Dateninventars mit klarer Datenverantwortung (Abschnitt 8.1)

- Erstellung eines Dateninventars (Abschnitt 8.1.1)
- Zuordnung der fachlichen und technischen Datenverantwortung (Abschnitt 8.1.2)

Initiale Umsetzungsschritte: Thema Einheitliche Datenklassifizierung und Schutzniveaus (Abschnitt 8.2)

- Schutzklassen und Mindestanforderungen an Sicherheitsmaßnahmen (Abschnitt 8.2.1)
- Metadaten (Abschnitt 8.2.2)
- Technische Umsetzung der Datenklassifikation (Abschnitt 8.2.3)

Initiale Umsetzungsschritte: Thema Analyse und Absicherung kritischer Datenflüsse (Abschnitt 8.3)

- Erfassung der Datenflüsse (Abschnitt 8.3.1)
- Festlegung sicherer Datenflüsse (Abschnitt 8.3.2)

Initiale Umsetzungsschritte: Thema Ausrichtung von Verschlüsselungsmaßnahmen am Schutzbedarf (Abschnitt 8.4)

- Erhebung der Ausgangslage (Abschnitt 8.4.1)
- Festlegung schutzbedarfsbezogener Mindeststandards (Abschnitt 8.4.2)
- Risikobasierte Behandlung von Legacy-Systemen (Abschnitt 8.4.3)
- Klar geregeltes Schlüsselmanagement (Abschnitt 8.4.4)
- Priorisierte Umsetzung (Abschnitt 8.4.5)

Initiale Umsetzungsschritte: Thema Einsatz einer resilienten Backup-Strategie (Abschnitt 8.5)

- Analyse der bestehenden Backup-Landschaft (Abschnitt 8.5.1)
- Aufbau einer widerstandsfähigen Backup-Architektur (Abschnitt 8.5.2)
- Ausrichtung von Backup-Strategien am Schutzbedarf (Abschnitt 8.5.3)

Initiale Umsetzungsschritte: Thema Verankerung von Wiederherstellungstests (Abschnitt 8.6)

- Fachliche und technische Festlegung der Wiederherstellungsziele (Abschnitt 8.6.1)
- Definition von Wiederherstellungsprozessen (Abschnitt 8.6.2)
- Durchführung regelmäßiger praktischer Wiederherstellungstests (Abschnitt 8.6.3)

Fortgeschrittene Maßnahmen (Abschnitt 8.7)

- Data-Security-Monitoring und Data-Loss-Prevention
- Software-Defined Storages
- Data-Governance-Modell mit Dienstleistern und Fachämtern
- Daten in Test- und Analyseumgebungen

Impressum

Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
www.sit.fraunhofer.de

DOI 10.24406/publica-9741

Autoren

Dr. Matthias Enzmann
Daniel Trick
Ruben Wolf

Hinweise

Dieser Beitrag entstand im Rahmen eines Projektes mit dem Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz.

Kontakt

Bei Fragen zum Aktionsprogramm Kommunale Cybersicherheit:
akc@innen.hessen.de

Bei Fragen die Forschungsförderung Cybersicherheit betreffend:
Innovationsmanagement.Cybersicherheit@innen.hessen.de

Bei Fragen zu dieser Handreichung:
info@sit.fraunhofer.de

Weitere Informationen

www.sit.fraunhofer.de/de/kommunen/

Fraunhofer SIT

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

HESSEN
Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz