Technologie und Mensch in der Kommune von morgen

Impulspapier IV zu Normen und Standards

DIN/DKE Smart City Standards Forum

DIN e. V. bedankt sich bei allen Teilnehmer*innen des Workshops „Cybersicherheit und Resilienz in Kommunen“ für ihre Mitwirkung und ihre wertvollen Beiträge, die die Basis für das Impulspapier geschaffen haben. Ein besonderer Dank gilt zudem allen Autor*innen des Impulspapiers sowie den Cybersicherheitsexperten des Smart City Standards Forums für den angenehmen Austausch mit durchweg interessanten und tiefergehenden Diskussionen, deren Ergebnisse in diesem Dokument zusammengefasst vorliegen.

Vielen Dank an:

- Laura Brandt (SVA System Vertrieb Alexander GmbH)
- Steffen Hess (Fraunhofer IESE)
- Philipp Lämmel (Fraunhofer FOKUS)
- Uwe Northmann (Northmann Consulting) – Redaktion
- Joachim Schonowski (Stadtwerke Lübeck) – Redaktion
- Nikolay Tcholtchev (Hochschule RheinMain & Fraunhofer FOKUS)
- Jan Uhlenbrok (Stadt Osnabrück)
- Balthasar Weitzel (Fraunhofer IESE)

Für die Erstellung des Vorworts danken wir zudem Jan Uhlenbrok.

Außerdem danken wir den Kolleg*innen der relevanten Normenausschüsse von DIN und DKE für die wertvollen Kommentare zum Entwurf dieses Impulspapiers.

Titelbild: © jamesteohart – istockphoto.com

Inhaltsverzeichnis

Vorwort 2

Mensch und Technik im Wandel 3

Normung und Standardisierung im Themenfeld Smart City 4

1 Einleitung und Motivation 5
1.1 Hypothesen aus dem Workshop 6
1.2 Begriffsklärung 8
1.3 Kommunales IKT-Ökosystem 8

2 Herausforderungen 12
2.1 Herausforderungen durch künstliche Intelligenz 13

3 Risiken 14

4 Chancen und Potenziale 15

5 Normung und Standardisierung 16
5.1 Cybersicherheitsverordnung und NIS2-Richtlinie 16
5.2 Cybersicherheitsrelevante Normungsgremien 17
5.3 Weitere relevante Akteure 17
5.4 Überblick bereits existierender Normen und Standards im Bereich Smart City 18

6 Fazit 21

7 Anhang 22

8 Themensammlung / Aktuelles und Links – Glossar 27
Glossar 28

Vorwort

Die fortschreitende Digitalisierung bietet deutschen Kommunen immense Möglichkeiten, ihre Strukturen zu modernisieren, ihre Dienstleistungen nachhaltiger zu gestalten und die Lebensqualität der Bürgerinnen und Bürger zu steigern. Die Entwicklung zur Smart City steht hierbei exemplarisch für eine datengetriebene, vernetzte und effiziente Verwaltung und Infrastruktur. Jedoch geht mit dieser Entwicklung eine immer größere Verantwortung einher, der wir uns als Kommunen bewusst sind: Die zunehmende Vernetzung und der intensive Einsatz digitaler Technologien machen Cybersicherheit zu einem zentralen Aspekt in der Gestaltung unserer Städte und Gemeinden.

Normen und Standards nehmen in diesem Kontext eine Schlüsselrolle ein. Sie schaffen einheitliche Standards, nach denen sich Kommunen, Unternehmen und Partner richten können, und gewährleisten damit die technisch wie organisatorisch notwendige Sicherheit. Besonders im Bereich von Smart Cities bieten Normen Orientierung und Sicherheit, insbesondere wenn es darum geht, sensible Daten zu schützen, Schnittstellen zwischen IT-Systemen zu harmonisieren und resiliente Strukturen zu schaffen. Sie ermöglichen kleineren und größeren Städten, unabhängig von den individuellen Ressourcen von technischen Innovationen zu profitieren, ohne die IT-Sicherheit zu gefährden.

Smart Cities sind ohne Vertrauen in digitale Systeme nicht denkbar. Bürgerinnen und Bürger erwarten, dass ihre Daten nicht nur effizient, sondern vor allem sicher verwaltet werden. Eine flächendeckende und einheitliche Umsetzung von Sicherheitsstandards stärkt dieses Vertrauen und schützt sowohl die Privatsphäre der Menschen als auch die Funktionsfähigkeit kritischer Infrastruktur wie Energie-, Abfall-, Wasser- oder Verkehrssysteme. Zudem entwickeln Normen nicht nur nationale, sondern auch internationale Strahlkraft.

Der Erfolg einer Smart City hängt entscheidend davon ab, dass Cybersicherheit nicht als Ergänzung, sondern als Grundpfeiler der digitalen Transformation betrachtet wird. Nur durch verlässliche Standards, bereichsübergreifende Kooperationen und ein kontinuierliches Bewusstsein für Sicherheitsanforderungen schaffen wir die Basis für eine digitale Zukunft, die innovativ, nachhaltig und geschützt zugleich ist.

Der nachfolgende Inhalt liefert einen ersten Impuls zu dem Thema Cybersicherheit für Kommunen. Er zeigt die Komplexität des kommunalen Ökosystems unter dem Blickwinkel der digitalen Transformation und der rasanten Technologiesprünge und die damit verbundene Zunahme von Sicherheitsanforderungen auf. Neben der Definition und Einordnung von Begrifflichkeiten verschiedener Technologien zeigt sich auch der Standardisierungsbedarf anhand der möglichen Vielzahl von Angriffsoptionen, sei es händisch oder autonom.

Jan Uhlenbrok
Teamleitung Smart City Osnabrück

Mensch und Technik im Wandel

Das Schlagwort „Smart City“, das aus der Kombination „Internet der Dinge“ und den Entwicklungen der Kommunikationstechnologie entstanden ist, ist längst über sich hinausgewachsen. Es umfasst heute bereits weit mehr als nur die „intelligente Stadt“, die die Lebensqualität der Bewohner*innen mit Sensorik, Automatisierung und verfügbaren Daten ressourcenschonend verbessert. Da das Schlagwort nur die Stadt nennt, wurde recht schnell nachgebessert und der Begriff um „Smart Region“ erweitert und in der Standardisierung unter dem Begriff der „intelligenten Kommune“ zusammengeführt. Als übergreifendes Kernthema dient nun das Leitbild einer nachhaltigen und bürger*innenzentrierten Stadtentwicklung. Bereits seit ca. 10 Jahren wurden weitere Schlagworte, wie u. a. resiliente, soziale, gerechte, zirkuläre oder klimaneutrale Stadt, einbezogen. Dabei wurde schnell klar, dass jedes dieser weiteren Schlagworte ein eigenes Handlungsfeld mit entsprechendem Tiefgang darstellt.

Neben dem Handlungsfeld Resilienz ist aktuell das Thema der digitalen Daseinsvorsorge als übergreifendes Kernthema hinzugekommen. Dieses entstand aus der Erfahrung vieler geförderter Pilotprojekte, die unter anderem durch fehlende Standards zu einem technologischen Flickenteppich geführt haben. Um auch für nicht geförderte Städte und ländliche Kommunen einen verlässlichen Grad der Digitalisierung zu ermöglichen, entstand die Notwendigkeit, die kommunale Daseinsvorsorge um die digitale Ebene zu erweitern. Beide Themen, Resilienz und digitale Daseinsvorsorge, müssen aber auch in Bezug auf die rasante Entwicklung der Digitalisierung selbst dringend betrachtet werden, da diese mit fortschreitender Durchdringung aller kommunalen Bereiche immer neue und zum Teil unbemerkte Möglichkeiten bietet, das kommunale digitale Ökosystem auf unterschiedlichsten Ebenen und durch alte oder neue Einfallstore anzugreifen. Diese beiden Themen müssen also hinsichtlich ihrer Inhalte und Auswirkungen in die „Digitalisierungslandkarte“ eingeordnet werden, um deren Relevanz für die IT-Ökosysteme im kommunalen Bereich richtig einordnen zu können.

Gerade in letzter Zeit hat die Anzahl und das Ausmaß von Cyberangriffen auf Kommunen stark zugenommen und aufgrund der rasanten (Weiter-)Entwicklung der Technologien gibt es stetig neue Bedrohungsszenarien. Trotz vieler Unterstützungsmaßnahmen und bereits existierender Initiativen und Dokumente ist es gerade für (kleinere) Kommunen immer schwieriger, mit den neuesten Entwicklungen in Sachen Cybersicherheit Schritt zu halten, den Überblick zu behalten und von Beginn an mit klar definierten Begriffen eine gemeinsame Sprache zu sprechen.

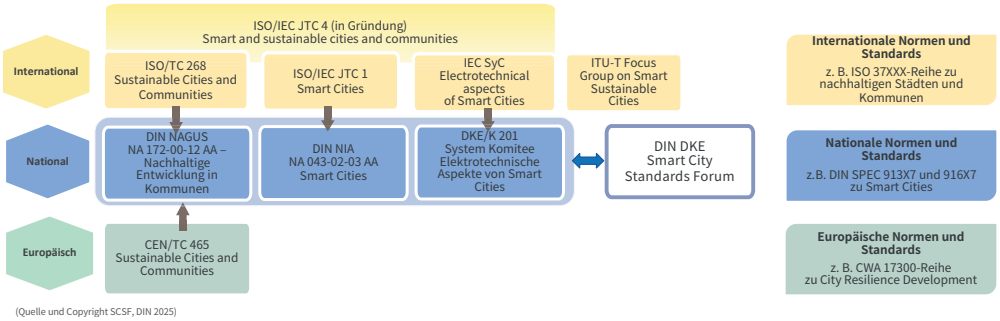
Aus diesem Grund greifen wir den Baustein „technische/digitale Resilienz“ aus dem Impulspapier II (Kapitel 3) wieder auf und wollen ihn mit unserem Impulspapier IV zum Thema „Cybersicherheit in Kommunen“ mit dem Fokus auf die technische Resilienz der digitalen Systeme vertiefen, um so Normungs- oder Standardisierungsbedarfe zu ermitteln, aus denen bei Bedarf ein umfassender Handlungsleitfaden als Hilfestellung für die Kommunen entstehen kann.

Viel Spaß beim Lesen

Klaus Illigmann, Uwe Northmann, Joachim Schonowski,
Smart City Standards Forum

Normung und Standardisierung im Themenfeld Smart City

In einer zunehmend digitalisierten Welt spielt das Konzept der Smart Cities eine wesentliche Rolle in der Stadtentwicklung und bietet vielfältige Chancen für eine nachhaltige und effiziente städtische Infrastruktur. Die Normung und Standardisierung im Bereich Smart City ist essenziell, um einheitliche Standards zu schaffen, die Implementierung innovativer Lösungen zu fördern und die Sicherheit und Nachhaltigkeit urbaner Lebensräume zu gewährleisten. Mehrere nationale Normenausschüsse und das DIN/DKE Smart City Standards Forum fokussieren sich explizit auf das Thema der nachhaltigen, intelligenten Stadt von morgen.



(Quelle und Copyright SCSF, DIN 2025)

Bild 1: Smart-City-relevante Normungsgremien und Smart City Standards Forum

Die Normungslandschaft im Bereich Smart City setzt sich aus verschiedenen Gremien auf nationaler, europäischer und internationaler Ebene zusammen. Zu den zentralen nationalen Gremien gehören der DIN-Arbeitsausschuss „Nachhaltige Entwicklung in Kommunen", der DIN-Arbeitsausschuss „Smart Cities" sowie das DKE-Komitee „Elektrotechnische Aspekte von Smart Cities". Da Smart City ein horizontales Querschnittsthema ist, ergeben sich auch zahlreiche Schnittstellen zu anderen Normungsgremien. Diese nationalen Gremien haben neben ihrer Normungsarbeit auf nationaler Ebene die Aufgabe, die entsprechenden europäischen und internationalen Gremien bei CEN, CENELEC, ISO, IEC und ETSI zu spiegeln und die national abgestimmten Positionen in die europäische und internationale Normung einzubringen. Um die Arbeiten der verschiedenen internationalen Gremien im Bereich Smart Cities und nachhaltige städtische Gemeinschaften effektiv zu bündeln und zu koordinieren, befindet sich derzeit das Gemeinschaftsgremium ISO/IEC JTC4 in der Gründung.

Das DIN/DKE Smart City Standards Forum (SCSF) spielt als Informations- und Vernetzungsplattform auf nationaler Ebene für Smart-City-Akteur*innen aus Kommunen, Politik, Zivilgesellschaft, Wirtschaft, Verbänden, Forschung und technischen Regelsetzern eine wichtige Rolle und kann als Einstieg in die Welt der Normung und Standardisierung im Bereich Smart City dienen. Durch den fachlichen Austausch im SCSF werden relevante Handlungsfelder für die Normung und Standardisierung im Bereich Smart City identifiziert, themenspezifische Workshops organisiert und neue nationale Standardisierungsaktivitäten initiiert. Dies ermöglicht die Entwicklung nationaler Standpunkte, die dann durch die oben genannten Spiegelgremien in die europäische und internationale Normung eingebracht werden können. Eine zentrale Aufgabe des SCSF ist es, „Schnittstellenthemen" und aufkommende Themen der digitalen Systeme einer Kommune frühzeitig zu erkennen, weiterzudenken und in die Standardisierung zu integrieren.

1 Einleitung und Motivation

Mit dem Einzug des „Internet der Dinge“ in die Stadtentwicklung hat die digitale Transformation Fahrt aufgenommen. Unter dem Schlagwort „intelligente Kommune“ (engl. Smart City) wird vor allem ein digital vernetztes kommunales Ökosystem verstanden. Ein solches Ökosystem umfasst eine Vielzahl unterschiedlicher Technologien und Fachökosysteme wie die Stromversorgung mit einem Smart Grid oder einem vernetzten Mobilitätsbereich, die dann u. a. mithilfe von übergreifenden IT-Systemen wie einer urbanen Datenplattform zusammengefasst werden. Dabei gibt es unterschiedliche Bedürfnisse, Anforderungen, Herangehensweisen, Ausgangslagen usw. für jede Kommune.

Allen gemein ist aber die Tatsache, dass die digitale Transformation immer stärker Einzug in das kommunale Leben halten wird und einige Bestandteile mittlerweile als eine digitale Daseinsvorsorge angesehen werden.

Neben typischen Anwendungen wie einer kommunalen App oder einem Digitalen Zwilling ist es dabei aber auch erforderlich, für die eingesetzten digitalen Systeme entsprechend die Cybersicherheit mitzudenken bzw. die Sicherheit dieser komplexen Systemlandschaft kontinuierlich auf dem neuesten Stand zu halten.

Häufig erhält das Thema der Cybersicherheit hierbei nicht die notwendige Aufmerksamkeit, dabei stellt es die Grundlage für eine erfolgreiche Digitalisierung dar und sollte von Anfang an mitgedacht werden.

Dies zeigen nicht nur die zunehmenden Cyberangriffe auf die Informations- und Kommunikations-Systeme (IKT) aller Sektoren der kommunalen Verwaltung. Wird ein System erfolgreich angegriffen, sind u. a. die Funktion, die Datenintegrität und damit das Ergebnis einer Anwendung massiv gestört bis außer Betrieb gesetzt oder es findet ein unberechtigter Datenabfluss statt.

Daher ist es dringend geboten, sich dieses relevanten Themas anzunehmen, da die Risiken und möglichen Schäden bei Eintritt immens sein können. Denn es ist klar: Jede Kommune in Deutschland ist Zielscheibe von Cyberangriffen. Die Frage ist daher nicht, ob ein Cyberangriff auf die Systeme passiert, sondern wann und wie weitreichend die Folgen sein werden.

Um einen besseren Überblick zu erhalten, lud das Smart City Standards Forum (SCSF) am 04. April 2025 zum Workshop „Cybersicherheit und Resilienz in Kommunen“ ein, in dem u. a. folgende Fragen diskutiert wurden:

→ Wie sieht ein kommunales Ökosystem im Kontext Cybersicherheit aus und gab es schon einmal Cyberangriffe? Welche Risiken und Gefahren bestehen und welche kritischen Anwendungen oder Handlungsfelder in einem kommunalen Ökosystem wären davon potenziell betroffen?
→ Welche Standards, Regularien und Handlungsempfehlungen existieren für ein kommunales Ökosystem in Bezug auf Cybersicherheit und welche davon werden von Ihnen genutzt? Sind diese aus Ihrer Sicht ausreichend?
→ Gab es bei Ihnen schon einmal Cyberangriffe im Zusammenhang mit KI und welche Gefahren/Risiken sehen Sie für die Zukunft?

Im nachfolgenden Dokument werden die Eindrücke und Ergebnisse des Workshops zusammengefasst und erste Schlussfolgerungen sowie Themensammlungen erarbeitet mit dem Ziel, ein mögliches Standardisierungspotenzial für Kommunen im Bereich der Cybersicherheit herauszuarbeiten und zu starten.

Laut einer Studie des Bitkom e. V. entsteht der deutschen Wirtschaft ein jährlicher Schaden von 203 Milliarden Euro durch Hackerangriffe[1]. In 2025 wird ein wirtschaftlicher Schaden von 289 Mrd. Euro für die deutsche Wirtschaft erwartet, so das Ergebnis der aktuellen Bitkom-Studie[2]. Dabei sind dem Lagebericht 2024 des BSI zufolge KMU, Kommunen sowie IT-Dienstleister als Teil der Lieferkette im Fokus[3]. Laut einer Umfrage des Deutschen Städte- und Gemeindebundes (DStGB) wurden in 2024 rund ein Viertel aller befragten Kommunen Ziel eines Cyberangriffs[4].

1.1 Hypothesen aus dem Workshop

1 **Information und Begriffe**
Der Begriff „Cybersicherheit" kann unterschiedlich verstanden und je nach Organisation oder Zweck auch divers ausdefiniert werden. Bei Cybersicherheit in einem kommunalen Ökosystem ist es herausfordernd, fachlich den Überblick zu behalten, die Regularien zu kennen und die Verantwortlichkeiten zuzuordnen bzw. einzufordern.

2 **Organisation**
Neben Fachverfahren für die klassischen Verwaltungsaufgaben entstehen durch Vernetzung der Verfahren übergreifende Zuständigkeiten, wodurch neue organisatorische und technische Schnittstellen entstehen. Bisher in sich geschlossene technische (wie organisatorische) Bereiche halten zur Verknüpfung Software-Schnittstellen bereit und werden dadurch an diesen zusätzlich angreifbar im Sinne einer digitalen Lieferkette. Dazu kommen noch externe Schnittstellen, die Einfluss auf das Gesamtsystem nehmen (Lieferant*innen, Bürger*innen usw.)

1 https://www.bitkom.org/Presse/Presseinformation/203-Milliarden-Euro-Schaden-pro-Jahr-durch-Angriffe-auf-deutsche-Unternehmen

2 https://www.speicherguide.de/management/cybersicherheit/bitkom-cyberangriffe-verursachen-289-mrd.-euro-schaden-26828.html

3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html?nn=132646

4 https://www.dstgb.de/themen/digitalisierung/aktuelles/zukunftsradar-2024-gemeinsamer-digitaler-sicherer/zukunftsradar-digitale-kommune-2024-iit-dstgb-web.pdf?cid=1bh4

3 **Technisch**

Die digitale Transformation führt zu einem quasi echtzeitvernetzten kommunalen Ökosystem mit einer zunehmenden Anzahl digitaler Systeme, Abhängigkeit und Nutzungsintensität. Aufgrund der vielen neuen und vor allem quasi echtzeitvernetzten digitalen Systeme steigt die Zahl der Angriffsflächen bzw. auch die mögliche negative Auswirkung eines Angriffs. Es gilt, u. a. Nutzer*innen, Endgeräte, Netzwerke und Schnittstellen sowie die Daten selbst vor Manipulation, Verfälschung, Diebstahl und Missbrauch zu schützen. Cyberangriffe haben unterschiedliche Zielsetzungen, von der Störung der kommunalen Ordnung, z. B. durch Ausfall der Ampelsteuerung, über die Mittelentwendung, u. a. durch digitale Geldentwendung, bis zur Datenmanipulation.

4 **Zunahme der Angriffsmethoden und Gefahrenlage durch KI**

Die Komplexität des kommunalen Ökosystems erhöht die Angriffsfläche und die rasant steigenden neuen technologischen, u. a. KI-basierten, teils autonom agierenden Möglichkeiten, wie etwa die Steuerung von Ampelanlagen, führen kontinuierlich zu verschiedenen und neuen Angriffsmethoden und -möglichkeiten.

5 **Resilienz und Resistenz der Systeme**

Das kommunale Ökosystem muss kontinuierlich auf Betriebssicherheit, Cybersicherheit, Ausübung der Kernfunktionen usw. geprüft werden. Resilienz und Resistenz sind hierbei Begriffe, die im Kontext von Smart Cities unterschiedliche Eigenschaften und Strategien beschreiben.

Resilienz beschreibt die Fähigkeit eines Systems, sich nach einer Störung oder einem Angriff schnell zu erholen und den Normalzustand wiederherzustellen. Es geht darum, flexibel und adaptiv auf Herausforderungen zu reagieren.

So wird z. B. ein Stromausfall aufgrund eines Sturms durch ein intelligentes Energienetz (Smart Grid) kompensiert, das die Stromversorgung mit alternativen Quellen wie Solarzellen oder Batteriepuffern sicherstellt.

Resistenz hingegen bezeichnet die Widerstandsfähigkeit oder Immunität eines Systems gegenüber äußeren Einflüssen, sodass es gar nicht erst zu einer Beeinträchtigung kommt. Es geht darum, präventiv Maßnahmen gegen potenzielle Bedrohungen zu implementieren. Daher soll ein Smart-City-Netzwerk durch starke Firewalls und verschlüsselte Kommunikation gegen Angriffe abgesichert sein, sodass von außen kein Zugang zu sensiblen Daten gewährt wird.

Resilienz ist somit reaktiv und zielt auf Erholung ab, während Resistenz proaktiv ist und Angriffen oder Störungen vorbeugen will.

Diese fünf Themen waren die Motivation, das Thema Cybersicherheit unter dem Aspekt der Standardisierung im kommunalen Ökosystem zu betrachten. Ziel ist es, Begriffe zu definieren, einzuordnen, Angriffssituationen darzustellen, relevante Standards zu identifizieren und diese in einem Standard zusammenzuführen. Dieser soll Kommunen einen verlässlichen Handlungsleitfaden auf Basis relevanter Standards und zurzeit aktuell genutzter Technologien wie KI bieten.

1.2 Begriffsklärung

In diesem Dokument ist wiederholt von Cybersecurity bzw. Cybersicherheit die Rede. Gleichzeitig kommen in diesem Zusammenhang auch häufig die Begriffe IT-Security/IT-Sicherheit, Datenschutz sowie OT-Sicherheit auf, oder es ist von der etwas weiter gefassten Informationssicherheit die Rede. Häufig werden diese Begriffe synonym genutzt, haben aber auch je nach Anwendungsbereich (z. B. Sensoren, Aktuatoren, Verwaltungsnetze, ...) und Kontext unterschiedliche Bedeutungen. Diese Ambiguität kann die Einführung von Sicherheitsmechanismen und generell die Diskussion darüber im Smart-City-Kontext erheblich erschweren. Aus diesem Grund ist eines der Hauptziele einer zukünftigen DIN SPEC, diese zu definieren und die Einordnung der relevanten Begriffe aus Sicht der Kommune und die Erarbeitung einer Taxonomie auf Basis existierender Standards vorzunehmen.

Begriffe werden im Begriffsglossar (8 Themensammlung / Aktuelles und Links – Glossar) erläutert.

1.3 Kommunales IKT-Ökosystem

Ein digitales kommunales Ökosystem ist ein komplexes Gebilde, bestehend aus verschiedenen Informations- und Kommunikationstechnologien bzw. -systemen, die eine Vielzahl von Daten bereitstellen. Nach DIN SPEC 91357 – *Referenzarchitekturmodell Offene Urbane Plattform* kann ein kommunales IKT-Ökosystem mithilfe einer schichtenbasierten Referenzarchitektur beschrieben werden. Die einzelnen Schichten werden auf Basis von sogenannten Capabilities (deutsch: Fähigkeiten/Eigenschaften) beschrieben, die die vielfältigen Aufgaben einer Schicht erfassen. Dabei dreht sich alles um die Akquise, Kommunikation, Haltung, Verarbeitung, Analyse und Bereitstellung von Daten. Die Datenakquise wird auf Basis von Sensoren oder durch die Bereitstellung von Behörden- und Firmendaten (z. B. als Open Data) realisiert. Diese Sensordaten werden anschließend über IoT-Kommunikationstechnologie (z. B. LoRaWAN, ZigBee, IEEE.802.15.4, 6LoWPAN, CoAP ...) oder Mobilfunk (z. B. NB-IoT, 5G ...) im Rahmen des Zugangsnetzes zu einer Basisstation / einem Gateway übertragen. Nachher werden die Daten über internetbasierende Kommunikationstechnologie (all-IP-Netzwerke) oder die klassischen Telekom-/Internetnetze an die weiteren Systeme wie Cloud oder Rechenzentren übertragen. Die Daten werden entsprechend in hochskalierbare Datenbanken (Stichwort Big Data) übertragen und anschließend in ihrer Qualität veredelt (Stichwort Formatierungsfehler) und mit anderen Datenquellen verschnitten. Darauf können verschiedene (KI-basierte) Datenanalysen laufen, sodass die Ergebnisse auf Endnutzergeräten (z. B. Laptops, Tablets, Smartphones, AR/VR-Geräte, ...) zur Verfügung gestellt werden können und somit neuartige Dienste und Applikationen im kommunalen und im Smart-City-Kontext entstehen. In diesem ganzen Ablauf spielt eine logisch zentralisierte urbane Datenplattform eine zentrale Rolle, indem sie als Drehscheibe für die Speicherung und Weiterverarbeitung der Eingaben aus den Datenquellen (z. B. Sensoren, Behördendaten, ...) agiert.

Die oben beschriebene Struktur lässt ein komplexes Bild in Bezug auf die Cybersicherheit, Resilienz und Resistenz des Gesamtökosystems erahnen, welche schematisch in Bild 2 dargestellt ist. Man beobachtet eine Vielzahl an Technologien auf verschiedenen Schichten/ Ebenen im gesamten Technologiestack. Diese Komponenten und Technologien werden von verschiedenen Herstellern geliefert und durch das Zusammenspiel einer Reihe von Akteur*innen zu einem integrierten, interoperablen Smart-City-Ökosystem zusammengefügt. Dabei werden verschiedene Komponenten und Teilbereiche des Ökosystems durch verschiedene Verantwortlichkeiten organisatorisch wie technisch in Bezug auf die Cybersicherheit behandelt. Die Sensorik im Feld wird dabei anders betrachtet und eventuell nach traditionellen Betriebstechnologien (Operative-Technologies (OT)-Prinzipien) behandelt. Die eingesetzten Mobilfunk- und Telekommunikationsnetze haben ihre spezifische Cybersicherheitsinfrastruktur, die im Rahmen des Telekomintegrators gepflegt und betrieben wird. Die Datenplattformen (Cloud oder Edge) werden gesondert betrieben und in Bezug auf Resilienz und Cybersicherheit behandelt. Dieses vielschichtige Gebilde zeigt die Komplexität der Cybersicherheitsherausforderungen in Smart Cities auf.

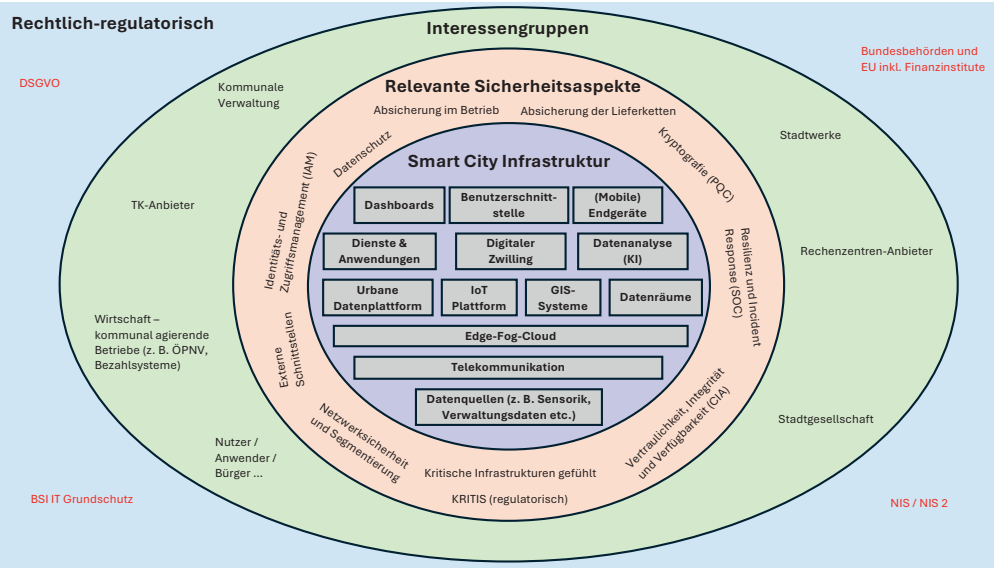


Bild 2: Grober Überblick über das kommunale digitale Ökosystem im Cybersicherheitskontext

Bild 2 gibt einen groben, nicht vollständigen Überblick über ein mögliches kommunales digitales Ökosystem im Kontext von Cybersicherheit. Die sich ständig verändernden Anforderungen u. a. durch neue digitale Technologien hinsichtlich der Sicherheitsaspekte und damit Resistenz und Resilienz umgeben dieses Ökosystem, auf das verschiedene Interessengruppen und rechtlich-regulatorische Anforderungen einwirken.

Das Herzstück einer intelligenten Kommune bildet ihre digitale Infrastruktur. Diese lässt sich in zwei grundlegende Aufgaben unterteilen: die Datenerfassung und -verarbeitung sowie die darauf aufbauenden Dienste und Applikationen. Die unterste Ebene bilden die Datenquellen. Hierzu zählen unzählige Sensoren im kommunalen Raum – von Umweltsensoren, die Luftqualität messen, über Verkehrssensoren bis hin zu intelligenten Zählern in Haushalten. Ergänzt werden diese Echtzeitdaten durch bereits vorhandene Verwaltungsdaten, wie z. B. aus dem Melderegister oder der Stadtplanung. Um diese Daten zu transportieren, bedarf es einer leistungsstarken und allgegenwärtigen Telekommunikationsinfrastruktur, die von Glasfaser bis zum 5G-Mobilfunk reicht. Die gesammelten Daten fließen in weiterverarbeitende Systeme: Eine urbane Datenplattform dient beispielsweise als Speicher- und Verwaltungsknoten, auf dem Daten aus unterschiedlichsten Quellen zusammengeführt, strukturiert, aufbereitet und für verschiedene Anwendungen bereitgestellt werden. Spezialisierte Plattformen wie eine IoT-Plattform stellen die Anbindung und Steuerung der unzähligen Sensoren und Aktoren sicher. Geoinformationssysteme (GIS) reichern die Daten mit einer räumlichen Komponente an und ermöglichen so eine kartografische Darstellung und Analyse. Die Verarbeitung dieser gewaltigen Datenmengen findet in einer hybriden Umgebung statt, die von Edge Computing (Verarbeitung direkt am Ort der Entstehung, z. B. in der intelligenten Ampel) über Fog Computing (auf einer Zwischenebene) bis hin zur zentralen Cloud reicht.

Auf Basis dieser Infrastruktur entstehen die Dienste und Anwendungen, die den Mehrwert für die Bürgerinnen und Bürger schaffen. Ein Digitaler Zwilling einer Kommune ermöglicht es beispielsweise, komplexe Szenarien wie Verkehrsflüsse oder die Auswirkungen von Baumaßnahmen zu simulieren und zu planen, bevor sie in der realen Welt umgesetzt werden. Mittels Datenanalyse und künstlicher Intelligenz können Muster erkannt, Vorhersagen getroffen und Prozesse optimiert werden – von der intelligenten Abfallentsorgung bis zur vorausschauenden Wartung der städtischen Infrastruktur. Dashboards visualisieren diese Informationen für Entscheidungsträger in der Verwaltung, während intuitive Benutzerschnittstellen auf mobilen Endgeräten der Verwaltung oder Nutzer*innen wie Einwohner*innen oder Reisenden den Zugang zu kommunalen Dienstleistungen erleichtern.

Dieses komplexe, interagierende kommunale digitale Ökosystem ist potenziellen Cyberangriffen ausgesetzt. Daher müssen Sicherheitsmaßnahmen auf allen Ebenen betrachtet und integriert werden. Die klassischen Schutzziele der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit (Confidentiality Integrity Availability (CIA)) – sind dabei von zentraler Bedeutung. Es muss sichergestellt werden, dass Daten nur von Befugten eingesehen werden können, nicht unbemerkt verändert werden und dass die Systeme und Dienste jederzeit zur Verfügung stehen. Um dies gewährleisten zu können, sind vielfältige technische und organisatorische Maßnahmen erforderlich, von denen die folgenden eine wichtige, aber keine erschöpfende Auswahl darstellen.

Eine strikte Netzwerksicherheit und -segmentierung sorgt dafür, dass verschiedene Teile des kommunalen Netzes (z. B. die Verkehrssteuerung und das Krankenhausnetz) voneinander getrennt sind, um die Ausbreitung eines Angriffs zu verhindern. Ein robustes Identitäts- und Zugriffsmanagement (IAM) regelt präzise, welche Person oder welches System auf welche Daten und Funktionen zugreifen darf. Der Datenschutz, insbesondere im Einklang mit der Datenschutzgrundverordnung (DSGVO), ist von höchster Priorität, um die Persönlichkeitsrechte von Nutzer*innen zu wahren. Moderne Kryptografie, zukünftig auch Post-Quanten-Kryptografie (PQC), schützt die Daten bei der Übertragung, Speicherung und Verarbeitung vor unbefugtem Zugriff. Da kein System hundertprozentig sicher sein kann, sind ein funktionierendes Krisen-

management und etablierte Notfallmaßnahmen (Incident Response) entscheidend. Die Stadt muss in der Lage sein, Angriffe schnell zu erkennen (z. B. durch ein Security Operations Center (SOC)), darauf zu reagieren und den Normalbetrieb so schnell wie möglich wiederherzustellen. Dies schließt auch die Absicherung der gesamten Lieferketten für Hard- und Software sowie die kontinuierliche Absicherung im laufenden Betrieb mit ein.

Eine sichere, intelligente Kommune ist kein isoliertes Projekt der Verwaltung, sondern das Ergebnis einer koordinierten Zusammenarbeit verschiedener Akteur*innen, deren Interessen sich gegenseitig ergänzen und bedingen. Die nachfolgend genannten Interessengruppen stellen dabei eine beispielhafte, nicht vollumfängliche Liste dar.

Die kommunale Verwaltung agiert als zentrale Steuerungs- und Koordinationsinstanz. Ihr Interesse an effizienten Prozessen und bürgernahen Dienstleistungen wird durch die innovativen Lösungen der lokalen Wirtschaft (z. B. im ÖPNV oder bei Bezahlsystemen) ergänzt, die wiederum auf eine stabile und sichere städtische Dateninfrastruktur angewiesen ist. Stadtwerke und andere Betreiber Kritischer Infrastrukturen (KRITIS) haben das primäre Ziel, die (digitale) Daseinsvorsorge zu gewährleisten. Dieses Ziel deckt sich mit dem Sicherheitsbedürfnis der gesamten Kommune. Durch die gemeinsame Nutzung von Sensor- und Verbrauchsdaten können Netze resilienter und effizienter gestaltet werden. Die kommerziellen Interessen von Telekommunikations- und Rechenzentren-Anbietenden am Aufbau des digitalen Rückgrats einer Kommune stehen im Einklang mit den Bedarfen aller anderen Akteur*innen an einer leistungsfähigen und sicheren Konnektivität. Letztlich hat die Stadtgesellschaft eine zentrale Relevanz für dieses Ökosystem. Das Interesse von Nutzer*innen (primär den Einwohner*innen) an transparenten, nützlichen Diensten und dem Schutz ihrer persönlichen Daten ist die entscheidende Voraussetzung für die Akzeptanz des gesamten Systems. Nur wenn Vertrauen herrscht, werden die digitalen Angebote angenommen.

Gleichfalls schaffen Bundesbehörden und EU-Institutionen durch den rechtlichen und regulatorischen Rahmen – wie bspw. die NIS-2-Richtlinie, den BSI-IT-Grundschutz und die DSGVO – eine verlässliche Grundlage. Diese Vorgaben sollen nicht nur die Einwohner*innen schützen, sondern geben auch den Betreibern und der Verwaltung klare Leitplanken für die sichere Ausgestaltung ihrer Systeme und fördern so das Vertrauen aller Beteiligten. Es soll ein System der geteilten Verantwortung entstehen, in dem die Sicherheit des Einzelnen zur Stabilität des Gesamten beiträgt und der Nutzen für die Gemeinschaft durch das Zusammenspiel aller Kräfte realisiert werden kann.

2 Herausforderungen

Die digitale Vernetzung bringt eine entscheidende Kehrseite mit sich: Jede neue Schnittstelle, jedes vernetzte Gerät und jede digitale Anwendung erweiterten die potenzielle Angriffsfläche. Die Herausforderungen in Smart Cities sind daher nicht nur technischer Natur, sondern betreffen ebenso Governance, Organisation und Recht. Sie erfordern ein tiefes Verständnis der Verwundbarkeiten auf allen Ebenen.

Mögliche Herausforderungen sind:

1 **Angreifbare Endpunkte**
Die Vielzahl an Sensoren, Aktoren und mobilen Endgeräten im öffentlichen Raum ist der erste kritische Risikofaktor. Diese Geräte sind oft physisch zugänglich, arbeiten mit eingeschränkten Sicherheitsfunktionen und erhalten nicht immer zeitnah Updates. Die Folge: Abhören unverschlüsselter Daten, Ausnutzen bekannter Firmware-Lücken oder direkte Manipulation sind realistische Szenarien. Schon ein einziges kompromittiertes Gerät kann als Einfallstor dienen, um in größere Teile der Smart-City-Infrastruktur einzudringen.

2 **Verletzliche Kommunikationswege**
Die Datenübertragung zwischen Endpunkten und zentralen Plattformen ist das Rückgrat der Smart City – und gleichzeitig ein bevorzugtes Angriffsziel. Funktechnologien wie LoRaWAN, NB-IoT oder Mobilfunk können durch Man-in-the-Middle-Angriffe, gezieltes Jamming oder die Injektion manipulierter Pakete ausgenutzt werden. Solche Angriffe gefährden unmittelbar die Verfügbarkeit kritischer Dienste, verfälschen Entscheidungsgrundlagen oder führen zu Kontrollverlust über städtische Prozesse.

3 **Gefährdete zentrale Plattformen**
IoT- und urbane Datenplattformen bündeln riesige Mengen sensibler Daten. Ihre Kompromittierung hat oft systemweite Folgen. Schwache Authentifizierung, Fehlkonfigurationen oder fehlende Segmentierung eröffnen Angreifern die Möglichkeit, Daten zu stehlen, zu manipulieren oder durch Ransomware unzugänglich zu machen. Ein erfolgreicher Angriff auf diese Systeme kann nicht nur einzelne Dienste lahmlegen, sondern in einer Kettenreaktion die Funktionsfähigkeit ganzer Stadtbereiche beeinträchtigen.

4 **Unsichere Anwendungen**
Bürgerportale, Apps und webbasierte Steuerungs-Tools sind Schnittstellen mit enormer Außenwirkung und hoher Anfälligkeit. Unsichere APIs, fehlende Prüfungen bei Drittanbieter-Integrationen oder Schwachstellen im Anwendungscode ermöglichen Unbefugten Zugriff oder Manipulation von Prozessen. Besonders gefährlich sind Eingriffe in algorithmische Entscheidungslogiken, da sie unbemerkt zu falschen Steuerbefehlen führen können.

5 **Neue Risiken durch künstliche Intelligenz**
KI-gestützte Systeme in Smart Cities (etwa für Verkehrssteuerung oder Umweltmonitoring) schaffen zusätzliche Angriffspunkte. Datenvergiftung/Datenverfälschung (engl. Data Poisoning) kann die Grundlage der Modelle verfälschen, Modellmanipulation kann Entscheidungen subtil beeinflussen und DoS-Angriffe können Analysen in kritischen Momenten verhindern. Das Problem: Solche Eingriffe sind oft schwer zu erkennen und wirken langfristig.

6 **Komplexität der Technologieintegration**
Die technische Vielfalt in Smart Cities ist Fluch und Segen zugleich. Unterschiedliche Hersteller, inkompatible Standards und proprietäre Lösungen erschweren eine konsistente Sicherheitsarchitektur. Unsichere Schnittstellen, unterschiedliche Verschlüsselungsverfahren und uneinheitliche Update-Strategien führen zu einem Flickenteppich an Sicherheitsniveaus. Das sind ideale Bedingungen für Angreifer*innen, um über schwächere Glieder ins Gesamtsystem vorzudringen.

7 **Strukturelle und organisatorische Defizite**
Technische Lösungen allein reichen nicht aus, wenn organisatorische Voraussetzungen bzw. das Bewusstsein und die Verantwortung in den Führungsetagen fehlen. Fachkräftemangel, unklare Zuständigkeiten, begrenzte Budgets und langsame Entscheidungsprozesse verhindern oft eine konsequente Umsetzung von Sicherheitsstrategien. Hinzu kommt, dass viele Projekte als Pilotvorhaben starten und Sicherheitsaspekte nicht in den Regelbetrieb übertragen werden. Das ist ein Nährboden für dauerhaft ungeschützte Systeme.

8 **Hoher regulatorischer Druck**
Neben den technischen und organisatorischen Anforderungen müssen Smart Cities eine Vielzahl komplexer Rechtsvorgaben erfüllen. DSGVO, NIS-2, CER, Open-Data-Richtlinie, EU Data Act und AI-Act setzen strenge Maßstäbe für Datenschutz, Informationssicherheit, Offenheit und Transparenz. Die Herausforderung: Sicherheit, Compliance und Innovationsgeschwindigkeit in Einklang zu bringen, ohne dass eine Anforderung die andere untergräbt.

2.1 Herausforderungen durch künstliche Intelligenz

Mit der zunehmenden Verbreitung von KI-Technologien wachsen die Anforderungen an die Cybersicherheit. Angriffe lassen sich heute kaum noch eindeutig auf KI-basierte oder klassische Methoden zurückführen – sie vermischen sich. Besonders perfide gestaltet sich Social Engineering, das durch KI-gestützte Sprachnachrichten, Chatbots oder personalisierte E-Mails die Erkennung und Abwehr massiv erschwert. Hinzu kommt, dass KI-Systeme selbstständig Verteidigungsmechanismen analysieren und neue Angriffsmuster entwickeln können. Die Grenze zwischen Verteidigung und Angriff verschwimmt: Während KI einerseits hilft, Angriffe frühzeitig zu erkennen, eröffnet sie andererseits neue Angriffsmethoden.

Ein Grundwissen über den Einsatz und die Risiken von künstlicher Intelligenz ist deshalb unverzichtbar. Nur so können Mitarbeitende in Kommunen lernen, mit KI zu arbeiten sowie KI-generierte Angriffe zu erkennen und sich effektiv gegen solche „lernenden Angriffssysteme“ zu schützen. Gleichzeitig muss auch die Kontrollierbarkeit der eingesetzten Systeme kritisch hinterfragt werden. Unüberlegtes Vertrauen in KI kann zu gefährlichen Fehleinschätzungen führen, insbesondere im Zusammenhang mit Datenschutz und der Entwicklung von Standards.

3 Risiken

Eine unzureichende Cybersicherheit stellt für Städte und Gemeinden ein erhebliches Risiko dar. Datenlecks, Ausfälle kritischer Infrastrukturen bis hin zu monetären Verlusten wie Geldtransfer bedrohen die Funktionsfähigkeit der Kommune. Neben dem finanziellen Schaden kommt es bei erfolgreichen Angriffen zu einem erheblichen Vertrauensverlust in die Kommune und das staatliche Handeln insgesamt. Solche Vorfälle führen außerdem zu Einschränkungen der Handlungsfähigkeit von Verwaltungen und können im schlimmsten Fall sogar Leib und Leben gefährden – etwa, wenn Rettungsdienste durch manipulierte Systeme nicht mehr erreicht werden, oder bei Datenmissbrauch im Gesundheitssektor.

Eine besondere Herausforderung ergibt sich durch die Gefahr von Datenmanipulationen: Sie können automatisierte Prozesse in Smart Cities auslösen oder fehlerhafte Entscheidungen provozieren, was im Extremfall zu einem Zusammenbruch der Daseinsvorsorge führen kann. Auch der Missbrauch kommunaler Daten und Infrastrukturen, etwa durch Erpressung oder das gezielte Streuen falscher Informationen, ist eine reale Bedrohung. Neben den technischen Schäden sind es vor allem Reputationsverluste und die daraus resultierende sinkende Akzeptanz digitaler Verwaltungsdienstleistungen, die Kommunen langfristig beeinträchtigen können.

4 Chancen und Potenziale

Die steigenden Risiken mit fortschreitender Digitalisierung und steigender Durchdringung kommunaler Prozesse mit künstlicher Intelligenz stellen Städte und Gemeinden vor erhebliche Herausforderungen. Dabei bieten gerade diese neuen Technologien den Kommunen zahlreiche Möglichkeiten, um ihre Widerstandsfähigkeit gegenüber digitalen Bedrohungen zu stärken und die digitale Transformation aktiv zu gestalten.

Kommunen können sich beispielsweise gezielt mit modernen Cybersicherheitslösungen ausstatten, die auf den Einsatz von KI-basierter Angriffserkennung setzen und dadurch das IT-Personal entlasten. Durch die Integration von Systemen zur Anomalieerkennung, die das Verhalten von Endgeräten, Netzwerken und Anwendungen überwachen, lassen sich verdächtige Aktivitäten frühzeitig identifizieren. Erweiterte Detektions- und Reaktionsmaßnahmen (XDR) helfen dabei, Bedrohungen schneller zu analysieren und wirkungsvoll abzuwehren. Die Einrichtung von eigenen oder interkommunal betriebenen Security Operations Centern (SOC) ermöglicht es, eine zentrale Überwachung und Steuerung aller sicherheitsrelevanten Prozesse zu etablieren.

Darüber hinaus steht Kommunen eine breite Palette an Präventionsmaßnahmen zur Verfügung: Durch Ethical Hacking, den Einsatz von Honey-Pots sowie regelmäßige Schwachstellenscans und Pentests können potenzielle Angriffsflächen proaktiv erkannt und geschlossen werden. Die Identifizierung und Vernetzung relevanter Bausteine im kommunalen Ökosystem fördert den Austausch von Best Practices und schafft Synergien im Bereich IT-Sicherheit.

Nicht zuletzt liegt ein entscheidender Hebel in der gezielten Weiterbildung und Sensibilisierung aller Mitarbeitenden. Schulungen zum sicheren Umgang mit KI-Systemen und zur Erkennung von KI-generierten Cyberangriffen erhöhen die Abwehrbereitschaft und stärken die Kompetenz der Verwaltung. So wird Cybersicherheit nicht nur zur Pflicht, sondern zur Chance: Kommunen können innovative Prozesse etablieren, die ihre digitale Zukunft sichern und gleichzeitig das Vertrauen der Bürger*innen in moderne Verwaltungsdienstleistungen stärken.

Trotz der vielfältigen und dynamischen Bedrohungslage ist es Kommunen also möglich, durch den klugen Einsatz technischer Lösungen, kontinuierliche Weiterbildung und interkommunale Zusammenarbeit aktiv für ihre Sicherheit und die ihrer Bürger*innen zu sorgen. Die Entwicklung robuster und integrierter Strategien eröffnet dabei nicht nur Schutz, sondern auch Gestaltungsspielräume für eine nachhaltige, sichere und lebenswerte digitale Stadt.

5 Normung und Standardisierung

5.1 Cybersicherheitsverordnung und NIS2-Richtlinie

Standardisierung legt technische Regeln fest und dient der Definition und Einhaltung des regulatorisch vorgegebenen Rahmens. Mehr zum Thema, wie die Normung auf europäischer Ebene funktioniert, finden Sie auf din.de[5]. Im Kontext der Cybersicherheit gilt in der Europäischen Union seit 2016 die NIS-Richtlinie (Network and Information Security Directive), welche 2022 von der NIS2-Richtlinie abgelöst wurde. Die NIS2-Richtlinie konzentriert sich auf die Sicherheit kritischer Infrastrukturen und Dienstleistungen in der EU, wie Energieversorgung, Transport, Banken und Gesundheitswesen, und legt den Grundstein für die Regulierung der Cybersicherheit im europäischen Raum. Sie verpflichtet Mitgliedstaaten, bestimmte Sicherheitsmaßnahmen umzusetzen und bedeutende Vorfälle zu melden, um die Widerstandsfähigkeit gegen Cyberangriffe zu erhöhen. Die NIS2-Richtlinie wird durch einen neuen Gesetzesvorschlag der Europäischen Union, die sogenannte Cybersicherheitsverordnung „Cyber Resilience Act" (CRA), ergänzt, welche darauf abzielt, umfassende Cybersicherheitsstandards für alle Produkte mit digitalen Elementen zu etablieren, unabhängig davon, ob sie in kritischen Sektoren eingesetzt werden oder nicht. Der Fokus liegt auf den Herstellern und der Produktentwicklung. Zudem wirkt der „Cyber Security Act" (CSA), welcher als EU-weiter Rahmen für Cybersicherheitszertifizierungen dienen soll.

In Deutschland betrifft die NIS2-Richtlinie Städte und Kommunen bislang nur indirekt. So ist die „Kernverwaltung" laut IT-PRL Beschluss explizit herausgenommen, soll aber dennoch mitgedacht werden.[6] Kommunalverwaltungen sind derzeit nicht verpflichtend eingebunden. Kommunale Unternehmen wie Stadtwerke, Krankenhäuser oder ÖPNV-Betriebe können jedoch unter die Richtlinie fallen, sofern sie bestimmte Schwellenwerte bei Mitarbeiterzahl, Umsatz oder Sektorzugehörigkeit erfüllen. Auch wenn keine gesetzliche Pflicht besteht, wird Kommunen empfohlen, proaktiv Maßnahmen zur IT-Sicherheit zu ergreifen.

So sollten Städte und Kommunen u. a. sicherstellen, dass die von ihnen verwendeten technischen Systeme und Produkte den neuesten Sicherheitsanforderungen entsprechen, um ihre Cybersicherheit zu gewährleisten. Schon bei der Auswahl und Beschaffung von IT-Produkten sollte verstärkt darauf geachtet werden, dass diese die Anforderungen des Gesetzes erfüllen. Ebenso kann es notwendig werden, dass Mitarbeiter*innen im Bereich IT und Cybersicherheit weitergebildet und entsprechend geschult werden, um die Einhaltung der Sicherheitsrichtlinien zu gewährleisten.

Insgesamt sollten Kommunen sich über eine Cybersicherheitsstrategie Gedanken machen, wobei sich an NIS2, CSA und CRA orientiert werden sollte. Dabei können Normen und Standards die Umsetzung der Gesetzgebung unterstützen, indem technische Anforderungen, Prozesse oder Begriffe definiert werden.

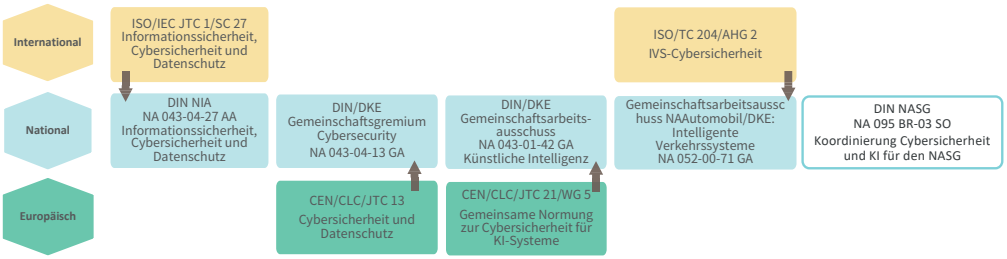
---

5 https://www.din.de/de/din-und-seine-partner/din-in-der-welt/din-in-europa/regulatorischer-kontext

6 Bundesregierung. (2025). *Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung*. Kapitel 1, § 28 Abschnitt 4, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf_2025.pdf?__blob=publicationFile&v=4

5.2 Cybersicherheitsrelevante Normungsgremien

Ähnlich zur Normungslandschaft im Bereich Smart City gibt es eine Reihe von nationalen Normungsgremien, die sich mit der Festlegung und Entwicklung von Standards im Bereich der Informations- und Cybersicherheit und des Datenschutzes befassen. Diese Gremien übernehmen sowohl nationale als auch internationale Aufgaben und arbeiten eng mit entsprechenden europäischen und internationalen Gremien bei CEN, CENELEC, ISO und IEC zusammen.



(Quelle und Copyright SCSF, DIN 2025)

Bild 3: Cybersicherheitsrelevante Normungsgremien

Die in Bild 3 dargestellten Normungsgremien mit Relevanz für den Bereich Cybersicherheit beinhalten nationale und internationale Ausschüsse, die sich mit der Entwicklung von Normen für Informations- und Cybersicherheit beschäftigen. Diese Gremien spiegeln die internationale und europäische Arbeit und sorgen dafür, dass deutsche Interessen in die internationale und europäische Normung einfließen und nationale Normen die globalen und europäischen Richtlinien erfüllen. Dazu gehören auch Ausschüsse, die sich auf die Cybersicherheit von KI-Systemen und intelligenten Verkehrssystemen konzentrieren.

Durch die Arbeit dieser Normungsgremien wird eine kohärente und umfassende Entwicklung von Normen und Standards, die einen wesentlichen Beitrag zur Sicherung digitaler Systeme in Deutschland und darüber hinaus leisten, ermöglicht.

5.3 Weitere relevante Akteure

BSI – Bundesamt für Sicherheit in der Informationstechnik
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cybersicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland. Durch Aufklärung, Beratung und gezielte Maßnahmen dient es als zentrale Instanz für IT-Sicherheit und prüft und zertifiziert IT-Produkte und Systeme, um deren Sicherheit gemäß geltenden Normen und Standards sicherzustellen. Das BSI entwickelt Standards, Richtlinien und Handlungsempfehlungen als Basis für eine sichere IT-Infrastruktur, sowohl national als auch im globalen Kontext.

5.4 Überblick bereits existierender Normen und Standards im Bereich Smart City

Die genannten Normungsgremien haben bereits einige Normungsdokumente zur Cybersicherheit entwickelt. Im Kontext Smart City umfasst das rund 250 Dokumente. (Übersicht der Dokumente siehe Kapitel 7, Anhang) Diese Dokumente decken eine breite Palette von Anwendungen und Sektoren ab und sind von entscheidender Bedeutung, um die Sicherheit in verschiedenen Bereichen der Informationstechnologie und deren Anwendungen zu gewährleisten. Sie bieten umfassende Leitlinien für Unternehmen, Organisationen und Einzelpersonen, die ihre Systeme und Daten gegen Bedrohungen schützen müssen.

Im Folgenden werden einige der derzeit verfügbaren Normen und Standards sowie weitere hilfreiche Dokumente im Bereich Cybersicherheit gelistet, die ganz oder teilweise relevant für die Anwendung auf kommunaler Ebene sein könnten. Diese Liste ist nicht endgültig und wird kontinuierlich durch die Erstellung neuer sowie durch die Überarbeitung bestehender Dokumente erweitert.

Auf internationaler Ebene sind folgende Dokumente hervorzuheben (Kurzbeschreibungen des Dokumenteninhalts siehe Kapitel 7 Anhang, Tabelle 1):

- **ISO 270XX Reihe**
- **ISO/IEC 27001** – *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*
- **ISO/IEC 27002** – *Information security, cybersecurity and privacy protection – Information security controls*
- **ISO/IEC 27005** – *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*
- **ISO/IEC 27014** – *Information security, cybersecurity and privacy protection – Governance of information security*
- **ISO/IEC 27017** – *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- **ISO/IEC 27018** – *Information security, cybersecurity and privacy protection – Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- **ISO/IEC 27033 Reihe** – *Information technology – Security techniques – Network security*
- **ISO/IEC DIS 27090** – *Cybersecurity – Artificial Intelligence – Guidance for addressing security threats to artificial intelligence systems*
- **ISO/IEC 27701** – *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines* (in Überarbeitung)
- **ISO/IEC TS 27570** – *Privacy protection – Privacy guidelines for smart cities*
- **ISO/IEC WD 25093-1** – *Cybersecurity – Confidential computing – Part 1: Overview and concepts* (aktuell in Erarbeitung)
- **ISO/IEC 30182** – *Smart city concept model – Guidance for establishing a model for data interoperability*
- **ISO/IEC 17917 –** *Smart cities – Guidance to establishing a decision-making framework for sharing data and information services*
- **IEC 62443 Reihe** – *Security for industrial automation and control systems*
- **IEC 62351 Reihe** – *Power systems management and associated information exchange – Data and communications security*

Zudem ist anzumerken, dass aktuell im internationalen Standardisierungskomitee ISO/IEC JTC 1/SC 27 die Thematik „Cybersecurity framework for smart cities" diskutiert wird und die Möglichkeit besteht, dass in der Zukunft ein Standard zu der Thematik entwickelt wird.

Neben den europäischen Übernahmen internationaler Dokumente, unverändert oder modifiziert, sind im europäischen Kontext folgende Dokumente hervorzuheben (siehe Anhang, Tabelle 2):

→ **EN 18037** – *Guidelines on a sectoral cybersecurity assessment*
→ **EN 17927** – *Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products*
→ **CEN/TS 18026** – *Three-level approach for a set of cybersecurity requirements for cloud services*

Wie bereits erwähnt, ist auf nationaler Ebene auch das BSI ein entscheidender Akteur im Hinblick auf die Entwicklung von Standardisierungsdokumenten mit dem Bezug zur Cybersicherheit. Folgende Dokumente bilden dabei die Basis und können Kommunen den ersten Weg in eine abgesicherte IT-Infrastruktur ebnen (siehe Bild 4).

→ Weg in die Basisabsicherung – WiBA (BSI)[7]
→ IT-Grundschutzprofil – Basis-Absicherung Kommunalverwaltung (AG Kommunale Basisabsicherung)[8]
→ BSI TR-03187 – Sicherheitsanforderungen an Urbane Datenplattformen (UDP) (BSI)[9]

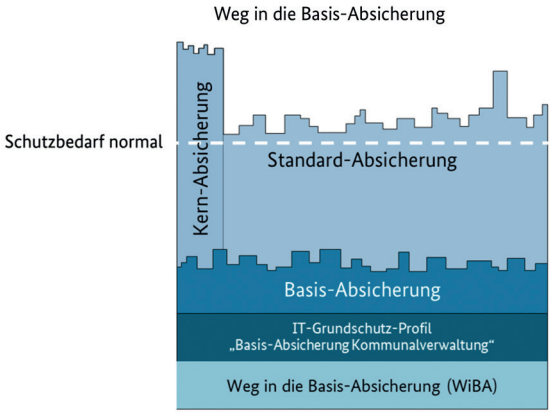


Bild 4: Stufen des BSI-IT-Grundschutzes [Quelle: BSI]

7 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/WIBA/Weg_in_die_Basis_Absicherung_WiBA_node.html

8 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.pdf?__blob=publicationFile&v=12

9 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03187/BSI-TR-03187.html

Weitere relevante Leitlinien für die öffentliche Verwaltung (siehe Anhang, Tabelle 3)

- **Branchenspezifischen Sicherheitsstandards (B3S) für KRITIS Betreiber**
- **DIN SPEC 27076 – IT-Sicherheitsberatung für Klein- und Kleinstunternehmen**
- **„Smart Cities/Smart Regions Informationssicherheit für IoT-Infrastrukturen“[10]**
- **Handreichung für Kommunen – „Informationssicherheit in Kommunalverwaltungen“ (Kommunale Spitzenverbände)[11]**
- **Handreichung „Kommunale IT-Krisen: Handlungsfähigkeit sichern – Ein Wegweiser zur Bewältigung und Prävention“[12]**

Weitere relevante Anlaufstellen

- IT-Planungsrat Schwerpunktthema Informationssicherheit
- BSI Dialog für Cybersicherheit
- Cybersicherheitskompass – Orientierungshilfe für Kommunen (Stiftung neue Verantwortung)
- Projekt REDIKOM – Resilienz Digitaler Kommunen in Krisenzeiten (vom BMFTR gefördertes Projekt)
- Government Innovation Board des GovTech Campus Deutschland e. V. (initiiert vom BMI)
- Cybersecurity Navigator

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartCity/Handlungsempfehlungen_Smart_City.pdf?__blob=publicationFile&v=3

11 https://www.staedtetag.de/files/dst/docs/Themen/2024/Handreichung-ISLL-2024.pdf

12 https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/wegweiser-kommunale-it-krisen_download.pdf?__blob=publicationFile

6 Fazit

Mit der normativen Umsetzung der Cybersicherheitsverordnung sowie der NIS2-Richtlinie sind in den nächsten Monaten und Jahren weitere Standardisierungsdokumente zu erwarten. Bestehende Standards und Handreichungen adressieren im Ansatz die technische und normative Umsetzung der Regelsetzung, wobei trotz dieser Vielfalt und Fülle an Dokumenten unklar ist, ob es aktuell einen Standard gibt, der sich spezifisch mit der Cybersicherheit von Kommunen und deren kommunalem Ökosystem befasst.

Kommunen stehen vor einzigartigen Herausforderungen in der Digitalisierung und werden zunehmend Ziel von Cyberattacken. Normen und Standards, die auf die besonderen Bedürfnisse und Strukturen kommunaler Systeme eingehen, würden helfen, eine konsistente und effektive Sicherheitsstrategie zu entwickeln.

Zudem sind weitere Aspekte zu betrachten, um die Standardisierungslandschaft zu verbessern. Ein Überblick der umfangreichen Dokumentenlandschaft sowie eine Einordnung der existierenden Dokumente würde zu einer besseren Orientierung und gezielten Anwendung dieser bei den Akteur*innen im kommunalen Kontext führen. Bereits existierende Normen und Standards sollten besser bekannt gemacht und die kommunalen Akteur*innen darüber informiert und aufgeklärt werden. Dabei spielt insbesondere das Zusammenspiel verschiedener Dokumente eine Rolle. Durch gezielte Aufklärung, z. B. in Workshops oder Webinaren, könnten den Verantwortlichen in Kommunen und anderen Organisationen eine klare Übersicht und Anleitung zur Implementierung bestehender Cybersecurity-Standards geboten werden. Dies könnte dazu beitragen, die Anwendung der richtigen Dokumente zu erleichtern und sicherzustellen, dass die entsprechenden Sicherheitsmaßnahmen effektiv und effizient umgesetzt werden.

Übersichtlichkeit sowie die Vermeidung von Überkomplexität solcher Dokumente sind ebenso wichtige Aspekte. Es wird der Bedarf deutlich, mehr Hilfestellungen und Leitlinien zu definieren, wobei u. a. der Wunsch nach einer Roadmap als Empfehlung zur Erfüllung verschiedener Standards aufkommt, um die IT-Sicherheit auf kommunaler Ebene zu stärken und zu verbessern. Zudem wird betont, dass trotz vorhandener Maßnahmenempfehlungen eine rechtliche Grundlage zur Umsetzung der Standards fehle, um ihre Effektivität sicherzustellen.

Die Entwicklung eines Standards für die Cybersicherheit in kommunalen Strukturen sowie einer Orientierungshilfe für die Nutzung bestehender Normen könnte eine wertvolle Ergänzung zur bestehenden Normungsarbeit darstellen und die Widerstandsfähigkeit dieser wichtigen gesellschaftlichen Bereiche gegen Cyberbedrohungen erheblich stärken.

7 Anhang

Tabelle 1: Ausschnitt internationaler Normungsdokumente mit Relevanz für Cybersicherheit und Smart City

Dokumentennummer	Dokumententitel	Inhalt
ISO/IEC 27001	Information security, cybersecurity and privacy protection – Information security management systems – Requirements	Beschreibt Anforderungen an Informations-Sicherheitsmanagement und legt den Rahmen für Planung, Implementierung, Überwachung und Verbesserung der IT-Sicherheit fest.
ISO/IEC 27002	Information security, cybersecurity and privacy protection – Information security controls	Bietet Leitlinien und Empfehlungen zur Umsetzung von IT-Sicherheitsstandards und enthält Praktiken zur Steuerung.
ISO/IEC 27005	Information security, cybersecurity and privacy protection – Guidance on managing information security risks	Beschreibt Methoden und Prozesse zur Identifizierung und Bewertung von Risiken sowie zur Festlegung von Maßnahmen zur Risikominderung.
ISO/IEC 27014	Information security, cybersecurity and privacy protection – Governance of information security	Bietet Leitlinien zur Einrichtung eines IT-Sicherheits-Governancesystems innerhalb von Organisationen.
ISO/IEC 27017 und ISO/IEC 27018	Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services & Information security, cybersecurity and privacy protection – Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors	Beziehen sich auf Leitlinien zur IT-Sicherheit bei Cloud-Diensten und den Schutz persönlicher Daten in der Cloud.

Dokumentennummer	Dokumententitel	Inhalt
ISO/IEC 27033 Reihe	Information technology – Security techniques – Network security	U. a. Design und Implementierung von IT-Sicherheit, Bedrohungen, Kontrollmechanismen.
ISO/IEC DIS 27090	Cybersecurity – Artificial Intelligence – Guidance for addressing security threats to artificial intelligence systems	Anleitung für Organisationen jeder Größe und Art, um Sicherheitsbedrohungen und -ausfälle in KI-Systemen während ihres gesamten Lebenszyklus zu verstehen, zu erkennen und zu mindern.
ISO/IEC WD 25093-1	Cybersecurity – Confidential computing – Part 1: Overview and concepts (aktuell in Erarbeitung)	Überblick und Konzept des vertraulichen Computings; ist relevant für Interessengruppen, die vertrauliches Computing nutzen möchten.
ISO/IEC 27701	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines	Bietet Anforderungen und Leitlinien zur Implementierung und kontinuierlichen Verbesserung eines Privacy Information Management Systems (PIMS) als Erweiterung der bestehenden Sicherheitsstandards.
ISO/IEC TS 27570	Privacy protection – Privacy guidelines for smart cities	Bietet bürgerzentrierte Leitlinien für den Schutz der Privatsphäre in Smart-City-Ökosystemen und zeigt, wie Standards von Organisationen jeder Art und Größe zur Wahrung der Bürgerrechte angewendet werden können.
ISO/IEC 30182	Smart city concept model – Guidance for establishing a model for data interoperability	Bietet ein Smart City Concept Model (SCCM) zur Förderung der semantischen Interoperabilität zwischen verschiedenen Systemen einer Smart City, indem es Konzepte und deren Beziehungen definiert, damit Organisationen, die städtische Dienstleistungen anbieten, Daten effektiv verwalten und nutzen können.

Dokumentennummer	Dokumententitel	Inhalt
ISO/IEC 17917	Smart cities – Guidance to establishing a decision-making framework for sharing data and information services	Bietet Leitlinien zur Entwicklung eines Entscheidungsrahmens für die Daten- und Informationsfreigabe in Smart Cities, indem Datentypen, die Kultur des Teilens, Rollen in der Wertschöpfungskette, Zwecke der Datennutzung, Zugriffsrechte und Formate behandelt werden, um Transparenz zu fördern und effektive Entscheidungen zu erleichtern, ohne nationale Sicherheitsfragen oder spezifische Vorschriften eines Rechtsraums abzudecken.
ISO/IEC TS 27570	Privacy protection – Privacy guidelines for smart cities	Bietet Leitlinien zum Schutz der Privatsphäre im Smart-City-Ökosystem aus einer multiagentiellen und bürgerzentrierten Perspektive und zeigt, wie Standards auf globaler und organisatorischer Ebene zum Nutzen der Bürger angewendet werden können, wobei es für alle Organisationstypen und -größen gilt, die in Smart-City-Umgebungen tätig sind.
IEC 62443 Reihe	Security for industrial automation and control systems	Legt Sicherheitsmaßnahmen und Kriterien fest, um die Integrität und Verfügbarkeit industrieller Automatisierungs- und Steuerungssysteme (IACS) zu verbessern. Sie hilft, Schwachstellen zu identifizieren und zu adressieren, um das Risiko von Informationskompromittierungen oder Produktionsausfällen zu reduzieren.
IEC 62351 Reihe	Power systems management and associated information exchange – Data and communications security	Umfasst Standards zur Sicherung von Energiemanagementsystemen und Kommunikationsnetzwerken im Energiesektor, indem sie Sicherheitsmaßnahmen wie rollenbasierte Zugriffssteuerung, Verschlüsselung und Authentifizierung für bekannte Protokolle integriert, um Datenvertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

Tabelle 2: Ausschnitt europäischer Normungsdokumente mit Relevanz zu Cybersicherheit und Smart City

Dokumentennummer	Dokumententitel	Inhalt
EN 18037	Guidelines on a sectoral cybersecurity assessment	Bietet Leitlinien, die bei der Ausarbeitung von Anforderungen an Zertifizierungssysteme für die Cybersicherheit für sektorale IKT-Dienste und -Systeme zu verwenden sind.
EN 17927	Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products	Beschreibt eine Methode zur Bewertung der Cybersicherheit von IoT-Produktplattformen, die SESIP-Methode, die eine Vergleichbarkeit und Wiederverwendung von Sicherheitsbewertungen über Hardware- und Software-Plattformteile hinweg ermöglicht.
CEN/TS 18026	Three-level approach for a set of cybersecurity requirements for cloud services	Beschreibung der Anforderungen an die Cybersicherheit für Cloud-Dienste, die für Organisationen gelten, die Cloud-Dienste anbieten, und für Organisationen, die Unterdienste anbieten.

Tabelle 3: weitere nationale, relevante Dokumente

Dokument	Inhalt
Branchenspezifische Sicherheitsstandards (B3S) für KRITIS Betreiber	KRITIS-Betreiber oder ihre Verbände können in „Branchenspezifischen Sicherheitsstandards" festlegen, wie Anforderungen zum Stand der Technik umgesetzt werden, und erhalten durch einen anerkannten Audit Rechtssicherheit. Diese B3S werden vom BSI geprüft und bei Eignung öffentlich zugänglich gemacht, wie etwa für Fernwärmenetze oder den kommunalen Straßenverkehr.
DIN SPEC 27076 – IT-Sicherheitsberatung für Klein- und Kleinstunternehmen	Ermöglicht kleinen und mittleren Unternehmen, einen standardisierten IT-Sicherheitscheck namens „CyberRisikoCheck" durchzuführen, um ihre aktuelle IT-Sicherheit zu evaluieren und konkrete Verbesserungsmaßnahmen zu empfehlen. Dieses Verfahren ist eine niederschwellige und praxistaugliche Lösung zur Verbesserung der IT-Sicherheit für Unternehmen, bei denen solche Prozesse sonst schwierig oder unmöglich umzusetzen wären. Das BSI war hier federführend und betrachtet das Dokument als ebenso geeignet für kommunale Unternehmen.

Dokument	Inhalt
Smart Cities/Smart Regions Informationssicherheit für IoT-Infrastrukturen (BSI)	Bietet Handlungsempfehlungen zur Unterstützung von Kommunen und Städten beim Aufbau sicherer IoT-Infrastrukturen. Es konzentriert sich auf die Informationssicherheit, die für digitale Dienstleistungen der kommunalen Daseinsvorsorge wie öffentlichen Nahverkehr und Abfallentsorgung entscheidend ist.
Handreichung für Kommunen – Informationssicherheit in Kommunalverwaltungen (Kommunale Spitzenverbände)	Bietet Kommunalverwaltungen ein praxisorientiertes Werkzeug zur Verbesserung der Informationssicherheit, indem es Grundlagen sowie anerkannte Standards wie ISO/IEC 27001 und IT-Grundschutz thematisiert. Mit der Ausgabe 2024 werden zudem erprobte Mustertexte, aktualisierte Schutzbedarfskategorien und Sicherheitsziele bereitgestellt, um die praktische Anwendung und Umsetzung eines Informationssicherheits-Managementsystems (ISMS) in der modernen Kommunalverwaltung zu erleichtern.
Handreichung „Kommunale IT-Krisen: Handlungsfähigkeit sichern – Ein Wegweiser zur Bewältigung und Prävention“	Bietet Kommunen einen Einstieg in das Thema IT-Krisen und hilft, Daten und Infrastrukturen effektiver vor Gefahren zu schützen, um die Folgen von Cyberangriffen zu minimieren. Die Handreichung enthält umfassende Informationen und praxisnahe Hinweise zu verwandten Themen, die die Auseinandersetzung mit IT-Gefahrenlagen erleichtern.
Weg in die Basisabsicherung – WiBA (BSI)	Vereinfacht den Einstieg in den IT-Grundschutz für Kommunen durch themenspezifische Checklisten und Prüffragen, um auch ohne tiefere Methodikkenntnisse notwendige Anforderungen zur Informationssicherheit zu identifizieren und umzusetzen.
IT-Grundschutzprofil – Basis-Absicherung Kommunalverwaltung (AG Kommunale Basisabsicherung)	Definiert Mindestsicherheitsmaßnahmen für Kommunalverwaltungen auf Grundlage des BSI-Standards 200-2, um grobe Fahrlässigkeit zu vermeiden, und erleichtert den Einstieg in die Informationssicherheit durch Aufdeckung und Beseitigung von Schwachstellen.
BSI TR-03187 – Sicherheitsanforderungen an Urbane Datenplattformen (UDP) (BSI)	Bietet Schutzlevel mit spezifischen Anforderungen für die Architektur, Authentifizierung/Autorisierung, Schnittstellen, Logging, Datenhaltung und IT-Sicherheitsorganisation von urbanen Datenplattformen, um deren Sicherheit zu erhöhen und einen einfachen Einstieg für diverse Stakeholder zu ermöglichen.

8 Themensammlung / Aktuelles und Links – Glossar

DIN e. V. – Technologie und Mensch in der Kommune von morgen – Impulspapier II zu Normen und Standards – Smart City, Juni 2021

Beispiel für IT-Architekturmodell der Stadt Osnabrück, Smart-City-Sicherheitskonzept:
https://gitlab.opencode.de/stadtosnabrueck/smart_city_sicherheitskonzept

Cybersicherheitskompass:
https://www.bmwsb.bund.de/SharedDocs/kurzmeldungen/Webs/BMWSB/DE/2023/09/smart-cities-cybersicherheitskompass.html

Cybersecurity Navigator:
https://cybersecurity-navigator.de/

Artikel zum Thema KI-gestützte Cybersecurity-Angriffe:
https://www.security-insider.de/unternehmen-ki-cyberangriffe-sicherheit-a-89981f9cad-b413590da8f2b26081d956/?cmp=nl-ede617ce-bb32-418b-8967-bc79e3a81876&u-uid=5CF425DB-F1E5-44D1-883D-73E64056C0BB

Beispiele für bekannte Sicherheitslücken:

- Cyberangriff auf Ellwangen:
  https://www.egovernment.de/cyberangriff-auf-die-stadtverwaltung-ellwan-gen-a-13ad71410bfab52218e603dc7f7fd62c/?cmp=nl-3d1c76fe-0d72-4f50-9d59-4f46c9f9f67e&uuid=B75F94B8-6F94-41C0-80EE50AC7B124F45
- Die Stadt Ellwangen betreibt smarte Ampeln mit KI in einer Testphase:
  https://www.egovernment.de/smarte-stadt-mit-smarter-ampel-a-59798fd65fea69bbe-acbf32139a38f76/?cflt=rel
- Digitaler Zwilling – ein Beitrag der ARD-Tagesschau-Mediathek am Beispiel der hochauflösenden Geodaten in NRW:
  https://www.tagesschau.de/investigativ/ndr-wdr/geodaten-digitaler-zwilling-nrw-100.html
- Enisa kooperiert mit CVE – neue EU-Datenbank listet bekannte IT-Sicherheitslücken:
  https://www.egovernment.de/neue-eu-datenbank-listet-bekannte-it-sicherheitslue-cken-a-fdd49ef3901f6a117d0da07bf1dc6dc8/?cmp=nl-3d1c76fe-0d72-4f50-9d59-4f46c9f-9f67e&uuid=B75F94B8-6F94-41C0-80EE50AC7B124F45

Glossar

Begriff	Erläuterung
Deepfakes	(engl.) Fälschungen durch Nutzung tiefer neuronaler Netze (deep neural networks) Durch künstliche Intelligenz werden Bilder oder Videos manipuliert oder gefälscht. BSI – Deepfakes – Gefahren und Gegenmaßnahmen
Denial of Service (DoS)-Attacken	(engl.) Verweigerung des Dienstes Bei einer DoS-Attacke wird ein System mit einer hohen Zahl an Anfragen geflutet, bis es unter der Last zusammenbricht und der angebotene Dienst nicht mehr zur Verfügung steht. BSI – Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS)
Identitäts-diebstahl	Kriminelle geben sich im Internet als eine andere Person aus, um sich selbst einen Vorteil zu verschaffen. BSI – So schützen Sie sich vor digitalem Identitätsdiebstahl und gehackten Accounts
Phishing	= Password Fishing, das Fischen nach Passwörtern Kriminelle senden z. B. E-Mails, um Empfänger mit einem Schad-programm oder Links zu gefälschten Webseiten nach persönlichen Daten wie Passwörtern auszuspionieren. BSI – Passwortdiebstahl durch Phishing E-Mails
Port Scanning	Beim Port Scanning werden IT-Systeme auf offene Schnittstellen und mögliche Angriffspunkte überprüft. BSI – Fragen und Antworten CERT-BUND
Ransomware	= Ransom Software, Lösegeld-Software Bei einem Ransomware-Angriff werden die Daten auf einem IT-System verschlüsselt und anschließend ein Lösegeld erpresst. Erst nach der Zahlung werden die Daten wieder entschlüsselt. BSI – Ransomware Angriffe
Social Engineering	Social Engineering ist ein Überbegriff für Angriffe wie Phishing, bei denen Menschen getäuscht und ausgenutzt werden, um das jeweilige Ziel der Kriminellen zu erreichen. BSI – Social Engineering – der Mensch als Schwachstelle
Vishing – Telefonanrufe	= Phishing via voice, das telefonische Fischen nach Passwörtern Eine Unterart des Phishings, bei dem Kriminelle ihre potenziellen Opfer anrufen, um vertrauliche Informationen wie Passwörter in Erfahrung zu bringen. BSI – Passwortdiebstahl durch Phishing E-Mails

Herausgeber

DIN e. V.
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin
Telefon: +49 30 2601-0
E-Mail: presse@din.de
Internet: www.din.de

Stand: November 2025

DIN