Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Smart Cities/Smart Regions – Informationssicherheit für IoT-Infrastrukturen

Handlungsempfehlungen

Änderungshistorie

Version	*Datum*	*Verfasser*	*Beschreibung*
1.0	Januar 2022	BSI, Referat DI 22	Erste Veröffentlichung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: smartcity@bsi.bund.de
Internet: https://www.bsi.bund.de

Danksagung

Die vorliegenden Handlungsempfehlungen sind das zentrale Ergebnis des BSI-Projekts „SMIoTI“ (Secure Municipal IoT-Infrastructures). Im Rahmen des Projekts erhielten das Bundesamt für Sicherheit in der Informationstechnik (BSI) und seine Partner BearingPoint GmbH Deutschland, HABBEL UG und TÜV NORD IT Secure Communications GmbH & Co. KG Einblicke in bestehende Smart-City-Projekte verschiedener Städte und Kommunen. Diese Informationen waren der entscheidende Beitrag zur Entwicklung bedarfsorientierter Handlungsempfehlungen zur IT-Sicherheit kommunaler IoT-Infrastrukturen.

Aus diesem Grund dankt das Bundesamt für Sicherheit in der Informationstechnik vertreten durch das Referat DI 22 den beteiligten Städten und Kommunen Delbrück, Dresden, Hamburg, Haßfurt, Kaiserslautern, Paderborn, Solingen, Ulm und Wolfsburg mit ihren Mitarbeiterinnen und Mitarbeitern für die wertvollen Einblicke und die engagierte Unterstützung.

Inhalt

Abbildungsverzeichnis

Management Summary

Smarte vernetzte Städte sind die Zukunft. Viele Städte und Gemeinden machen sich derzeit auf, die Vorteile der digitalen Welt für sich und ihre Bürgerinnen und Bürger zu nutzen. Mit der Verfügbarkeit von Technologien aus dem Internet der Dinge (Internet of Things, IoT) ist es nun möglich, wesentliche Funktionen und Prozesse des städtischen Lebens in den Bereichen Mobilität, Transport, Energie, Logistik, Gesundheit, Umwelt oder Verkehr zu digitalisieren. Neueste IKT (Informations- und Kommunikationstechnik) kommt so zum Einsatz mit dem Ziel, Ressourcen zu schonen, die Lebensqualität für alle Bewohnerinnen und Bewohner zu verbessern, die Wettbewerbsfähigkeit der Stadt und der ansässigen Wirtschaft zu steigern und den Schulterschluss zur Nachhaltigkeitspolitik von Bund, Land und Kommune zu erreichen. Diesen erhofften Vorteilen stehen jedoch neue Gefahren gegenüber. Fehlt es an ausreichender Sicherheit, sind die vernetzten Städte anfällig für Cyberangriffe, die schwerwiegende Folgen haben können. In den ersten Digitalisierungsprojekten werden zwar zunächst allenfalls lose verknüpfte Anwendungsfälle wie smarte Mülleimer, smarte Straßenbeleuchtungen und intelligente Ampeln getestet und betrieben. Deren künftiges Zusammenspiel und Erweiterungen um beispielsweise ein intelligentes Gebäudemanagement, eine intelligente Verkehrslenkung oder eine bedarfsgerechte und nachhaltige Wasser- und Energieversorgung, werden aber für Angreifer zunehmend interessanter. Eine umfassend digitalisierte Kommune muss sich mit der Komplexität der dafür nötigen Systeme, den entstehenden Abhängigkeiten von digitalen Lösungen und der wachsenden Angriffsfläche auseinandersetzen. Dabei werden entsprechende Risiken identifiziert und analysiert, um diese beispielsweise durch präventive Maßnahmen angemessen zu kontrollieren. Als Zielvorstellung dient der sichere kontinuierliche Betrieb von kommunalen IoT-Infrastrukturen, die insbesondere aus Sicht der Anwender relevante Prozesse digitalisieren und somit einen echten Mehrwert darstellen.

In diesem Sinne sollen die folgenden Handlungsempfehlungen kommunalen Entscheidungstragenden und operativ Verantwortlichen Orientierung und Unterstützung im Umfeld „Informationssicherheit von IoT-Infrastrukturen“ geben. Aus diesen, basierend auf den Ergebnissen des Projekts „Secure Municipal IoT Infrastructures (SMIoTI)“ abgeleiteten, Handlungsempfehlungen, können folgende vier Vorschläge extrahiert werden, die schon in der Planungsphase (siehe Kapitel 3.2) einer IoT-Infrastruktur wichtig und nötig sind:

1. Digitalisierungsbestrebungen in einer Kommune sollten in eine Digitalisierungsstrategie münden oder darauf aufbauen, um einen nachhaltigen Digitalisierungsprozess inklusive der dafür notwendigen übergeordneten Steuerung zu etablieren.
2. Rollen, Verantwortung und mögliche Stakeholder sollten definiert/identifiziert sein, um ein strukturiertes Vorgehen zu unterstützen.
3. Anwendungsfälle (insbesondere deren Nutzen) und deren Anforderungen (z. B. organisatorisch, technisch, finanziell, personell, regulatorisch und insbesondere sicherheitsbezogen) sollten diskutiert und dokumentiert werden, um konkrete Zielvorstellungen mit Mehrwert zu entwickeln und eine vorrausschauende Ressourcenplanung zu ermöglichen.
4. Anhand der dokumentierten Anforderungen sollten Schutzbedarf bzw. Schutzziele der verarbeiteten Daten und Informationen ermittelt werden, um notwendige Sicherheitsmaßnahmen identifizieren und letztendlich umsetzen zu können.

1 Einleitung

1.1 Hintergrund und Motivation

Die digitale Transformation wird die Wirtschaft und Gesellschaft in den nächsten Jahrzehnten weiter entscheidend verändern. Bei der Vernetzung der analogen Welt spielt das Internet der Dinge (IoT) eine wesentliche Rolle. Der Umgang mit Sensoren und Kommunikationsmodulen und deren Integration hin zu Cloud-Anwendungen sind die Voraussetzung für neue Anwendungen und Geschäftsmodelle.

Der digitale Wandel im kommunalen Umfeld umfasst nicht nur die klassischen Verwaltungsdienste, sondern zunehmend auch Infrastrukturen zur Daseinsfürsorge wie z. B. Verkehr und Beförderung, Wasser- und Energieversorgung oder Müll- und Abwasserbeseitigung. Diese Aktivitäten werden oft öffentlichkeitswirksam mit den Begriffen „Smart City“ und „Smart Region“ verbunden. Diesen Begriffen wird hier folgende Bedeutung zugrunde gelegt: In einer Smart City/Smart Region wird intelligente Informations- und Kommunikationstechnologie verwendet, um Teilhabe und Lebensqualität zu erhöhen und eine ökonomisch, ökologisch und sozial nachhaltige Kommune oder Region zu schaffen[1]. In nachfolgender Abbildung 1 werden mögliche Anwendungsbereiche für Smart Cities (der Begriff wird im Folgenden immer auch synonym für die smarte Region verwendet) zusammengefasst.

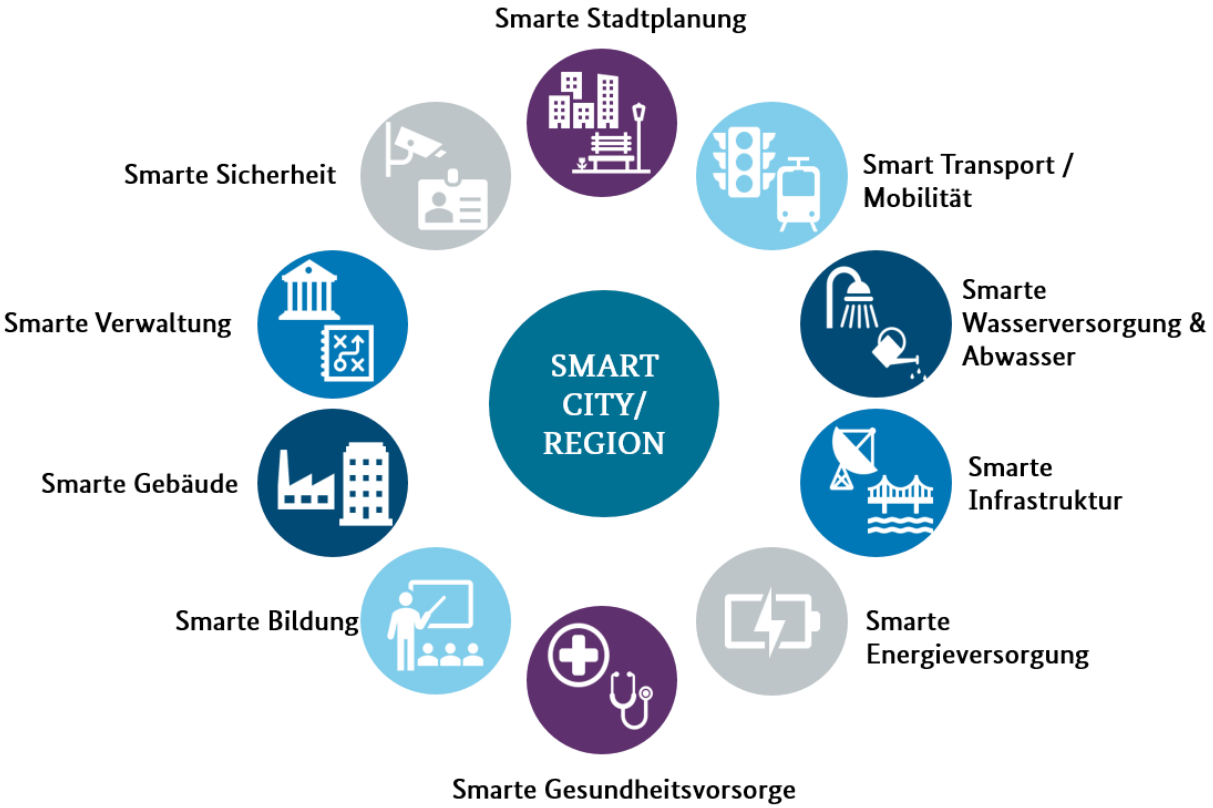

Abbildung 1 Smart City Domänen

Kommunale Infrastrukturen zur Daseinsfürsorge, die im Stadt-/Gemeindegebiet verteilte und digital vernetzte Sensoren zur Datenaufnahme und/oder Aktoren zur Steuerung nutzen, werden in diesem Dokument als „kommunale IoT-Infrastrukturen“ bezeichnet. Als technische Basis für solche Infrastrukturen und insbesondere für deren Vernetzung werden oftmals Datenplattformen verwendet, welche Daten aus verschiedenen Quellen bündeln und übergreifend nutzbar machen.

Mit zunehmender Einflussnahme digitalisierter Versorgungsdienste auf den Alltag erhöhen sich auch die Risiken z. B. durch Ausfall oder Missbrauch der dafür nötigen Infrastrukturen. Die Notwendigkeit adäquater

[1] vgl. (11)

Informationssicherheitsmaßnamen wird dadurch sichtbar. In der Studie „Zukunft wird vor Ort gemacht“ (1), wünschen sich 81 % der befragten Kommunen Unterstützung in der Digitalisierung durch den Bund. Primär soll die Unterstützung projektspezifisch sein, diese wird aber auch in Form von Dokumenten wie z. B. Leitfäden nachgefragt. Ferner geben die meisten befragten Kommunen an, dass fehlende Expertise noch vor fehlenden finanziellen Ressourcen der Hauptgrund sei, keine Digitalstrategien zu entwickeln. Das zeigt, dass kommunale Akteure einen Bedarf an Digitalisierungskompetenz haben, der daraus abgeleitet zwangsläufig auch die Thematik der Informationssicherheit umfasst.

Um diesen Unterstützungsbedarf der Kommunen zu adressieren und um die Informationssicherheit in der Digitalisierung kommunaler IoT-Infrastrukturen zu gestalten, wurden im Rahmen des BSI Projekts „SMIoTI“ (Secure Municipal IoT-Infrastructures) bestehende Smart-City-Projekte verschiedener Städte und Kommunen im Hinblick auf deren Informationssicherheit analysiert, u. a. mit dem Ziel, bedarfsorientierte Handlungsempfehlungen zu entwickeln und die Ergebnisse für künftige kommunale IoT-Projekte nutzbar zu machen. Die Empfehlungen orientieren sich dabei am Lebenszyklus einer IoT-Infrastruktur von der Idee über die Planung, ihre Implementierung und den Betrieb bis hin zur Ablösung oder Außerbetriebnahme.

1.2 Geltungsbereich und Struktur des Dokuments

Die Handlungsempfehlungen richten sich vorrangig an Kommunen oder kommunale Unternehmen, die Projekte zu IoT-Infrastrukturen initiieren und vorantreiben. Die Empfehlungen dienen dem Aufbau bzw. dem Ausbau von sicheren IoT-Infrastrukturen in Deutschland und bieten damit nützliche Hinweise für deren Realisierung.

Die Handlungsempfehlungen haben empfehlenden Charakter und sollen Kommunen oder kommunale Unternehmen und deren Umfeld beim Aufbau sicherer kommunaler IoT-Infrastrukturen unterstützen.

Die Empfehlungen liefern hierbei einen Einstieg in eine strukturierte Herangehensweise bezüglich der Informationssicherheit von kommunalen IoT-Infrastrukturen die z. B. durch die Nutzung der BSI Standards 200-x und des BSI Grundschutz Kompendiums[2] fortgeführt werden können.

Zum besseren Verständnis und zur Einordnung der Empfehlungen werden diese anhand der Phasen des Lebenszyklus einfach und strukturiert erläutert. So können sich Kommunen oder kommunale Unternehmen bei der Umsetzung auf die für sie in der aktuellen Phase relevanten Empfehlungen konzentrieren.

Dabei muss aber berücksichtigt werden, dass die Empfehlungen keinen Anspruch auf Vollständigkeit erheben.

Das vorliegende Dokument strukturiert sich in vier Bereiche:

- In der **Einleitung** werden Hintergrund und Motivation beschrieben.
- Im folgenden Kapitel werden die **Grundlagen** (technisch und organisatorisch) für kommunale IoT-Infrastrukturen erläutert.
- Die darauffolgenden **Handlungsempfehlungen** orientieren sich an diesen Grundlagen und dem Lebenszyklus.
- Abschließend wird zu den Ergebnissen ein **Ausblick** gegeben.

[2] Eine Sammlung der BSI-Standards ist unter (2) zu finden. Das Vorgehen zu dem Aufbau und Betrieb eines ISMS wird beispielsweise im BSI Standard-2 (3) beschrieben; die nötigen Maßnahmen sind im IT-Grundschutz Kompendium (12) zu finden.

2 Grundlagen

Zur Entwicklung einer Smart City bedarf es zunächst einer Strategie, die alle relevanten Stakeholder aus Verwaltung, Wirtschaft, Gesellschaft, Wissenschaft zusammenbringt, um gemeinsam Handlungsfelder und Anwendungsfälle zur Verbesserung des Gemeinwohls einer Kommune zu erarbeiten. Für die Zukunftsfähigkeit der Kommune sollten alle Bereiche der Gesellschaft in einem ausgewogenen Verhältnis berücksichtigt werden. Inhalte dieser Strategie[3] sollte unter anderem die Klärung von Verantwortlichkeiten sowie die Festlegung von Zielen für die einzelnen Handlungsfelder sein. Für die Handlungsfelder werden Anwendungsfälle entwickelt, die grob folgende Themen behandeln und in Form einer Projektskizze beschrieben werden sollten:

- Ziel und Mehrwert des Anwendungsfalles
- Beschreibung der High-Level IoT-Architektur inkl. Systeme und Komponenten
- Benennung der Beteiligten wie Projektverantwortliche, Projektmitarbeitende, Externe (z. B. Dienstleistende, Herstellende, kommunale Unternehmen, Beratende) sowie von Nutzenden (z. B. nur verwaltungsintern, Bürgerschaft, Wirtschaft)
- Beschreibung funktionaler/nicht funktionaler Anforderungen
- Erste Beschreibung der genutzten/anfallenden Daten und deren Speicherung
- Schätzung des Aufwandes (zeitlich, finanziell, sonstige Ressourcen).

Mit Hilfe der Projektskizzen erlangen die Beteiligten ein besseres Verständnis für die weitere Ausgestaltung und Planung der Anwendungsfälle. Mittels einer Roadmap gewinnt die Kommune ein umfassendes Bild für ihren Weg zu einer sicheren Smart City.

Um den Geltungsbereich dieser Handlungsempfehlung bezogen auf die Anforderungen an die Informationssicherheit für einen Anwendungsfall zu beschreiben, wird beispielhaft eine IoT-Infrastruktur skizziert. Anhand dieser werden organisatorische und technische Empfehlungen im Kapitel Handlungsempfehlungen gegeben.

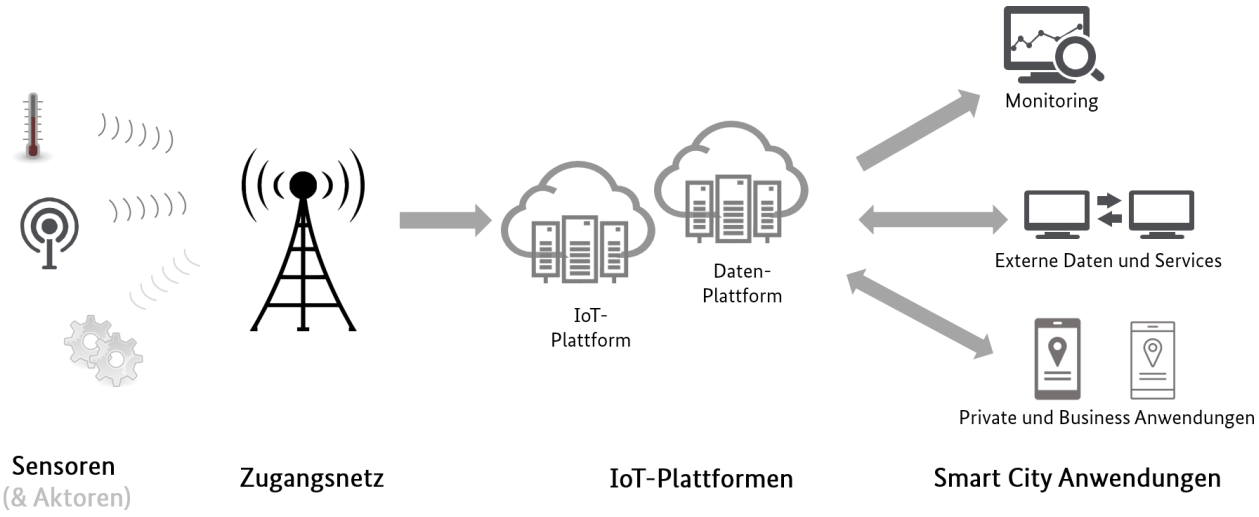

Abbildung 2 Schematische Darstellung von Smart City Komponenten

Abbildung 2 zeigt die typischen technischen Komponenten einer IoT-Infrastruktur. Die Sensoren sind über Zugangsnetze angebunden, in vielen Fällen drahtlos. Bei der mobilen Nutzung von Sensoren sind Funknetze eine Voraussetzung, aber auch stationäre Sensoren können in eine vorhandene Netzinfrastruktur eingebunden werden. Die Daten fließen von den Sensoren über das Zugangsnetz weiter zu den IKT-Plattformen. Dabei kümmern sich IoT-Plattformen insbesondere um die Verwaltung der

[3] Hinweise zu einer Smart City Strategie gibt der „Leitfaden zu Smart Cities & Regions“ (6).

verteilten Sensoren und Aktoren. Datenplattformen hingegen führen Datenströme und damit Informationen aus verschiedenen Quellen zusammen, die für eine spezielle Anwendung benötigt werden. Es ist ein wesentlicher Aspekt bei übergreifenden Digitalisierungsprojekten ist, dass Daten aus unterschiedlichen Quellen zusammengefasst und für weitere Anwendungen nutzbar gemacht werden. Je nach Anwendungsfall werden diese Informationen zur Steuerung von Aktoren verwendet. Nicht immer ist es nötig bzw. vorteilhaft zentrale Lösungen einzusetzen; so können Daten auch lokal und dezentral per Edge-/Fog Computing[4] genutzt, bzw. Steuerungsentscheidungen getroffen werden. Auch wenn die organisatorischen Details von Smart City Projekten sehr stark von der lokalen bzw. regionalen Stakeholderlandschaft abhängen, können abstrakte Rollen definiert werden, welche die Formulierung und das Verständnis der Handlungsempfehlungen erleichtern. Dabei ist es möglich, dass ein Stakeholder mehrere Rollen einnimmt. Die Rolle des Nutzers/der Nutzerin bzw. Endanwenders/Endanwenderin wird im Bezug zu diesen Empfehlungen nicht näher betrachtet, da sich diese auf den Aufbau von IoT-Infrastrukturen fokussieren[5]. Nachfolgend werden die möglichen Rollen kurz beschrieben:

Verantwortliche:

Im Kontext kommunaler IoT-Infrastrukturen sorgen Verantwortliche der Kommunen oder kommunalen Unternehmen (z. B. Digitalagenturen, Stadtwerke) dafür, dass die Anwendungsfälle der Infrastrukturen identifiziert und daraus resultierende Anforderungen adäquat umgesetzt sind.

Betreibende:

Betreibende von IoT-Infrastrukturen sorgen für einen ordnungsgemäßen technischen Betrieb der kommunalen IoT-Infrastrukturen. Betreibende stellen oftmals das Hauptkontingent an Ressourcen (z. B. Personal, Hardware), um Betriebsprozesse zu realisieren. Betreibende (z. B. Administrierende einer kommunalen Datenplattform) können beispielsweise externe Dienstleistende (z. B. Netzbetreibende), kommunale Unternehmen oder kommunale Organisationsformen sein.

Integrierende:

Integrierende sind für die technische Konzeption und den Aufbau einer kommunalen IoT-Infrastruktur zuständig. Sie sorgen dafür, dass die Voraussetzungen zur (technischen) Umsetzungen von Anforderungen an die IoT-Infrastruktur geschaffen sind. Dafür werden Produkte von Herstellenden/Entwickelnden ausgewählt und deren Integration in die IoT-Infrastruktur vorbereitet und durchgeführt. Hier sind dies meist externe Dienstleistende (z. B. Beratende, aber auch Herstellende/Entwickelnde, die ein Gesamtprodukt bereitstellen) aber auch kommunale Unternehmen oder die kommunalen Organisationsformen selbst.

Herstellende/Entwickelnde:

Herstellende/Entwickelnde sind die Bereitsteller von Produkten für kommunale IoT-Infrastrukturen (z. B. IoT-Geräte, Kommunikationsgateways, Softwarekomponenten). Diese werden oft nicht nur für die exklusiven Bedarfe bestimmter kommunaler IoT-Infrastrukturen hergestellt/entwickelt und bedürfen einer besonderen Integration in eine IoT-Infrastruktur z. B. durch Konfiguration der Produkte. Oft wird diese Rolle von externen Dienstleistenden gestellt. In bestimmten Fällen kann diese Rolle insbesondere bei der Softwareentwicklung für kommunale Anwendungen auch durch kommunale Organisationsformen oder kommunale Unternehmen ausgefüllt werden.

[4] Edge und Fog Computing bezeichnen Konzepte, bei denen im Gegensatz zum Cloud Computing Ressourcen z. B. zur Datenverarbeitung oder Speicherung nicht zentral sondern dezentral bereitgestellt werden.

[5] Die adäquate Berücksichtigung der Erwartungen und Anforderungen der Endanwender ist ein entscheidender Erfolgsfaktor bei Digitalisierungsprojekten.

3 Handlungsempfehlungen

Mit den Handlungsempfehlungen wird der Leitfrage nachgegangen, wie sichere IoT-Infrastrukturen für Smart Cities aufgebaut werden können. Dies zum Anlass nehmend, wollen die nachfolgend aufgeführten Empfehlungen kommunalen Entscheidungstragenden und operativ Verantwortlichen Orientierung und Unterstützung auf dem Weg zur Gestaltung sicherer Smart Cities geben. Um die Empfehlungen anwendbar zu gestalten, werden diese anhand der organisatorischen Rollen (siehe Kapitel Grundlagen) und eines typischen Lebenszyklus von informationstechnisch basierten Anwendungen ausgearbeitet. Die Nutzung der Phasen des Lebenszyklus (siehe *Abbildung 3*) ist ein direktes Ergebnis der Untersuchungen der verschiedenen Kommunen im Rahmen des eingangs beschriebenen Projektes SMIoTI.

Alle Empfehlungen zu den einzelnen Phasen sind jeweils unterschieden in:

- Organisatorische und prozessuale Empfehlungen sowie
- Technische Empfehlungen

Abbildung 3 Lebenszyklus einer IoT-Infrastruktur

Im Anschluss werden die Ergebnisse für jede Phase zusammengefasst.

Die Empfehlungen stellen in ihrer Gesamtheit eine Sammlung von Lösungen und Vorgehensweisen zur Informationssicherheit kommunaler IoT-Infrastrukturen bereit. Dabei orientieren sich diese unter anderem an den BSI 200-x Standards (2), dem BSI IT-Grundschutz Kompendium (3), dem BSI Cloud Computing Katalog (C5) (4) sowie der ISO/IEC 27001 (5), die standardisierte Vorgehensweisen zum Schutz der eingesetzten Informationstechnik beschreiben.

3.1 Experimentierphase

Die Experimentierphase ist gekennzeichnet vom Ausprobieren und Ausloten verschiedener technischer Ideen. In dieser Phase geht es weniger darum, effiziente Betriebsprozesse zu implementieren oder umfangreiche Konzepte und Dokumentationen zu erstellen. Vielmehr gilt es mögliche technische Ausgestaltungen von IoT-Infrastrukturen zu untersuchen und Rahmenbedingungen für spätere Betriebsprozesse zu analysieren.

Gleichzeitig bietet die Experimentierphase das Potenzial, den für den neuen Anwendungsfall aufkeimenden Pioniergeist zu nutzen und mit einer minimalen Dokumentation (z. B. bei der Diskussion neuer Architekturmodelle im Rahmen von Brainstormings) die Grundlage für spätere Projektphasen zu schaffen. Verantwortliche für den jeweiligen Anwendungsfall bekommen einen Eindruck von der Leistungsfähigkeit technischer Lösungen und von den technischen und organisatorischen Voraussetzungen. Betreibende, Integrierende und Herstellende/Entwickelnde sammeln wertvolle Erfahrungen für den Einsatz und Betrieb der digitalen Lösungen in der Realität. Aus Sicht der Informationssicherheit ergeben sich dabei die folgenden Aktivitäten:

Organisatorische und prozessuale Empfehlungen

- Schon in der Experimentierphase sollten alle Stakeholder und ihre Rollen (siehe Kapitel 2) klar benannt und somit insbesondere die Verantwortlichkeiten identifiziert werden. Damit wird auch verständlich, welche Vereinbarungen später mit externen Partnern getroffen werden müssen. Wichtig ist auch hier, dass die Zustimmung der Leitung zur Planung des IoT-Vorhabens vorhanden ist.
- Der Anwendungsfall in Verbindung mit der IoT-Infrastruktur sollte anhand einer passenden Projektskizze (siehe auch Kapitel Planungsphase) in Form und Umfang ausreichend beschrieben

werden. So können im Rahmen der Experimentierphase getroffene Entscheidungen und deren Auswirkungen auf die technische Umsetzung später einfacher nachvollzogen werden.

- Die Verantwortlichen sollten sich mit dem Schutzbedarf der verarbeiteten Daten befassen, mögliche Gefährdungen[6] in Betracht ziehen und mit den anderen relevanten Stakeholdern daraus resultierende Rahmenbedingungen zur Umsetzung ableiten. Zu bedenken ist dabei z. B.
  - um welche Daten es sich insbesondere bei personenbezogenen Daten handelt,
  - welche Anforderungen diese an Vertraulichkeit, Integrität und Verfügbarkeit haben und
  - welche groben Maßnahmen insbesondere bzgl. der technischen und organisatorischen Konzeption einer IoT-Infrastruktur zu deren Erfüllung notwendig sind.

Technische Empfehlungen

- Ausgehend von der Projektskizze sollten die an dem Anwendungsfall beteiligten Komponenten hinreichend in einem Architekturmodell dokumentiert werden, um eine strukturierte Betrachtung zu ermöglichen. Dabei sollten einzelne Geräte (z. B. Sensoren und Aktoren), Systeme (z. B. Datenbanken) sowie Netze (z. B. Long Range Wide Area Networks, LoRaWAN) und die dabei genutzten Schnittstellen erfasst werden.
- Die Beschreibung von bereits existierenden, wiederverwendeten Komponenten ist dabei ebenfalls erforderlich, da sich unter Umständen die Anforderungen an diese auf Grund des neuen Anwendungsfalls verändern können.

Im Ergebnis der Experimentierphase hat die Kommune ein Verständnis dafür:

- welche Daten wie verarbeitet werden und welchen Nutzen der Anwendungsfall generieren kann,
- wie die Projekt- und Betriebsorganisation aufzubauen ist,
- welche Schnittstellen zu definieren sind und
- welche Vereinbarungen zwischen den Verantwortlichkeiten nötig sind.

3.2 Planungsphase

Während in der Experimentierphase erste Erkenntnisse hinsichtlich Organisation, Technik, Schnittstellen und der erwarteten Mehrwerte der IoT-Infrastruktur gewonnen werden konnten, wird in der Planungsphase die konkrete, für den Anwendungsfall genutzte IoT-Infrastruktur strukturiert in ihren Details definiert, beschrieben und geplant. Das IoT-Vorhaben sollte in die Digitalisierungs-/IT-Strategie eingebunden sein. Verantwortliche für die jeweiligen Anwendungsfälle stellen sicher, dass alle relevanten Aspekte angemessen berücksichtigt sind und für andere Rollen (Betreibende, Integrierende, Herstellende/Entwickelnde, siehe Kapitel 2) hinsichtlich der weiteren Projektphasen klare Aufgaben identifiziert wurden. An der Planung beteiligte Betreibende, Integrierende und Herstellende/Entwickelnde hingegen stellen sicher, dass die Voraussetzungen zur Erfüllung entsprechender Aufgaben vorhanden sind.

Aus Sicht der Informationssicherheit ergeben sich dabei die folgenden Aktivitäten:

Organisatorische und prozessuale Empfehlungen

- Informationssicherheitsbeauftragte und Datenschutzbeauftragte sollten benannt sein und eingebunden werden, um die Anforderungen an Informationssicherheit und Datenschutz zu identifizieren und für deren Umsetzung zu sorgen.
- Für alle informationssicherheitstechnischen Belange sollten klare Verantwortlichkeiten mit daran geknüpften Pflichten und Aufgaben (z. B. operativ oder kontrollierend) definiert und dokumentiert

[6] Die Auflistung möglicher Gefährdungen inkl. der nötigen Maßnahmen sind im IT-Grundschutz Kompendium (12) zu finden.

werden. Dies gilt sowohl innerhalb der Kommune als auch bei weiteren Stakeholdern (beispielsweise externen Dienstleistende) und unterstützt die praktische Umsetzung von Sicherheitsmaßnahmen sowie die Nachverfolgung der Umsetzung. Für die Entscheidung, welche Teile der IoT-Infrastruktur unter Zuhilfenahme externer Dienstleistenden geplant, implementiert und betrieben werden, sollten IT-sicherheitsrelevante Aspekte ebenfalls berücksichtigt werden. Dabei sollten insbesondere folgende Aspekte bedacht werden:

  - Knowhow bzgl. des Aufbau/Betriebs sicherer IoT-Infrastrukturen
  - Handlungsfähigkeit im Krisenfall (z. B. Reaktion auf Cyberangriffe oder kritische Schwachstellen inkl. deren proaktive Identifikation z. B. durch Abgleich mit Schwachstellendatenbanken).
- Bei der Identifikation von Anforderungen sollten folgende Aspekte berücksichtigt werden, um beispielsweise bei Beschaffungen und Beauftragungen sowie in der Implementierungsphase nötige Sicherheitsmaßnahmen zu berücksichtigen:
  - Prüfung der Relevanz von Regularien (z. B. spezialgesetzliche Regulierung im Rahmen des Messstellenbetriebsgesetzes),
  - Prüfung der Schutzwürdigkeit der IoT-Infrastruktur mit Hilfe der Schutzbedarfsfeststellung,
  - Erfassung von Gefährdungen und deren Bewertung anhand einer Risikoanalyse.
- Bei der Planung von Beschaffungen und Beauftragungen sollten, z. B. bei der Erstellung von Ausschreibungsunterlagen, folgende Themen berücksichtigt werden, um die notwendigen Grundlagen für einen sicheren Betrieb zu legen:
  - Beschreibung von Sicherheitsanforderungen
  - Nachweis der Umsetzung von Sicherheitsanforderungen (z. B. Zertifizierungen[7], Testate[8], Bereitstellung von relevanter Dokumentation wie Auditreports)
  - Prüfung, inwieweit sich die Kommune in einen Lock-In[9] begibt:
    - Abhängigkeit vom Dienstleistenden bei Ausfall
    - Aufwand bei einem Wechsel des Dienstleistenden (z. B. Datenmigration)
    - Abhängigkeit von spezifischen Kenntnissen/Erfahrungen, wenn diese nicht in der Kommune selbst vorgehalten werden
    - Aufwand bei Migration/Weiterentwicklung von Anwendungen und IT-Systemen insb. hinsichtlich der Gefahr vom Versions-Lock-In (Minimale Anpassungen von Software kann je nach Lizenzvereinbarung zu Verpflichtungen führen. Um daraus resultierende Lock-In Effekte zu minimieren, lohnt sich in der Planungsphase eine Analyse welche Lizenzvereinbarungen zu treffen sind und bis zu welchem finanziellen Schwellwert ein Lock-In akzeptiert werden kann.)
  - Für Dienstleistende sind die DL-Verträge gemäß den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit auszugestalten und die funktionalen/nicht-funktionalen Anforderungen und Service-Management Prozesse zu beschreiben.
- Erarbeitung von Notfallszenarien, die in Notfallmaßnahmen (z. B. Backup) münden sollten. Mit dem Test der Notfallmaßnahmen (Wiederherstellung des Betriebszustands) sollten Verfügbarkeitsanforderungen der IoT-Infrastruktur inkl. aller IoT-Komponenten validiert werden.

[7] Detailliertere Informationen zum Thema Zertifizierung sind unter (8) verfügbar.
[8] Testierung ist im grundlegenden Konzept hinter dem Kriterienkatalog Cloud Computing C5 enthalten. Dieses ist unter (9) verfügbar.
[9] Lock-In: Kunde ist an ein Produkt, eine Dienstleistung oder einen Anbieter gebunden und ein Wechsel ist aufgrund entstehender Wechselkosten oder sonstiger Barrieren unwirtschaftlich.

- Zur Absicherung der IoT-Infrastruktur sollten je Einsatzzweck geeignete kryptografische Verfahren ausgewählt, implementiert und dokumentiert werden. Dabei sollte sichergestellt sein, dass über den gesamten Lebenszyklus geeignete, sicher implementierte Algorithmen verwendet werden. Dazu ist der Einsatz etablierter und überprüfter Algorithmen und Implementierungen besonders geeignet. Empfohlen wird beispielsweise die Berücksichtigung der BSI TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“[10], insbesondere wenn die Implementierung getestet wurde.

Technische Empfehlungen

- Die Planung der IoT-Infrastruktur (z. B. Architektur, Schnittstellen, Datenfluss) sollte so dokumentiert werden, dass alle Komponenten in ihrer Funktionalität, insbesondere bezüglich der IT-Sicherheit verständlich beschrieben sind, um eine fundierte Analyse von Gefährdungen/Risiken, einen sicheren Betrieb und eine schnelle und adäquate Reaktion im Notfall zu ermöglichen.
- Bei der Identifikation von technischen Anforderungen von IoT-Komponenten (Sensoren/Aktoren, Komponenten für Zugangsnetze, IKT-Plattformen) sollten folgende Aspekte berücksichtigt werden:
  - Ergebnisse aus Schutzbedarfsfeststellungen, Gefährdungs- und Risikoanalysen fließen in Sicherheitsanforderungen ein
  - Sichere, effiziente Update-Möglichkeit, um z. B. Schwachstellen in der Implementierung schnell beheben zu können
  - Planung eines Komponentenmanagements beispielsweise zur Kontrolle der Installation von Software auf Betriebssystemen/Firmware, um den Zustand der IoT-Infrastruktur überwachen zu können
  - Planung Authentifizierungsmechanismen, Rollen und Berechtigungen (Zugangs- und Zugriffskontrolle)
  - Monitoring von sicherheitsrelevanten Ereignissen, wobei Protokollierungsdaten als Träger kritischer Informationen auch schützenswert sind.
- Um die IoT-Infrastruktur dauerhaft abzusichern, sollte für alle Aktualisierungen (Patches) und Änderungen ein einheitliches bzw. auf verschiedene Dienstleistende abgestimmtes Patch- und Änderungsmanagement etabliert werden. Bei Änderungen/Aktualisierungen oder bei der Implementierung neuer geschäftskritischer Anwendungen und Systeme in der IoT-Architektur, sollten stets Tests und Überprüfungen auf Funktionalität und Sicherheit vorgesehen sein, um negative Auswirkungen auf die IoT-Infrastruktur zu verhindern.

Im Ergebnis der Planungsphase ist die Kommune in die Lage versetzt, strukturiert die Implementierung vorzunehmen und hat ein Verständnis dafür:

- wie schutzbedürftig die verarbeiteten Daten und die dazugehörige IoT-Infrastruktur sind und welchen Gefahren/Risiken diese ausgesetzt ist,
- welche externen Dienstleistungen benötigt werden,
- welche Aufgaben die Verantwortlichen für Informationssicherheit und Datenschutz zu bewältigen haben,
- welche dieser Maßnahmen ggf. priorisiert umgesetzt werden sollten und
- wie im Falle eines geringfügigen Ausfalls von Systemen und Daten bzw. Notfalls gehandelt werden, sollte.

[10]BSI TR-02102 umfasst verschiedene Dokumente, welche unter (10) verfügbar sind.

3.3 Implementierungsphase

Sowohl die Planungs- als auch die Implementierungsphase sollten als Projekt aufgesetzt werden. Das heißt, dass alle nötigen technischen, organisatorischen und prozessualen Aktivitäten und Maßnahmen in ein Projektmanagement integriert werden. Mit Hilfe des strukturierten Projektmanagements werden Risiken und Schwierigkeiten frühzeitig erkannt und es ist möglich, die IoT-Infrastruktur in Zeit, Ressourcen und Budget aufzubauen. Die für den Anwendungsfall Verantwortlichen haben hierbei zentrale Steuerungs- und Überwachungsaufgaben, während Integrierende und Herstellende/Entwickelnde mit der Umsetzung der Sicherheitsmaßnahmen betraut sind, um die Voraussetzungen für einen sicheren Betrieb zu schaffen.

Organisatorische und prozessuale Empfehlungen

- In dieser Phase sollten die für den späteren Betrieb nötigen Dokumente (z. B. Betriebskonzept mit Rollen und Zuständigkeiten) erstellt werden.
- Für den künftigen Betrieb sollten die notwendigen Ressourcen (z. B. Administratoren) verfügbar und ausreichend geschult sein, um die IoT-Infrastruktur zu betreiben.
- Oftmals nutzen Kommunen für den Betrieb ihrer IoT- Infrastruktur externe Dienstleistende. Diese sollten so gesteuert werden, dass die Anforderungen der Kommune abgedeckt werden. Für die Steuerung sollten sowohl regelmäßige Abstimmungen mit dem Dienstleistenden initiiert als auch Eskalationswege, Kennzahlen zur Messung der Leistungsfähigkeit des Dienstleistenden definiert, ein kontinuierliches Reporting etabliert und die Erfüllung der Vertragsbestandteile regelmäßig überprüft werden.
- Das Berechtigungsmanagement sollte nach dem „Need-to-Know"-Prinzip[11] entwickelt und „Segregation of Duties[12]" möglichst eingehalten werden.

Technische Empfehlungen

- Während der sicheren Installation und Konfiguration der IoT-Geräte sollte überprüft werden, welche Funktionen auf den Geräten installiert bzw. aktiviert sind. Dabei kann es sich um Protokolle, Dienste, Benutzererkennungen oder (Funk-) Schnittstellen handeln. Nicht benötigte Funktionen sollten deaktiviert oder ganz deinstalliert, bzw. schon bei der Auswahl ausgeschlossen sein, mindestens aber z. B. über Firewalls unterbunden werden. IoT-Geräte sollten erst nach sicherer Konfiguration in die IoT-Infrastruktur integriert werden.
- Für die Kommunikationssicherheit sollten die geplanten kryptografischen Methoden implementiert und zugehöriges Schlüsselmaterial sicher gemanagt werden (Erzeugung, Verteilung, Speicherung, Vernichtung).
- Das Incidentmanagement der Kommune ist auf die IoT-Infrastruktur auszuweiten.

Im Ergebnis der Implementierungsphase ist die IoT-Infrastruktur bereit ordnungsgemäß betrieben zu werden und die Kommune ist in die Lage versetzt, den Betrieb strukturiert einzuleiten, da:

- die IoT-Infrastruktur sicher konfiguriert, getestet und dokumentiert ist,
- Betriebsprozesse aufgebaut sind und
- entsprechende Mitarbeitende geschult wurden.

[11] Das „Need-to-Know-Prinzip" (Kenntnis nur, wenn nötig) beschreibt ein Konzept zum Schutz vertraulicher Informationen. Personen bekommen nur dann Zugriff auf vertrauliche Informationen, wenn diese Personen entsprechende Informationen für die Erfüllung ihrer Aufgaben benötigen.

[12] „Segregation of Duties" (Aufgaben-/Funktionstrennung) beschreibt ein Konzept zum Schutz der Integrität von Prozessen. Unterschiedliche Funktionen im Rahmen eines Prozesses sind unterschiedlichen Personen zugeordnet, um beispielsweise das Aufkommen unerkannter Fehler und krimineller Handlungen zu erschweren.

3.4 Betrieb

Es kann sinnvoll sein, die Betriebsphase in eine Pilotierungsphase und Rollout-Phase zu unterteilen, um nötige Erkenntnisse für den Betrieb zu sammeln. Die für den Anwendungsfall Verantwortlichen haben hierbei übergeordnete Steuerungs- und Überwachungsaufgaben (z. B. Steuerung der Dienstleistenden), während die Betreibenden einen sicheren Betrieb garantieren. Integrierende und Herstellende/Entwickelnde stehen bereit, um insbesondere auf kritische Schwachstellen zeitnah reagieren zu können und Änderungen zu planen und umzusetzen.

Organisatorische und prozessuale Empfehlungen

- Betriebsprozesse sollten wie geplant umgesetzt werden, damit geplante Sicherheitseigenschaften erreicht werden.
- Regelmäßig sollten folgende Aktivitäten durchgeführt werden, um Informationssicherheit dauerhaft zu erhalten:
  - Aktualisierung von Schutzbedarfs- und Risikoanalyse,
  - Überprüfung der regulatorischen Anforderungen,
  - Aktualisierung der Sensibilisierungsschulungen für Mitarbeitende,
  - Aktualisierung der Notfallmaßnahmen,
  - Prüfung der Umsetzung des Backup-Konzepts,
  - Prüfung und Aktualisierung der Berechtigungen und
  - Prüfung der Einhaltung vereinbarter Anforderungen an externe Dienstleistende z. B. an Monitoring, Reporting, Aktualität der Testate und Zertifizierungen.

Technische Empfehlungen

- Es sollten regelmäßige Audits der IoT-Infrastruktur veranlasst werden, um einen sicheren Betrieb der IoT-Infrastruktur nachzuweisen.
- Betriebs- und sicherheitsrelevante Ereignisse sollten kontinuierlich ausgewertet werden, um frühzeitig Ressourcenengpässe oder Sicherheitsvorfälle zu erkennen.
- Um die IoT-Infrastruktur dauerhaft abzusichern, sollte für alle Aktualisierungen (Patches) und Änderungen ein einheitliches Patch- und Änderungsmanagement betrieben werden, welches proaktiv potenzielle Schwachstellen (z. B. durch Abgleich mit Schwachstellendatenbanken) identifiziert und insbesondere die Installation kritischer Sicherheitsupdates gewährleistet und Änderungen an der IoT-Infrastruktur dokumentiert.
- Der Incidentmanagementprozess sollte auf die gegenwärtigen Gegebenheiten angepasst sein.
- Das Schlüsselmanagement und die eingesetzten kryptografischen Verfahren sollten auf ihre Aktualität regelmäßig überprüft werden.

Im Ergebnis der Betriebsphase

- wird die IoT-Infrastruktur kontinuierlich (Business Continuity)[13] betrieben,
- wird im Falle eines Sicherheitsvorfalls adäquat reagiert und Wiederherstellungsmaßnahmen sofort eingeleitet und die bestehende IoT-Infrastruktur ohne Informationsverlust angepasst.

[13] Der BSI-Standard 200-4 (7) stellt Methoden bereit, mit denen eine Institution ein Business Continuity Management initiieren und steuern kann.

3.5 Aussonderung/Datenmigration

Der Vollständigkeit halber sei aufgeführt, dass es auch zu einer Ablösung der IoT-Infrastruktur kommen kann. Beispielsweise, weil der Bedarf sich ändert, was zu einer Neuplanung führt, ein anderer Dienstleistender gebraucht, die Infrastruktur vollständig aktualisiert oder weil die IoT-Infrastruktur nicht mehr benötigt wird. Sollte die IoT-Infrastruktur ausgesondert werden, ist es insbesondere wichtig, die Dokumentation darüber aufzubewahren, entsprechende Schnittstellen in anderen Infrastrukturen zu deaktivieren und etwaige Berechtigungen zu löschen.

4 Ausblick

Die Digitalisierung kommunaler Infrastrukturen zur Daseinsvorsorge steht in vielen Fällen noch am Anfang. Dennoch treiben viele Kommunen im Sinne einer Smart City die dafür notwendigen Prozesse voran. Um die mit voranschreitender Digitalisierung einhergehenden Informationssicherheitsrisiken für die Daseinsfürsorge zu minimieren, liefern die vorliegenden Handlungsempfehlungen einen Einstieg in eine strukturierte Auseinandersetzung mit dem Thema.

In Zukunft werden hochverfügbare Kommunikationsnetzwerke und Plattformen für diverse IoT-Infrastrukturen mit hohen Anforderungen an die Integrität entsprechender Systeme eine immer wichtigere Rolle spielen. Entsprechende Systeme bedürfen diesbezüglich einer genaueren Betrachtung. Hierbei ist geplant, auf Basis standardisierter und praxisrelevanter Modelle, konkrete Sicherheitsanforderungen zu definieren. Unter Verwendung geeigneter Prüfkriterien entsteht so die Grundlage für nachweisbar sichere Komponenten kommunaler IoT-Infrastrukturen.

Um entsprechende Anforderungen konsistent umsetzen zu können, ist ein Ökosystem notwendig, in dem alle Stakeholder befähigt sind, ihre Rolle angemessen auszufüllen. Das BSI unterstützt die Etablierung eines solchen Ökosystems nicht zuletzt durch diese Handlungsempfehlungen, die Bereitstellung des IT-Grundschutzes und einer Plattform zur Erstellung von IT-Grundschutz-Profilen durch die Anwender-Community sowie das Angebot der Zertifizierung für Managementsysteme und Produkte.

Literaturverzeichnis

1. **Initiative Stadt.Land.Digital [Hrsg.].** Zukunft wird vor Ort gemacht. [Online] Dezember 2018. [Zitat vom: 10. Dezember 2021.] https://www.de.digital/DIGITAL/Redaktion/DE/Publikation/stadt-land-digital-digitalisierung-und-intelligente-vernetzung-deutscher-kommunen.pdf.

2. **Bundesamt für Sicherheit in der Informationstechnik.** BSI-Standards. [Online] [Zitat vom: 10. Dezember 2020.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html.

3. **Bundesamt für Sicherheit in der Informationstechnik**. BSI-Standard 200-2, IT-Grundschutz-Methodik. [Online] Oktober 2017. [Zitat vom: 10. Dezember 2021.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf.

4. **Bundesamt für Sicherheit in der Informationstechnik**. Cloud Computing Compliance Criteria Catalogue – C5:2020 – Kriterienkatalog Cloud Computing. [Online] Oktober 2020. [Zitat vom: 10. Dezember 2021.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf.

5. **International Organization for Standardization (Hrsg.).** *ISO/IEC 27001:2013 Information technology – Security techniques – Information securitymanagement systems – Requirements.* 2013.

6. **Ministerium für Wirtschaft, Innovation, Digitales und Energie des Landes Nordrhein-Westfalen [Hrsg.].** Leitfaden zu Smart Cities & Regions. [Online] März 2021. [Zitat vom: 10. Dezember 2021.] https://www.wirtschaft.nrw/sites/default/files/asset/document/smart_city_leitfaden-final.pdf.

7. **Bundesamt für Sicherheit in der Informationstechnik.** BSI-Standard 200-4, Business Continuity Management - Community Draft. [Online] Januar 2021. [Zitat vom: 10. Dezember 2021.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD.pdf.

8. **Bundesamt für Sicherheit in der Informationstechnik**. Der Wert der Informationssicherheit: Zertifizierung und Anerkennung durch das BSI. [Online] [Zitat vom: 10. Dezember 2021.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/zertifizierung-und-anerkennung_node.html.

9. **Bundesamt für Sicherheit in der Informationstechnik**. C5 Einführung. [Online] [Zitat vom: 10. Dezember 2021.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Einfuehrung/C5_Einfuehrung_node.html.

10. **Bundesamt für Sicherheit in der Informationstechnik**. BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. [Online] [Zitat vom: 10. Dezember 2021.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html.

11. **Hollekamp, Thomas.** *Datensicherheit als konzeptionelle Voraussetzung für Smart Cities.* 2018.

12. **Bundesamt für Sicherheit in der Informationstechnik.** IT-Grundschutz-Kompendium. [Online] [Zitat vom: 10. Dezember 2021.] https://www.bsi.bund.de/kompendium.