Bundesinstitut
für Bau-, Stadt- und
Raumforschung

im Bundesamt für Bauwesen
und Raumordnung

Informationssicherheit in Kommunen

Maßnahmen gegen digitale Angriffe

IMPRESSUM

Herausgeber
Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR)
im Bundesamt für Bauwesen und Raumordnung (BBR)
Deichmanns Aue 31–37
53179 Bonn

Wissenschaftliche Begleitung
Bundesinstitut für Bau-, Stadt- und Raumforschung
Referat RS 5 „Digitale Stadt, Risikovorsorge und Verkehr“
Dr. Ralf Schüle
ralf.schuele@bbr.bund.de

Auftragnehmer
Fraunhofer-Institut für Experimentelles Software Engineering IESE, Kaiserslautern
Chwalek, Jessica
jessica.chwalek@iese.fraunhofer.de

Berg, Matthias
matthias.berg@iese.fraunhofer.de

Eichholz, Lutz
lutz.eichholz@iese.fraunhofer.de

Hübsch, Volker
volker.huebsch@iese.fraunhofer.de

Stand
Juli 2025

Gestaltung
Fraunhofer-Institut für Experimentelles Software Engineering IESE, Kaiserslautern
Bettina Wassermann

Druck
Kerker Druck GmbH, Kaiserslautern
Gedruckt auf Recyclingpapier

Bestellungen
publikationen.bbsr@bbr.bund.de; Stichwort: Informationssicherheit in Kommunen

Bildnachweis
Titelbild: Bettina Wassermann

DOI 10.58007/zw66-ep50
ISBN 978-3-98655-120-9 Bonn 2025

Informationssicherheit in Kommunen

Maßnahmen gegen digitale Angriffe

Bundesministerium
für Wohnen, Stadtentwicklung
und Bauwesen

ExWoSt

Das Projekt des Forschungsprogramms „Experimenteller Wohnungs- und Städtebau (ExWoSt)“ wurde vom Bundesinstitut für Bau-, Stadt- und Raumforschung (BBSR) im Auftrag des Bundesministeriums für Wohnen, Stadtentwicklung und Bauwesen (BMWSB) durchgeführt.

Inhaltsverzeichnis

Abbildung 1: Symbolbild für geschlossenes Bürgeramt

Quelle: Fraunhofer IESE

Wenn der Ernstfall eintritt

Montagmorgen, das Telefon klingelt. Eine IT-Mitarbeiterin ruft Sie an – in der Nacht gab es einen Angriff und alle IT-Systeme mussten heruntergefahren werden. Nichts geht mehr. Mitarbeitende im Rathaus hasten ratlos über die Flure. Vor dem Bürgercenter haben sich lange Reihen von Menschen gebildet, die ungeduldig mit dem Personal diskutieren. Wichtige Dokumente können nicht mehr ausgestellt, dringend benötigte Leistungen nicht mehr ausgezahlt werden. Keine Anmeldung von Wohnsitzen, keine Beantragung von Ausweisdokumenten, keine Verwaltung von Sozialleistungen und Baugenehmigungen. Niemand scheint zu wissen, was gerade passiert und wo genau die Ursache für die aktuell verfahrene Situation liegt. Fest steht bislang nur: Sämtliche IT ist ausgefallen – und Sie, als verantwortliche Führungskraft im Rathaus, stehen mitten im Geschehen. Der vermeintlich unwahrscheinliche Angriff durch Hacker hat unerwartet das eigene Rathaus getroffen. Wie konnte es nur so weit kommen? Und wie geht es jetzt eigentlich weiter?

IT-Angriffe nehmen zu

Dies ist keine Schilderung eines fiktiven Schreckensszenarios, sondern die Darstellung einer realen Bedrohung, die Unternehmen wie auch Kommunen betrifft. So stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Lagebericht zur IT-Sicherheit in Deutschland 2023 fest, dass Kommunalverwaltungen und **kommunale Versorgungsbetriebe** überproportional häufig von Ransomware-Angriffen betroffen waren.

Dabei spielte die Größe der Kommunen keine Rolle – von eher ländlichen Gemeinden mit 2.800 Einwohnerinnen und Einwohnern bis hin zu Großstädten mit über 1,8 Mio. Einwohnerinnen und Einwohnern reicht das Spektrum der betroffenen Kommunen. Betrachtet man die in den letzten Jahren bekannt gewordenen IT-Sicherheitsvorfälle in Kommunalverwaltungen, so zeigt sich ein deutliches Bild der Zunahme von Angriffen (siehe Abbildung 2).

Konkrete Beispiele finden Sie unter anderem auf der Webseite „**Kommunaler Notbetrieb**“. Dort werden öffentliche Informationen und Meldungen über IT-Sicherheitsvorfälle in Kommunalverwaltungen bereitgestellt (Kommunaler Notbetrieb o. J.).

Cyberkriminelle nutzen Schwachstellen in IT-Systemen aus, um Schäden zu verursachen. Es gibt verschiedene Akteurinnen und Akteure hinter diesen Angriffen. Einige handeln im Auftrag von Staaten, andere sind international verstreute Kollektive, die Hacking als Geschäftsmodell verfolgen. Wieder andere sind Einzelpersonen, die Angriffe durchführen, einfach weil sie die Fähigkeiten dazu haben.

Die Angriffe reichen von sogenannten Ransomware-Attacken mit Erpressung über den Diebstahl sensibler Daten bis hin zur Sabotage von Hard- und Software. Allen gemeinsam ist das Potenzial, den kompletten Verwaltungsbetrieb innerhalb kürzester Zeit lahmzulegen.

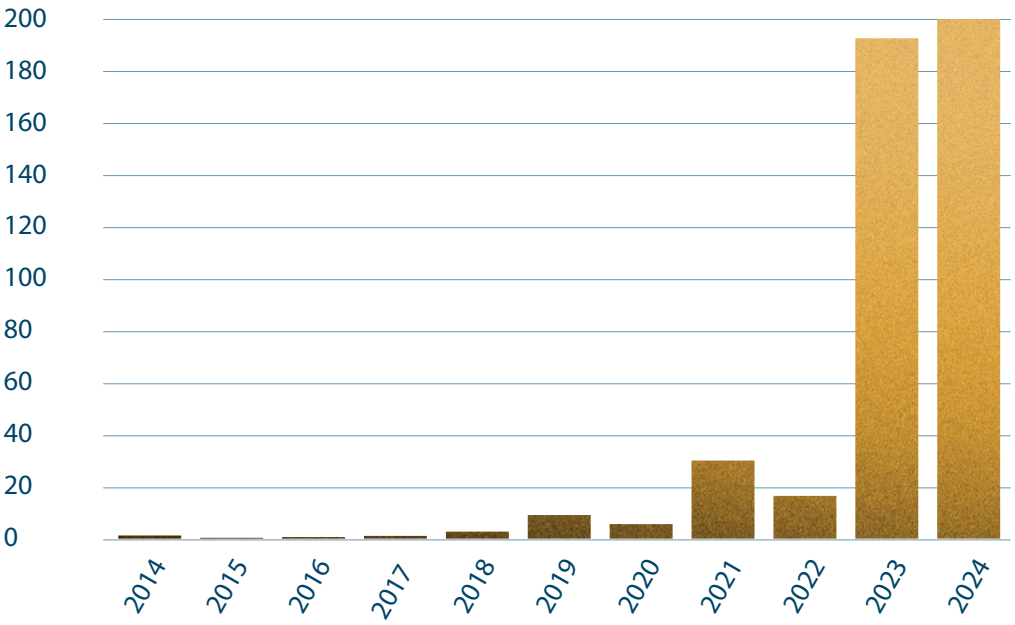


Abbildung 2: Bekannte IT-Sicherheitsvorfälle in Kommunalverwaltungen

Quelle: Fraunhofer IESE nach Kommunaler Notbetrieb o. J.

Abbildung 3: IT-Sicherheitsvorfälle in Kommunalverwaltungen von 2010–2025

Quelle: Kommunaler Notbetrieb o. J.

Digitalisierung kommunaler Dienstleistungen und Prozesse

Parallel schreitet die Digitalisierung in Kommunen stetig voran. Angefangen bei der Anmeldung von Wohnsitzen und Kraftfahrzeugen über die Beantragung von Ausweisdokumenten bis hin zur Verwaltung von Sozialleistungen und Kindergeld – all diese Aufgabenfelder basieren auf IT-gestützten Verfahren. Zusätzlich basieren Dienstleistungen und Handlungsfelder der kommunalen Daseinsvorsorge zunehmend auf digitalen Dateninfrastrukturen, aus denen sich fortschreitende Abhängigkeiten von IT-Systemen ergeben. Im Normalfall funktionieren diese Systeme einwandfrei, selbst wenn es hin und wieder zu kurzfristigen Ausfällen oder Störungen kommt.

Cyberattacken stellen für die Funktionssicherheit von kommunalen IT-Systemen eine große Herausforderung dar. Abhängig von Hintergrund und Zielen der Angreifenden muss mit langfristigen Ausfallzeiten, erheblichen Investitionen in IT-Infrastruktur und Lösegeldforderungen zur Wiederherstellung verschlüsselter Betriebsdaten gerechnet werden. Beispielsweise war der **Landkreis Anhalt-Bitterfeld** nach einem Cyberangriff im Juli 2021 (vgl. Guth/Reuters/Dpa 2021) über mehrere Wochen hinweg in seiner Handlungsfähigkeit stark eingeschränkt. Der Katastrophenfall wurde ausgerufen und erst nach etwa sieben Monaten wieder aufgehoben (vgl. MDR 2022). Nicht zu unterschätzen sind zudem die immateriellen Schäden, die entstehen, wenn sich aus dem anfänglichen Chaos neben Unverständnis und wachsender Unsicherheit in der Bevölkerung schließlich Misstrauen gegenüber der Behörde und den handelnden Akteurinnen und Akteuren entwickelt. Bürgerinnen und Bürger erwarten letztlich den vollständigen Schutz ihrer Daten und die uneingeschränkte Verfügbarkeit der ihnen zustehenden Dienstleistungen.

Es liegt an Ihnen, sicherzustellen, dass Ihre Kommune für diese Herausforderungen gewappnet ist.

DEF

Informationssicherheit

Informationssicherheit schützt umfassend alle Informationen, unabhängig davon, ob sie digital, auf Papier oder mündlich vorliegen. Sie gewährleistet den Schutz vor Verlust, unbefugtem Zugriff und Manipulation. Wichtige Aspekte sind die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, ergänzt durch Authentizität, Nichtabstreitbarkeit und Zurechenbarkeit. Ziel ist es, alle Informationen vor Gefahren und wirtschaftlichen Schäden zu sichern. Organisatorische Maßnahmen wie Richtlinien, Sensibilisierung und dokumentierte Prozesse spielen eine entscheidende Rolle und sollten regelmäßig überprüft und angepasst werden.

IT-Sicherheit ist Chefsache

Die Frage der Gesamtverantwortung ist vor dem Hintergrund der bestehenden Ämterhierarchie schnell geklärt:

Ob Bürgermeisterin oder Bürgermeister, Landrätin oder Landrat, Dezernatsleitung oder Amtsleitung – als Führungskraft in der kommunalen Verwaltung tragen Sie die Verantwortung für die Abläufe in Ihrem Zuständigkeitsbereich. Dazu gehört auch, geeignete Rahmenbedingungen für einen sicheren und zuverlässigen IT-Betrieb zu schaffen und durchzusetzen und bei möglichen Cyberangriffen vorbereitet zu sein.

Informationssicherheit ist dabei eine strategische Führungsaufgabe – kein technisches Randthema. Sie verlangt klare Priorisierung, verbindliche Entscheidungen und Ihr aktives Vorantreiben aller notwendigen Maßnahmen.

Als Führungskraft spielen Sie eine Schlüsselrolle in der IT-Sicherheit Ihrer Kommune. Sie sind nicht nur dafür verantwortlich, dass Ihre IT-Systeme sicher sind, sondern auch dafür, dass Ihre Mitarbeitenden über die notwendigen Kenntnisse und Fähigkeiten verfügen, um diese Sicherheit zu gewährleisten. Sie müssen in Wort und Tat zeigen, dass IT-Sicherheit ein Grundpfeiler für das erfolgreiche Wirken der Behörde darstellt und somit eine hohe Priorität besitzt.

DEF

IT-Sicherheit

IT-Sicherheit ist ein Teilbereich der Informationssicherheit und umfasst alle Maßnahmen zum Schutz von informationstechnischen Systemen und Netzwerken vor unbefugtem Zugriff, Missbrauch, Manipulation, Datenverlust und Zerstörung. Zu den technischen Maßnahmen zählen Firewalls, Antivirenprogramme, Verschlüsselung, regelmäßige Software-Updates und Zugriffskontrollen. Organisatorische Vorkehrungen wie die klare Definition von Verantwortlichkeiten und Sicherheitsrichtlinien sind ebenfalls wichtig. Ziel der IT-Sicherheit ist es, die Verfügbarkeit, Vertraulichkeit und Integrität von IT-Systemen zu gewährleisten.

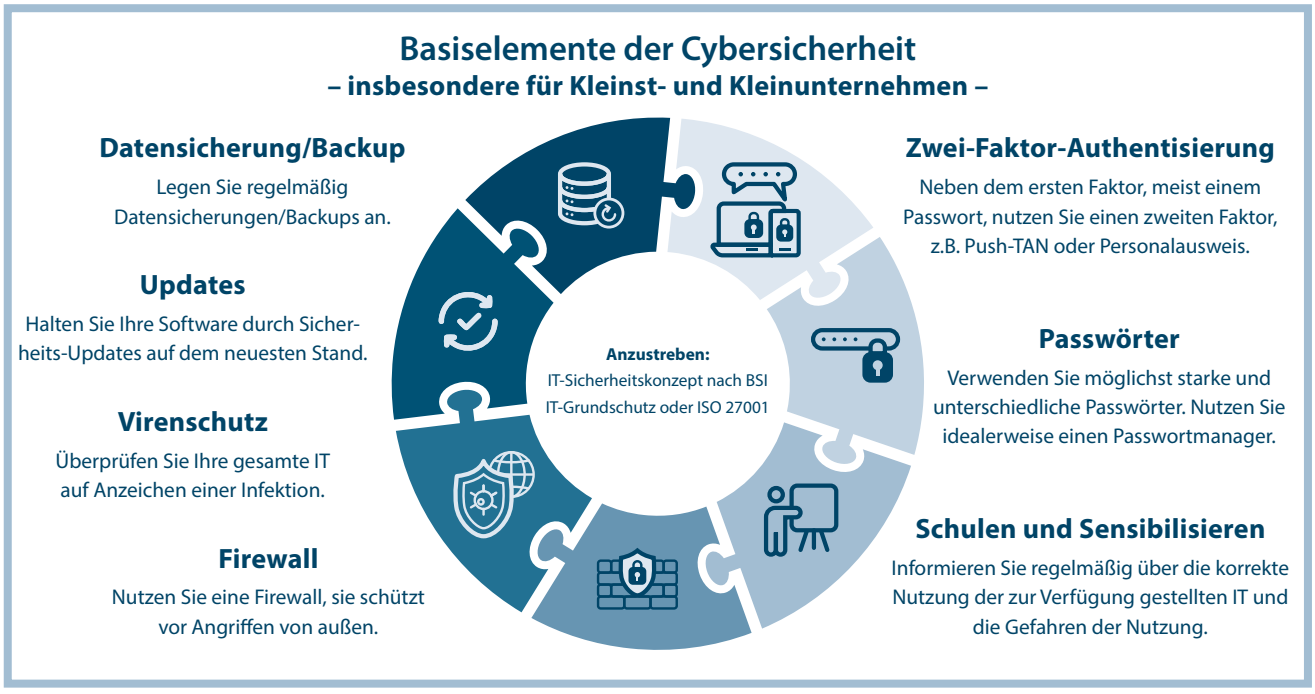


Abbildung 4: Auswahl an Elementen der Cyber-Sicherheit

Quelle: Fraunhofer IESE nach BSI o. J.b

Abbildung 5:
Kommunale Führungskräfte
als Verantwortliche für
die IT-Sicherheit

Quelle: Fraunhofer IESE

CHECKLISTE FÜR FÜHRUNGSKRÄFTE

- [ ] **Habe ich die Gesamtverantwortung für die Informationssicherheit übernommen und lasse mich mindestens alle zwei Monate über den aktuellen Stand informieren?**
  Stellen Sie sicher, dass Sie sich regelmäßig über den Stand der Informationssicherheit in Ihrer Verwaltung informieren, einschließlich des Sicherheitsstatus und der Maßnahmen externer IT-Dienstleister.

- [ ] **Habe ich eine Informationssicherheitsbeauftragte/einen Informationsbeauftragten (ISB) benannt und sie/ihn mit notwendigen Mitteln und Befugnissen ausgestattet?**
  Stellen Sie sicher, dass die/der ISB alle Belange rund um die Informationssicherheit Ihrer Institution steuert und koordiniert, um die erforderlichen Prozesse zu organisieren und Sie von der praktischen Umsetzung zu entlasten. Die Gesamtverantwortung für die IT-Sicherheit liegt jedoch weiterhin bei Ihnen.

- [ ] **Ist eine aktuelle und umfassende Bestandsaufnahme Ihrer IT-Systeme und -Prozesse vorgenommen worden?**
  Stellen Sie sicher, dass Sie jederzeit einen aussagekräftigen, vollständigen Überblick über Ihre Systeme und Prozesse erhalten können. Hierzu bedarf es einer angemessenen aktuellen Dokumentation sowohl der technischen IT-Infrastruktur (Hardware und Software) als auch der für den geregelten Betrieb erforderlichen Prozesse.

- [ ] **Verfügen wir über ein effektives Risikomanagement?**
  Stellen Sie sicher, dass Sie einen verbindlichen gesteuerten Prozess etablieren, um potenzielle Gefährdungen frühzeitig zu erkennen und damit verbundene Risiken abschätzen und behandeln zu können (siehe BSI-Standard 200-3 Risikomanagement (vgl. BSI 2017b)).

- [ ] **Haben wir klare Regelungen für die Meldung von Sicherheitsvorfällen?**
  Stellen Sie durch einen verbindlichen Meldeprozess sicher, dass jeder Vorfall umgehend und in geeigneter Form an die hierfür zuständigen Stellen gemeldet wird.

- [ ] **Liegt ein Notfallplan für den Fall eines Cyberangriffs vor?**
  Stellen Sie sicher, dass ein dokumentierter Notfallplan existiert, der Schritte zur Eindämmung eines Angriffs, zur Wiederherstellung der Systeme und zur Kommunikation mit Bürgerinnen und Bürgern umfasst.

- [ ] **Ist das notwendige Budget für IT-Sicherheit eingeplant?**
  Stellen Sie sicher, dass genügend finanzielle Mittel bereitstehen, um alle Maßnahmen, die zur Etablierung und Aufrechterhaltung eines angemessenen IT-Sicherheitsniveaus erforderlich sind, umgesetzt werden können.

- [ ] **Verfügen wir über qualifiziertes Personal für die IT-Sicherheit?**
  Stellen Sie sicher, dass ausreichendes qualifiziertes Fachpersonal zur Gewährleistung eines reibungsfreien IT-Betriebs zur Verfügung steht. Zur Orientierung: Empfohlen wird zum Beispiel für privatwirtschaftliche Unternehmen, je 100 Mitarbeitende mindestens eine Vollzeitkraft ausschließlich für IT-Sicherheitsaufgaben einzuplanen.

- [ ] **Tauschen Sie sich regelmäßig mit anderen Kommunen oder Fachleuten aus?**
  Stellen Sie sicher, dass Sie und Ihre IT-Fachkräfte einen regelmäßigen Austausch mit Fachleuten sowie Kolleginnen und Kollegen aus anderen Kommunen im Bereich IT-Sicherheit pflegen. Aufgrund der rasanten Entwicklungen ist es wichtig, dass Sie ihr Wissen in diesem Bereich abgleichen, aktuell halten und bestenfalls aus erster Hand über aktuelle Gefährdungslagen informiert werden.

Die kommunale IT-Sicherheitslage

Ist-Zustand: Vielfältige Bedrohungslagen

Der jährliche Lagebericht des BSI (vgl. BSI o. J. a) unterstreicht eine alarmierende Entwicklung: Kommunalverwaltungen sind immer häufiger das Ziel von sogenannten Ransomware-Angriffen. In den Jahren 2023 (vgl. BSI 2023a) und 2024 (vgl. BSI 2024) traf es durchschnittlich zwei Kommunen beziehungsweise kommunale Betriebe pro Monat. Die Folgen: Nicht nur sensible Bürgerdaten wurden kompromittiert. Auch die Funktionsfähigkeit der Verwaltung war teils massiv eingeschränkt. In einigen Fällen lagen zentrale Dienstleistungen wochenlang lahm – mit Auswirkungen, die noch Monate später spürbar waren.

Die Bedrohungslage für kommunale Verwaltungen ist vielfältig:

- **Ransomware** – eine Schadsoftware, die Computersysteme blockiert und Daten verschlüsselt – gehört zu den größten Gefahren.
- Ebenso kritisch sind **Advanced Persistent Threats (APTs)**, bei denen hochspezialisierte Hacker gezielt über einen längeren Zeitraum Netzwerke ausspionieren, um sensible Informationen zu stehlen oder Manipulationen an den IT-Systemen vorzunehmen.
- Zusätzlich stellen offene oder **schlecht konfigurierte Onlinedienste** ein erhebliches Risiko dar, da sie Angreifenden unbeabsichtigt Zugang zu vertraulichen Verwaltungsdaten ermöglichen.

Die Lageberichte des BSI aus den letzten Jahren zeigen eindrücklich, wie breit die Angriffe gestreut sind. Außerdem trafen die Angriffe nicht nur die Kernverwaltungen, sondern auch Nahverkehrsbetriebe, Energieversorger, Wohnungsbaugesellschaften, Stadtreinigungen oder Schulämter. In einem Fall wurde ein Schulamt mit Verantwortung für 75 Schulen lahmgelegt. Diese Vorfälle zeigen deutlich die Dringlichkeit einer umfassenden und spezifisch angepassten **IT-Sicherheitsstrategie** auf kommunaler Ebene.

IT-Sicherheitsstrategie

Eine IT-Sicherheitsstrategie ist ein umfassender, systematischer Plan, der die Ziele, Maßnahmen und Vorgehensweisen zur Gewährleistung der IT-Sicherheit innerhalb einer Organisation festlegt. Die Strategie bezieht sich auf die gesamte IT-Landschaft und umfasst sowohl technische als auch organisatorische Aspekte.

Die wachsende Bedrohungslage resultiert sowohl aus der Zunahme von Angriffen wie auch der Anfälligkeit von Kommunen. Im Gegensatz zu Bundesbehörden, die auf gesicherte Regierungsnetze mit zentralen Abwehrmaßnahmen zurückgreifen können, erhalten Kommunen oft nicht in ausreichendem Maße Unterstützung. Das BSI bietet Schulungen und vermittelt Expertinnen und Experten über die **Allianz für Cybersicherheit** (vgl. Allianz für Cybersicherheit o. J.), räumt jedoch ein, dass eine flächendeckende Beratung beziehungsweise Unterstützung vor Ort für Kommunen nicht möglich ist (vgl. VPN Haus 2024). Darüber hinaus fehlen verbindliche bundesweite Vorgaben zur IT-Sicherheit oder Meldepflichten für IT-Sicherheitsvorfälle. Die neue **EU-Richtlinie NIS-2 zur Verbesserung der Cybersicherheit für Unternehmen und öffentliche Verwaltungen** berücksichtigt kommunale Behörden in Deutschland nicht, obwohl sie häufig Opfer von Cyberangriffen werden (Opetz 2025). Hinzu kommen vielerorts

unzureichende finanzielle Mittel, kaum ausreichende Fachkompetenz und personelle Engpässe. In den Stellenplänen vieler Kommunen fehlen Positionen für Informationssicherheitsbeauftragte, entweder aufgrund fehlender Haushaltsmittel oder mangelnder Priorisierung (vgl. Stuffrein 2024). Gleichzeitig schreiten die technischen Möglichkeiten der Angreifenden schneller voran, als die IT-Sicherheit Schritt halten kann.

Soll-Zustand: Gewährleistung von Sicherheitsniveaus

Die Risiken für die kommunale IT-Sicherheit sind vielfältig. Studien wie die des Deutschen Städtetags (2023) zeigen, dass dringender Handlungsbedarf besteht, um Verwaltungen besser vor digitalen Bedrohungen zu schützen. Wie ist jedoch ein angemessenes Sicherheitsniveau für eine Kommune zu gewährleisten?

Das Bundesamt für Sicherheit in der Informationstechnik bietet in diesem Zusammenhang mit dem allgemein anwendbaren **IT-Grundschutz-Kompendium** (vgl. BSI 2023d) eine umfassende Antwort auf die Frage, wie der Aspekt Informationssicherheit idealerweise angegangen werden sollte. Dieses Kompendium, das auf den Aufbau eines ISO 27001-kompatiblen Managementsystems zur Informationssicherheit (Information Security Management System – ISMS) abzielt, richtet sich jedoch in erster Linie an mittlere und große Unternehmen und hat sich für kleinere Organisationen als eher unpraktikabel erwiesen. Daher wurden im Lauf der Zeit zunehmend schlankere Ansätze entwickelt.

Mittlerweile gibt es daher mit dem „**Weg in die Basis-Absicherung (WiBA)**“ und dem „**IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung**“ speziell auch für Kommunen ein angepasstes Vorgehen, das einen elementaren Einstieg zur Verbesserung der Informationssicherheit bietet (vgl. BSI 2023e; BSI 2017a).

Informationssicherheitsmanagement-System (ISMS)

Ein ISMS ist ein systematischer Ansatz zur Gewährleistung, Steuerung und kontinuierlichen Verbesserung der Informationssicherheit in einer Organisation. Es umfasst Richtlinien, Prozesse und technische Maßnahmen, um Daten vor unbefugtem Zugriff, Verlust oder Manipulation zu schützen. Als operatives Ergebnis einer IT-Sicherheitsstrategie setzt ein ISMS deren Ziele und Vorgaben praktisch und strukturiert um. Es basiert häufig auf internationalen Standards wie ISO/IEC 27001 und hilft, Sicherheitsrisiken zu identifizieren, zu bewerten und zu minimieren.

ISO 27000-Serie – Internationale Standards für IT-Sicherheit

Die ISO/IEC 27001 definiert Anforderungen für die Einführung und Pflege eines Informationssicherheitsmanagementsystems (ISMS). Sie ist zusätzlich Grundlage für Zertifizierungen.

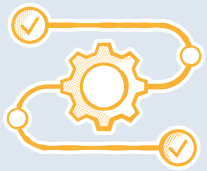
Die ISO/IEC 27002 ist ein praktischer Leitfaden zur Auswahl und Umsetzung von Sicherheitsmaßnahmen. **Sie ist besonders hilfreich für Kommunen, die internationale Standards einhalten müssen oder eine Zertifizierung nach ISO/IEC 27001 anstreben.**

HANDLUNGS-FELDER

Über die genannten Standards und Vorgaben hinaus bedarf es auf kommunaler beziehungsweise regionaler Ebene eine systematische Vorgehensweise, die aus folgenden Bausteinen bestehen sollte:

Sensibilisierung

Stellen Sie sicher, dass Ihre Mitarbeitenden die Risiken von Cyberangriffen verstehen. Ein geschärftes Bewusstsein für die möglichen Schäden – von finanziellen Einbußen bis hin zum Verlust des Bürgervertrauens – ist die Grundlage für eine sichere Verwaltung.



Organisatorische Prozesse

Informationssicherheit kann nur gelingen, wenn die Vielzahl der damit verbundenen Aufgaben und Tätigkeiten in einem verbindlichen Rahmen geregelt werden. Alle Verantwortlichen sind hier in Prozesse und Strukturen einzubinden, die gesteuert, überwacht und dokumentiert werden.

Technische Maßnahmen

Die Gewährleistung von Informationssicherheit umfasst viele technische Einzelmaßnahmen, welche sich direkt auf die Funktion oder den Betrieb der IT-Systeme beziehen, wie zum Beispiel die verbindliche Vorgabe von Sicherheitsrichtlinien, regelmäßige Software-Aktualisierungen oder die zuverlässige Sicherung kritischer Daten.

CHECKLISTE FÜR DIE IT-SICHERHEIT

Um die IT-Sicherheit in Ihrer kommunalen Verwaltung kontinuierlich zu verbessern und sicherzustellen, dass alle Maßnahmen effektiv umgesetzt werden, sollten Sie regelmäßig folgende Aspekte überprüfen:

Sicherheitsrichtlinien:

- ☐ Überprüfen Sie, ob klare und umfassende Sicherheitsrichtlinien existieren, die regelmäßig aktualisiert werden.

- ☐ Diese Richtlinien sollten alle Aspekte der Informationssicherheit abdecken, einschließlich Datenschutz, Zugangskontrollen und Notfallmanagement.

- ☐ Stellen Sie sicher, dass diese Richtlinien für alle Mitarbeitenden zugänglich sind und deren Verständnis gefördert wird. Organisieren Sie regelmäßige Informationsveranstaltungen, um die Richtlinien zu erläutern und offene Punkte zu klären.

Zugriffsmanagement:

- ☐ Stellen Sie jederzeit sicher, dass nur autorisierte Personen Zugang zu sensiblen Daten haben. Dies wird beispielsweise durch die regelmäßige Überprüfung von Benutzerrechten gewährleistet wie auch deren Anpassung an veränderte Anforderungen oder Rollen innerhalb Ihrer Verwaltung.

- ☐ Etablieren Sie sichere Zugriffsprotokolle, um unbefugten Zugriff zu verhindern. Veranlassen Sie Lösungen wie Mehr-Faktor-Authentifizierung, um das Sicherheitsniveau weiter zu erhöhen.

Schulungsangebote:

(siehe *Grundlegende Maßnahmen für die IT-Sicherheit – Maßnahme 2: Sensibilisierung der Mitarbeitenden: IT-Sicherheit als gemeinsame Aufgabe*, S. 28)

- ☐ Bieten Sie regelmäßige Schulungen und interaktive Workshops an, in denen Ihre Mitarbeitenden nicht nur über aktuelle Bedrohungen und Sicherheitspraktiken informiert werden, sondern diese auch praktisch erproben können. Schaffen Sie attraktive Fortbildungsangebote, die zum freiwilligen Engagement motivieren. Fördern Sie den Austausch von Erfahrungen und Best Practices auch zu anderen Kommunen, um das Sicherheitsbewusstsein in Ihrer Verwaltung nachhaltig zu stärken.

Notfallpläne:

(siehe *Maßnahmen im Krisenfall – Notfallmanagement*, S. 33)

- ☐ Überprüfen Sie die Tauglichkeit Ihrer Notfallpläne mindestens einmal pro Jahr. Lassen Sie alle Mitarbeitenden an den Übungen teilnehmen, damit sie im Ernstfall wissen, welche Schritte zu unternehmen sind.

(siehe *Maßnahmen im Krisenfall – Notfallmanagement*, S. 33)

- ☐ Stellen Sie sicher, dass die Ergebnisse der Notfallübungen dokumentiert werden und nutzen Sie diese Informationen, um Ihre Pläne kontinuierlich anzupassen und zu verbessern. Führen Sie Nachbesprechungen durch, um Feedback zu sammeln und Optimierungsmöglichkeiten zu identifizieren.

Technische Infrastruktur:

(siehe *Grundlegende Maßnahmen für die IT-Sicherheit – Maßnahme 3: Organisatorische Aspekte*, S. 29)

- ☐ Veranlassen Sie regelmäßige Sicherheitsüberprüfungen Ihrer IT-Systeme. Beauftragen Sie bei Bedarf auch externe Expertinnen und Experten, um Schwachstellen zu identifizieren und die Sicherheitsarchitektur zu bewerten.

(siehe *Grundlegende Maßnahmen für die IT-Sicherheit – Maßnahme 4: Technische Aspekte*, S. 30)

- ☐ Halten Sie sich und Ihr Team über aktuelle Bedrohungen und Sicherheitstechnologien informiert, um Ihre Systeme kontinuierlich zu optimieren. Entwickeln Sie gemeinsam mit Ihren IT-Verantwortlichen eine Strategie für regelmäßige Software-Updates und Patch-Management (die gezielte Installation von Sicherheitsupdates zur Behebung von Schwachstellen), um Sicherheitslücken zu schließen.

Risikomanagement:

- ☐ Implementieren Sie eine Methode des Risikomanagements, zum Beispiel auf der Basis des IT-Grundschutzes (BSI-Standard 200-3). (siehe *Grundlegende Maßnahmen für die IT-Sicherheit – Maßnahme 3: Organisatorische Aspekte*, S. 29)
- ☐ Veranlassen Sie regelmäßig Risikoanalysen, um neue Bedrohungen zu erkennen, zu bewerten, Gegenmaßnahmen abzuleiten und die zukünftigen Sicherheitsmaßnahmen entsprechend anzupassen. (siehe *Grundlegende Maßnahmen für die IT-Sicherheit – Maßnahme 3: Organisatorische Aspekte*, S. 29)

Business Continuity Management (BCM):

- ☐ Setzen Sie den BSI-Standard 200-4 um, der Anforderungen und Vorgehensweisen festlegt, wie der Notbetrieb aufrecht erhalten werden kann (Business Continuity Management). Erstellen Sie ein umfassendes Konzept, das über reine Notfallpläne hinausgeht und ganzheitlich die Aufrechterhaltung kritischer Verwaltungsprozesse bei verschiedenen Störungsszenarien sicherstellt. (siehe *Maßnahmen im Krisenfall – Sicherstellen der Handlungsfähigkeit*, S. 32)

Dokumentation und Audits:

- ☐ Veranlassen Sie eine umfassende Dokumentation aller sicherheitsrelevanten Aktivitäten. Führen Sie regelmäßige Audits durch, um die Angemessenheit ihrer Maßnahmen zu bestätigen. (siehe *Grundlegende Maßnahmen für die IT-Sicherheit – Maßnahme 3: Organisatorische Aspekte*, S. 29)
- ☐ Nutzen Sie diese Audits, um Ihre Sicherheitsvorkehrungen kontinuierlich zu optimieren, die Einhaltung der gesetzlichen Vorgaben sicherzustellen und auch bestehende Schwachstellen im System zu erkennen. (siehe *Grundlegende Maßnahmen für die IT-Sicherheit – Maßnahme 3: Organisatorische Aspekte*, S. 29)

Durch die konsequente Umsetzung der genannten Aspekte kommen Sie schrittweise dem Ziel näher, dass die Informationssicherheit in Ihrer Verwaltung nicht nur eingehalten, sondern auch kontinuierlich verbessert wird. Ihre aktive Rolle als Führungskraft ist hierbei von entscheidender Bedeutung für den Erfolg dieser Maßnahmen. Informationssicherheit ist dabei keine einmalige Aufgabe, sondern ein fortlaufender Prozess, der ständige Aufmerksamkeit und Anpassung erfordert.
Schaffen Sie eine Kultur der Sicherheit, in der alle Mitarbeitenden ihre Verantwortung ernst nehmen und aktiv zur Verbesserung der Informationssicherheit beitragen. Auf diese Weise stärken Sie nicht nur die Sicherheit Ihrer Verwaltung, sondern auch das Vertrauen der Bürgerinnen und Bürger in die digitale Verwaltung.

Grundlagen

Die Erreichung des Soll-Zustands der IT-Sicherheit ist ein Prozess, der von der individuellen Lage einer jeden Kommune abhängig ist. Nichtsdestotrotz gibt es dabei **grundlegende Orientierungspunkte**: Rechtliche Vorgaben, Rollen in der kommunalen IT-Sicherheit und Orientierung über die Vorgehensweisen des IT-Grundschutzes nach dem BSI.

Rechtliche Vorgaben

Rechtliche Vorgaben im Bereich der IT-Sicherheit auf nationaler und internationaler Ebene sind notwendig, um eine stabile und sichere IT-Infrastruktur zu ermöglichen. Zu den wichtigsten Vorgaben zählen unter anderem:

- **BSI-Kritisverordnung** (vgl. BSI-KritisV 2016): Die KRITIS-Verordnung richtet sich an Betreiber kritischer Infrastrukturen zur Versorgung mit Gütern und Dienstleistungen von besonderer Bedeutung wie Wasser, Energie oder medizinischen Angeboten. Dies kann auch kommunal verantwortete Einrichtungen betreffen. Betreiber solcher Infrastrukturen müssen ihre IT-Systeme in Krisensituationen funktionsfähig halten, Schutzmaßnahmen implementieren und Notfallpläne entwickeln. Die Verordnung zielt darauf ab, die Resilienz kritischer Infrastrukturen in Deutschland zu stärken und die öffentliche Sicherheit zu gewährleisten.

- **IT-Sicherheitsgesetz 2.0** (vgl. BSI 2021a): Dieses Gesetz verpflichtet Betreiber kritischer Infrastrukturen und öffentliche Stellen zu umfassenden Sicherheitsmaßnahmen und zur Meldung von Sicherheitsvorfällen.

- **NIS2-Richtlinie** (vgl. BSI 2025d): Diese EU-Richtlinie verlangt einheitliche Mindestanforderungen an die Netz- und Informationssicherheit für kritische Einrichtungen und verpflichtet Mitgliedstaaten zur Entwicklung nationaler Cybersicherheitsstrategien. Sie setzt eine Meldepflicht für erhebliche Sicherheitsvorfälle innerhalb von 24 Stunden fest und fördert die Zusammenarbeit zwischen nationalen Behörden und Computer-Notfallteams (CSIRTs) auf nationaler und europäischer Ebene. Besonders hervorzuheben ist, dass diese Richtlinie auf nationaler Ebene umgesetzt werden muss, jedoch keine explizite Umsetzungspflicht für einzelne Kommunen besteht.

- **Datenschutz-Grundverordnung (DSGVO)** (vgl. Intersoft Consulting 2018): Die DSGVO stellt sicher, dass personenbezogene Daten in der EU geschützt und nur rechtmäßig verarbeitet werden. Sie gibt Betroffenen umfassende Rechte, wie das Auskunftsrecht und das Recht auf Löschung ihrer Daten. Zudem verpflichtet sie Unternehmen, Datenschutzmaßnahmen zu ergreifen und Verstöße unverzüglich zu melden.

Datenschutz

Der Schutz personenbezogener Daten ist ein eigenständiger, rechtlich klar geregelter Bereich, der sich vom Thema IT-Sicherheit unterscheidet, aber eng mit ihm verbunden ist. Während IT-Sicherheit darauf abzielt, Systeme, Netzwerke und Informationen aller Art vor unbefugtem Zugriff, Missbrauch oder Ausfall zu schützen, konzentriert sich der Datenschutz gezielt auf personenbezogene Daten – also Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Somit ist der Datenschutz ein wichtiger Teilbereich der Informationssicherheit.

Im Rahmen der Datenschutz-Grundverordnung (DSGVO) sind Kommunen verpflichtet, sicherzustellen, dass personenbezogene Daten ihrer Bürgerinnen und Bürger nur zweckgebunden, transparent und sicher verarbeitet werden. Diese Vorgaben gelten unabhängig vom Speichermedium – ob digital oder analog, etwa in Papierarchiven.

Datenschutzmaßnahmen umfassen sowohl technische Lösungen wie die Verschlüsselung von Daten oder Zugriffsbeschränkungen, als auch organisatorische Vorkehrungen, darunter Schulungen für Mitarbeitende oder die Benennung eines Datenschutzbeauftragten.

- **Bundesdatenschutzgesetz (BDSG)** (vgl. BDSG 2017): Das BDSG ergänzt die DSGVO und regelt den Datenschutz in Deutschland. Das BDSG enthält spezifische Bestimmungen zur Verarbeitung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen. Es definiert unter anderem Regelungen für Beschäftigtendaten, die Benennung eines Datenschutzbeauftragten und den Schutz sensibler Daten.

- **Leitlinie für Informationssicherheit des IT-Planungsrats** (vgl. IT-Planungsrat 2020; IT-Planungsrat 2024): Mit der Leitlinie für Informationssicherheit und dem zugehörigen Umsetzungsplan schafft der IT-Planungsrat einen verbindlichen Rahmen, um auch Kommunen beim Aufbau eines verlässlichen IT-Sicherheitsniveaus zu unterstützen. Vorgesehen sind stufenweise Maßnahmen bis 2025, darunter automatisierte Verfahren zur Erkennung und Abwehr von Bedrohungen, flexible Sicherheitsarchitekturen wie Zero Trust sowie quantensichere Verschlüsselung zum Schutz besonders sensibler Verfahren. Risikobasierte Entscheidungsgrundlagen, kontinuierliche Sicherheitstests sowie standardisierte IT-Notfallpläne stärken insbesondere die Krisenfestigkeit kommunaler IT-Infrastrukturen. Begleitend werden Mitarbeitende durch Schulungen und praxisnahe Notfalltrainings gezielt sensibilisiert – auch in kleineren Verwaltungseinheiten.

- **Onlinezugangsgesetz (OZG)** (vgl. BMI 2017) und **Gesetz zur Änderung des Onlinezugangsgesetzes (OZGÄndG)** (vgl. BMI 2024): Mit der Verpflichtung zur Digitalisierung von Verwaltungsleistungen stellt das OZG neue Anforderungen an die Sicherheit der IT-Infrastruktur. Dazu gehören unter anderem die Berücksichtigung des BDSG und der in diesem Gesetz definierten Kommunikationsstandards. Das OZGÄndG zielt auf eine Beschleunigung des Onlinezugangsgesetzes. Es erleichtert die Vernetzung von Registern – Datenbanken öffentlicher Stellen – und fördert einheitliche, benutzerfreundliche Onlinedienste.

Die Umsetzung dieser Prinzipien in den Verwaltungsprozessen sowie die Sicherstellung der gesetzlichen Vorgaben sind zentrale Aufgaben im Führungsbereich. Dabei ist die enge Zusammenarbeit mit dem behördlichen Datenschutzbeauftragten unerlässlich.

Wichtige Grundprinzipien des Datenschutzes

Zweckbindung: Daten dürfen nur für den festgelegten Zweck verarbeitet werden.

Datenminimierung: Es dürfen nur die für die jeweilige Aufgabe erforderlichen Daten erhoben und gespeichert werden.

Integrität und Vertraulichkeit: Daten müssen durch geeignete technische und organisatorische Maßnahmen vor unbefugtem Zugriff, Verlust und Veränderung geschützt werden.

Rechtmäßigkeit, Treu und Glauben, Transparenz: Die Verarbeitung personenbezogener Daten muss ausdrücklich erlaubt sein. Betroffene müssen über die Verarbeitung ihrer Daten informiert werden.

Richtigkeit: Personenbezogene Daten müssen korrekt und aktuell sein. Falsche und veraltete Daten dürfen nicht verarbeitet werden. Sie müssen korrigiert und gelöscht werden.

Rollen in der kommunalen IT-Sicherheit

Die vielschichtigen Bedrohungen der IT-Sicherheit in Kommunen erfordern ein koordiniertes und engagiertes Handeln aller Mitarbeitenden. Die Verteilung von Rollen definiert Zuständigkeiten und unterstützt den Schutz sowie die Funktionsfähigkeit der Kommune.

Führungskräfte tragen die Gesamtverantwortung für die IT-Sicherheit innerhalb ihrer Ämter und müssen sicherstellen, dass Sicherheit in der Kommune – ob nun IT-Sicherheit, Informationssicherheit oder auch die Datensicherheit – als strategische Priorität wahrgenommen wird. Sie sind nicht nur dafür zuständig, die notwendigen Ressourcen bereitzustellen, sondern auch eine klare IT-Sicherheitskultur zu fördern. Sie sollten daher stets mit gutem Beispiel vorangehen und geltende Sicherheitsrichtlinien nicht untergraben – etwa indem dienstliche Mails auf privaten Geräten abgerufen werden.

Der **Informationssicherheitsbeauftragte** hält die Schlüsselrolle in der Koordination und Überwachung aller Informationssicherheitsmaßnahmen. Er entwickelt Sicherheitsstrategien und -richtlinien, führt regelmäßige Risikomanagementanalysen durch und identifiziert potenzielle Schwachstellen in der IT-Infrastruktur. Zudem organisiert er Schulungen für Beschäftigte, um das Bewusstsein für Sicherheitsrisiken zu schärfen und sicherzustellen, dass alle Beteiligten über die notwendigen Kenntnisse verfügen, um Bedrohungen zu erkennen und Fehlverhalten zu vermeiden.

IT-Administratorinnen und Administratoren sind die technischen Expertinnen und Experten, die die Sicherheitsrichtlinien in die Praxis umsetzen. In dieser Rolle sind sie unter anderem verantwortlich für die Verwaltung der IT-Infrastruktur, das Durchführen regelmäßiger Software-Updates und die Überwachung der Netzwerke auf verdächtige Aktivitäten. Deren technische Expertise ist entscheidend, um Sicherheitsvorfälle schnell zu identifizieren und zu beheben, bevor sie ernsthafte Schäden anrichten können.

In vielen Verwaltungen ist die oder der **Datenschutzbeauftragte** eine unverzichtbare Rolle, die sicherstellt, dass alle datenschutzrechtlichen Vorgaben eingehalten werden. Sie/er berät in Fragen des Datenschutzes und organisiert Schulungen zum richtigen Umgang mit sensiblen Daten und zur Sensibilisierung von den Mitarbeitenden. Die/der Datenschutzbeauftragte spielt eine entscheidende Rolle im Schutz der personenbezogenen Daten von Bürgerinnen und Bürgern sowie der Einhaltung der DSGVO.

Die **Mitarbeitenden der Fachabteilungen** sind die Frontlinie im täglichen Umgang mit IT-Sicherheit. Sie müssen sich der Risiken bewusst sein, die mit ihrer Arbeit verbunden sind, und die festgelegten Sicherheitsrichtlinien einhalten. Durch die Meldung von Sicherheitsvorfällen und Verdachtsmomenten tragen sie beispielsweise aktiv zur Sicherheit der gesamten Verwaltung bei. Ihre Sensibilisierung und ihr Engagement sind von entscheidender Bedeutung, um eine Sicherheitskultur zu etablieren.

Nicht zuletzt sind **externe Dienstleistende** wichtiger Partner in der Gewährleistung der IT-Sicherheit. Sie bieten Unterstützung bei der Implementierung von Sicherheitslösungen, führen Audits durch und helfen bei der Schulung von Mitarbeitenden. Ihre Expertise ergänzt die internen Ressourcen und trägt dazu bei, die Sicherheit der digitalen Systeme auf ein höheres Niveau zu heben.

Abbildung 6:
Rollen in der kommunalen IT-Sicherheit

Quelle: Fraunhofer IESE

Vorgehensweisen nach dem BSI

Der BSI IT-Grundschutz bietet eine systematische Methodik zur Identifikation und Umsetzung von IT-Sicherheitsmaßnahmen, die Organisationen dabei unterstützt, ihre IT-Systeme und Geschäftsprozesse abzusichern. Der modulare Ansatz ermöglicht einen Einstieg mit einzelnen Bausteinen, um Sicherheitsmaßnahmen schrittweise auszubauen. Das BSI hat verschiedene Einstiege und Ebenen der IT-Sicherheit definiert, die auf unterschiedliche Anforderungen und Ressourcen von Organisationen zugeschnitten sind. Diese Ansätze bauen aufeinander auf; jede Ebene verfügt über spezifische Richtlinien und Leitfäden. Auf diese Weise können Kommunen nicht nur die Anforderungen des gewählten und passenden Einstiegs oder der Ebene erfüllen, sondern auch ihre Sicherheitsmaßnahmen strategisch ausrichten und zukunftssicher gestalten – stets im Einklang mit nationalen sowie internationalen Standards. Das BSI unterscheidet dabei folgende Ebenen (siehe Abbildung 7).

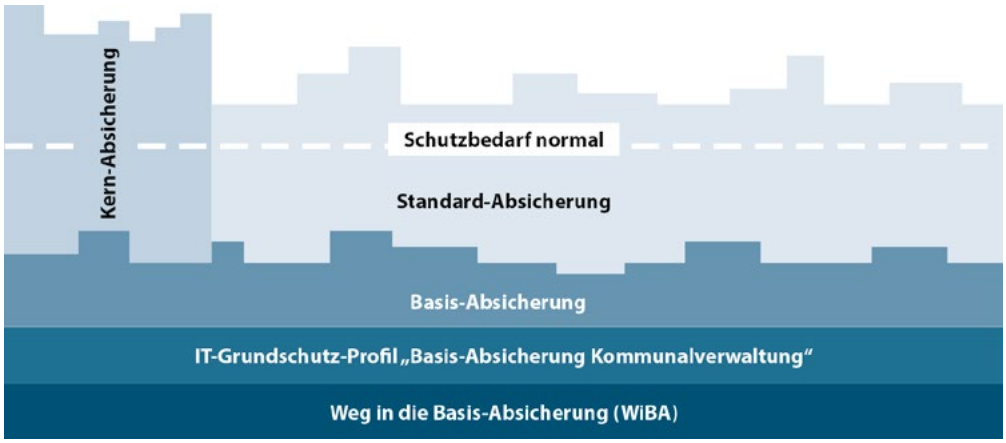


Abbildung 7:
Übersicht der Vorgehensweisen nach dem BSI

Quelle: Fraunhofer IESE nach BSI

Einstieg 1: Weg in die Basis-Absicherung (WiBA)

Ein erster Zugang ist der **Weg in die Basis-Absicherung (WiBA)** (vgl. BSI 2023e) nach dem IT-Grundschutz. Diese niedrigschwellige Einstiegshilfe wurde initiiert, um insbesondere kleineren Kommunen mit begrenzten Ressourcen die ersten Schritte zum IT-Grundschutz zu erleichtern. Das BSI bietet mit dem WiBA praxisorientierte **Checklisten** und einfache **Prüffragen** an, die wesentliche Aspekte der Absicherung abdecken, um einen direkten Sicherheitsmehrwert zu erreichen. Der Einfachheit halber sind diese Listen nach Priorität kategorisiert, beginnend mit grundlegenden und organisatorischen Maßnahmen und spezielleren Themen im weiteren Verlauf.

Einstieg 2: IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung"

Auf den WiBA aufbauend und weiterhin ein praxisnaher Einstieg ist das **IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung"** (vgl. BSI 2023f). Dieses Profil berücksichtigt die spezifischen Anforderungen und Gegebenheiten von Kommunen und stellt sicher, dass grundlegende Sicherheitsmaßnahmen etabliert werden. Die Anforderungen für diese Maßnahmen werden in **Prozess- und System-Bausteine** kategorisiert. Tabelle 2 stellt exemplarisch eine solche umzusetzende Anforderung dar. Durch die Anwendung dieses Profils können Kommunen ein solides Fundament für ihre Informationssicherheit schaffen, selbst, wenn dieser Einstieg noch nicht alle Anforderungen für eine Zertifizierung nach ISO 27001 (Standard zur Einführung und Pflege eines Informationssicherheitsmanagementsystems) erfüllt.

Nr.	zu prüfende Anwendung	Aufwand	erfüllt?		
			ja	nein	nicht relevant
6.	Erfordern Aktionen mit administrativen Rechten eine vorherige sichere Authentisierung?	1			
	Es sollte mindestens ein sicheres Passwort genutzt werden. Falls möglich, sollte hierfür eine Mehr-Faktor-Authentisierung genutzt werden.				
	Notizen				

Tabelle 1: Beispielhafte Frage aus der Checkliste „IT-Administration" des BSI WiBA
Quelle: Fraunhofer IESE nach BSI

Baustein	Anforderungen	Besonderheiten
INF.7	**INF.7.A1 –A2; A6 – A7**	INF.7.A6 Da im Bürgerbüro reger Publikumsverkehr herrscht, müssen Mitarbeitende besonders darauf achten, dass sie vertrauliche Informationen Unbefugten nicht (unfreiwillig) zugänglich machen.
		INF.7.A7 Da stets (unbekannte) Besucher im Bürgerbüro zu Gast sind, müssen vertrauliche Informationen und Datenträger sicher aufbewahrt werden.

Tabelle 2: Beispielhafte Anforderung aus dem Systembaustein „Infrastruktur" des BSI IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung"
Quelle: Fraunhofer IESE nach BSI

Basis-Absicherung

Durch die Umsetzung weiterer Bausteine wird die Ebene der **Basis-Absicherung** (vgl. BSI 2024b) nach dem BSI erreicht. Diese Vorgehensweise betrifft Organisationen, bei denen die Geschäftsprozesse keine erhöhten Risiken für die Informationssicherheit beinhalten. Auch werden keine immateriellen oder materiellen Werte verarbeitet, deren Verlust oder Beschädigung ernste Folgen für die Organisation hätte. Zudem werden geringfügige Sicherheitsvorfälle hier als akzeptabel eingestuft.

Das Niveau der Basis-Absicherung wird in mehreren Schritten erreicht: Zunächst wird bestimmt, in welchen Geltungsbereichen die Vorgehensweise angewendet werden soll. Anschließend werden die relevanten Bausteine identifiziert und priorisiert.

Die Umsetzung der zugehörigen Basis-Anforderungen erfolgt mithilfe des sogenannten **IT-Grundschutz-Kompendiums** (vgl. BSI 2023d), ein weiteres Dokument des BSI, das eine Sammlung standardisierter Bausteine, Maßnahmen und Anforderungen zur Informationssicherheit enthält.

PRAXISBEISPIEL

Basis-Absicherung in einer Kreisstadt

Eine mittelgroße Kreisstadt mit 5.000 Einwohnerinnen und Einwohnern kann erste Schritte zur IT-Sicherheit auf der Ebene der Basis-Absicherung umsetzen, indem sie **unter anderem**:

- einen Informationssicherheitsbeauftragten benennt
  - Basis-Anforderung *ISMS.1.A4 Benennung eines oder einer Informationssicherheitsbeauftragten*
- eine grundlegende Definition von Sicherheitsvorfällen für das Einwohnermeldeamt bereitstellt, sowie eine Richtlinie zur Behandlung dieser erstellt
  - Basis-Anforderung *DER.2.1.A1 Definition eines Sicherheitsvorfalls* und *DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen*
- einfache Sicherheitsrichtlinien für den Umgang mit Bürgerdaten einführt
  - Basis-Anforderung *CON.2.A1 Umsetzung Standard-Datenschutzmodell*

Diese Liste ist **nicht vollständig** und zeigt einen kleinen Ausschnitt in der Umsetzung der Basis-Absicherung. Nach diesem Prinzip wird Schritt für Schritt die Basis-Absicherung nach dem BSI erreicht. Die Zuständigkeit für die IT-Sicherheit in Einrichtungen von Kommunen einer solchen Größe ist nicht immer einheitlich geregelt und wird häufig im Einzelfall betrachtet, weshalb diese Thematik hier unberücksichtigt bleibt.

Standard-Absicherung

Die nächste Ebene ist die **Standard-Absicherung** (vgl. BSI 2017a). Sie entspricht der klassischen IT-Grundschutz-Vorgehensweise und zielt auf eine umfassende Absicherung aller Prozesse und Bereiche einer Institution. Ähnlich wie bei der Basis-Absicherung ist zunächst der Geltungsbereich festzulegen, um mit einer Analyse des Ist-Zustands und der Feststellung des Schutzbedarfs von Prozessen und Assets zur Auswahl der umzusetzenden Sicherheitsanforderungen zu gelangen. Je nach Schutzbedarf sind Basis-Anforderungen, Standard-Anforderungen oder Anforderungen des erhöhten Schutzbedarfs aus dem IT-Grundschutz-Kompendium zu erfüllen. Die Standard-Absicherung ist kompatibel mit einer ISO-27001-Zertifizierung.

Kern-Absicherung

Liegt der Fokus zunächst auf der vorrangingen Absicherung der besonders gefährdeten Geschäftsprozesse und Assets, bietet sich hierfür die Vorgehensweise der **Kern-Absicherung** (vgl. BSI 2017a) an. Diese existiert **parallel zur Standard-Absicherung**. Die Kern-Absicherung schützt gezielt existenziell wichtige Assets, wobei kleinere, nicht existenzbedrohende Sicherheitsvorfälle als akzeptabel gelten. Eine ISO-27001-Zertifizierung für die gesicherten Assets ist ebenfalls möglich.

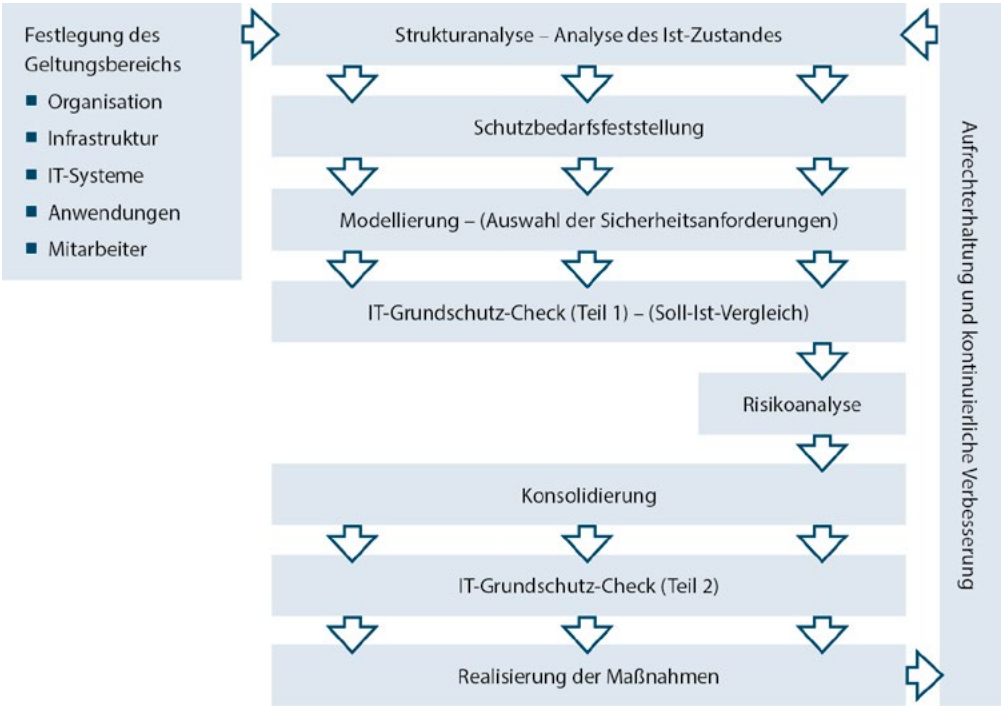


Abbildung 8:
Erstellung einer Sicherheitskonzeption im Rahmen der Standard-Absicherung aus dem BSI Standard 200-2

Quelle: Fraunhofer IESE nach BSI

PRAXISBEISPIEL

Standard-Absicherung nach BSI

Eine Kreisverwaltung, die sensible Bürgerdaten in verschiedenen Fachverfahren verarbeitet, setzt auf eine systematische IT-Sicherheitsstrategie gemäß den Vorgaben des BSI. Nach der Feststellung der Schutzbedarfe hat die Kreisstadt sich **unter anderem** für die Erfüllung dieser Anforderungen entschieden:

- **Dokumentiertes ISMS**: Einführung eines Informationssicherheitsmanagementsystems (ISMS) zur strukturierten Verwaltung und kontinuierlichen Verbesserung der IT-Sicherheit
  - Erfüllung der geeigneten Anforderungen aus dem Punkt *ISMS.1 Sicherheitsmanagement*
- **Regelmäßige Sicherheitsaudits**: Überprüfung aller Abteilungen auf Schwachstellen, um Sicherheitslücken frühzeitig zu erkennen und zu beheben
  - Erfüllung der geeigneten Anforderungen aus den Punkten *DER.3.1 Audits und Revisionen* und *DER.2.1 Behandlung von Sicherheitsvorfällen*
- **Notfallübungen für IT-Ausfälle**: Simulation von Krisenszenarien, insbesondere für das Bürgeramt und die Finanzverwaltung, um Abläufe zu testen und eine schnelle Wiederherstellung zu gewährleisten.
  - Erfüllung der geeigneten Anforderungen aus dem Punkt *DER.4 Notfallmanagement*

Durch **diese und weitere Maßnahmen** wird der Schutz sensibler Daten nach der Standard-Absicherung erhöht. Es ist zu beachten, dass die genaue Dauer und der Aufwand für die Umsetzung dieser Maßnahmen je nach Einzelfall variieren können und daher schwer abschätzbar sind.

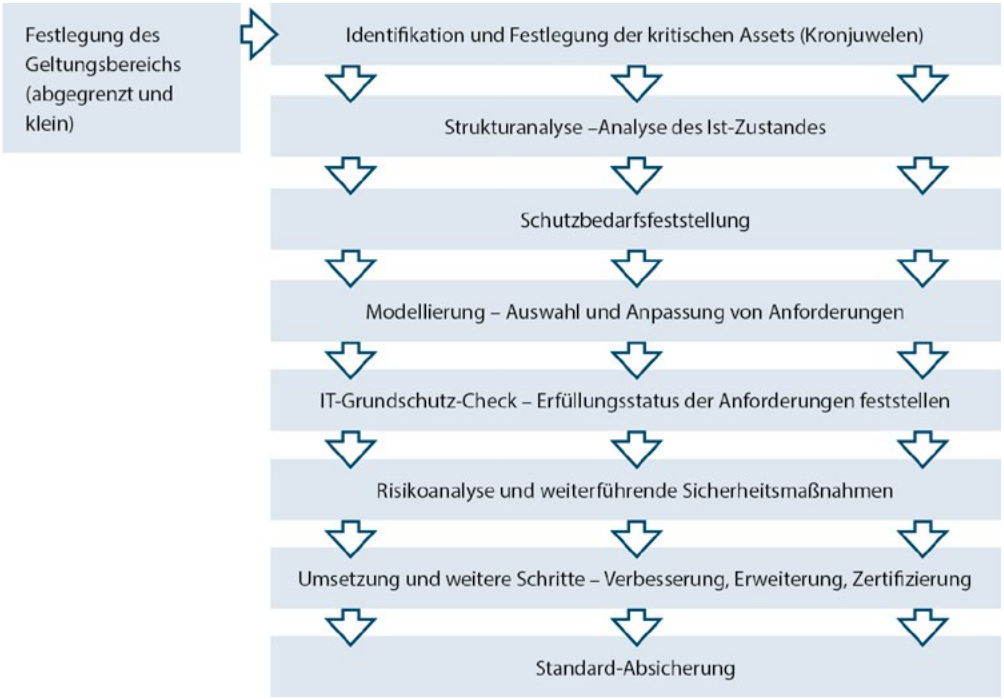


Abbildung 9: Vorgehensweise der Kern-Absicherung aus dem BSI Standard 200-2

Quelle: Fraunhofer IESE nach BSI

Grundlegende Maßnahmen für die IT-Sicherheit

IT-Sicherheit erfordert die Entwicklung einer umfassenden Strategie, die auf Prävention, schnelles Handeln und stetige Verbesserung ausgerichtet ist. Folgende wesentliche Aspekte der IT-Sicherheit unterstützen Kommunen dabei, ihre digitalen Systeme vor Bedrohungen zu schützen und das Vertrauen der Bürger in die Verwaltung zu festigen:

Maßnahme 1: Entwicklung einer IT-Sicherheitsstrategie

Die Entwicklung einer **IT-Sicherheitsstrategie** ist der zentrale Schritt, um die digitale Sicherheit einer Kommune nachhaltig zu gewährleisten. Sie beginnt mit einer detaillierten Analyse der bestehenden IT-Infrastruktur sowie möglicher Bedrohungen und organisatorischer Schwachstellen. Darauf aufbauend werden klare Sicherheitsziele definiert und geeignete Maßnahmen festgelegt. Dazu gehören technische Schutzmaßnahmen wie Firewalls, Zugriffskontrollen und Verschlüsselung, aber auch organisatorische Aspekte wie regelmäßige Schulungen, klare Verantwortlichkeiten und Notfallpläne. Wichtiger Bestandteil einer IT-Sicherheitsstrategie ist die Implementierung eines **Informationssicherheitsmanagement-Systems (ISMS)**, welches anerkannten Standards wie der **ISO/IEC 27001** folgt und sich an bewährten Handlungsempfehlungen orientiert, etwa dem IT-Grundschutz des **BSI** (BSI 2021b).

▸ Im Anhang finden Sie entsprechende Angebote.

Ein Beispiel aus dem Sicherheitskonzept der Stadt Osnabrück (2025) verdeutlicht, wie wichtige Sicherheitsmaßnahmen in die digitale Infrastruktur integriert werden. Das Konzept legt besonderen Wert auf die Analyse der Sicherheitsanforderungen auf verschiedenen Ebenen, darunter Sensoren, Datenübertragung und IoT-Plattformen. Zum Beispiel werden Sicherheitsmaßnahmen wie Verschlüsselung und Zugriffskontrollen bei der Datenübertragung implementiert, um sicherzustellen, dass die sensiblen Daten, die von Sensoren erfasst werden, geschützt sind. Darüber hinaus wird empfohlen, regelmäßige Sicherheitsüberprüfungen und Schulungen für Mitarbeitende durchzuführen, um das Bewusstsein für Cyberrisiken zu schärfen und die Sicherheit der städtischen Systeme zu verbessern.

Maßnahme 2: Sensibilisierung der Mitarbeitenden: IT-Sicherheit als gemeinsame Aufgabe

Die größte Schwachstelle in der IT-Sicherheit ist viel zu oft der Mensch selbst. Daher ist die Sensibilisierung aller Mitarbeitenden der erste entscheidende Schritt, um die Situation zu verbessern. Die Führungsebene spielt eine Schlüsselrolle, indem sie hierfür Verantwortung übernimmt, und die erforderlichen Ressourcen zur Durchführung angemessener Sensibilisierungsmaßnahmen bereitstellt. Hierzu zählen beispielsweise:

Schulungen und Weiterbildung: Regelmäßige Schulungen tragen dazu bei, das Bewusstsein für IT-Sicherheit auf allen Ebenen der Verwaltung zu stärken. Sie ermöglichen es sowohl Verwaltungsangestellten als auch Führungskräften, die Bedeutung sicherer IT-Praktiken zu verstehen und Risiken frühzeitig zu erkennen. Praxisnahe Trainings und Weiterbildungen können Mitarbeitende sensibilisieren und sie befähigen, aktiv zur Abwehr potenzieller Bedrohungen beizutragen und die digitale Sicherheit der ganzen Organisation zu stärken.

Praktische Maßnahmen: Informationskampagnen, interaktive Sicherheits-Workshops und festgelegte Verhaltensrichtlinien stellen Mittel dar, um das Bewusstsein für IT-Sicherheit zu schärfen.

Ziel ist es, Mitarbeitende für sicherheitsrelevante Themen zu sensibilisieren und ihnen praktische Handlungsmöglichkeiten aufzuzeigen – etwa im sicheren Umgang mit Passwörtern, der Erkennung von Phishing-Versuchen und anderen alltäglichen Bedrohungen. Durch praxisnahe Angebote erhalten sie das nötige Wissen, um IT-Sicherheitsaspekte in ihrem Arbeitsalltag zu berücksichtigen und so zum Schutz der Organisation beizutragen.

Maßnahme 3: Organisatorische Aspekte

Organisatorische Aspekte umfassen die Definition verantwortlicher Stellen, Gremien und tragender Prozesse, die eine strukturierte Umsetzung von IT-Sicherheitsmaßnahmen ermöglichen. Sie erleichtern die Einhaltung gesetzlicher Vorgaben, fördern eine schnelle Reaktionsfähigkeit und tragen zur Stabilität der IT-Infrastrukturen bei.

Steuerung und Richtlinien – Verantwortungsvolle Führung und klare Regeln

Ein wirksames **IT-Steuerungsmodell** legt Prozesse, Regeln und Strukturen fest, um IT-Ressourcen sicher und effizient zu nutzen. Es stellt sicher, dass gesetzliche Vorgaben wie die DSGVO eingehalten werden. Dazu zählen unter anderem Sicherheitsrichtlinien, die regelmäßig überprüft und an neue Bedrohungen angepasst werden müssen.

Ein gut etabliertes Steuerungsmodell trägt so zu nachhaltiger IT-Sicherheit bei und reduziert rechtliche sowie sicherheitsrelevante Risiken. Auch externe Dienstleister, die Zugriff auf kommunale Daten haben, sollten vertraglich zur Einhaltung der festgelegten Sicherheitsstandards verpflichtet werden.

Risikomanagement – Potenzielle Gefahren erkennen und behandeln

Der BSI-Standard 200-3 (vgl. BSI 2017b) bietet einen Ansatz zur Identifikation, Bewertung und Steuerung von Risiken. Zunächst wird der Schutzbedarf der eigenen Informationen und IT-Systeme ermittelt. Anschließend erfolgt die **Identifikation potenzieller Risiken**, die sowohl technische als auch organisatorische Schwachstellen umfassen können. Durch die **Risikobewertung** werden Eintrittswahrscheinlichkeit und das potenzielle Schadensausmaß analysiert. Darauf aufbauend werden Maßnahmen entwickelt, um erkannte Risiken zu behandeln. Das Risikomanagement umfasst zudem die **Überprüfung** und **Anpassung der Prozesse**, um auf neue Bedrohungen und Veränderungen angemessen reagieren zu können.

Überwachung und Audits

Eine wiederkehrende Bewertung des Sicherheitsniveaus dient dazu, Mängel und Schwächen zu identifizieren. **Sicherheitsaudits**, also systematische Prüfungen der IT-Systeme, helfen dabei, Schwachstellen frühzeitig zu erkennen. Eine kontinuierliche Überwachung von Netzwerken und Protokollen sorgt dafür, dass verdächtige Aktivitäten in Echtzeit ggf. automatisiert erkannt und Sicherheitsvorfälle schnell eingedämmt werden können.

Zugriffs- und Identitätsmanagement – Schutz vor unbefugtem Zugriff

Um unbefugten Zugriff zu verhindern, ist ein striktes **Zugriffsmanagement** erforderlich. Dazu gehören die Vergabe klar definierter Benutzerrechte, der Einsatz von **Mehr-Faktor-Authentifizierung** und die regelmäßige Überprüfung von Zugriffsberechtigungen. Ein solides **Identitätsmanagement** stellt sicher, dass nur autorisierte Personen auf Systeme zugreifen können.

DEF

Mehr-Faktor-Authentifizierung

Ein Sicherheitsverfahren, bei dem mehr als ein Authentifizierungsfaktor (zum Beispiel Passwort, Token, Biometrie) zur Verifizierung der Identität verwendet wird.

Maßnahme 4: Technische Aspekte

Der gezielte Einsatz moderner Sicherheitstechnologien unterstützt Kommunen dabei, ihre IT-Infrastrukturen widerstandsfähig zu gestalten und Ausfallzeiten zu reduzieren.

Hinweis für Führungskräfte:

Nutzen Sie diese Übersicht als Gesprächseinstieg für einen Austausch mit Ihrer IT-Abteilung. Eine enge Kommunikation über Abteilungen und Rollen hinweg ist entscheidend, um realistische und wirksame IT-Sicherheitsstrategien zu entwickeln.

Netzwerksicherheit

Ein grundlegendes Instrument für die Netzwerksicherheit ist die **Firewall**. Sie fungiert als eine Art Schutzschild, das den Datenverkehr zwischen internen Systemen und dem Internet überwacht. Unbekannte oder verdächtige Verbindungen werden dabei bei Angriffen oder unberechtigten Zugriffen auf die IT-Infrastruktur blockiert.

Ein **Virtual Private Network (VPN)** ist besonders beim mobilen Arbeiten oder beim Zugriff auf sensible Daten aus externen Netzwerken sinnvoll. Es verschlüsselt die Verbindung zwischen einem Gerät und dem internen Netzwerk, sodass Informationen nicht von Dritten mitgelesen werden können – selbst wenn man sich in einem unsicheren WLAN, etwa in Zügen, befindet.

Die **sichere Konfiguration von Routern** ist ein weiterer Aspekt der Netzwerksicherheit. Diese Netzwerkgeräte leiten die Datenpakete zwischen verschiedenen Netzwerken (insbesondere dem lokalen Netzwerk und dem Internet) weiter. Durch den Einsatz starker Passwörter, Zugriffskontrollen und aktueller Verschlüsselungsstandards wie WPA3 im WLAN kann die Sicherheit der Verbindung verbessert werden. Eine regelmäßige Überprüfung der Konfiguration dient zur Bereinigung von veralteten Einstellungen und zur Deaktivierung unnötiger Funktionen, um potenzielle Angriffsflächen zu minimieren.

Datensicherung und Wiederherstellung

Auch bei guten Schutzmaßnahmen ist es wichtig, **Datensicherung** und **Wiederherstellung** zu berücksichtigen. Sensible Daten sollten **verschlüsselt** gespeichert werden, um den Zugriff auf autorisierte Personen zu beschränken. Regelmäßige **Backups** bieten die Möglichkeit, wichtige Informationen nach einem Verlust oder Angriff wiederherzustellen. Ein **Notfallwiederherstellungsplan** hilft zudem, die IT-Systeme im Fall eines Vorfalls schnell wieder in Betrieb zu nehmen.

Verfügbarkeit und Redundanz

Für einen stabilen und kontinuierlichen Betrieb kann **Redundanz** eingesetzt werden, um kritische Komponenten abzusichern. Bei einem Serverausfall übernimmt beispielsweise ein Ersatzsystem automatisch, um den Betrieb aufrechtzuerhalten. **Lastverteilung** sorgt zusätzlich dafür, dass sich viele Anfragen gleichmäßig auf mehrere Systeme verteilen, sodass Engpässe vermieden werden. Eine Kombination aus unterbrechungsfreier Stromversorgung (USVs) und Notstromaggregat sorgt dafür, dass essenzielle Systeme auch bei Stromausfällen funktionsfähig bleiben.

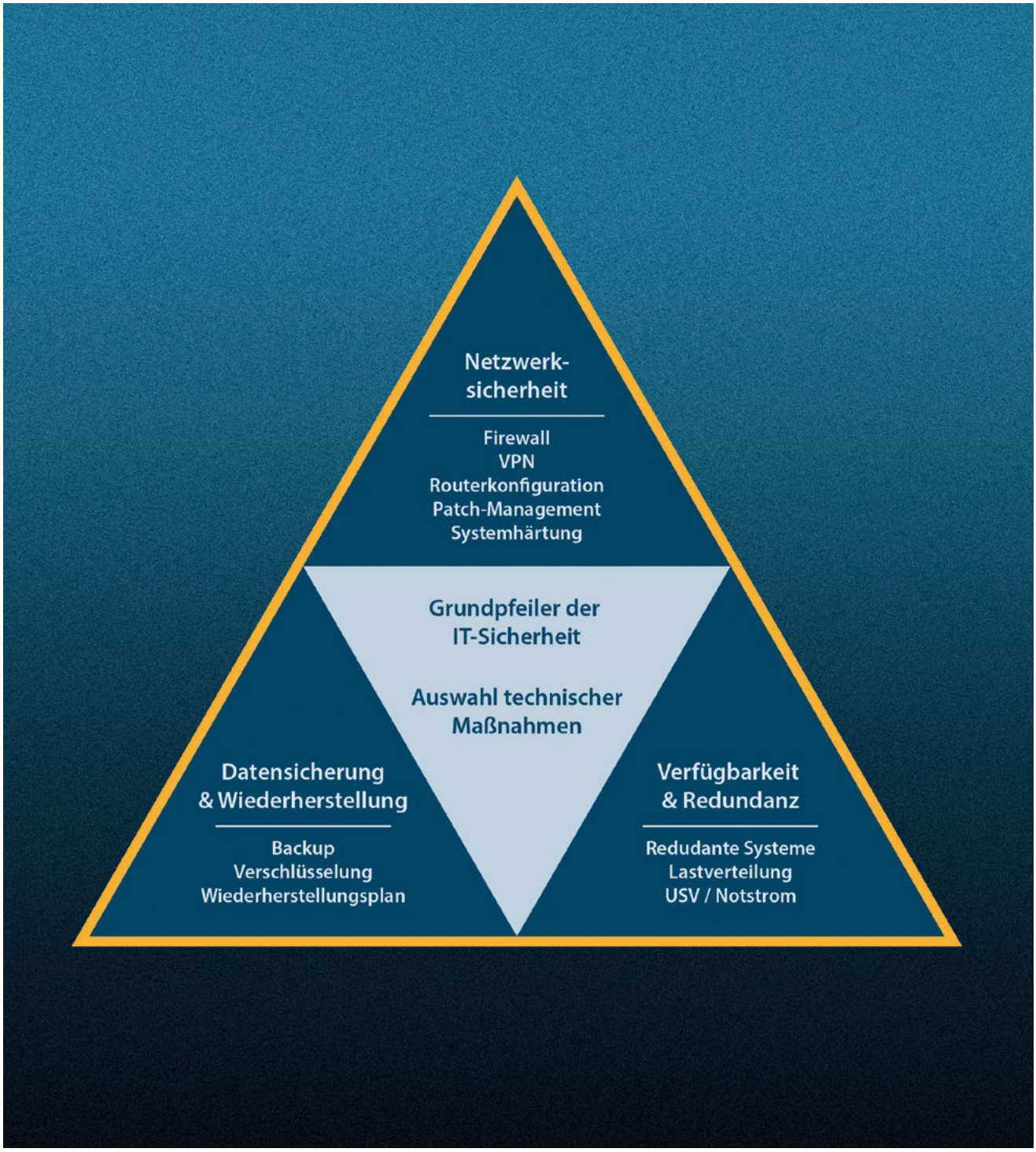
Technisches Sicherheitsmanagement

Ein Bereich des technischen Sicherheitsmanagements umfasst die regelmäßige Aktualisierung von Software und Betriebssystemen, um bekannte Sicherheitslücken zu schließen, was als **Patch- und Update-Management** bezeichnet wird. Zudem kann das Deaktivieren unnötiger

Funktionen in Systemen dazu beitragen, potenzielle Angriffspunkte zu reduzieren – eine Maßnahme, die als Systemhärtung bezeichnet wird.

Abbildung 10:
Technische Maßnahmen als Grundpfeiler der IT-Sicherheit

Quelle: Fraunhofer IESE



Maßnahmen im Krisenfall

Auch bei umfassender IT-Sicherheitsvorsorge lassen sich Störungen und Krisensituationen nicht vollständig ausschließen. Deshalb kommt es im Ernstfall darauf an, schnell, strukturiert und koordiniert zu handeln. Es gilt dabei:

Maßnahme 1: Umfassend vorbereitet sein

Die Grundlage ist ein systematischer Blick auf die kritischen Abläufe der Verwaltung. Dazu gehören:

- die Identifikation besonders schützenswerter Prozesse
- das Erstellen von **Notfallplänen** für deren Fortführung
- die Festlegung klarer Kommunikations- und Entscheidungswege

Technische Schutzmaßnahmen (zum Beispiel Firewalls, Zugriffskontrollen, Verschlüsselung) sind wichtige Bestandteile der Vorsorge (wie in 5 Grundlegende Maßnahmen für die IT-Sicherheit – Maßnahme 4: Technische Aspekte zu lesen) – doch organisatorische Vorkehrungen sind ebenso entscheidend.

Maßnahme 2: Im Vorfall handlungsfähig bleiben

Kommt es trotz aller Vorsichtsmaßnahmen zu einem Sicherheitsvorfall, ist schnelles und strukturiertes Handeln gefragt. Die Umsetzung einer eingespielten **Kommunikationsstrategie** stellt sicher, dass relevante Stellen informiert sind und Gegenmaßnahmen unverzüglich eingeleitet werden. Die Analyse des Problems begrenzt mögliche Schäden und die Koordination der Wiederherstellung betroffener Systeme geschieht auf Basis vorher definierter Abläufe, festgesetzt im **Business Continuity Management**. Dabei sind auch gesetzliche Meldepflichten und externe Unterstützungsangebote (zum Beispiel durch das BSI) zu berücksichtigen.

Maßnahme 3: Regelmäßig üben und verbessern

Damit im Ernstfall alles greift, müssen Abläufe trainiert werden. Übungen helfen, Rollen zu klären, Schwachstellen aufzudecken und Prozesse realitätsnah zu prüfen. Wichtig ist dabei ein bereichsübergreifender Ansatz: Nicht nur die IT, sondern auch Fachbereiche, Führungskräfte und gegebenenfalls externe Partner müssen eingebunden sein.

Sicherstellen der Handlungsfähigkeit

Die Sicherstellung der Handlungsfähigkeit kommunaler Verwaltungen in Krisensituationen ist eine zentrale Führungsaufgabe. Unvorhergesehene Ereignisse wie Naturkatastrophen, Cyberangriffe oder Pandemien können reguläre Arbeitsabläufe stören oder lahmlegen. In diesem Kontext sind **Notfallmanagement** und **Business Continuity Management (BCM)** entscheidend.

Während das **Notfallmanagement** auf die sofortige Krisenbewältigung fokussiert ist und Instrumente wie den **Notfallplan** und **Notfallübungen nutzt**, umfasst das **Business Continuity Management** Maßnahmen sowie langfristige Strategien zur Aufrechterhaltung des Betriebs bei erheblichen Störungen. Die Integration beider Konzepte erfordert die Schaffung entsprechender Prozesse und Strukturen. Im Gegensatz zur IT-Sicherheit, die vor Angriffen und Datenverlust schützt, geht es bei Notfallmanagement und BCM um die Wiederherstellung und den Fortbestand von Betriebsabläufen.

Business Continuity Management

Zentrales Ziel des Business Continuity Managements (BCM) in kommunalen Verwaltungen ist die **langfristige Sicherstellung der kontinuierlichen Funktionsfähigkeit** ihrer Dienstleistungen, selbst in Krisensituationen. Der Fokus liegt auf der **Fortsetzung der Kernaufgaben** und der Minimierung langfristiger Auswirkungen. Dazu werden wesentliche Prozesse und Ressourcen identifiziert sowie priorisiert, potenzielle Störungen definiert und geeignete Maßnahmen entwickelt, um den Betrieb bei Notfällen aufrechtzuerhalten oder schnellstmöglich wiederherzustellen. Der BSI-Standard 200-4 (vgl. BSI 2023b) bietet Kommunen eine strukturierte Methodik, um ein effektives BCM aufzubauen und zu betreiben.

Notfallmanagement

Das Notfallmanagement fokussiert auf die **akute Reaktion auf Notfallereignisse**. **Ziel** ist die **kurzfristige Bewältigung** von Krisen durch schnelle, koordinierte Maßnahmen zur **Schadensbegrenzung** und Aufrechterhaltung kritischer Abläufe. Im **Ernstfall** ermöglicht ein systematisches Vorgehen eine gezielte Reaktion zur Minimierung direkter Auswirkungen und Schaffung der Basis für die Wiederherstellung. Für die Umsetzung empfiehlt sich ein systematisches Vorgehen entlang etablierter Standards. Das BSI bietet hierbei den BSI-Standard 100-4 „Notfallmanagement“ (vgl. BSI 2008).

Notfallplan

Ein **Notfallplan** ist ein Instrument des Notfallmanagements, das im Ernstfall eine schnelle und gezielte Reaktion ermöglicht. Er enthält die relevanten Maßnahmen, Zuständigkeiten und Abläufe, die in einer Krisensituation notwendig sind, um den Betrieb aufrechtzuerhalten oder wiederherzustellen.

Welche Prozesse sind für die Kernaufgaben der Verwaltung unerlässlich? Welche IT-Systeme, Infrastrukturen und Ressourcen sind dafür erforderlich?

Analyse der kritischen Geschäftsprozesse

Im ersten Schritt wird geprüft, welche Prozesse für die Erfüllung der wesentlichen Aufgaben der kommunalen Verwaltung unerlässlich sind, da sie für Bürgerinnen und Bürger von Bedeutung sind. Beispiele hierfür sind Sicherung der Funktionen in Einwohnermeldeämtern, der Organisation des Katastrophenschutzes oder der Leistungen der Sozialhilfe. Neben der Identifikation dieser Prozesse ist zu untersuchen, welche IT-Systeme, Infrastrukturen und Ressourcen für ihre Durchführung notwendig sind.

Welche Gefahren könnten die Prozesse stören oder komplett lahmlegen? Welche Abhängigkeiten bestehen zwischen Prozessen, IT-Systemen, und Ressourcen?

Identifikation von Gefahren und Abhängigkeiten

Mögliche Gefahren, die Prozesse in der kommunalen Verwaltung beeinträchtigen oder zu Ausfällen führen könnten, sind zu identifizieren und zu dokumentieren. Dabei werden auch Abhängigkeiten zwischen Prozessen, IT-Systemen und Ressourcen berücksichtigt.

Wie schnell müssen Prozesse oder Systeme wieder funktionsfähig sein? Welche Mindestleistungen müssen während eines Notfalls bereitgestellt werden?

Definition von Wiederherstellungszielen

Ein Notfallplan für die IT-Sicherheit sollte klare Ziele festlegen, die eine schnelle Wiederherstellung von IT-Systemen und -Diensten ermöglichen. Dabei ist es wichtig, die Wiederherstellungszeit für kritische Systeme und Prozesse nach einem Ausfall zu definieren. Für zentrale IT-Dienste wie Notfallmanagement-Systeme oder Kommunikationstools ist eine schnelle Wiederherstellung innerhalb weniger Stunden erforderlich. Ebenso sollte festgelegt werden, welche grundlegenden IT-Dienste auch während eines Notfalls weiterhin verfügbar bleiben müssen, etwa Systeme zur Verarbeitung von Notfalldaten oder zur Bereitstellung wichtiger Onlinedienste. Diese Punkte tragen dazu bei, die Resilienz der IT-Infrastruktur im Notfall zu gewährleisten.

Dokumentation von Maßnahmen und Abläufen

Ein Notfallplan umfasst eine detaillierte Dokumentation von Maßnahmen und Abläufen, die im akuten Krisenfall umzusetzen sind. Die Dokumentation sollte so strukturiert und verständlich sein, dass alle Beteiligten im Ernstfall schnell darauf zugreifen und umgehend handeln können. Ein Bestandteil des Plans ist ein Maßnahmenkatalog, der beschreibt, welche Schritte in verschiedenen Krisenszenarien – etwa bei einem Cyberangriff, einer Datenpanne oder einem Systemausfall – zu ergreifen sind. Ferner sind Zuständigkeiten festzulegen, um die Verantwortung für spezifische Aufgaben zu regeln. Definierte Kommunikationswege helfen, relevante Informationen schnell und präzise zu übermitteln.

Notfallübungen

Notfallübungen im Bereich der IT-Sicherheit haben das Ziel, die Notfallpläne auf ihre **Praxistauglichkeit und Vollständigkeit** zu überprüfen. Die Übungen dienen auch der Schulung von **Mitarbeitenden und Führungskräften**, um Rollen und Verantwortlichkeiten in Krisensituationen zu verstehen und praktisch zu erproben. Zudem bieten sie die Gelegenheit, die Reaktionsfähigkeit zu testen und Schwächen in Abläufen zu erkennen. Die Erkenntnisse aus den Übungen tragen dazu bei, die Notfallpläne zu verfeinern und die Organisation in Bezug auf IT-Sicherheit und Krisenbewältigung zu stärken.

Erfolgsfaktoren für einen Notfallplan

Aktualisierung: Ein veralteter Notfallplan verliert schnell an Wirksamkeit. Aktualisieren Sie ihn regelmäßig und sorgen Sie dafür, dass Änderungen in Prozessen, Infrastruktur oder Technik umgehend an die Verantwortlichen des Notfallplans weitergeleitet werden, um Anpassungen zu ermöglichen (vgl. BSI 2025a).

Schulungen und Notfallübungen: Stellen Sie sicher, dass ihre Mitarbeitenden Notfallsituationen regelmäßig einüben.

Kommunikation: Effektive Kommunikation durch eine Kommunikationsstrategie im Notfall trägt dazu bei, Missverständnisse zu vermeiden und ermöglicht eine schnellere sowie fundiertere Entscheidungsfindung bei jenem Notfall.

PRAXISBEISPIEL

Notfallplan für ein Einwohnermeldeamt

Das Szenario: Ein Cyberangriff legt die gesamte IT-Infrastruktur eines Einwohnermeldeamts lahm. Weder der Zugriff auf Meldedaten noch die Nutzung digitaler Verwaltungsprozesse ist möglich. Dadurch können Bürgeranliegen nicht bearbeitet werden, und es entstehen Verzögerungen bei wichtigen behördlichen Vorgängen wie Anmeldungen oder Ausweisbeantragungen.

Die Zielsetzung: Um die Handlungsfähigkeit des Einwohnermeldeamts zu erhalten, soll der Betrieb innerhalb von 24 Stunden zumindest in reduziertem Umfang wieder aufgenommen werden. Wichtige Dienstleistungen, wie die Ausstellung vorläufiger Dokumente oder die Bearbeitung dringender Meldevorgänge, müssen weiterhin gewährleistet sein.

Die Risikoanalyse: Ein vollständiger IT-Ausfall im Einwohnermeldeamt führt zu konkreten Risiken:

- **Datenzugriff**: Ohne Zugriff auf Meldedaten können An-, Ab- und Ummeldungen nicht durchgeführt werden.
- **Betriebsausfälle**: Die Bearbeitung von Personaldokumenten, Wohnsitzbestätigungen oder Meldebescheinigungen kommt zum Erliegen.
- **Datenverlust**: Falls keine aktuellen Backups vorhanden oder zugänglich sind, droht der Verlust wichtiger Meldedaten.
- **Kommunikationsausfall:** Die Verbindung zu zentralen Registern und anderen Behörden ist unterbrochen, was Arbeitsabläufe verzögert oder unmöglich macht.
- **Sicherheitsrisiken:** Sensible personenbezogene Daten könnten durch den Angriff kompromittiert worden sein.

Die Maßnahmen: Um die Auswirkungen zu begrenzen, sind verschiedene Vorkehrungen erforderlich:

- **Datenverfügbarkeit:** Regelmäßige Backups auf separaten, gesicherten Servern ermöglichen eine schnelle Wiederherstellung.
- **Notfallarbeitsplätze:** Mobile oder autarke Systeme mit Offline-Funktionalitäten sichern den Zugriff auf wesentliche Verwaltungsabläufe.
- **Krisenmanagement:** Ein Notfallteam übernimmt die Koordination der Wiederherstellungsmaßnahmen und die interne sowie externe Kommunikation.
- **Alternative Prozesse:** Vordefinierte analoge Abläufe, wie die temporäre Bearbeitung von Anliegen in Papierform, sorgen für eine Übergangslösung.
- **Kommunikation:** Bürgerinnern und Bürger werden über alternative Kontaktmöglichkeiten informiert, um dringende Anfragen trotz IT-Ausfall bearbeiten zu können.

Verschiedene Formen von Notfallübungen (vgl. BSI 2023c)

Notfallübungen können in unterschiedlichen Formaten durchgeführt werden, abhängig von den Zielen und dem gewünschten Realitätsgrad.

Beispielhaft zu erwähnen sind:

Planbesprechungen
Bei dieser Übung erfolgt eine Szenario-basierte Besprechung, in der Verantwortliche und Führungskräfte den Ablauf eines hypothetischen oder bereits eingetretenen Notfalls durchgehen. Dabei wird analysiert, welche Maßnahmen erforderlich wären oder in der Vergangenheit hätten ergriffen werden sollen.

Ziel: Verständnis der Abläufe vertiefen und die Entscheidungsfindung trainieren

Beispiel: Szenario eines Stromausfalls in der Verwaltung, bei dem die Teilnehmenden die erforderlichen Schritte und Kommunikationswege im Einzelnen durchgehen und diskutieren

Test der technischen Vorsorgemaßnahmen
Bei diesen Übungen liegt der Fokus auf der Überprüfung der IT-Systeme und technischen Infrastruktur. Diese sollen sicherstellen, dass alle Systeme im Ernstfall wie geplant funktionieren.

Ziel: Überprüfung der technischen Resilienz und Rückversicherung, dass die Systeme auf Ausfälle vorbereitet sind

Beispiel: Test der Wiederherstellung kritischer Daten aus dem Backup-Systems oder der Test der Notstromversorgung

Simulation von Szenarien
Diese Übungen simulieren eine Notfallsituation so realitätsnah wie möglich und beziehen alle relevanten Akteure innerhalb einer Organisation ein. Sie bieten die Möglichkeit, den gesamten Notfallplan oder einen Teil davon unter echten Bedingungen zu testen, einschließlich der Zusammenarbeit verschiedener Abteilungen.

Ziel: Überprüfung der Gesamtkoordination, der Kommunikationswege und der Effektivität der Maßnahmen in einer realistischen Umgebung

Beispiel: Simulation eines Cyberangriffs, bei dem die IT-Abteilung, der Datenschutzbeauftragte und die Kommunikationsabteilung zusammenarbeiten müssen, um den Betrieb wiederherzustellen und die Öffentlichkeit zu informieren

Kommunikationsstrategie

In Krisensituationen ist eine klare und strukturierte Kommunikation erforderlich. Wenn Informationen unklar oder zu spät weitergegeben werden, führt das nicht nur zu Missverständnissen, Verzögerungen und Fehlentscheidungen, sondern kann auch das Image der Verwaltung nachhaltig schädigen. Ein zuvor erarbeiteter Kommunikationsplan hilft dabei, diese Probleme zu vermeiden und sorgt für eine effiziente Kommunikation im Notfall. Er stellt sicher, dass alle relevanten Beteiligten – von der Führungskraft über Fachabteilungen bis hin zur Öffentlichkeit – rechtzeitig die notwendigen Informationen erhalten und entsprechend reagieren können.

Die Bestandteile eines Kommunikationsplans

In einem Kommunikationsplan werden Abläufe und Zuständigkeiten festgelegt, um zu bestimmen, welche Personen zu welchem Zeitpunkt über welche Kanäle welche Informationen erhalten und wer die Verantwortung für deren Übermittlung

trägt. So lassen sich Informationslücken, Doppelmeldungen und Missverständnisse vermeiden. Eine präzise Rollenverteilung sorgt dafür, dass alle relevanten Akteure – von der Verwaltungsspitze bis hin zu externen IT-Dienstleistern – in die Kommunikationsstruktur eingebunden sind. Die regelmäßige Überprüfung und Anpassung der Kommunikationsstrategie unterstützen eine koordinierte Reaktion im Ernstfall.

Definition von Kanälen und Technologien

Kommunikationskanäle müssen auch bei Ausfällen von IT oder Telefonnetz zuverlässig funktionieren. Ergänzende Systeme wie Messenger-Dienste, Funkgeräte, Krisenplattformen oder Satellitenkommunikation können dabei unterstützen, die Kommunikation aufrechtzuerhalten. Neben bewährten Kanälen wie Telefon und E-Mail können eben jene Optionen genutzt werden, um flexibel auf verschiedene Situationen reagieren zu können. Ein zentraler Kommunikationsknoten im Krisenstab sorgt dafür, dass die Informationsweitergabe gezielt gesteuert wird, alle relevanten Akteure auf dem neuesten Stand bleiben und eine schnelle, strukturierte Reaktion auf unvorhergesehene Ereignisse möglich ist.

Vordefinierte Botschaften

Vorab vorbereitete Standardtexte für verschiedene Zielgruppen helfen in Krisensituationen, Verzögerungen zu vermeiden und die Konsistenz der Informationen sicherzustellen. In der **internen Kommunikation** wird sichergestellt, dass Führungskräfte und Mitarbeitende die notwendigen Anweisungen erhalten, um Maßnahmen umzusetzen. In der **externen Kommunikation** werden Bürgerinnen und Bürger sowie Medien zeitnah über die aktuelle Lage und ergriffene Maßnahmen informiert.

Regelmäßige Kommunikationstrainings

Ein gut durchdachter Kommunikationsplan allein reicht nicht aus – seine Wirksamkeit hängt wie immer von der Vorbereitung der Beteiligten ab. Regelmäßige Schulungen und Übungen, organisiert durch die Kommune oder beauftragte Dienstleister, schaffen die Grundlage für mehr Handlungssicherheit und eine konsistente Kommunikation im Notfall.

Empfehlungen des BSI

Das BSI betont in seinen Leitfäden die Bedeutung einer modernen, vielseitigen Kommunikationsstrategie. Neben klassischen Kanälen wie E-Mail und Telefon sollten auch digitale Plattformen und Social-Media-Kanäle genutzt werden, um Bürgerinnen und Bürger im Krisenfall schnell und zielgerichtet zu informieren.

Fazit und Ausblick

IT-Sicherheit ist eine wesentliche Aufgabe für Kommunen und angesichts wachsender Cyberbedrohungen müssen Führungskräfte proaktiv handeln. Maßnahmen müssen ergriffen werden, um das Vertrauen von Bürgerinnen und Bürgern in die digitale Verwaltung zu erhalten und die Handlungsfähigkeit in Krisensituationen zu bewahren.

Kommunen müssen ihre Maßnahmen zur IT-Sicherheit kontinuierlich anpassen und weiterentwickeln. Schulungen und der Austausch von Informationen tragen dazu bei, immer auf dem neuesten Stand zu bleiben. Die Entwicklung robuster Notfallpläne und die Umsetzung von Risikomanagementmaßnahmen helfen, um im Bedrohungsfall schnell reagieren zu können.

Auf technischer Ebene sollten Kommunen innovative als auch bewährte Technologien und Verfahren nutzen, um die IT-Infrastruktur zu stärken. Indem Sie das Sicherheitsbewusstsein jedes Einzelnen schärfen und eine Sicherheitskultur fördern, in der alle Mitarbeitenden Verantwortung übernehmen, schaffen Sie die Grundlage für eine widerstandsfähige Verwaltung.

Literaturverzeichnis

Allianz für Cybersicherheit, o. J.: Über uns. Zugriff: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Ueber-uns/ACS/acs_node.html [abgerufen am 23.06.2025].

BMDS – Bundesministerium für Digitales und Staatsmodernisierung, 2025: Kommunale Förderprogramme. Zugriff: https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/kommunen/foerderprogramme/foerderprogramme.html [abgerufen am 23.06.2025].

BMI – Bundesministerium des Innern und für Heimat, 2017: Onlinezugangsgesetz (OZG). Zugriff: https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/das-gesetz/info-ozg-wortlaut/ozg-im-wortlaut-node.html [abgerufen am 23.06.2025].

BMI – Bundesministerium des Innern und für Heimat, 2024: OZG-Änderungsgesetz – Paket für die digitale Verwaltung. Zugriff: https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/das-gesetz/ozg-aenderungsgesetz/ozg-aenderungsgesetz-node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, o. J. a: Archiv Lageberichte BSI. Zugriff: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/Archiv-Lageberichte/archiv-lagebericht_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, o. J. b: Kleine- und Mittlere Unternehmen – Informationen und Hilfestellungen für KMU. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/KMU_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, o. J. c: IT-Grundschutz-Schulungen. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/it-grundschutzschulung_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2008: BSI-Standard 100-4 – Notfallmanagement. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-100-4-Notfallmanagement/bsi-standard-100-4-notfallmanagement_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2017a: BSI-Standard 200-2 IT-Grundschutz-Methodik. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/bsi-standard-200-2-it-grundschutz-methodik_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2017b: BSI-Standard 200-3 Risikomanagement. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2021a: Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). Zugriff: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2021b: IT-Grundschutz Informationssicherheit mit System. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2023a: Die Lage der IT-Sicherheit in Deutschland 2023. Zugriff: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2023b: BSI-Standard 200-4 – Business Continuity Management. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2023c: Übungsbaukasten – 0.2 Übungsplanung. Zugriff: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/UPK/upk-uebk_02-uebungsplanung.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2023d: IT-Grundschutz-Kompendium – Werkzeuge für Informationssicherheit. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2023e: Weg in die Basis-Absicherung (WiBA). Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/WIBA/Weg_in_die_Basis_Absicherung_WiBA_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2023f: IT-Grundschutz-Profil – Basis-Absicherung Kommunalverwaltung. Zugriff: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html [abgerufen 24.06.2025]

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2024: Die Lage der IT-Sicherheit in Deutschland 2024. Zugriff: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2025a: Kapitel 9: Notfallmanagement verbessern. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/9_NotfallmanagementVerbessern/nfm09_01.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2025b: Startseite. Zugriff: https://www.bsi.bund.de/DE/Home/home_node.html [abgerufen am 12.05.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2025c: CERT-Bund. Zugriff: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html [abgerufen am 23.06.2025].

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2025d: EU-Richtlinien zur Netzwerk- und Informationssicherheit (EU-NIS-Richtlinie). Zugriff: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-Richtlinien/nis-richtlinien_node.html [abgerufen am 23.06.2025].

BSI-Kritisverordnung (BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958), zuletzt durch Artikel 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339) geändert. Zugriff: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html [abgerufen am 23.06.2025].

Bundesdatenschutzgesetz (BDSG) vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist. Zugriff: https://www.gesetze-im-internet.de/bdsg_2018/ [abgerufen am 23.06.2025].

CERT-Verbund, 2025: Überblick. Zugriff: https://www.cert-verbund.de/ [abgerufen am 12.05.2025].

CIO Bund – Der Beauftragte der Bundesregierung für Informationstechnik, 2025: IT-Grundschutz Tool. Zugriff: https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-konsolidierung/dienstekonsolidierung/it-massnahmen/gs-tool/gs-tool-node.html [abgerufen am 23.06.2025].

Deutscher Städtetag, 2024: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen. Zugriff: https://www.staedtetag.de/files/dst/docs/Themen/2024/Handreichung-ISLL-2024.pdf [abgerufen am 23.06.2025].

Deutschland sicher im Netz e. V., o. J.: Startseite. Zugriff: https://www.sicher-im-netz.de/ [abgerufen am 13.05.2025].

Flourish, o. J.: Visualisierung kommunaler Cybervorfälle. Zugriff: https://public.flourish.studio/visualisation/22022248/ [abgerufen am 23.06.2025].

Guth, M.; Reuters; Dpa, 2021: Erster Cyber-Katastrophenfall in Deutschland: Landkreis liegt lahm. FAZ, 10. Juli. Zugriff: https://www.faz.net/pro/digitalwirtschaft/erster-cyber-katastrophenfall-in-deutschland-landkreis-liegt-lahm-17431739.html [abgerufen am 23.06.2025].

Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz, Referat VI 3 – Hessen CyberCompetenceCenter (Hessen3C), 2025: Cybersicherheitsnetzwerk Hessen. Zugriff: https://hessen3c.de/ [abgerufen am 23.06.2025].

Intersoft Consulting, 2018: Datenschutz-Grundverordnung (DSGVO), 2018. Zugriff: https://dsgvo-gesetz.de/ [abgerufen am 23.06.2025].

IT-Planungsrat, 2020: Umsetzung der Leitlinie für Informationssicherheit. Zugriff: https://www.it-planungsrat.de/projekte/umsetzung-der-leitlinie-fuer-informationssicherheit [abgerufen am 23.06.2025].

IT-Planungsrat, 2024: Zielbild für das Schwerpunktthema: Informationssicherheit. Zugriff: https://www.it-planungsrat.de/fileadmin/it-planungsrat/der-it-planungsrat/schwerpunktthemen/250314_IT-PLR_Zielbilder_final_Informationssicherheit.pdf [abgerufen am 23.06.2025].

Lange, J., o. J.: Kommunaler Notbetrieb. Zugriff: https://kommunaler-notbetrieb.de [abgerufen am 23.06.2025].

MDR, 2022: Katastrophenfall nach Cyberangriff in Anhalt-Bitterfeld aufgehoben. 02. Februar 2022. Zugriff: https://www.mdr.de/nachrichten/sachsen-anhalt/dessau/bitterfeld/cyberangriff-katastrophenfall-anhalt-bitterfeld-aufgehoben-100.html [abgerufen am 23.06.2025].

NKCS – Nationales Koordinierungszentrum für Cybersicherheit Deutschland, 2025: Förderprogramme Horizont Europa und Digitales Europa der EU. Zugriff: https://www.nkcs.bund.de/de/foerderprogramme [abgerufen am 23.06.2025].

Opetz, M., 2025: Kommunale IT-Sicherheit – die NIS-2-Richtlinie. Zugriff: https://kommunal.de/kommunale-it-sicherheit-neue-Richtlinie [abgerufen am 23.06.2025].

Stiftung Neue Verantwortung, 2025: Cybersicherheitskompass - Nordrhein-Westfalen. Zugriff: https://cybersicherheitskompass.de/nordrhein-westfalen [abgerufen am 23.06.2025].

Stuffrein, C., 2024: Fraunhofer FOKUS Kompetenzzentrum Öffentliche IT: Stärkung der gesamtstaatlichen Resilienz durch Informationssicherheit: Herausforderungen und Lösungen für Kommunen. Zugriff: https://www.oeffentliche-it.de/-/staerkung-der-gesamtstaatlichen-resilienz-durch-informationssicherheit-herausforderungen-und-loesungen-fuer-kommunen [abgerufen am 23.06.2025].

VPN Haus, 2024: Förderprogramme für die Cybersicherheit von Kommunen. Zugriff: https://www.vpnhaus.com/de/2024/foerderprogramme-fuer-die-cybersicherheit-von-kommunen [abgerufen am 23.06.2025].

Weiterführende Informationen

Anlaufstellen

In Deutschland haben sich verschiedene Institutionen etabliert, die Kommunen bei wachsenden Cyberbedrohungen gezielt helfen – von Beratung bis zur direkten Unterstützung im Ernstfall.

Bundesamt für Sicherheit in der Informationstechnik (vgl. BSI 2025b): Die zentrale Anlaufstelle für IT-Sicherheit. In Zusammenarbeit mit den zuständigen Landesbehörden und kommunalen Spitzenverbänden unterstützt das BSI Kommunen beim Einstieg oder der Weiterentwicklung ihrer Informationssicherheit. Zudem stellt es zielgruppenspezifische Produkte, wie Arbeitshilfen und Blaupausen, zur Verfügung. Die IT-Grundschutzkataloge bieten Verwaltungen wertvolle Orientierung.

CERT-Bund (vgl. BSI 2025c): Das CERT-Bund, beim BSI angesiedelt, ist die zentrale Anlaufstelle für IT-Sicherheitsvorfälle. Es koordiniert Gegenmaßnahmen, warnt vor Bedrohungen und bietet präventive Handlungsempfehlungen. Das Team weist auf Schwachstellen hin, schlägt Behebungsmaßnahmen vor und unterstützt bei der Reaktion auf Vorfälle. Zudem bietet CERT-Bund eine 24-Stunden-Rufbereitschaft und einen Warn- und Informationsdienst.

Landes-CERTs (vgl. CERT-Verbund 2025) und **kommunale IT-Dienstleister**: Regionale Expertinnen und Experten, die Lösungen für lokale Verwaltungen entwickeln. Sie beraten direkt vor Ort und unterstützen bei der Implementierung sicherer IT-Systeme.

Unterstützungsangebote und Beratungsstellen

Neben den zentralen Akteuren gibt es eine Vielzahl von Unterstützungs- und Beratungsangeboten, die speziell auf Kommunen zugeschnitten sind:

IT-Grundschutz des BSI

Der **BSI IT-Grundschutz** (vgl. BSI 2024d) ist ein modulares Konzept, das Kommunen dabei hilft, systematisch und effizient ihre IT-Sicherheit zu verbessern. Er enthält praxisorientierte Bausteine für den Aufbau eines umfassenden Sicherheitsmanagementsystems, das sich flexibel an die Größe und die Bedürfnisse der jeweiligen Organisation anpassen lässt. Der IT-Grundschutz umfasst auch Tools wie den **GSTOOL** (vgl. CIO Bund 2025), das die Planung und Dokumentation von Sicherheitsmaßnahmen unterstützt. Eine Vielzahl von Handbüchern und Leitfäden stehen online zur Verfügung.

Förderprogramme für Cybersicherheit

Um die IT-Sicherheitsmaßnahmen in Kommunen zu verbessern, stellen Bund und Länder verschiedene Förderprogramme bereit (vgl. BMDS 2025). Im Speziellen bietet der Bund Informationen zu Förderprogrammen, aber auch Informationen und Beratung zu Fördermöglichkeiten und aktuellen Ausschreibungen, gebündelt auf der Seite des **Nationalen Koordinierungszentrums für Cybersicherheit** (vgl. NKCS 2025) zur

Verfügung. Dazu gehören das Programm „**Digitales Europa**“, das Projekte zum Schutz kritischer Infrastrukturen und den Aufbau von Sicherheitszentren unterstützt, sowie „**Horizont Europa**“, das innovative Lösungen zur Verbesserung der Cybersicherheit fördert.

Beratung und Weiterbildung

Über verschiedene Institutionen können Kommunen auf Beratungsleistungen und Schulungen zugreifen. Das **Hessen CyberCompetenceCenter** (vgl. Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz, 2025) bietet beispielsweise speziell auf kommunale Bedürfnisse zugeschnittene Beratungen und Schulungen an, um IT-Verantwortliche und Mitarbeitende auf den neuesten Stand der Cybersicherheit zu bringen. Auch der **Cybersicherheitskompass** (2025) führt eine Liste mit entsprechenden Angeboten. Diese Fortbildungsangebote tragen dazu bei, das Bewusstsein für Cybergefahren zu schärfen und konkrete Maßnahmen zur Risikominimierung zu ergreifen.

Die **Kommunalen Spitzenverbände** bieten eine Handreichung (vgl. Deutscher Städtetag 2024) an, die eine Einführung in zentrale Begriffe der Informationssicherheit sowie eine Übersicht über vier etablierte Standards für Informationssicherheits-Managementsysteme, darunter ISO/IEC 27001 und den BSI-IT-Grundschutz mit dem „Weg in die Basis-Absicherung“, enthält. Ergänzend werden die Vorgaben der Leitlinie des IT-Planungsrats dargestellt, dem zentralen Steuerungsgremium für die föderale IT-Zusammenarbeit von Bund und Ländern. Zur Unterstützung der praktischen Anwendung wurden Mustertexte für die Erstellung behördenspezifischer Informationssicherheitsleitlinien ergänzt. Zudem wurden Beispiele für Schutzbedarfskategorien und Sicherheitsziele aktualisiert, um eine Anpassung an die Anforderungen der kommunalen Verwaltung zu ermöglichen.

Die **interaktive Webseite Cybersicherheit_SmartCity4** (vgl. Flourish o. J.) stellt eine strukturierte Übersicht relevanter Normen und Standards zur Verfügung, die im Kontext der Cybersicherheit von Smart-City-Anwendungen zu berücksichtigen sind.

Weitere Anlaufstellen und Netzwerke

Darüber hinaus gibt es zahlreiche Netzwerke und Initiativen, die Kommunen in Fragen der Cybersicherheit unterstützen:

Deutschland sicher im Netz (DsiN):

Die Initiative **Deutschland sicher im Netz** (vgl. Deutschland sicher im Netz o. J.) unterstützt nicht nur Unternehmen, sondern auch Kommunen bei der Aufklärung und Beratung im Bereich IT-Sicherheit. Sie bietet Schulungsmaterialien und Informationsangebote, um IT-Fachkräfte für aktuelle Bedrohungen zu sensibilisieren und ihre Handlungsfähigkeit im Krisenfall zu stärken.

KMU-innovativ: Informations- und Kommunikationstechnologie (IKT):

Das Programm KMU-innovativ des Bundesministeriums für Bildung und Forschung (vgl. BMBF 2025) richtet sich an kleine und mittlere Unternehmen (KMU), die innovative Lösungen im Bereich der IT-Sicherheit entwickeln möchten. Mit finanzieller Unterstützung können Unternehmen Projekte in Forschung und Entwicklung realisieren, die der Verbesserung der Cybersicherheit dienen. Für Kommunen ist dies von Bedeutung, da sie durch die Zusammenarbeit mit KMU ihre digitale Infrastruktur sowie den Schutz sensibler Daten verbessern können. Dies ist ein wesentlicher Aspekt für die Entwicklung sicherer Dienstleistungen und zur Förderung des Vertrauens der Bürgerinnen und Bürger.

Weitere BSI-Dokumente

BSI-Standard 100-4: Notfallmanagement

Dieses Dokument beschreibt die Anforderungen und die Methodik zur Einführung und Pflege eines behörden- oder unternehmensweiten Notfallmanagements (vgl. BSI, 2025i). Es unterstützt dabei, die Widerstandsfähigkeit kritischer Geschäftsprozesse zu erhöhen und im Krisenfall schnell und strukturiert zu reagieren. Der Standard bietet ein systematisches Vorgehen mit klaren Prozessphasen – von der Vorbereitung über die Bewältigung bis zur kontinuierlichen Verbesserung. Besonders hilfreich ist er für Institutionen, die ihr Notfallmanagement mit etablierten IT-Grundschutz-Methoden verzahnen möchten.

BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)

Dieses Dokument (vgl. BSI, 2025j) legt die Anforderungen und die Methodik zur Einführung eines Informationssicherheitsmanagementsystems (ISMS) fest. Es bietet die Grundlage, um Informationssicherheit als kontinuierlichen und strukturierten Prozess in der Organisation zu verankern. Besonders relevant für die Basis-Absicherung ist der Fokus auf Schutzbedarfsanalysen und ein einfaches Sicherheitskonzept.

BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise

Dieser Standard (vgl. BSI 2025k) beschreibt die konkrete Methodik zur Umsetzung der IT-Grundschutz-Vorgehensweise. Für die Basis-Absicherung ist der vereinfachte Einstieg über die vereinfachte Modellierung und die Verwendung von Mustervorlagen besonders wichtig. Kommunen können sich hier an vorgefertigten Bausteinen orientieren, die für typische IT-Komponenten und Prozesse entwickelt wurden.

BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz

Die Risikoanalyse ist ein zentraler Baustein, um über die Basis-Absicherung hinaus gezielt Risiken zu bewerten, die durch die standardisierten Maßnahmen nicht vollständig abgedeckt sind. Dieses Dokument (vgl. BSI 2025l) hilft, gezielt Abweichungen und Schwachstellen zu identifizieren und zu adressieren.

BSI-Standard 200-4: Business Continuity Management (BCM)

Dieser Standard (vgl. BSI 2025c) definiert die Anforderungen und Vorgehensweisen zur Einführung und Aufrechterhaltung eines Business Continuity Managements (BCM). Ziel ist es, die Betriebsfähigkeit einer Organisation auch in Krisensituationen sicherzustellen. Der Standard gibt konkrete Hilfestellungen zur Identifikation kritischer Geschäftsprozesse, zur Entwicklung von Notfallplänen sowie zur Durchführung regelmäßiger Übungen und Tests. Ein Schwerpunkt liegt auf der Etablierung eines strukturierten Krisenmanagements, das klare Kommunikations- und Koordinationswege in Notfällen sicherstellt.

IT-Grundschutz-Kompendium

Das BSI IT-Grundschutz-Kompendium (vgl. BSI 2024b) enthält standardisierte Bausteine, Maßnahmen und Anforderungen zur Umsetzung des IT-Grundschutzes. Das Kompendium wird regelmäßig aktualisiert und umfasst verschiedene Themenbereiche wie Netzwerksicherheit, organisatorische Sicherheitsmaßnahmen und Notfallmanagement.

BSI-IT-Grundschutz-Leitfäden und Webressourcen:

Neben den Standards und dem Kompendium stellt das BSI ergänzende Leitfäden, Whitepaper zu Themen wie unter anderem Informationssicherheit in Smart Cities und Smart Regions (vgl. BSI 2022) und Online-Materialien zur Verfügung. Besonders hilfreich sind hier:

- **Leitfäden für kleine und mittelgroße Organisationen,** die spezifisch auf die Einstiegshürden kleinerer kommunaler Verwaltungen eingehen (vgl. BSI, o. J. b).
- **BSI-Webinare und E-Learning-Angebote,** die Verantwortlichen die wichtigsten Grundlagen vermitteln und praktische Umsetzungsschritte erläutern. Ein Beispiel hierfür ist der Online-Kurs: Informationssicherheit mit IT-Grundschutz der IT-Grundschutz-Schulungen Reihe (vgl. BSI o. J. c).

Glossar

Asset
Bezeichnet im kommunalen Kontext alle materiellen und immateriellen Werte, die für die Funktionsfähigkeit und Sicherheit einer Kommune von Bedeutung sind. Dazu gehören physische Infrastruktur wie Gebäude, Straßen und Fahrzeuge sowie digitale Ressourcen wie IT-Systeme, Netzwerke, Datenbanken und sensible Verwaltungsinformationen.

Backup
Die Sicherstellung der Verfügbarkeit von kritischen Daten durch regelmäßige Sicherung auf separaten Servern.

Backup-Management
Der Prozess der regelmäßigen Sicherung und Speicherung von Daten, um im Falle eines Datenverlustes eine Wiederherstellung zu ermöglichen.

BCM (Business Continuity Management)
Ein systematischer Ansatz zur Sicherstellung der Betriebsfähigkeit kritischer Geschäftsprozesse im Krisenfall.

BSI (Bundesamt für Sicherheit in der Informationstechnik)
Bundesbehörde, die für die Entwicklung von Standards, Leitlinien und Maßnahmen zur Gewährleistung der IT-Sicherheit in Deutschland zuständig ist.

Cyberangriffe
Angriffe auf IT-Systeme, um Daten zu stehlen, Systeme zu beschädigen oder den Betrieb zu stören, zum Beispiel durch Ransomware.

Cybersicherheit
Schutz von Systemen, Netzwerken und Daten im digitalen Raum vor Angriffen wie Hacking, Malware oder Cyberkriminalität. Sie umfasst Maßnahmen wie Bedrohungsanalyse, Incident Response und Sicherheitsarchitekturen, um digitale Infrastrukturen zu sichern.

Datensicherheitsmaßnahmen
Maßnahmen, die dazu dienen, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu schützen, zum Beispiel durch Verschlüsselung und regelmäßige Backups.

Datenschutz
Schutz personenbezogener Daten vor unbefugtem Zugriff, Missbrauch und Verlust, insbesondere durch die Einhaltung der Datenschutz-Grundverordnung (DSGVO).

Datenschutz-Grundverordnung (DSGVO)
Europäische Verordnung, die den Schutz personenbezogener Daten regelt und in allen EU-Mitgliedstaaten gilt.

Desktop-Übungen
Theoriegestützte Szenarien, bei denen die Verantwortlichen den Ablauf eines Notfalls durchsprechen, um die Handlungsfähigkeit zu testen.

Informationssicherheit
Schutz von Informationen in jeglicher Form durch technische, organisatorische und prozessuale Maßnahmen. Ziel ist es, Vertraulichkeit, Integrität und Verfügbarkeit von Daten durch Richtlinien, Schulungen und Sicherheitskultur zu gewährleisten.

ISO 27000-Serie
Internationale Normenreihe, die Standards und Leitlinien für Informationssicherheitsmanagementsysteme (ISMS) bietet. Besonders relevant sind ISO/IEC 27001 und ISO/IEC 27002.

ISO/IEC 27001
Standard für die Einführung, Umsetzung und Pflege eines Informationssicherheitsmanagementsystems (ISMS), der häufig als Grundlage für Zertifizierungen genutzt wird.

ISO/IEC 27002
Leitfaden zur Auswahl und Umsetzung von Sicherheitsmaßnahmen, der praxisnahe Empfehlungen für Organisationen bietet.

IT-Grundschutz
Methodik des BSI zur systematischen Absicherung von IT-Infrastrukturen und -Prozessen in Organisationen. Sie beinhaltet eine Sammlung von Maßnahmen, Bausteinen und Standards.

IT-Grundschutz-Kompendium
Sammlung von Bausteinen, die für typische IT-Prozesse und -Infrastrukturen spezifische Sicherheitsanforderungen und Maßnahmen bereitstellen.

IT-Grundschutz-Vorgehensweise (BSI-Standard 200-2)
Methodische Vorgehensweise des BSI zur schrittweisen Umsetzung von IT-Sicherheitsmaßnahmen, besonders für Organisationen mit begrenzten Ressourcen.

IT-Sicherheit
Schutz von Computersystemen und Netzwerken vor unbefugtem Zugriff, Manipulation oder Zerstörung. Sie fokussiert auf technische Maßnahmen wie Firewalls, Verschlüsselung und Zugangskontrollen, um Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen.

IT-Sicherheitsstrategie
Ein systematischer Plan, der Ziele, Maßnahmen und Vorgehensweisen zur Sicherstellung der IT-Sicherheit einer Organisation festlegt.

Kommunikationspläne
Strukturierte Kommunikationsstrukturen und -prozesse, die in Krisensituationen eine effektive und klare Kommunikation sicherstellen.

Mehr-Faktor-Authentifizierung (MFA)
Ein Sicherheitsverfahren, bei dem mehr als ein Authentifizierungsfaktor (zum Beispiel Passwort, Token, Biometrie) zur Verifizierung der Identität verwendet wird.

Ransomware-Angriffe
Eine Cyberattacke, bei der Schadsoftware Daten verschlüsselt oder den Zugriff darauf blockiert, um Lösegeld für die Freigabe zu erpressen.

Verschlüsselung
Technologie zur Umwandlung von Daten in eine unlesbare Form, die nur durch den Besitz eines Entschlüsselungsschlüssels wieder zugänglich gemacht werden kann.

Zugriffsmanagement
Der Prozess, der regelt, wer auf welche Daten und IT-Ressourcen zugreifen darf, basierend auf den jeweiligen Bedürfnissen und Aufgaben der Nutzer.

www.bbsr.bund.de

ISBN 978-3-98655-120-9