Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe

Bundesamt
für Sicherheit in der
Informationstechnik

Kommunale IT-Krisen: Handlungsfähigkeit sichern

Ein Wegweiser zur Bewältigung und Prävention

Fachinformation

BBK. Gemeinsam handeln. Sicher leben.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Bundesamt für Sicherheit in der Informationstechnik

Kommunale IT-Krisen: Handlungsfähigkeit sichern

Ein Wegweiser zur Bewältigung und Prävention

Herausgebende Behörden
Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) erfüllt die Aufgaben des Bundes im Zivilschutz, dem Schutz der Bevölkerung im Verteidigungsfall, sowie konzeptionelle, planerische und operative Aufgaben in der Zivilen Verteidigung. Dem *All-Gefahren-Ansatz* folgend strebt das BBK an, Cybergefahren in das allgemeine Risiko- und Krisenmanagement zu integrieren. Das BBK setzt dabei den Schwerpunkt auf die Schnittstelle zwischen Cyberraum und physischer Welt. So berät das BBK bspw. zu Fragestellungen des Risiko- und Krisenmanagements, um reaktionsfähige Bewältigungsstrukturen zu fördern.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das Ziel, den sicheren Einsatz von Informations- und Kommunikationstechnik in Staat, Wirtschaft und Gesellschaft zu ermöglichen. Die Informationssicherheit soll als Voraussetzung der Digitalisierung verstanden und eigenverantwortlich umgesetzt werden. Neben der Entwicklung von Standards gehört auch die Beratung der Zielgruppen bei der Umsetzung geeigneter Maßnahmen zu den Kernaufgaben.

Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe

Bundesamt
für Sicherheit in der
Informationstechnik

Dank für Mitwirkung
Unser Dank gilt allen Personen und Einrichtungen, die uns bei der Erstellung dieses Wegweisers unterstützt haben und durch lehrreiche Fachgespräche im Vorfeld oder Ergänzungen, Korrekturen und Rückmeldungen zu Zwischenständen einen entscheidenden Beitrag geleistet haben, insbesondere:

- Moritz Aberle
- Konstantin Haase, Komm.ONE
- Regina Holzheuer, Ministerium für Umwelt, Klima und Energiewirtschaft Baden-Württemberg
- Jonas Kapitain, Kreisstadt Bergheim
- Esther Kern, Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH (BIGS)
- Clemens Körner, Rhein-Pfalz-Kreis
- Jörg Naumann, Stadt Chemnitz
- Claudia Parton, SIS/KSM
- Thomas Schmidt, Kommunale Informationsverarbeitung Sachsen – KISA
- AK Informationssicherheit (AKIS) des DST
- BfV
- BND
- ITK Rheinland
- Stadt Rodgau

Unser Dank gilt selbstverständlich auch allen Mitarbeitenden in BBK und BSI, die an der Erstellung dieses Wegweisers beteiligt waren, vom initialen Anschieben des Projekts über die Zulieferung von Beiträgen bis zum Einbringen von Fachexpertise im Rahmen von Nachfragen und Kommentierungen.

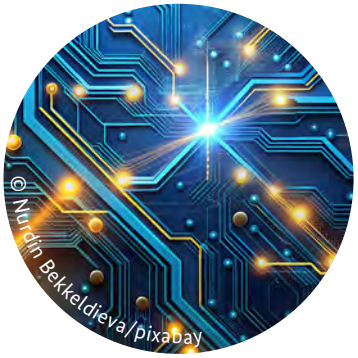

© Gerd Altmann/pixabay


corporations
wikileaks
servers
internet
backdoor
remote administration tools
SSL government
trojan
bitcoin
root
data
spoofing
CYBER
SECURITY
data dump
porn
keylogger
antivirus
adwares
database
whitehat
blackhat
hackers
firewall
worm
malwares
distributed denial of service
defacement
script
world wide web
surveillance
stuxnet
encrypt
access
warez
activism
© Darwin Laganzon/pixabay


© Gerd Altmann/pixabay


© Gerd Altmann/pixabay


© Cliff Hang/pixabay


© Nurdin Bekkeldieva/pixabay

Inhalt

Management Summary

Als im Juli 2021 das allererste Mal ein Landkreis den Katastrophenfall aufgrund eines Cyberangriffes ausrief, erregte dies große mediale Aufmerksamkeit. Zeitweise war von einer „Cyberkatastrophe“ die Rede. Die Kommune war von jetzt auf gleich stark in ihrer Handlungsfähigkeit eingeschränkt. Viele Dienstleistungen konnten nicht mehr erbracht werden. Auch heute sind öffentliche Einrichtungen weiterhin ein Ziel für Cyberangriffe.

Kommunale Behörden sind von grundlegender Bedeutung für die gesamtstaatliche Verwaltung in Deutschland: Sie haben direkten Kontakt zu den Bürgerinnen und Bürgern, erheben und verarbeiten große Mengen sensibler Daten und erbringen wichtige Dienstleistungen auch für andere administrative Ebenen. In ihrem Handeln sind Kommunalverwaltungen bereits heute stark von informationstechnischen Systemen abhängig und gegenüber deren Ausfall entsprechend verwundbar. Immer wieder führen menschliches Versagen, unerwartete technische Fehler, Naturereignisse und insbesondere auch Cyberangriffe zu IT-Ausfällen, die teilweise zu einem monatelangen Stillstand in den betroffenen Verwaltungen führen. Lange Ausfallzeiten haben weitreichende Auswirkungen auf das Leben der Bürgerinnen und Bürger sowie auf die lokale Wirtschaft. Der Abfluss vertraulicher Informationen und Zweifel an einem effektiven Umgang mit der Situation können das Vertrauen in die Verwaltung nachhaltig erschüttern. Ein Cyberangriff ist kein reines IT-Szenario, sondern fordert die gesamte Notfall- und Krisenorganisation einer Kommune.

Der vorliegende Wegweiser wurde gemeinsam vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet. Er bietet einen Einstieg in das Thema kommunale IT-Krisen mit dem Ziel, Daten und Infrastrukturen in Kommunalverwaltungen effektiver vor Gefahren zu schützen und die Handlungsfähigkeit in der Lage zu verbessern. Der Wegweiser richtet sich zunächst an diejenigen, die für das kommunale Krisenmanagement Verantwortung tragen, denn den vorbeugenden und vorbereitenden Maßnahmen muss „von oben“ die notwendige Priorität einschließlich der entsprechenden Ressourcen eingeräumt werden. Darüber hinaus wendet er sich an alle Mitarbeitenden der Verwaltung, deren Aufgabenbereich mit dem Management von IT-Krisen verbunden ist: vom *IT-Betrieb* über das interne Notfallmanagement bis zu den Verantwortlichen für die externe Kommunikation. Der Wegweiser ist keine Blaupause – für eine passgenaue Vorbereitung müssen immer die lokalen organisatorischen und technischen Gegebenheiten berücksichtigt werden. Er bietet jedoch einen niedrigschwelligen Einstieg, kann ohne spezifische IT-Fachexpertise genutzt werden und zeigt eine Reihe von Maßnahmen mit vergleichsweise geringem Ressourcenbedarf auf. Die Unterteilung in verschiedene Themenfelder erleichtert den Überblick, ermöglicht aber auch eine modulare Anwendung: Man muss sich nicht zwingend von vorne nach hinten durcharbeiten, sondern kann dort anfangen, wo es vor Ort am dringlichsten oder auch am besten umsetzbar ist.

Ausgangspunkt und roter Faden des Wegweisers ist das Szenario eines *Ransomware*-Angriffs auf eine fiktive Kommunalverwaltung (→ *Kapitel 2*). Es schließen sich Hinweise für die konkrete Bewältigung eines solchen Vorfalls (→ *Kapitel 3*) sowie die anschließende Wiederherstellung der IT-Infrastruktur an (→ *Kapitel 4*). Damit solche Akutmaßnahmen in der Lage schnell und erfolgreich umgesetzt werden können, bedarf es nicht nur entsprechend geschulter Mitarbeitender und vorgedachter interner Strukturen, auch das Hinzuziehen externer Hilfe durch andere Behörden oder private Dienstleister sollte geplant sein (→ *Kapitel 3.2* und → *Kapitel 5.3*).

Kommunalverwaltungen werden tagtäglich von Cyberkriminellen angegriffen. Dass diese Angriffe stattfinden, können Kommunen nicht verhindern – aber die Wahrscheinlichkeit, dass die Angreifer erfolgreich sind, kann entscheidend gesenkt werden. Dazu ist es unabdingbar, dass die

Leitungsebene die Verantwortung für die Informationssicherheit übernimmt und die nötigen Strukturen geschaffen und personell hinterlegt werden. Die Etablierung eines *Informationssicherheitsmanagementsystems* (ISMS, → *Kapitel 5.1.1*) und die Benennung eines Informationssicherheitsbeauftragten (→ *Kapitel 5.1.3*) sind besonders wichtige Schritte.

Wie so oft gilt auch in Bezug auf IT-Krisen: Prävention ist besser, schneller und günstiger als Reaktion! Mit einigen einfacheren technischen Maßnahmen kann die IT-Sicherheit bereits entscheidend verbessert werden (→ *Kapitel 5.1.4*). Kommt es doch zu einem Vorfall, gilt es, dessen Auswirkungen so weit wie möglich zu reduzieren. Essenziell ist hier, dass *IT-Betrieb* (ggf. inkl. IT-Dienstleister) und Ansprechpersonen für das Notfall- und Krisenmanagement eng im Austausch stehen und Strukturen und Prozesse aufeinander abgestimmt sind (→ *Kapitel 5.2.1* und → *Kapitel 5.2.2*).

Die Bestandsaufnahme aller in der Kommunalverwaltung genutzten Fachverfahren ist eine wichtige Informationsgrundlage, um nach einem erfolgten Angriff zunächst in den Notbetrieb zu gehen, später auch das Wiederanlaufen der Systeme zu unterstützen. Eine solche Bestandsaufnahme unter Einbindung aller betroffenen Bereiche durchzuführen und diese ausführlich (auch offline!) zu dokumentieren gehört zu den wichtigsten Vorbereitungsmaßnahmen überhaupt, die eine Grundlage für einen vollständigen Wiederanlaufplan liefern (→ *Kapitel 5.2.3*). Das Bereithalten einer Notfallinfrastruktur, um auch im Ernstfall rudimentär arbeitsfähig zu bleiben und die weitere Bewältigung der Situation zu bewerkstelligen, rundet das Maßnahmenpaket ab (→ *Kapitel 5.2.4*). Ein IT-Vorfall, insbesondere wenn er mit längeren Ausfallzeiten einhergeht, bleibt nicht unbemerkt – zuerst merken die eigenen Mitarbeitenden, dass etwas nicht stimmt, nur kurze Zeit später werden all diejenigen, die auf die Leistungen der kommunalen Behörden zugreifen möchten, mit den Folgen konfrontiert. Gute Krisenkommunikation ist also vonnöten (→ *Kapitel 5.2.5*)! Regelmäßige Durchführung von Tests und Übungen hilft dabei, die Prozesse, Strukturen und technischen Vorkehrungen zu überprüfen und die Handlungssicherheit bei den beteiligten Mitarbeitenden zu erhöhen (→ *Kapitel 5.2.6*).

Eine wirksame Vorsorge für Cybergefahren und ein effizienter Umgang mit IT-Krisen wird von der öffentlichen Verwaltung erwartet – gerade vor dem Hintergrund der aktuellen sicherheitspolitischen Lage. Dieser Wegweiser erleichtert Ihnen die Auseinandersetzung mit der Thematik. Sollte Ihnen das Thema noch neu sein, nutzen Sie den Wegweiser als Einstieg. Wenn Sie schon weiter fortgeschritten sind, reflektieren Sie mithilfe des Wegweisers den erreichten Stand und schärfen Sie bei Bedarf noch einmal nach. Wichtig ist, dass Sie anfangen und dranbleiben.

Daher: Nehmen Sie sich direkt einen Baustein des Wegweisers vor und gehen Sie den wichtigen nächsten Schritt!

Einleitung

Warum dieser Wegweiser?

Kommunale Behörden bilden das Rückgrat der deutschen Verwaltung. Die Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)[1] benennt die kommunale Verwaltungsebene nicht nur als wichtigen Partner beim Schutz Kritischer Infrastrukturen, sie ist auch Teil des KRITIS-Sektors Staat und Verwaltung. Kommunale Behörden haben direkten Kontakt zu den Bürgerinnen und Bürgern, erheben und verarbeiten große Mengen sensibler Daten und binden diese in Geschäftsprozesse ein. Gemäß dem Recht der kommunalen Selbstverwaltung regeln sie alle Angelegenheiten der örtlichen Gemeinschaft im Rahmen der Gesetze in eigener Verantwortung. Sie erbringen darüber hinaus wichtige Verwaltungsdienstleistungen auch für andere staatliche Ebenen, sodass Einschränkungen zu Auswirkungen führen, die über die lokale Ebene hinausgehen. In ihrem Handeln sind sie stark von informationstechnischen Systemen abhängig – und gegenüber deren Ausfall entsprechend verwundbar. Immer wieder führen menschliches Versagen, unerwartete technische Fehler, Naturereignisse und insbesondere auch Cyberangriffe zu IT-Ausfällen – von begrenzten *IT-Störungen* bis hin zu monatelangem Stillstand in den betroffenen Verwaltungen. Cyberkriminelle überlasten bspw. gezielt kommunale Webseiten und andere netzbasierte Angebote, um Kommunen politisch unter Druck zu setzen.

[1] Siehe [BMI09] (→ *Anhang 2*).

Ebenso greifen sie Kommunen mit *Ransomware* an, um diese finanziell zu erpressen. Dabei stehlen die Angreifer häufig Daten und verschlüsseln die Systeme der Betroffenen.

In Anbetracht der vielfältigen Bedrohungen, die speziell auf ihre technischen Einrichtungen gerichtet sind, müssen Kommunen die eigene Handlungsfähigkeit sicherstellen. Rechtsvorschriften stellen aktuell bereits gewisse Anforderungen an die Informationssicherheit der kommunalen Verwaltungen. Werden personenbezogene Daten verarbeitet, fordert die europäische Datenschutz-Grundverordnung (DS-GVO)[2] „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten". Durch das Subsidiaritätsprinzip haben Kommunen auch Pflichten zur Absicherung ihrer Leistungen und zur Gewährleistung ihrer Verfügbarkeit. Zudem beinhalten die allgemeinen Haushaltsgrundsätze in der Regel eine Verpflichtung zur Sicherstellung einer stetigen Aufgabenerfüllung. Darüber hinaus empfiehlt der deutsche IT-Planungsrat die Umsetzung der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung"[3]. Auch länderspezifisch gibt es unterschiedliche Vorgaben, teils begleitet von entsprechenden Unterstützungsangeboten der Landesbehörden.

Fraglich ist nicht, ob Kommunen von Cyberkriminellen angegriffen werden.[4] Die Angriffe laufen tagtäglich, massenhaft und häufig automatisiert – sie treffen jeden. Viel zu häufig fallen Kommunen diesen Angriffen auch zum Opfer. Die Ursachen dafür sind vielfältig: Gerade im *IT-Betrieb* fehlt Fachpersonal, in anderen Bereichen wiederum sind technisches IT-Wissen und der Zugang zur Thematik häufig nicht hinreichend vorhanden. Begrenzte Haushaltsmittel, die große Fülle dringlicher Aufgaben oder ein mangelndes Bewusstsein für die abstrakten Cybergefahren erschweren eine gute Vorbereitung. Nicht selten fehlt es auch an einem Zugang und einem guten Einstiegspunkt zu diesem vielschichtigen Themenfeld. Hier setzt dieser Wegweiser an: Er soll durch einen starken Szenariobezug die Problemlage allgemein verständlicher machen und anschaulich vor Augen führen, um dabei zu helfen, einen Prozess zur Verbesserung der Informationssicherheit und der Vorbereitung auf schwere IT-Sicherheitsvorfälle in deutschen Kommunalverwaltungen anzustoßen.

Viele der im Wegweiser vorgestellten Schritte gehen zudem mit einem vergleichsweise geringen Ressourcenbedarf einher – sowohl in finanzieller Hinsicht als auch in Bezug auf notwendiges (IT-)Fachpersonal. Durch den durchgängigen Szenariobezug, aber auch durch die bereitgestellten Kernpunkte und Prüffragen, ermöglicht der Wegweiser einen Einstieg zur Verbesserung von Risiko- und Krisenmanagement sowie Informationssicherheit, für den kaum Vorkenntnisse benötigt werden. So können wichtige Schritte selbst bei Ressourcenknappheit unternommen werden.

Für wen ist dieser Wegweiser?

Dieser Wegweiser richtet sich zunächst an **diejenigen, die für das kommunale Krisenmanagement Verantwortung tragen**, insbesondere an die Hauptverwaltungsbeamtinnen und -beamten, also an (Ober-)Bürgermeisterinnen und (Ober-)Bürgermeister, Landrätinnen und Landräte sowie ggf. Ratsvorsitzende. Denn eines ist klar: Eine ausgewachsene *IT-Krise* bleibt nicht auf den *IT-Betrieb* beschränkt. Sie erfasst die gesamte Verwaltung, hat erhebliche Außenwirkung, verursacht sehr hohe Kosten, erzeugt einen enormen Koordinationsaufwand und erfordert eine zielgerichtete Abarbeitung. Vorbeugenden und vorbereitenden Maßnahmen muss „von oben" die notwendige Priorität einschließlich der entsprechenden Ressourcen eingeräumt werden, um den Eintritt von Krisenlagen möglichst zu vermeiden bzw. im Bedarfsfall den Schaden zu begrenzen und eine rasche Rückkehr in den geordneten Betrieb zu ermöglichen.

Es ist wichtig, sich ein Bild davon machen zu können, was eine *IT-Krise* für die eigene Kommune bedeuten kann. Die Darstellung von Ablauf und Auswirkungen eines Cyberangriffs anhand

[2] Siehe [EU16] (→ *Anhang 2*).

[3] Siehe [ITP18] (→ *Anhang 2*).

[4] Siehe [Lange24] (→ *Anhang 2*).

des Beispielszenarios macht das abstrakte Thema greifbar.

Für die **Mitarbeitenden der Verwaltung**, insbesondere in den Bereichen ***IT-Betrieb*** sowie **Notfall- bzw. behördliches Krisenmanagement**, fasst der Wegweiser die wichtigsten Aspekte zur Prävention und Krisenreaktion zusammen, unterstützt damit bei den ersten konkreten Schritten und gibt Hinweise darauf, wie es von hier aus praktisch weitergehen kann. Auch Mitarbeitende in der **Öffentlichkeitsarbeit** oder mit **Kontakt zu Bürgerinnen und Bürgern** können von den Ausführungen zur Krisenkommunikation profitieren.

Die zahlreichen Verweise auf weiterführende Publikationen und Standards erlauben allen Nutzenden eine tiefergehende Auseinandersetzung mit der Thematik.

Wie kann mit diesem Wegweiser gearbeitet werden?

Der Wegweiser soll im ersten Schritt auf das Gefahrenpotenzial und die Tragweite von Cyberangriffen auf Kommunalverwaltungen aufmerksam machen und an alle oben genannten Akteure appellieren, tätig zu werden: Auch wenn ein vollumfänglicher Schutz von IT-Systemen nicht erreichbar ist, kann durch ein gutes *Risikomanagement* ein angemessenes Schutzniveau erreicht werden. Ein gutes *Krisenmanagement* kann im Bedarfsfall Schlimmeres verhindern helfen. In der Regel gilt: **Prävention ist besser, schneller und günstiger als Reaktion!**

Ist die Entscheidung getroffen und die Ressourcenfrage geklärt, kann der Wegweiser bei Einführung oder Weiterführung eines *Risikomanagement*- und Informationssicherheitsprozesses in Kommunen eingesetzt werden. Es handelt sich um ein **niedrigschwelliges Angebot**, das auch ohne spezifische IT-Fachexpertise genutzt werden kann. Der Wegweiser beschreibt erste konkrete und essenzielle Schritte zur Verbesserung von Prävention und Bewältigungskapazitäten. Es ist jedoch notwendig, sich anschließend mit weiterführenden Informationsangeboten auseinanderzusetzen. Die zahlreichen, im Wegweiser enthaltenen Verweise auf Fachpublikationen, Standards und Modelle rund um Informationssicherheit und Krisenmanagement helfen dabei, gezielt vorzugehen.

Der Wegweiser ist nicht dafür konzipiert, von vorne nach hinten durchgearbeitet zu werden. Er stellt eine Umsetzungshilfe dar, die **modular** verwendet werden kann: Die Unterteilung in verschiedene Themenfelder erleichtert den Überblick und den Einstieg in die Thematik. Die Teilbereiche, die aus der eigenen Perspektive am dringlichsten erscheinen oder die zu anderen gerade anstehenden Arbeitspaketen am besten passen, können zuerst angegangen werden. Sofern z. B. ein Kommunikationshandbuch er- oder überarbeitet wird, bietet sich der Einstieg mit → *Kapitel 5.2.5* („Kommunikation während Vorfällen“) an, sodass die spezifischeren Bedarfe für den Fall von Cyberangriffen gleich integriert werden können. Ein umfassendes → *Glossar* und → *Abkürzungsverzeichnis* unterstützen beim Verständnis der verwendeten Begrifflichkeiten auch ohne vorheriges Studium aller anderen Kapitel. Alle im Glossar näher erläuterten Bezeichnungen wurden zur erleichterten Handhabung im Text kursiv kenntlich gemacht.

Der Wegweiser zielt darauf ab, möglichst für alle Kommunen Hilfestellungen zu bieten. Dies bedeutet gleichzeitig, dass nicht alle individuellen Rahmenbedingungen vollständig berücksichtigt werden können. Daher kann der Wegweiser keine vollständige Schritt-für-Schritt-Anleitung aller notwendigen Vorbereitungen sein. Für die maßgeschneiderte Vorbereitung auf einen Cyberangriff und die Erhöhung des Sicherheitsniveaus sowie für die akute Vorfallbewältigung vor Ort müssen die jeweiligen lokalen organisatorischen und technischen Gegebenheiten berücksichtigt werden. Dafür ist eine individuelle Auseinandersetzung mit den möglichen Abhängigkeiten von informationstechnischen Systemen, bereits existierenden Vorbereitungen sowie zur Verfügung stehenden Umsetzungsmöglichkeiten und Unterstützungsangeboten erforderlich.

Dieser Wegweiser konzentriert sich zudem ganz bewusst auf die Kommunalverwaltung selbst. Daher werden andere Aufgaben, bspw. die spezifische Rolle von Kommunen als Betreiber von *Kritischen Infrastrukturen* in anderen Sektoren als

Staat und Verwaltung (etwa Strom, Wasser, Gas), nicht näher betrachtet. Hierfür wird stattdessen auf andere, sektorale Handreichungen verwiesen, die spezifischer auf die relevanten Anforderungen eingehen. Zudem gelten ggf. die erhöhten rechtlichen Anforderungen der BSI-Kritisverordnung, für deren Einhaltung spezielle Informationen für KRITIS-Betreiber zur Verfügung gestellt werden.[5] Dennoch gilt: Das kommunale Krisenmanagement ist selbstverständlich auch beim Ausfall anderer Infrastrukturen gefragt (→ *Anhang 4.6*).

Wie ist der Wegweiser aufgebaut?

Ein fiktives Szenario, inspiriert von realen Cyberangriffen, illustriert in → *Kapitel 2.1* anschaulich den Ablauf von einer *IT-Störung* über den *IT-Notfall* bis hin zur *IT-Krise*. Die aktuelle Hauptbedrohung durch *Ransomware* wird im darauffolgenden Abschnitt genauer erläutert. Anschließend folgt eine Übersicht über kriminelle Gruppierungen im Cyberraum und ihre jeweiligen Motive.

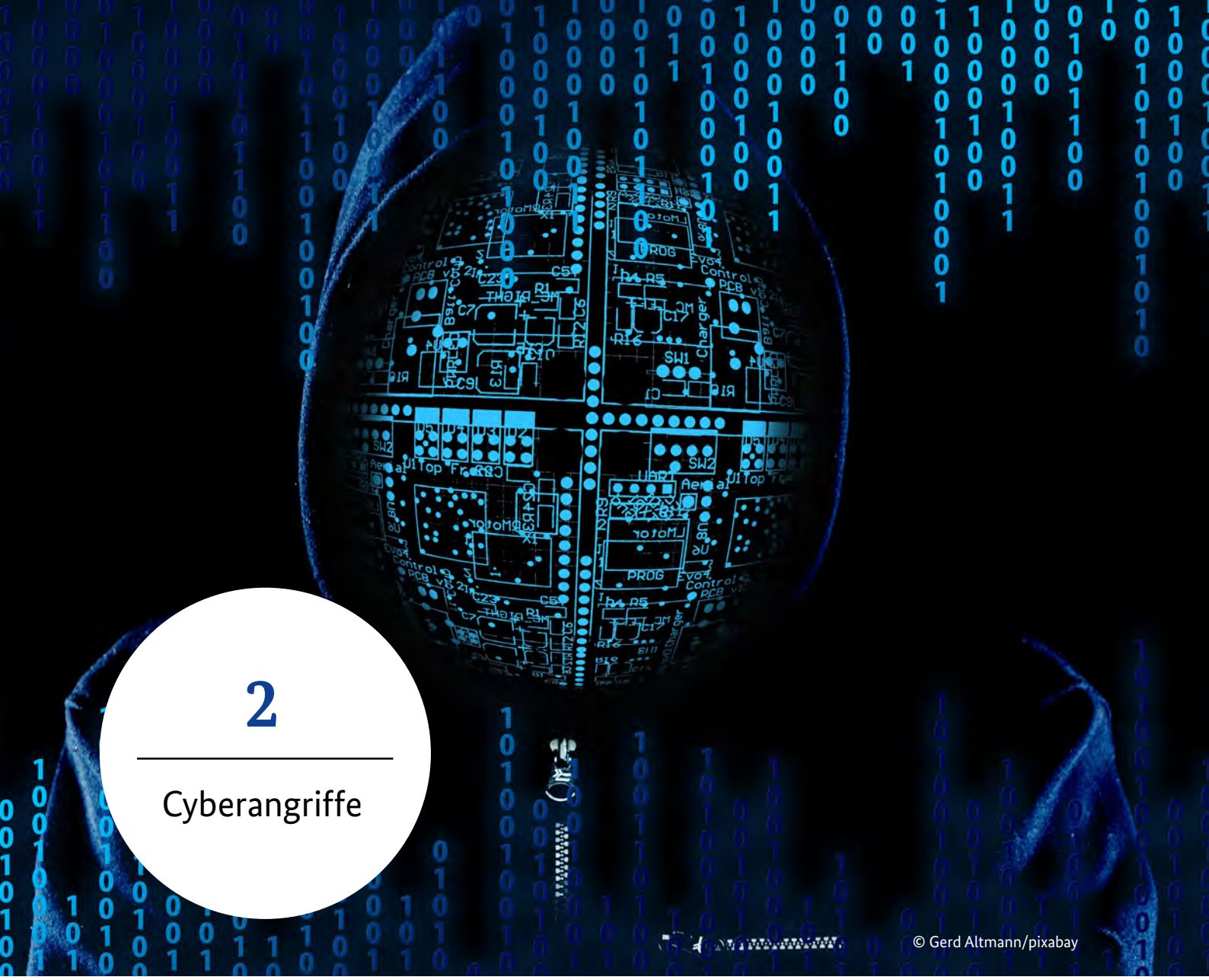
→ *Kapitel 3* schließt unmittelbar an das geschilderte Szenario an, gibt stichpunktartig Best-Practice-Hinweise, weist auf Fragestellungen und Aspekte für die konkrete Bewältigung eines bereits eingetretenen IT-Vorfalls hin und zeigt externe Unterstützungsmöglichkeiten auf.

Daran anschließend beschreibt → *Kapitel 4* die Phase der Nachbereitung des Vorfalls. Insbesondere die Wiederherstellung der Systeme nach einem Cyberangriff steht im Mittelpunkt.

→ *Kapitel 5* stellt das zentrale Kapitel dieses Wegweisers dar. Hier werden vorbereitende Maßnahmen zur Prävention und Detektion sowie zur besseren Bewältigung erläutert. Neben Empfehlungen zur Stärkung der Informationssicherheit werden auch interne organisatorische Planungen und externe Unterstützungsmöglichkeiten vorgestellt, bevor → *Kapitel 6* den Wegweiser mit einigen Schlussbemerkungen resümiert.

Die darauffolgenden Anhänge liefern neben Glossar und externen Quellenverweisen auch Hinweise zu übergreifender weiterführender Literatur (→ *Anhang 3*). Diese sollte zurate gezogen werden, wenn die Erstmaßnahmen dieses Wegweisers bereits umgesetzt sind. Zudem werden weitere Szenarien und verwandte Themen skizziert, die bezüglich der Prävention oder Vorbereitung Berührungspunkte mit IT-Vorfällen aufweisen (→ *Anhang 4*).

[5] Siehe auch: https://www.bsi.bund.de/dok/12218780.



© Gerd Altmann/pixabay

2

Cyberangriffe

Cyberangriffe auf Kommunen

Wie kann man sich den Ablauf eines Cyberangriffs vorstellen? Welche Akteure haben es auf öffentliche Verwaltungen abgesehen? Im folgenden Kapitel wird ein *Ransomware*-Angriff auf eine fiktive Kommunalverwaltung in Deutschland nacherzählt.[6] Während sich IT-Sicherheitsvorfälle natürlich individuell unterscheiden, lassen sich bestimmte Muster aus der Analyse vergangener Angriffe ableiten. Diese werden hier bewusst sehr deutlich dargestellt, um daran anknüpfend Hilfestellungen für die Vorsorge und das Handeln in der Lage hervorzuheben.

[6] Für eine plastische Beschreibung des Themas können darüber hinaus verschiedene Podcasts sowie Hintergrund-Recherchberichte von Onlinemedien zu vergangenen Vorfällen bei Kommunalverwaltungen dienen.

2.1 Ransomware in Rodenburg

Für die plastische und lesbare Schilderung der Abläufe mussten Festlegungen bezüglich der konkreten Art der betroffenen Kommunalverwaltung getroffen werden. Das im Folgenden beschriebene Szenario bezieht sich daher auf eine fiktive Stadt. Die Prozesse können jedoch analog auf kommunale Gebietskörperschaften sowie Gemeinden übertragen werden.

Neben den jeweiligen Abschnitten des fortschreitenden Cyberangriffs finden sich jeweils erste Verweise, wo im vorliegenden Wegweiser Hinweise darauf zu finden sind, wie der Verlauf hätte abgemildert oder sogar teilweise verhindert werden können.

Phase 1: Infektion

Es ist Mittwoch, der 26. April, als Norbert Schmidt, Bürosachbearbeiter für Personalangelegenheiten der Kleinstadt Rodenburg, aus der Mittagspause zurück an seinem Schreibtisch Platz nimmt. Als er den PC mit seinem Passwort entsperrt, sieht er, dass während seiner Abwesenheit eine neue E-Mail eingegangen ist. „Initiativbewerbung für die Buchhaltung", schreibt ein Maximilian Schuster in dieser Nachricht, die Herrn Schmidt von seiner Kollegin über die Sammeladresse info@stadt-rodenburg.de weitergeleitet wurde. „Sehr geehrte Damen und Herren, bitte entnehmen Sie meine Bewerbung dem angehängten Dokument. Danke und freundliche Grüße!", liest Herr Schmidt in der Vorschau seines Mailprogramms und öffnet die angehängte Datei per Doppelklick.

Blitzschnell geht ein neues Fenster auf. Seitdem die IT auch seinen Arbeitsplatz aufgerüstet hat, laufen die Anwendungen richtig flüssig, freut sich Herr Schmidt. Auf seinem Bildschirm erscheint ein Hinweis dort, wo eigentlich der Inhalt stehen sollte: „Dieses Dokument wurde mit einer älteren Programmversion erstellt, bitte klicken Sie auf Bearbeitung aktivieren, um den Kompatibilitätsmodus zu starten." Es gibt wohl noch ein paar Schwierigkeiten mit dem neuen Update, denkt er sich und klickt die gelben Banner weg. Endlich kommt der Lebenslauf von Maximilian Schuster zum Vorschein. Auch wenn gerade keine Stelle in der Stadtkämmerei ausgeschrieben ist, scheint ihm Herr Schuster ein passabler Kandidat. Die Bewerbung legt er in der zentralen Dateiablage für später ab.

Das angehängte Word-Dokument in der E-Mail enthielt *Makros*, also eingebetteten Programmcode, der nach dem Klick auf die Schaltfläche „Inhalte aktivieren" ausgeführt wurde und im Hintergrund Schadsoftware aus dem Internet nachlud. Durch die Weiterleitung der E-Mail von seiner Kollegin und den plausiblen Hinweis auf technische Inkompatibilitäten war es für ihn auf den ersten Blick nicht ersichtlich, dass es sich hierbei um einen Angriffsversuch handelte. Da sich eine Informationssicherheitsrichtlinie erst noch in Arbeit befand, waren präventive Maßnahmen, wie die Kennzeichnung externer E-Mails oder das systemweite Deaktivieren von *Makros*, nicht umgesetzt. Die bösartige E-Mail wurde von den Cyberkriminellen tausendfach verschickt, es handelt sich hierbei in den seltensten Fällen um einen gezielten Angriff auf eine bestimmte Kommune.

Zur Sensibilisierung siehe → Kapitel 5.1.5

Siehe → Kapitel 5.1

Phase 2: Erkundung, Rechteerweiterung und Ausbreitung

„Der schmeißt mich ständig aus der Verbindung raus“, beschwert sich Herr Schmidt am folgenden Dienstag am Telefon bei Frau Christina Seiler, Anwendungsbetreuerin aus dem IT Bereich, und fügt gleich darauf an: „So kann ich im Homeoffice un möglich arbeiten.“ Frau Seiler ist diese aufbrausenden Support Anrufe gewöhnt und kennt die Problematik aus den Hochzeiten der Covid 19 Pandemie nur zu gut. Mit ruhiger Stimme entgegnet sie routiniert, dass der VPN Server immer nur eine Verbindung pro Nutzer gleichzeitig zulasse und Herr Schmidt doch bitte sein Gerät neu starten solle. Mit dem Neustart des Rechners scheint das Problem vorerst beho ben, denn den Rest der Woche meldet sich Herr Schmidt nicht mehr.

Durch die versteckt heruntergeladene Schadsoftware haben die Angreifer einen initialen Zugriff auf Herrn Schmidts PC Arbeitsplatz im Rathaus. Sie versuchen nun das Netzwerk auszukundschaften, um herauszufinden, ob es sich hierbei um ein lohnendes Ziel handelt, und um ihre Zugriffsrechte auf das Sys tem zu erweitern. Leider verfügten die IT Systeme der Kommune nicht über technische Mittel, um diese verdächtigen Aktivitäten frühzeitig zu detektieren.

Siehe → Kapitel 5.1.4

Phase 3: Datenabfluss und Verschlüsselung

Das Diensthandy klingelt IT Leiter Thomas Jäger am Sonntag früh um 5.30 Uhr aus dem Bett. Eigentlich hatte er sich auf ein langes Wochenende gefreut, doch jetzt erklärt ihm ein aufgeregter Mitarbeiter der Frühschicht des Fachbereichs Öffent liche Sicherheit und Ordnung, dass alle fünf Computer und sämtliche Telefone in der kommunalen Außenstelle ausgefallen seien. Als er sich mit Kaffee und Laptop bewaffnet einen Überblick über die Systeme verschafft, ahnt er bereits Böses. Sämt liche Dateien sind verschlüsselt, Intranet und Telefonserver nicht erreichbar.

Jetzt heißt es Schadensbegrenzung: Auf dem Weg zum Rathaus informiert er Bürgermeisterin Manuela Wirth sowie seine IT Mitarbeitenden und schaltet, dort angekommen, gegen 6.00 Uhr erst einmal alle Server ab oder trennt sie vom Netz werk. Bei seiner schnellen Erstüberprüfung ist er auf folgende Nachricht gestoßen, die die Cyberkriminellen hinterlassen haben:

„Alle Ihre Dateien wurden von der CyberVolk Ransomware verschlüsselt. Bitte ver suchen Sie nie, Ihre Dateien ohne den Schlüssel wieder zu erlangen, den ich Ihnen nach einer Zahlung gebe. Ihre Dateien könnten ganz verschwinden. [...] Zahlen Sie 1000 Bitcoin auf die untenstehende Adresse“, muss er dort lesen (siehe Abbildung 1).

Siehe → Kapitel 5.2.2

Abbildung 1: Ransomnote der Gruppierung CyberVolk
(Quelle: Aufnahme des BSI vom Bildschirm eines Betroffenen)

Sämtliche Arbeitsplätze und Fachanwendungen der Kommune stehen nicht mehr zur Verfügung. Lediglich die städtische Website, die bei einem externen Anbieter betrieben wird, ist noch online. Als Bürgermeisterin Wirth im Rathaus eintrifft und sich von Herrn Jäger unterrichten lässt, ist ihr klar, dass dies spätestens am morgigen Montag bei Dienstbeginn für großes Chaos bei allen Mitarbeitenden und vor allem in den Organisationseinheiten mit Bürgerkontakten sorgen wird. Sie ruft den Krisenstab zusammen, während Herr Jäger die Landesbehörden informiert – sofern an diesem Sonntag jemand ans Telefon geht.

Ohne Systeme zur Detektion werden *Ransomware*-Angriffe erst dann festgestellt, wenn es bereits zu spät ist. Innerhalb weniger Stunden verschlüsseln Cyberkriminelle das gesamte Netzwerk und machen es damit unbrauchbar. Was Herr Jäger noch nicht weiß, ist, dass die Angreifer einen Großteil der Dateien zuvor auch noch exfiltriert, also gestohlen und auf ihre Server kopiert haben. Durch die Verschlüsselung hat er die Kontrolle über seine IT-Systeme verloren und kann als Akutmaßnahme lediglich sämtliche Server abschalten und in den Krisenmodus übergehen. Die Erpressergruppierung verlangt ein Lösegeld zur Freigabe der IT-Systeme und droht mit einer Veröffentlichung von sensiblen Daten, falls keine Zahlung erfolgen sollte. Es folgen nun stressige und chaotische Arbeitstage.

Phase 4: Eskalation in den Krisenmodus

Ohne Zugriff auf die Kontaktdaten in den digitalen Personalakten konnte der Krisenstab gestern lediglich manche Führungskräfte der wichtigsten Funktionsbereiche über den IT-Ausfall in Kenntnis setzen. Zum Dienstbeginn am Montag um 7.30 Uhr warten nun bereits einige Bürgerinnen und Bürger mit dringenden Anliegen auf ihren Termin. Auch die Mitarbeitenden erfahren erst durch einen handschriftlichen Aushang vor Ort von der Problematik. Um 9.30 Uhr macht die Nachricht von einer technischen Störung der Verwaltung öffentlich die Runde: „Wurde unsere Stadt Rodenburg gehackt?" Auch die Lokalzeitung wird darauf aufmerksam und hält die Gerüchte für bestätigt, nachdem sowohl die Telefonnummer als auch die E-Mail-Adresse der Pressestelle nicht erreichbar sind. Daraufhin lässt Frau Wirth auf der städtischen Website einen Hinweis einstellen: „Technische Probleme, das Bürgerbüro bleibt heute geschlossen." Der IT-Bereich hatte den ganzen Sonntag durchgearbeitet und konnte einen ersten Zwischenstand ermitteln: Fast alle wichtigen Systeme und Daten sind verschlüsselt und auch die Backups sind unbrauchbar. Eine kurzfristige Wiederherstellung ist wohl ausgeschlossen.

In der Folge kommt es zu Fragen und Schwierigkeiten in allen Bereichen der Kommunalverwaltung: Bürgergeldauszahlungen gestalten sich schwierig, ebenso wie Kfz-Zulassungen. Sterbeurkunden können nicht mehr ausgestellt und somit keine Bestattungen durchgeführt werden. Der Aufenthaltsstatus festgenommener Personen kann nicht direkt überprüft werden. Es müssten Zwangsmaßnahmen durchgeführt werden, um gewisse Schornsteine zu kehren. Aber wo? Und wer trägt die Verantwortung, wenn es dort zwischenzeitlich zu einem Brandereignis kommt? In der Bücherei ist unklar, welche Bücher sich derzeit wo befinden. Die Auswirkungen sind einfach überall zu spüren.

Siehe → Kapitel 5.2.1

Siehe → Kapitel 5.2.5

Siehe → Kapitel 3.1

Ohne existierenden Notfallplan muss nun unter Hochdruck und quasi ohne Informationen mit der Wiederherstellung zumindest der wichtigsten Dienstleistungen begonnen werden. Der Ausfall der IT-Systeme macht dabei nicht nur die eigentliche Arbeit der Mitarbeitenden unmöglich, sondern erschwert auch die Arbeit des *Krisenstabs*, da kein Zugriff auf bspw. Personallisten erfolgen kann und noch immer die Telefone nicht funktionieren. Glücklicherweise gelingt die Kommunikation der Führungsebene über dienstliche Handys und private Kanäle. Der Stab beginnt die Prozesse und Fachverfahren der Kommune zu priorisieren, um einen Notbetrieb der wichtigsten Dienstleistungen sicherzustellen. Ohne Vorlagen ist die Kommunikation mit den Einwohnern und der Presse währenddessen ziemlich chaotisch angelaufen. Nach dem erschütternden Zwischenbericht des IT-Bereichs liegt alle Hoffnung darauf, dass die Magnetbandsicherungen im Keller verschont geblieben sind. Aber auch deren Sichtung und Forensik sowie die darauf basierende Wiederherstellung werden Monate in Anspruch nehmen.

Siehe → Kapitel 5.2.4

Siehe → Kapitel 5.2.3

Siehe → Kapitel 5.2.5

Siehe → Kapitel 3 und *→ Kapitel 4*

2.2 Ransomware: Biete Daten gegen Lösegeld

Kernpunkte:

- Angreifer setzen *Ransomware* ein, um Daten zu verschlüsseln und Lösegeld zu fordern.
- Bei einer *Double Extortion* (doppelten Erpressung) werden zusätzlich sensible Daten gestohlen, um mit Veröffentlichung zu drohen.
- Bei einer *Triple Extortion* werden im nächsten Schritt zusätzliche Maßnahmen angedroht, um den Zahlungsdruck weiter zu erhöhen.
- Generell verläuft ein Angriff in drei Phasen: Infektion (Eindringen in das System); Erkundung, Rechteerweiterung und Ausbreitung im Netzwerk; Verschlüsselung.

Im beschriebenen Beispielszenario wird die Kommunalverwaltung mit sogenannter *Ransomware* angegriffen. Cyberangriffe mit dieser Art von Schadsoftware ziehen meist die langwierigsten Auswirkungen nach sich, da nicht selten alle Geschäftsprozesse zum Erliegen kommen. In den zurückliegenden Jahren hat der Einsatz von *Ransomware* bei Cyberangriffen rapide zugenommen. Im Jahre 2019 wurden die Schäden in Deutschland noch auf etwa 5,3 Mrd. Euro geschätzt. Zwei Jahre später, im Jahr 2021, wurden Schäden von ca. 24,3 Mrd. Euro durch *Ransomware* bekannt.[7] Alleine 2023 wurden über 800 Angriffe auf Unternehmen und Institutionen zur Anzeige gebracht. Die Dunkelziffer ist jedoch sehr hoch.[8] *Ransomware*-Angriffe sind derzeit die größte Cyberbedrohung für kommunale Verwaltungen.

Wird *Ransomware* eingesetzt, handeln die Angreifer oft aus finanzieller Motivation. Die Täter haben die Absicht, dass ihre Opfer den Angriff deutlich bemerken und dadurch in der Arbeit eingeschränkt werden. Insgesamt muss man jedoch verschiedene Akteure im Cyberraum unterscheiden. So gehören bspw. ausländische Nachrichtendienste zu potenziellen Angreifern, die anders motiviert sind und anders vorgehen: Sie zielen eher darauf ab, möglichst lange und unentdeckt Informationen auszuspionieren (→ *Kapitel 2.3*).

Was ist *Ransomware*?

Der Begriff *Ransomware* setzt sich aus den englischen Worten Ransom, zu Deutsch Lösegeld, und Software zusammen. Es handelt sich also um Schadsoftware, mit der Lösegeld erpresst werden soll. Angreifer verschlüsseln damit möglichst viele Dateien und Systeme des Opfers, wodurch der Zugriff hierauf unmöglich wird. Für die Entschlüsselung wird vom Opfer ein Geldbetrag in digitaler Kryptowährung gefordert. Die Täter behaupten, nach Zahlung des Lösegelds einen Schlüssel zu liefern. Mit diesem soll es möglich sein, die verschlüsselten Daten wieder lesbar zu machen. Es gibt aber keinerlei Garantie, dass die Täter ihr Versprechen halten, und es ist völlig unklar, ob durch eine Lösegeldzahlung die verschlüsselten Daten wieder verfügbar gemacht werden können. Auf jeden Fall wird durch die Lösegeldzahlung eine kriminelle Organisation und damit weitere Angriffe finanziert. Unter anderem deshalb wird von einer Lösegeldzahlung dringend abgeraten.

Sicher ist: Die Bewältigung eines *Ransomware*-Angriffs dauert lange, selbst wenn ein eventuell sogar funktionierender Schlüssel vorhanden ist. IT-Sicherheitsexperten müssen das Einfallstor für die Angreifer entdecken und schließen. Forensiker müssen prüfen, ob die Schadsoftware tatsächlich vollständig entfernt ist und die Angreifer eine Hintertür hinterlassen haben.

[7] Siehe [BKA22b] (→ *Anhang 2*).

[8] Siehe [BKA23] (→ *Anhang 2*).

Andernfalls können die Opfer später erneut angegriffen werden. Erfolgreich angegriffene Systeme sind deshalb in der Regel komplett neu aufzubauen. Üblicherweise dauert es mehrere Monate, bis sämtliche Geschäftsprozesse wieder normal ablaufen.

Zudem werden die Daten regelmäßig nicht nur verschlüsselt, sondern zuvor auch gestohlen. Durch die Drohung, die entwendeten Daten zu veröffentlichen oder zu verkaufen, wird zusätzlicher Druck auf das Opfer ausgeübt. Daher nennt man dieses Vorgehen *Double Extortion*, zu Deutsch „Doppelte Erpressung". Diese Herangehensweise kann derzeit bei fast jedem *Ransomware*-Angriff beobachtet werden. Aufgrund dessen kommt es im Nachgang von *Ransomware*-Angriffen häufig zur Veröffentlichung gestohlener Dateien, darunter auch sensibler Informationen und personenbezogener Daten. Bei einer *Triple Extortion* werden in einem nächsten Schritt zusätzliche Maßnahmen angedroht, um den Zahlungsdruck weiter zu erhöhen. Dies können etwa Angriffe gegen die Verfügbarkeit von Systemen des Opfers sein (*(D)DoS-Angriffe*). In anderen Fällen wird im Zuge dieser Dreifacherpressung manchmal versucht, Kunden der Opfer zu erpressen. Da diese ebenfalls kein Interesse an einer Veröffentlichung der sie betreffenden abgeflossenen Daten haben, sollen nun auch sie zur Kasse gebeten werden.

Wie läuft ein typischer Angriff ab?

Ein *Ransomware*-Angriff läuft in mehreren Phasen ab. Vereinfacht lassen sich drei Phasen unterscheiden: Die erste Phase ist die **Infektion**, also das Eindringen in das Netzwerk, die zweite Phase ist die Erkundung, Rechteerweiterung und **Ausbreitung** im Netzwerk und die dritte Phase ist die **Verschlüsselung** aller Systeme.

Zunächst muss ein Angreifer in das Zielsystem eindringen, denn nur dann können Daten entwendet und verschlüsselt werden. Nach erfolgreichem Eindringen bezeichnet man das System als kompromittiert. Damit unterscheidet sich ein *Ransomware*-Angriff von anderen Angriffsarten, wie etwa einem *Denial of Service*-Angriff (DoS). Bei Letzterem ist es nicht notwendig, in das Zielsystem einzudringen, nur der Zugriff von außen, z. B. durch Bürgerinnen und Bürger, soll gestört werden.

Es gibt verschiedene Wege, in ein Zielsystem einzudringen. Die wichtigsten beiden Arten sind Softwareschwachstellen und *Phishing*.

Im beschriebenen Szenario wird eine *Phishing*-Methode eingesetzt: Den Mitarbeitenden werden Nachrichten geschickt, um diese zu einer Handlung zu bewegen. Unwissentlich hilft diese Handlung dann dem Angreifer, in das System einzudringen. Dies kann darüber erfolgen, dass Mitarbeitende dazu gebracht werden, ihre Zugangsdaten auf einer imitierten Login-Seite einzugeben, die dem Angreifer gehört. Zum Erlangen von Login-Daten werden neben E-Mails auch SMS- oder Messenger-Nachrichten sowie Telefonanrufe genutzt. Klassisches Beispiel ist aber auch eine E-Mail mit der Aufforderung, einen Link anzuklicken. Durch Anklicken dieses Links wird dann eine Schadsoftware installiert.[9]
Diese ermöglicht dem Angreifer Zugang zum System. Anhänge mit versteckter Schadsoftware, die durch Öffnen des Anhangs ausgeführt wird, sind ein weiteres Beispiel. *Phishing*-Nachrichten sind teilweise sehr schwer von legitimen Nachrichten zu unterscheiden. So kann eine *Phishing*-Nachricht etwa als Antwort in einem legitimen Mail-Austausch getarnt sein.[10] Bei solch gezieltem und auf ein Opfer zugeschnittenem *Phishing* spricht man von *Spear-Phishing*.

Softwareschwachstellen eröffnen einen anderen Weg in die Systeme. Um eine Schwachstelle ausnutzen zu können, muss ein Angreifer diese zunächst kennen. Zuvor unbekannte Schwachstellen, sogenannte *Zero-Day-Schwachstellen*, zu finden ist sehr aufwendig und nur sehr fähige und gut ausgestattete Akteure suchen nach solchen Lücken. Daher versuchen die meisten

[9] Durch Schulungen können die Mitarbeitenden für solche *Phishing*-Versuche sensibilisiert werden (→ *Kapitel 5.1.5*). Dies ist jedoch keinesfalls als alleinige Abwehrmaßnahme geeignet!

[10] Die Schadsoftware Emotet liest bspw. bei Betroffenen Teile der E-Mail-Korrespondenz und Kontaktbeziehungen aus. Dann verbreitet sie sich weiter, indem vermeintliche Antworten auf aufgefundene E-Mails an die jeweiligen Kommunikationspartner gesendet werden. Dies erschwert das Erkennen.

Angreifer bereits bekannte Schwachstellen auszunutzen. Für öffentlich bekannte Schwachstellen gibt es vom Hersteller meist Updates oder *Patches*, welche die Lücken der Software schließen. Teilweise werden auch Methoden genannt, um die Schwachstellenausnutzung bis zur Veröffentlichung eines Updates zu verhindern, sogenannte Workarounds. Werden jedoch *Patches* und Workarounds nicht zeitnah umgesetzt, ist ein System generell verwundbar. Es gibt weltweit unzählige Systeme, welche für verschiedene Schwachstellen anfällig sind.[11] Daher lohnt es sich für Angreifer, automatisiert nach Systemen mit bekannten Schwachstellen zu suchen.

Für *Phishing* und das Ausnutzen von Schwachstellen gilt, dass Angreifer opportunistisch vorgehen. Dies bedeutet, dass sie ihre Ziele danach auswählen, wie leicht diese angegriffen werden können. Meist passiert dies auch weitgehend automatisiert, bspw. durch das massenhafte Versenden von *Phishing*-E-Mails oder das automatische Absuchen des Internets nach verwundbaren Servern. Dadurch ist die Gefahr, dass ein schlecht gesichertes System (ohne aktuelle Updates) kompromittiert wird, sehr hoch.

An dieser Stelle kurz zu den Folgen einer Kompromittierung: Ist ein Angreifer in ein System eingedrungen und dies wird erkannt, muss das System überprüft und oft komplett neu aufgebaut werden. Dann werden die Systeme als Erstmaßnahme zumeist abgeschaltet oder zumindest vom Netz getrennt. Dies soll verhindern, dass der Angreifer weiteren Schaden anrichten kann. Jedoch ist ein System durch Abschaltung oder Trennung vom Netz auch für seine eigentlichen Anwender nicht mehr benutzbar. Die Maßnahmen sind also rigoros und die Folgen unterscheiden sich zunächst kaum von den Folgen einer tatsächlichen Datenverschlüsselung – die Systeme stehen erst einmal nicht zur Verfügung. Allerdings ist die Dauer des Ausfalls meist kürzer. Insofern kann man durch das rechtzeitige Erkennen einer Kompromittierung den Schaden zumindest begrenzen. Hierbei sollte beachtet werden, dass das Abschalten des Systems ggf. Spuren vernichtet, was die forensische Untersuchung erschweren kann. Daher ist es prinzipiell sinnvoller, das System zu isolieren.

Nachdem ein Angreifer erfolgreich in ein System eingedrungen ist, beginnt die **zweite Phase** des Angriffs. Zunächst sichern sich Angreifer dauerhaft den Zugang zum System. So verschaffen sie sich etwa Rechte, über die sie weitere Programme installieren oder Daten exfiltrieren können. Im nächsten Schritt versuchen die Angreifer sich im System auszubreiten, ihr Ziel ist der Zugang zu allen Teilen des Netzwerks. Dabei suchen sie nach Ablageorten sensibler Informationen und Speicherorten von Backups. Zudem sind auch andere Informationen interessant, etwa über die Zahlungsfähigkeit des Opfers. Die Ausbreitung dient im Wesentlichen zwei Zielen. Zum einen wollen die Angreifer sichergehen, die wichtigsten Systeme im Netzwerk zu verschlüsseln. Zum anderen wollen sie möglichst viele sensible Daten entwenden. Auch hier gilt: Je mehr Daten betroffen sind, desto höher der Druck auf das Opfer.

Die **dritte Phase** des Angriffs ist die Verschlüsselung des Systems. Der Zeitraum zwischen der ersten Kompromittierung und dem Beginn der Verschlüsselung kann mehrere Monate betragen. Üblich sind mehrere Tage bis zu wenigen Wochen. Die Verschlüsselung selbst dauert in der Regel mehrere Stunden. Viele Angriffe werden erst mit der Verschlüsselung erkannt. Wird der Angriff in einer frühen Phase oder die Verschlüsselung zu Beginn bemerkt, kann der Schaden oft noch durch Sofortmaßnahmen begrenzt werden (→ *Kapitel 3.1*). Bei einer aktiv laufenden Verschlüsselung ist das Abschalten aller Systeme meist die sinnvollste Option. Dadurch wird die Verschlüsselung zunächst unterbrochen und die unverschlüsselten Daten können gesichert werden. Um unbemerkt zu bleiben, lösen Angreifer die Verschlüsselung meist außerhalb regulärer Arbeitszeiten aus. Spät nachts oder an Wochenenden und Feiertagen sind daher bevorzugte Zeiträume.

[11] Durch eine systematisierte Vorgehensweise bspw. im Rahmen eines ISMS kann die Angriffsfläche an dieser Stelle verringert werden (→ *Kapitel 5.1.1*). Durch die (zum Teil historisch gewachsene und unüberschaubare) Vernetzung der Systeme untereinander können nämlich Schwachstellen in unbeachteten, kleinen Systemen Auswirkungen auf das gesamte Netzwerk haben.

Nach Abschluss der Verschlüsselung sind die betroffenen IT-Systeme nicht mehr benutzbar. In der Regel wird auf den Systemen ein Erpresserschreiben hinterlassen (→ *Abbildung 1*). Im Erpresserschreiben finden sich Informationen, wie man mit den Angreifern in Kontakt treten soll. Manche enthalten bereits detaillierte Anweisungen samt Lösegeldsumme. Auf die Lösegeldforderungen sollte nicht eingegangen werden. Generell wird geraten, keinen eigenständigen Kontakt mit den Kriminellen aufzunehmen, sondern die Kommunikation der Polizei oder dem hinzugezogenen IT-Dienstleister zu überlassen.

Kein Lösegeld zahlen!

- Lösegeld finanziert das Geschäftsmodell der Cyberkriminellen. Jedes zahlende Opfer macht Ransomware-Angriffe zu einem lohnenden Unterfangen.
- Lösegeldzahlungen motivieren die tatsächlichen Angreifer und weitere potenzielle Akteure zur Fortsetzung und Weiterentwicklung der Angriffe.
- Es gibt keine Garantie, dass Kriminelle nach einer Zahlung tatsächlich einen funktionierenden Schlüssel liefern.
- Selbst wenn ein Schlüssel funktioniert, muss das System vollständig bereinigt werden.
- Es gibt keine Garantie, dass nicht weitere Forderungen erhoben werden.
- Oftmals sind schon Daten gestohlen: Es besteht das Risiko, dass die Angreifer sie trotz Lösegeldzahlung weiterverkaufen.

Weiterführende Literatur:


Umgang mit Lösegeldforderungen bei Angriffen mit Verschlüsselungstrojanern auf Kommunalverwaltungen

Empfehlungen der Bundesvereinigung der kommunalen Spitzenverbände, des Bundeskriminalamtes und des Bundesamtes für Sicherheit in der Informationstechnik

Berlin, März 2020

Umgang mit Lösegeldforderungen bei Angriffen mit Verschlüsselungstrojanern auf Kommunalverwaltungen
DST, DLT, DStGB, BKA, BSI, 2020
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/Ransomware-Kommunen-Empfehlung.html

Empfehlungen der Bundesvereinigung der kommunalen Spitzenverbände, des Bundeskriminalamtes und des Bundesamtes für Sicherheit in der Informationstechnik.

Ransomware – Fakten und Abwehrstrategien
BSI, 2024
https://www.bsi.bund.de/dok/ransomware-links

Die Webseite liefert eine Übersicht der zur Verfügung gestellten Materialien rund um das Thema Ransomware – von Erläuterungen zu Bedrohungslage und Entwicklung von Ransomware im Detail zu Maßnahmen bei Prävention und Reaktion.

2.3 Gegner: Cyberkriminelle, Auslandsspionage, APT-Akteure

Kernpunkte:

- Man unterscheidet Akteure nach ihrer Motivation (finanziell, politisch), ihren Absichten (Erpressung, Spionage) und dem Modus Operandi (*Ransomware, Spyware*, (D)DoS).
- Die *Attribuierung*, also Zuordnung eines Angriffs zu einer Angreifergruppierung bzw. deren Herkunftsland, ist meist nicht abschließend möglich.
- Nicht jeder Systemausfall ist ein Cyberangriff: Konfigurationsfehler, Defekte und Extremwetter etc. können ebenfalls den *IT-Betrieb* beeinträchtigen.

Hinter Angriffen mit *Ransomware*, wie in diesem Wegweiser ausführlicher erläutert, stecken in der Regel kriminelle Akteure mit finanziellen Motiven. Manche Cybercrime-Gruppierungen verfolgen aber auch ganz andere Interessen und setzen verschiedenste Werkzeuge zum Erreichen ihrer Ziele ein. Dieses Unterkapitel soll einen Überblick über Akteure und ihre Motivationen im Cyberraum geben.

Cyberkriminalität (engl. *Cybercrime*) umfasst alle Straftaten, die sich gegen das Internet als technische Basisinfrastruktur, weitere Datennetze oder informationstechnische Systeme oder deren Daten richten. Cyberkriminalität im weiteren Sinne umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden, wie z. B. Cybermobbing. Die Motivation von Cyberkriminellen ist vorrangig finanzieller Art. Die Bandbreite reicht von organisierter Cyberkriminalität, mit erheblichem Ressourceneinsatz und vertieftem Fachwissen, bis hin zu Kleinkriminellen, die mit geringem Aufwand und begrenzten Kenntnissen meist opportunistisch agieren. Für Erpressungs- und Betrugsdelikte setzen die Akteure Schadsoftware (bspw. *Ransomware*) ein oder versuchen mit *Phishing* und *Social Engineering* persönliche Daten und Zugangsinformationen zu stehlen oder Adressaten zu manipulieren. Das Vorgehen cyberkrimineller Gruppen hat sich in den letzten Jahren oftmals stark professionalisiert: Gruppierungen sind mitunter in unternehmensähnlichen Strukturen organisiert, haben feste Prozesse zur Kommunikation mit Betroffenen etabliert und bieten z. B. die eigene Schad- bzw. *Ransomware* anderen als Dienstleistung (*Ransomware-as-a-Service*, kurz *RaaS*) an. Aber auch durch *Phishing* erbeutete Zugangsdaten und durch eigene Scans gefundene unge*patch*te Schwachstellen werden im Darknet vermarktet. Daher ist auch die Rede von „Cybercrime-as-a-Service“ (CaaS).

Die Angreifergruppierungen im cyberkriminellen Bereich sind hoch dynamisch. Innerhalb von Monaten tauchen neue Akteure auf, verschwinden wieder oder benennen sich um. Mitglieder wechseln zudem häufig zwischen den Gruppierungen. Dadurch ist es schwierig, einen Überblick über die aktiven Angreifergruppierungen zu behalten, und dies erschwert die Strafverfolgung der Mitglieder.

Bei *Advanced Persistent Threats (APT)* handelt es sich um lang geplante, zielgerichtete Cyberangriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus. Sie sind in der Regel schwierig zu detektieren. APT-Gruppierungen werden meist mit staatlich gesteuerten Angriffen in Verbindung gebracht. Staatliche Akteure haben vor allem politische, wirtschaftliche und militärische Interessen und sind insbesondere an Spionage sowie der Manipulation oder Sabotage von IT-Infrastruktur interessiert.

Vor allem autoritäre Regime setzen teilweise große personelle und finanzielle Kapazitäten ein,

um westliche Demokratien durch verschiedene Cyberangriffsmethoden *(Ransomware/Social Engineering/(D)DoS/Spyware)* zu schädigen und Devisen zu beschaffen. Auch Deutschland steht im Fokus zahlreicher ausländischer Nachrichtendienste. Dabei agieren staatlich gesteuerte Gruppierungen mitunter wie gewöhnliche Cyberkriminelle und sind daher nicht klar als solche erkennbar.

Ausländische Nachrichtendienste können auch im Rahmen der hybriden Bedrohungen (→ *Anhang 4.3*) das Ziel verfolgen, durch Cyberangriffe auf kommunale Strukturen das Vertrauen in öffentliche Institutionen zu untergraben bzw. die Handlungsfähigkeit von Behörden infrage zu stellen. Letztlich geht es darum, eine politische und gesellschaftliche Destabilisierung zu erreichen. Die Beeinträchtigung der öffentlichen Ordnung, Sicherheit und der staatlichen Handlungsfähigkeit auf dieser bürgernahen Ebene ist ein wichtiges Ziel fremdstaatlicher Cyberangriffe.

Als Hacktivismus bezeichnet man die Beeinträchtigung oder Manipulation von IT-Systemen als Protestakt zur Durchsetzung bestimmter ideologischer Ziele. Typische Aktivitäten aus diesem Bereich sind das Manipulieren von Webseiten (*Defacement*) sowie Überlastungsangriffe (*(Distributed) Denial of Service*, kurz: (D)DoS). Dies wird oft auch zur Überbringung einer öffentlichkeitswirksamen Botschaft bzw. zur Propaganda eingesetzt. So gab es etwa im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine mehrfach politisch motivierte *(D)DoS-Angriffe* auf kommunale Websites und andere netzbasierte Angebote. Diese hatten das Ziel, die Bevölkerung zu beunruhigen und das Vertrauen in staatliche Institutionen zu untergraben.

Grundsätzlich besteht immer auch eine Gefahr ausgehend von sogenannten Innentätern. Dabei handelt es sich meist um Mitarbeitende von betroffenen Einrichtungen, die bspw. aus persönlicher Enttäuschung oder Frustration heraus einen Angriff durchführen. Durch die ihnen zugeordneten legitimen Zugangsdaten zum Netzwerk und zu den Systemen kann diesen Angriffen kaum mit ausschließlich technischen Mitteln begegnet werden. Hier empfehlen sich ein ganzheitlicher Umgang und eine entsprechende

Sonderfall: ethische Hacker

Im Gegensatz zu Cyberangreifern sind auch ethisch handelnde Sicherheitsforschende (auch ethische Hacker oder White Hat Hacker genannt) der Zivilgesellschaft zu erwähnen, die bspw. aus (intrinsischem) Eigeninteresse Systeme auf Sicherheitslücken untersuchen, um diese anschließend den Entwicklern oder Betreibern zu melden. Dieses Verfahren zur Offenlegung von Schwachstellen, auch Responsible Disclosure bzw. Coordinated Vulnerability Disclosure (CVD) genannt, kann zu einem höheren Schutz der Systeme beitragen.[a]

Voraussetzung dafür ist, dass die Akteure bestimmte Grenzen einhalten und im besten Fall frühzeitig in Kontakt treten. Dazu bietet sich die Zurverfügungstellung einer security.txt-Datei auf der eigenen Website an, die es den Forschenden erleichtern soll, sicherheitsrelevante Informationen an den Website-Betreiber weiterzugeben.[b]

Um es in aller Deutlichkeit zu sagen: Ethische Hacker möchten keinen Schaden anrichten, sondern vielmehr dabei helfen, Schäden zu verhindern. Aus Sicht einer Kommune sind die Aktivitäten dieser Sicherheitsforschenden daher grundsätzlich zu begrüßen.

[a] Siehe [ACS18b] (→ *Anhang 2*) und https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.pdf.
[b] Weiter gehende Informationen zur Erstellung finden sich unter [RFC22] (→ *Anhang 2*).

Gefährdungseinschätzung im Rahmen der Personalbetreuung und -führung (→ *Anhang 4.4*).

Die Zuordnung von Cyberangriffen zu einer bestimmten Gruppierung, auch *Attribuierung* genannt, ist oft nicht abschließend möglich. Zwar finden sich durch forensische Untersuchungen von Protokolldateien und Schadsoftware Indizien, diese sind jedoch nur schwer bestimmten Angreifergruppen zuzuordnen. Zunehmend verschwimmt auch die Abgrenzung zwischen Cyberkriminalität und staatlich gelenkter Spionage. In vielen Fällen ist nicht klar zu bestimmen, ob eine Gruppierung selbstständig agiert oder einem ausländischen Nachrichtendienst zugehörig ist bzw. nachrichtendienstlich gesteuert wird. Trotz aller Schwierigkeiten sind regelmäßig auch Ermittlungserfolge, insbesondere international abgestimmte Aktionen, gegen Cyberkriminelle zu verzeichnen.[12]

Cyberangriffe haben in den letzten Jahren stark zugenommen und stehen daher auch im Mittelpunkt dieses Wegweisers. Bei aller berechtigten Aufmerksamkeit für diese Gefahrenart darf man allerdings nicht vergessen: Ein Vorfall bzw. Ausfall der Informationstechnik kann auch ganz andere Ursachen haben. Neben weiteren Angriffsformen wie physischer Sabotage kann der *IT-Betrieb* bspw. durch folgende häufig auftretende Probleme negativ beeinflusst werden:

- menschliche Fehler bei der Konfiguration,
- unerwartete Wechselwirkungen innerhalb der eigenen Systeme, z. B. nach einem Update,
- Defekte der Hardware,
- Stromausfall,
- Kühlungsausfall im Serverraum,
- Folgen von Extremwetter (z. B. Überflutungen durch Starkregen),
- andere physische Einflüsse (z. B. bei Bauarbeiten durchtrennte Kabel, Rohrbrüche im Gebäude, Rauchentwicklung oder eindringender Staub, Befall durch Schadnager).

Im Rahmen eines *All-Gefahren-Ansatzes* sollten auch diese Szenarien berücksichtigt werden.

[12] Siehe [BMI24c] (→ *Anhang 2*).

© Gerd Altmann/pixabay

Vorfallbewältigung: Handeln in der Lage

Dieses Kapitel widmet sich einem akuten Cyberangriff, listet stichpunktartig entsprechende Notfallmaßnahmen auf und weist auf externe Unterstützungsmöglichkeiten hin. Es kann für ein Handeln in der Lage herangezogen werden. Es ersetzt jedoch keinesfalls eigene Vorbereitungen im Rahmen des (IT-)Notfallmanagements (→ *Kapitel 5*), die die Handlungsfähigkeit im Ereignisfall entscheidend beschleunigen und verbessern können.

Kernpunkte:

- Ruhe bewahren und Notfallmaßnahmen ergreifen
- Rechtliche Meldepflichten beachten
- Falls erforderlich möglichst frühzeitig externe Expertise hinzuziehen

3.1 Akutmaßnahmen bei einem Cyberangriff

Im Folgenden werden mögliche Maßnahmen bei einem Cyberangriff vorgestellt, die je nach Eskalationsstufe ergriffen werden können. **Allgemein gilt es dabei stets, Ruhe zu bewahren und keinesfalls unüberlegte oder übereilte Entscheidungen zu treffen. Insbesondere sollte nicht eigenständig Kontakt mit den Angreifergruppierungen aufgenommen und, im Falle eines *Ransomware*-Angriffs, keinesfalls Lösegeld gezahlt werden** (→ *Kapitel 2.2*). Bei Bedarf sollten frühzeitig externe Unterstützung und spezielle Fachexpertise hinzugezogen werden (→ *Kapitel 3.2*).

Denken Sie zurück an das Szenario des Ransomware-Angriffs auf die fiktive Stadt Rodenburg (→ Kapitel 2.1):

IT-Leiter Thomas Jäger ist am frühen Sonntagmorgen überraschend in den Dienst gerufen worden. Er muss feststellen, dass sämtliche Dateien verschlüsselt und sowohl Intranet als auch Telefonserver nicht erreichbar sind.
Um zu verhindern, dass die Angreifer weiteren Schaden anrichten können, schaltet er als Erstmaßnahme alle Systeme ab oder trennt sie zumindest vom Netz.
Damit ist die gesamte IT der Kommunalverwaltung nicht mehr benutzbar. Was nun?

Sichern

- Datensicherungen entkoppeln und gewissenhaft aufbewahren (→ *Kapitel 4*).
- Ausmaß des Angriffs einschätzen und betroffene Systeme identifizieren.[13]
- Informationen über das Ereignis sammeln (bspw. Protokolldateien, Screenshots, Berichte über Nutzeraktivitäten).[14]
- Nach Rücksprache mit qualifizierten Vorfallbearbeitern Internetzugang trennen (bei Clients die WLAN-Verbindung und/oder das LAN-Kabel, ggf. die mobile Datenverbindung) und ggf. verdächtige Systeme abschalten.[15]
- Rechner, welche sich nicht im Betrieb befinden, nicht mit dem Netz koppeln oder nicht einschalten.
- *Virtual Private Network (VPN)* der Benutzerinnen und Benutzer im Homeoffice trennen.
- Weiter gehende relevante Punkte finden sich auch unter „Ich habe einen Vorfall – Checkliste Technik“ der Allianz für Cyber-Sicherheit.[16]

Melden

- Alle nötigen internen Stellen (z. B. Verwaltungsspitze, *IT-Betrieb*, die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten (ISB), die Datenschutzbeauftragte oder den Datenschutzbeauftragten, Pressesprecherin oder Pressesprecher) alarmieren.
- Mitarbeitende in Kenntnis setzen und Sprachregelungen für Nachfragen bereitstellen.
- Strafanzeige bei der Polizei stellen (über Zentrale Ansprechstelle Cybercrime[17] bzw. bei der örtlichen Polizeidienststelle).
- Bei Spionageverdacht Landesamt für Verfassungsschutz informieren.
- Weitere Meldepflichten und Fristen beachten (→ *Kapitel 5.2.2*):
  - Falls personenbezogene Daten (nach DS-GVO) betroffen sind: Datenschutzaufsichtsbehörde.[18]

[13] Keinesfalls darf eine Anmeldung mit Administratorkonten auf einem potenziell infizierten System erfolgen.

[14] An die forensische Beweissicherung denken! Keine ermittlungsrelevanten Daten verändern oder zerstören.

[15] Achtung: Durch ein Abschalten können Spuren vernichtet und ermittlungsrelevante Daten verändert, zerstört oder gelöscht werden, sodass eine forensische Untersuchung unbrauchbar wird. Im Zweifel betroffene Systeme möglichst schnell vom restlichen Netz trennen und nicht mit Verbindung zum Internet betreiben sowie bis zu einer forensischen Beweissicherung die Systeme möglichst unverändert lassen.

[16] Siehe [ACS24] (→ *Anhang 2*).

[17] Kontaktdaten unter [BKA24] (→ *Anhang 2*).

[18] Vorgaben der Datenschutzaufsichtsbehörde können die konkret anliegenden Aufgaben im Rahmen der Vorfallbewältigung in erheblichem Umfang ergänzen. Hier kann bspw. eine Kategorisierung der vorhandenen Daten auf den verschiedenen Speicherpfaden „aus dem Gedächtnis“ durch alle Mitarbeitenden erforderlich werden. Dabei hilft eine konkrete Vorbereitung, z. B. mit einer Regelung zur Löschung von Daten, um den Umfang eines möglichen Datenabflusses zu reduzieren (→ *Anhang 4.5*).

  - Falls *Kritische Infrastruktur* (nach *BSI-KritisV*[19]) betroffen ist: Bundesamt für Sicherheit in der Informationstechnik.
  - Ggf. vertragliche Meldepflichten für kommunale Datennetze beachten.
  - Vorfall ggf. der übergeordneten Behörde oder dem CERT des Bundeslandes melden.
- Vorfall ggf. der Cyberversicherung melden.
- Dienstleister mit Kommunikationsbeziehungen über Vorfall informieren.
- Vorfall ggf. der Allianz für Cyber-Sicherheit beim BSI melden.
- Da ein solcher Vorfall in der Regel publik wird und auch Auswirkungen auf die Bevölkerung hat, proaktiv auch in Richtung Öffentlichkeit kommunizieren (→ *Kapitel 5.2.5*).

Organisieren

- Ggf. kurzfristigen Notbetrieb aufbauen, um eingeschränkte Arbeitsfähigkeit wiederherzustellen (hierfür eignen sich vor allem mobile Endgeräte wie Laptops, → *Kapitel 5.2.4*).
- Ggf. externe Unterstützung anfordern (→ *Kapitel 3.2* und → *Kapitel 5.2.1* bezüglich der Einbindung der IT-Dienstleister).
- Kommunalen *Verwaltungs-/Krisenstab* einberufen (hier darauf achten, dass die IT mit einer sprechfähigen und entscheidungsbefugten Führungskraft im *Krisenstab* vertreten ist) (→ *Kapitel 5.2.1*).
- Methoden für eine strukturierte Entscheidungsfindung anwenden (z. B. FOR-DEC-Methode[20]), die Entscheidungen samt deren Grundlagen, darauf aufbauenden Maßnahmen und den so erzielten Fortschritten dokumentieren und an der Entscheidungsfindung beteiligte Personen benennen.
- Fürsorgepflicht beachten! Die Reaktion auf einen IT-Sicherheitsvorfall ist ein Marathon mit Sprinteinlagen. Achten Sie auf Ihr Personal, schützen Sie es ggf. auch vor sich selbst!
- Führungsrhythmus etablieren (z. B. morgendliche Lagebesprechung) und aktiv Pausenzeiten bestimmen.
- Versorgung und Erholungsphasen nicht vergessen (Getränke, Mahlzeiten, Obst bzw. gesunde Zwischenmahlzeiten, Ruhe/Schlaf)!
- Arbeitsumgebung einrichten und nutzen (Material, Räume, abgetrennte, aber gut erreichbare Bereiche) (→ *Kapitel 5.2.1: Das Handbuch IT-Notfallmanagement*).
- Falls nicht im Vorfeld bereits geschehen: Kritische Dienstleistungen bzw. Geschäftsprozesse bestimmen oder bei Bedarf situativ deren Bewertung prüfen (→ *Kapitel 5.2.3*).

Auswahl relevanter Fragen zur Entscheidungsfindung für den *Krisenstab*[21]

- Was ist genau passiert?
  (Sorgfältig zwischen Vermutungen und Fakten trennen zwecks realistischer Lageeinschätzung!)
- Wie ist der Vorfall aufgefallen? Wurde er durch Externe gemeldet?
  Dann halten Sie den Kontakt zu diesen aufrecht, sofern dort gewünscht, um zu verhindern, dass der Vorfall aus einem Gefühl der Vernachlässigung heraus vorzeitig publik gemacht wird.
- Welche Auswirkungen hat der Vorfall auf die Betroffenen (Mitarbeitende, Bevölkerung)? Daraus leiten sich auch Inhalte der FAQ ab (→ *Kapitel 5.2.5: Welche Inhalte?*).
- Welche Auswirkungen kann die Situation direkt auf die Kerndienstleistungen der Kommune haben?
  - Muss der Weiterbetrieb um jeden Preis gewährleistet werden? Dies wirkt sich möglicherweise negativ auf forensische Beweissicherung und Analyseergebnisse aus.
  - Besteht ausreichend zeitlicher Spielraum, um das Problem umfassender zu analysieren und zu bewältigen?
  - Ist eine Strafverfolgung oder spätere Regressforderung vorgesehen? Muss deshalb beweissicher gehandelt und besonders gründlich dokumentiert werden?

---

[19] Nach § 8b Abs. 4 BSIG müssen KRITIS-Betreiber, die der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) unterliegen, bestimmte *Störungen* unverzüglich an das BSI melden.

[20] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Bewaeltigung.pdf

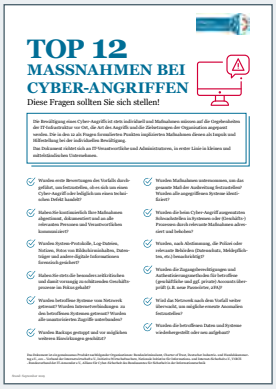
[21] Das grundsätzliche Training des Entscheidungsfindungsprozesses in Stäben bzw. der Stabsarbeit insgesamt findet bspw. in Schulungen an der BABZ statt. Die BABZ und auch einzelne Bundesländer empfehlen klare Ablaufprozesse zum Sitzungsverlauf und zur Entscheidungsfindung. Die hier gelisteten Fragen können dabei eine Rolle spielen und bei Bedarf durch weitere ergänzt werden (→ *Kapitel 5.2.1*).

- Welche Auswirkungen kann der Vorfall auf Kunden, Partner oder die Öffentlichkeit haben? Ergibt sich daraus zusätzlicher Handlungsbedarf? Sollen ggf. Nachbarkommunen, deren Fachanwendungen im gleichen Verbund betreut werden, gewarnt werden?
- Was hat zu dem Vorfall geführt? Gibt es Hinweise auf ein gezieltes Vorgehen? Sind wir nur eines von vielen potenziellen Opfern?[22]
- Wie können die psychischen Auswirkungen auf die Mitarbeitenden abgemildert werden?
  - Durchhaltefähigkeit insbesondere des IT-Personals beachten (Stress, Belastung, Überarbeitung etc.).
- Unterbeschäftigung in herunterpriorisierten bzw. in ohne IT nicht arbeitsfähigen Bereichen abfangen: Können sinnvolle Abwesenheitsregelungen getroffen werden? Gibt es andere Aufgaben, die im günstigsten Fall die Lagebewältigung unterstützen?
- Gute Fehlerkultur etablieren: Ein offensives Stellen der Schuldfrage erhöht die Belastung. Eine gute interne Kommunikation sollte den Fokus auf eine schnelle Bewältigung und ein konstruktives Lernen aus dem Vorfall lenken.

Weiterführende Literatur:

Erste Hilfe bei einem schweren IT-Sicherheitsvorfall
BSI, 2020
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html

Dieses Papier dient als Notfalldokument für Informationssicherheitsbeauftragte, Chief Information Security Officers (CISOs) und Systemadministratorinnen und Administratoren von kleinen und mittleren Unternehmen (KMU) sowie von kleineren Behörden bei einem schweren IT-Sicherheitsvorfall.



TOP 12 Maßnahmen bei Cyber-Angriffen
Allianz für Cyber-Sicherheit, 2019
https://www.bsi.bund.de/dok/notfallkarte-massnahmen

Die Übersicht richtet sich an IT-Verantwortliche und Administratorinnen und Administratoren. Sie ist nicht abschließend und nicht individuell auf alle Adressaten zugeschnitten, liefert allerdings erste Impulse und Hilfestellungen bei der Reaktion auf einen Vorfall.

[22] Die Fragen sind in der Akutphase nur relevant, wenn sie Einfluss auf die Entscheidungen haben. Hier kommt es noch nicht zur detaillierten Ursachenuntersuchung.

3.2 Externe Unterstützung in *Notfall* und *Krise*

Die im Folgenden beschriebenen Organisationen können bei der Bewältigung von einem *IT-Notfall* oder einer *IT-Krise*, also bei der Ad-hoc-Reaktion im Ernstfall, unterstützen (zu den präventiven Angeboten → *Kapitel 5.3*). Auch erfahrene Response-Dienstleister benötigen, um effektiv helfen zu können, Detailinformationen über das konkrete betroffene Netzwerk. Sie sind somit fortwährend auf einen engen Kontakt zu internen Mitarbeitenden angewiesen. Für die Kontaktaufnahme und die Kommunikation mit Dritten muss immer ein Gerät verwendet werden, das nicht mit dem mutmaßlich kompromittierten Netzwerk verbunden ist (ein externes Gerät mit separatem Internetanschluss).

IT-Sicherheitsdienstleister

Die Vorfallbearbeitung, insbesondere aber die Forensik, gehört üblicherweise nicht zum Leistungsspektrum eines gewöhnlichen IT-Dienstleisters. Daher ist es anzuraten, sich Hilfe bei einem spezialisierten IT-Sicherheitsdienstleister zu suchen. Wird ein solcher hinzugezogen, muss berücksichtigt werden, dass dieser nicht mit der internen IT-Infrastruktur vertraut ist und entsprechend Informationen (z. B. vorhandene Netzpläne) und Unterstützung durch die Kommunalverwaltung oder den zugehörigen IT-Dienstleister benötigt.

Allgemein ist bei der Auswahl eines Forensik-Unternehmens zu beachten, dass die Unternehmen unterschiedliche Analyseschwerpunkte haben. Die Bandbreite des Know-hows reicht dabei von der Analyse netzwerkbasierter Angriffe bis hin zur Wiederherstellung von physisch zerstörten Festplatten. Daher sollte der Unterstützungsbedarf bei der Anfrage möglichst klar beschrieben werden.

Das BSI arbeitet im Rahmen der Allianz für Cyber-Sicherheit mit etablierten Unternehmen mit dem Schwerpunkt Computerforensik aus Deutschland zusammen. Daneben hat das BSI eine Liste qualifizierter APT-Response-Dienstleister veröffentlicht. Zu prüfen ist ebenfalls, ob ggf. über Rahmenverträge oder abgeschlossene Cyberversicherungspolicen kurzfristig Unterstützung beauftragt werden kann.

Weiterführende Information:

Listen zertifizierter Dienstleister und Experten
Das BSI stellt eine Liste qualifizierter Dienstleister für die Bewältigung von APT-Angriffen bereit:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

Falls es sich bei einem IT-Vorfall nicht um eine Kompromittierung, sondern um einen (D)DoS-Angriff handelt, steht darüber hinaus eine Liste zertifizierter (D)DoS-Mitigations-Dienstleister zur Verfügung:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.html

Landesinstitutionen

Einige Bundesländer bieten im Akutfall Unterstützungsleistungen für ihre Kommunen an. Dies kann von Beratung bis hin zur Entsendung von *CERT*-Mitarbeitenden für die eigentliche technische Vorfallbewältigung reichen. Spezifische Informationen können beim jeweiligen CISO des Landes eingeholt werden.

Verbände und benachbarte Kommunen

Wenn Ihre Kommune Mitglied in einem Verband ist, können Sie ggf. auch von dieser Seite Unterstützung erhalten. Nutzen Sie Ihre Netzwerke und Beziehungen, um ggf. (Amts-)Hilfen, Unterstützung, Personalverstärkung, Entlastung, Übernahme von Teilservices als temporäre Alternative etc. zu erhalten (→ *Kapitel 5.3*).

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das BSI ist ein kompetenter Ansprechpartner im Fall eines schweren IT-Sicherheitsvorfalls. Es ist generell ratsam, kommunale Cyberangriffe im *Notfall-* oder *Krisenstadium* über die Allianz für Cyber-Sicherheit an das BSI zu melden[23]. Das BSI verfügt über fundierte Kenntnisse bei der Behandlung von Angriffen. Bei den folgenden Punkten kann Sie das BSI im Rahmen freier Ressourcen unterstützen:

- Dokumente mit Empfehlungen und Vorgehensweisen,
- Vermittlung von (Forensik-)Expertinnen und (Forensik-)Experten und
- Besprechung von Maßnahmen.

Das BSI kann jedoch nur in absoluten Ausnahmefällen im Rahmen seiner gesetzlichen Möglichkeiten selbst aktiv unterstützen. Die Vorgabe von § 3 Abs. 1 S. 2 Nr. 18 BSIG lautet: „Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 5a." Ein herausgehobener Fall nach § 5b Abs. 2 BSIG liegt „insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist". Vor allem eine Infektion mit gängiger *Ransomware*, auch bei Kommunen, fällt hier regelmäßig nicht darunter – es sei denn, der Angriff hat Auswirkungen auf die kritischen Dienstleistungen eines KRITIS-Unternehmens.

Weiterführende Information:

Unterstützung bei der Vorfallsbearbeitung
BSI, 2023
[BSI23] (→ *Anhang 2*)
Meldeformular: https://mip2.bsi.bund.de/meldungen/meldung-ohne-registrierung-erstellen/?meldestelle=10&formular=32

[23] Bei einem mutmaßlich kompromittierten System bzw. Netzwerk sollte hierfür ein externes Gerät mit eigenem Internetanschluss genutzt werden.

© Gerd Altmann/pixabay

Wiederherstellung: Zurück zur Normalität

Dieses Kapitel widmet sich den Maßnahmen, die nach der akuten Bewältigungsphase ergriffen werden müssen, um wieder zum regulären Geschäftsbetrieb zurückkehren und weiteren Vorfällen ähnlicher Art präventiv entgegenwirken zu können.

Kernpunkte:

- Systeme bereinigen und wiederaufsetzen
- Aufgedeckte Schwachstellen und Sicherheitslücken schließen
- Netzwerk und IT-Systeme intensiv überwachen
- IT-Sicherheitsarchitektur und Notfallmanagement kontinuierlich weiterentwickeln

Eine Bereinigung der Systeme sollte erst nach der Vorfallanalyse und auf der Basis der so gewonnenen Erkenntnisse stattfinden[24]. In einigen Fällen reicht die Beseitigung der Schadsoftware bzw. schadhafter Dateien zwar bereits aus. Meistens ist eine tatsächliche Bereinigung jedoch aufwendiger und kann das Neuaufsetzen der Systeme notwendig machen. Werden in solchen Fällen vorschnell lediglich Schadsoftware oder schadhafte Dateien beseitigt, besteht die Gefahr, dass Informationen verloren gehen[25], Beweise vernichtet werden oder gar die Bereinigung unvollständig ausfällt. Daher sollte die Wahl der Vorgehensweise immer auf die Bereinigung durch eine Neuinstallation des Betriebssystems fallen, wenn bei der Aussagefähigkeit der Analyseergebnisse Bedenken bestehen oder die Vorfallanalyse keine hinreichenden Resultate liefern konnte.

Nach erfolgreicher Bereinigung der Systeme können diese wieder in den Produktivbetrieb überführt werden. Diesbezüglich sollte eine geordnete Reihenfolge bestimmt werden, die sich an der Priorität des jeweiligen Systems orientiert. Hier hilft eine im Vorfeld durchgeführte Analyse und Priorisierung der Geschäftsprozesse und Fachverfahren, z. B. durch eine *Business Impact Analyse (BIA)* (→ *Kapitel 5.2.3*). Dabei gilt es zudem, mögliche Systemabhängigkeiten zu beachten, die bei der Wiederherstellung bzw. dem Wiederanlauf eine nicht zu vernachlässigende Rolle spielen. Idealerweise kann man sich dabei auf einen bereits im Vorfeld erarbeiteten Wiederanlaufplan und Wiederherstellungsplan[26] stützen (→ *Kapitel 5.2.3*). Liegen diese nicht vor oder erweisen sich Teile als nicht hinreichend praktikabel, dann lohnt sich in dieser Phase eine detaillierte Dokumentation der getroffenen Abwägungen sowie aufgefundenen Schwierigkeiten, um im Anschluss die Vorbereitungen überarbeiten bzw. ergänzen zu können.

Wenn als Zwischenlösung ein separates Netzwerk aufgebaut wurde, bietet es sich ggf. an, die bereinigten Systeme in das neu aufgesetzte Netz zu überführen und dieses weiter als Produktivnetz zu nutzen. Häufig werden beim Aufbau des Notnetzes aufgrund der benötigten Geschwindigkeit bestimmte Kompromisse getroffen, die auf Kosten der Sicherheit gehen. Daher sollte im Nachgang geprüft werden, ob nicht doch ein von Grund auf wohlüberlegtes und strukturiertes IT-Netzwerk zu bevorzugen ist.

Ggf. müssen Kommunikationsverbindungen zu und gemeinsame Fachverfahren mit externen Partnern wiederhergestellt werden; daher sollten frühzeitig die entsprechenden Bedingungen der Partner für einen erneuten Anschluss erfragt werden. Selbstverständlich lohnt es sich im Gegenzug, auch die eigenen Bedingungen dafür zu formulieren, dass man einen möglicherweise kompromittierten Partner wieder an das eigene Netz anschließt (→ *Kapitel 5.2.1: Das Handbuch IT-Notfallmanagement*).

Sollten Ad-hoc-Lösungen eingeführt worden sein, sollten sie vor Überführung in den Normalbetrieb noch einmal darauf geprüft werden, dass im langfristigen Betrieb von ihnen keine übermäßigen Zusatzaufwände oder Schwierigkeiten bei der Administration ausgehen. Idealerweise wird dies direkt bei Einführung von Ad-hoc-Lösungen mitbedacht, ansonsten sollte es spätestens beim Übergang in die Wiederherstellung erfolgen.

Die durch die forensische und/oder Vorfallanalyse aufgedeckten Schwachstellen und Sicherheitslücken sollten beim Wiederaufsetzen der Systeme bereits bedacht und geschlossen werden. Dabei empfiehlt sich eine prinzipielle Prüfung des eigenen Schwachstellen- und *Patch*-Managementprozesses.[27]

---

[24] Liefert die forensische Untersuchung Erkenntnisse über den Angriffsvektor, so können diese dabei zudem direkt in eine Stärkung der präventiven Maßnahmen umgesetzt werden.

[25] Bei vorschneller Löschung kann unter Umständen nicht mehr nachvollzogen werden, wie Angreifer vorgegangen sind, was sie erreichen konnten, welche Daten sie möglicherweise erbeutet haben und wo vielleicht noch Reste einer Kompromittierung zu finden wären. Es werden wertvolle Spuren verwischt.

[26] Im Wiederanlaufplan ist geregelt, wie Institutionen ausgefallene Ressourcen etwa durch Ersatzlösungen kompensieren können. Beim Wiederanlauf werden Maßnahmen ergriffen, um in einen zuvor geregelten Notbetrieb wechseln zu können, der die Geschäftsfortführung sicherstellt. Ziel der Wiederherstellung ist hingegen, einen Zustand zu erreichen, in dem der Normalbetrieb wieder möglich ist. Die Wiederherstellung findet daher parallel zum Wiederanlauf und zum Notbetrieb statt.

[27] Für weiter gehende Empfehlungen hierzu siehe [ACS18a] (→ *Anhang 2*).

Die Systeme und das Netzwerk sollten nach dem Vorfall besonders intensiv auf ungewöhnliche Aktivitäten überwacht werden, um sicherzustellen, dass sie einwandfrei funktionieren und ein erneuter Angriff rechtzeitig erkannt werden kann: Eventuell nicht bereinigte Artefakte der Angreifer (sogenannte „Second Chance Backdoors“) können einen zweiten Angriff ermöglichen; aber auch das bloße Bekanntwerden eines folgenreichen Angriffs kann das System und dessen Betreiber attraktiv für weitere Angreifer machen. Sind bei dem Angriff Daten abgeflossen, könnten diese für *Social Engineering* missbraucht werden.

Zum Abschluss der Vorfallbearbeitung sollte eine Aufarbeitung des Vorfalls (z. B. in einem Gespräch) mit dem zuständigen IT-Sicherheitsdienstleister stattfinden, um sowohl das eigene Notfallmanagement als auch die eigene Prävention zu verbessern. Für das Gespräch können folgende Fragestellungen hilfreich sein:

- Wie schnell und wodurch wurde der IT-Sicherheitsvorfall erkannt und behoben?
- Haben die Meldewege funktioniert?
- Welche kurz- und langfristigen Maßnahmen müssen ergriffen werden?
- Was ist im Prozess der Vorfallbearbeitung gut gelaufen?
- Wo gibt es Verbesserungsbedarf im Prozess der Vorfallbearbeitung?
- Welche Sicherheitsmaßnahmen könnten verbessert werden?
- Welche Schulungs- und Sensibilisierungsmaßnahmen müssen angestoßen werden?

Auch intern sollte der Vorfall mit den verschiedenen *Stakeholdern* (Krisenmanagement, Verwaltungsspitze, betroffene Fachbereiche, IT) besprochen und aufgearbeitet werden. Im Sinne einer konstruktiven Fehlerkultur muss dabei die Identifikation von Verbesserungsbedarfen im Vordergrund stehen, um zukünftige Vorfälle effizienter bewältigen zu können.

Die Ergebnisse der Nachbereitung sollten dokumentiert werden. Die IT-Sicherheitsarchitektur, aber auch insbesondere das Notfallmanagement sollten kontinuierlich weiterentwickelt werden (→ *Kapitel 5*). Hier gilt eindeutig: Informationssicherheit ist ein Prozess und kein Zustand – nach dem Vorfall ist möglicherweise vor dem Vorfall!

© Cliff Hang/pixabay

Vorbereitung: Prävention und Detektion vor Reaktion

Dieses Kapitel stellt das zentrale Kapitel dieses Wegweisers dar. Es führt die sinnvollen eigenen Vorbereitungen im Rahmen des (IT-)Notfallmanagements auf. Diese sollen die Eintrittswahrscheinlichkeit von IT-Vorfällen senken (→ *Kapitel 5.1*) bzw. im Ereignisfall die Auswirkungen reduzieren sowie die eigene Handlungsfähigkeit entscheidend beschleunigen und verbessern (→ *Kapitel 5.2*). Es werden Hinweise auf diverse Anlaufstellen gegeben, bei denen im Rahmen der Vorbereitung auf IT-Vorfälle Unterstützung in Form von Informationen, Schulungen oder Förderung erhalten werden kann bzw. wo sich ein verstetigter Austausch zum Thema anbietet (→ *Kapitel 5.3*).

5.1 Stärkung der Informationssicherheit

Kernpunkte:

- Angriffe treffen meist „*Low-hanging Fruits*“.
- Ein angemessenes Informationssicherheitsniveau ist notwendig zur Prävention.
- Die Implementierung eines *Informationssicherheitsmanagementsystems* als ganzheitlicher Ansatz wird empfohlen.
- Der „Weg in die Basis-Absicherung“ (WiBA) hilft beim Einstieg.
- Verantwortlich ist die Verwaltungsspitze, Informationssicherheitsbeauftragte helfen bei verbindlicher Umsetzung.
- Die Sensibilisierung der Mitarbeitenden ist essenziell.

Wir erinnern uns zurück an den Ausgangspunkt des Szenarios in unserer fiktiven Stadt Rodenburg (→ Kapitel 2.1):

Zunächst lässt nichts erahnen, dass der Arbeitsalltag demnächst auf den Kopf gestellt wird. Herr Schmidt kommt aus der Mittagspause zurück und widmet sich den zwischenzeitlich eingegangenen E-Mails.
Er öffnet einen Anhang und blitzschnell geht ein neues Fenster auf. Seitdem die IT auch seinen Arbeitsplatz aufgerüstet hat, laufen die Anwendungen richtig flüssig, freut sich Herr Schmidt. Auf seinem Bildschirm erscheint ein Hinweis dort, wo eigentlich der Inhalt stehen sollte: „Dieses Dokument wurde mit einer älteren Programmversion erstellt, bitte klicken Sie auf Bearbeitung aktivieren, um den Kompatibilitätsmodus zu starten.“
Es gibt wohl noch ein paar Schwierigkeiten mit dem neuen Update, denkt er sich und klickt die gelben Banner weg.

Eine der wichtigsten Präventionsmaßnahmen gegen folgenreiche Cyberangriffe ist die Stärkung der Informationssicherheit innerhalb der Organisation. Daher ist es besonders wichtig, dass die Führungsebene „Informationssicherheit“ als Handlungsfeld anerkennt und die Verantwortung dafür übernimmt. So können die Prozesse und Strukturen der Organisation darin eingebettet und mit den notwendigen Ressourcen ausgestattet werden. Ein angemessenes Niveau an Informationssicherheit ist zwingend nötig, denn *Ransomware*-Angriffe treffen meist die „*Low-hanging Fruits*“. Gemeint sind Ziele mit bekannten Sicherheitslücken, die von Cyberkriminellen einfach ausgenutzt werden können (→ *Kapitel 2.2*). In aller Regel können diese Sicherheitslücken durch Sicherheitsmaßnahmen mit wenig Aufwand, aber dafür viel Mehrwert, geschlossen werden. Dazu muss niemand das Rad neu erfinden. Es existieren bereits eine Vielzahl von Frameworks, Best Practices und Empfehlungen, um die Informationssicherheit der eigenen Organisation zu stärken. Die folgenden Unterkapitel geben einen Überblick.

Aus der Praxis: Welche verbreiteten Probleme machen es Angreifern leicht?

- Kein Überblick über administrative Accounts
- Verwendung administrativer Accounts anstatt spezifischer Berechtigungen für bestimmte Aufgaben
- Verwendung von einfachen Passwörtern und Standardkennungen
- Einfache Authentisierungsmethoden
- Unzureichendes Patch- und Schwachstellen-Management
- Mangelhafte Härtung von Systemen
- Systeme laufen mit Standardeinstellungen der Hersteller
- Backups nicht segmentiert und mit administrativem Zugriff
- Lokale Protokollierung mit Standardeinstellung des Herstellers ohne (zeitnahe) Auswertung, die frühzeitig Probleme identifizieren könnte

5.1.1 Aufbau eines *Informationssicherheits-managementsystems* (ISMS)

Das Themenfeld der Informationssicherheit umfasst weit mehr als nur IT-Sicherheit. Es sollte immer ein ganzheitlicher und strukturierter Ansatz gewählt werden, der über technische Einzelmaßnahmen hinausgeht und eine umfassende Betrachtungsweise für die Informationssicherheit einnimmt.

Ein Managementsystem für Informationssicherheit umfasst alle Regelungen, die für die Steuerung und Lenkung des Schutzes von Informationen in der Institution nötig sind. Es legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert). Um mögliche Synergie-Effekte nutzen zu können, ist eine Verknüpfung mit z. B. dem Compliance-Management und dem *Business Continuity Management* sinnvoll.

Für die Einführung eines ISMS gibt es diverse Standards und Modelle. Bekanntestes Beispiel ist die international anerkannte Norm ISO/IEC 27001. Der Standard und die assoziierten Unternormen beschreiben ein umfassendes, komplexes ISMS, das deshalb vor allem für große Unternehmen in Betracht kommt. Kleine Organisationsformen mit begrenzten Ressourcen können davon erst einmal überfordert sein.

Im deutschsprachigen Raum und besonders im Behördenumfeld weitverbreitet ist der **IT-Grundschutz** des Bundesamts für Sicherheit in der Informationstechnik (BSI). Er bietet den Anwendern konkrete Hilfestellungen, um die generischen ISO-Anforderungen zu erfüllen. Der IT-Grundschutz umfasst folgende Standards:

- 200-1 Managementsysteme für Informationssicherheit (ISMS),
- 200-2 IT-Grundschutz-Methodik,
- 200-3 Risikoanalyse auf Basis von IT-Grundschutz,
- (200-4 Business Continuity Management).

Damit stellt das BSI eine erprobte und etablierte ganzheitliche Methodik zur Einführung eines ISMS bereit. Die Systematik erlaubt zudem eine iterative Implementierung, von der Basis-Absicherung über die Kern-Absicherung bis hin zur vollumfänglichen Standard-Absicherung. Sie kann damit besonders an die individuellen Bedürfnisse unterschiedlicher kleinerer bis mittlerer Organisationsgrößen angepasst werden.

Um den Einstieg in die Informationssicherheit, auf Basis des IT-Grundschutzes, noch einfacher zu gestalten, bietet das BSI diverse Umsetzungshinweise und Arbeitshilfen an, wie z. B. das **IT-Grundschutz-Profil „Basis-Absicherung**

Kommunalverwaltung“[28]. Mit dem von der Arbeitsgruppe kommunale Basis-Absicherung (AG koBA) der kommunalen Spitzenverbände erstellten IT-Grundschutz-Profil stellt das BSI eine dezidierte Liste von Mindestsicherheitsanforderungen für die Informationssicherheit von Kommunalverwaltungen bereit, die auf dem BSI-Standard 200-2 aufbaut. Gerade kleineren Kommunalbehörden soll so der Einstieg in die Informationssicherheit erleichtert werden, um auf diesem Weg ein Mindestsicherheitsniveau und letztlich die Gewährleistung des gesetzlichen Auftrages zu erreichen. Weiterhin bietet die Umsetzung des IT-Grundschutz-Profils einen nahtlosen Übergang zur höheren Standard-Absicherung.

Da auch die Umsetzung eines IT-Grundschutz-Profils gerade in der Initialphase viele Ressourcen bindet, hat das BSI zusätzlich zum oben genannten IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ das Projekt **„Weg in die Basis-Absicherung“ (WiBA)**[29] initiiert.

WiBA bietet einen unkomplizierten und ressourcenschonenden Einstieg in das Thema Informationssicherheit. Anhand von themenspezifischen Checklisten mit einfachen Prüffragen und zugehörigen Hilfsmitteln können Kommunen die dringlichsten Maßnahmen selbst identifizieren und umsetzen. So kann ein erster, aber wesentlicher Schritt in Richtung systematischer Informationssicherheit erfolgen. Die Checklisten decken fundamentale Sicherheitsanforderungen für relevante Bereiche der Informationssicherheit ab, die bei der Absicherung vorrangig betrachtet und tatsächlich umgesetzt werden müssen. Dazu gehören technisch orientierte Checklisten wie bspw. „Serversysteme“ oder „Backups“, aber auch organisatorisch orientierte wie „Vorbereitung für Sicherheitsvorfälle“. Für die Umsetzung vom WiBA sind keine Kenntnisse der IT-Grundschutz-Methodik notwendig. Mit dieser Einstiegsebene können Kommunen ein grundlegendes Schutzniveau aufbauen, das sie im Anschluss zum oben bereits erwähnten IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ weiterentwickeln können (→ *Abbildung 2*).

Neben dem BSI-IT-Grundschutz gibt es auch verschiedene weitere **länderspezifische oder in der Wirtschaft verwendete Standards**, wie z. B. die Norm „CISIS12“ des IT-Sicherheitsclusters e. V.[30], welche besonders den Implementierungsprozess eines ISMS anhand von zwölf Schritten in den Fokus stellt. Mithilfe eines Maßnahmenkatalogs und begleitenden Handbuchs soll der Aufwand gering gehalten werden, um die Umsetzung

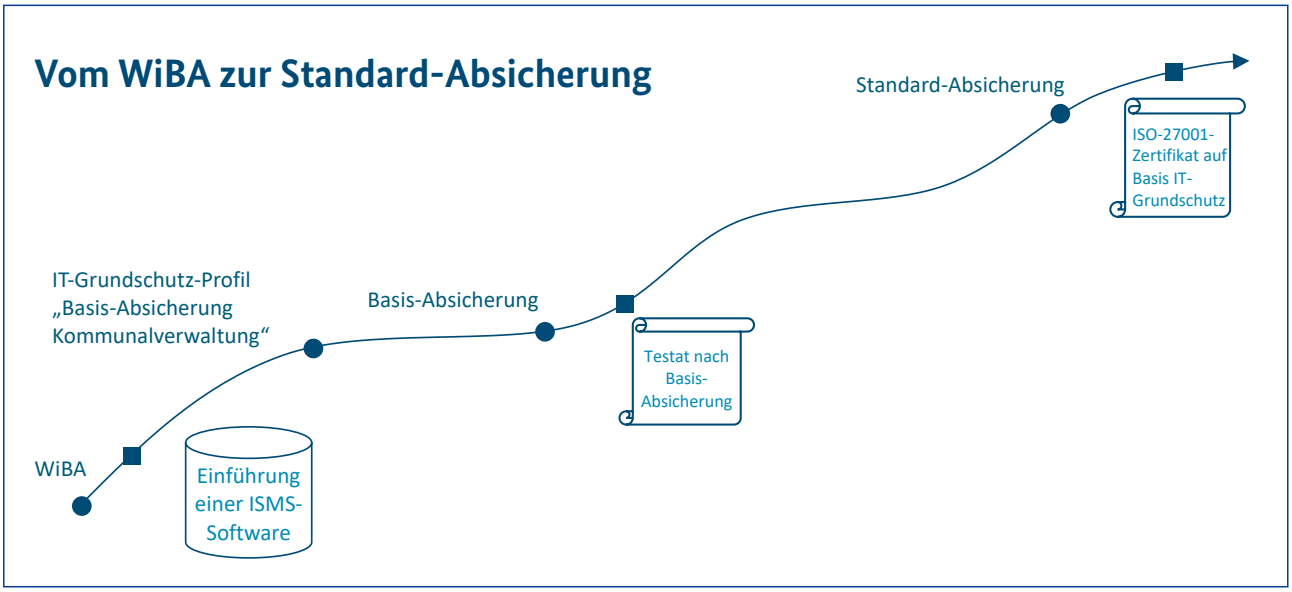


Abbildung 2: Vom Weg in die Basis-Absicherung (WiBA) zur Standard-Absicherung (Quelle: BSI, 2024)

[28] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html

[29] https://www.bsi.bund.de/dok/WIBA

[30] Siehe [SWI24] (→ *Anhang 2*).

besonders in kleinen Kommunen und Betrieben zu erleichtern.

Auch auf Landesebene wird Unterstützung für den Aufbau eines ISMS angeboten. Das geschieht z. B. über Frameworks wie „SiKoSH“ des Landes Schleswig-Holstein[31] oder Arbeitshilfen wie das Informationssicherheitskonzept „ISK V 4.0“ der Innovationsstiftung Bayerische Kommune[32], dessen erfolgreiche Umsetzung mit dem Siegel „Kommunale IT-Sicherheit“ bestätigt wird.

Unter bestimmten Umständen wird die Einführung eines solchen Systems auf kommunaler Ebene länderspezifisch gefördert.

Weitere Angebote kommen aus der Wirtschaft, wie z. B. die Richtlinie „VdS 10000“ der VdS Schadenverhütung GmbH[33]. Diese Richtlinie katalogisiert Maßnahmen zur Einführung eines ISMS für kleinere bis mittlere Organisationen. Sie basieren u. a. auf dem IT-Grundschutz des BSI und der Norm ISO/IEC 27001, sind jedoch speziell auf die limitierten personellen und finanziellen Ressourcen der Zielgruppe angepasst. Falls gewünscht, kann die Umsetzung der Richtlinie durch die VdS zertifiziert werden.

Um den Dokumentationsaufwand gering zu halten und die Arbeit zu erleichtern, bietet es sich an, eine spezielle ISMS-Software zu benutzen. Diese gibt es in verschiedenen Preiskategorien und für die verschiedenen Frameworks und Normen. Zur Umsetzung des IT-Grundschutzes bietet das BSI eine Liste von Anbietern, die einen Lizenzvertrag mit dem BSI geschlossen haben, an.[34] Bei der Auswahl sind vorhandene Abhängigkeiten z. B. von IT-Dienstleistern oder übergeordneten Vorgaben zu beachten.

Weiterführende Literatur:

BSI IT-Grundschutz-Standards 200-1 bis 200-4
BSI, 2024
https://www.bsi.bund.de/dok/6603458

5.1.2 Übernahme der Gesamtverantwortung durch die Verwaltungsspitze

Der wichtigste Schritt beim Aufbau eines ISMS ist die Übernahme der Gesamtverantwortung durch die Verwaltungsspitze. Diese ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren der Institution und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Die Leitungsebene hat auch im Bereich Informationssicherheit eine Vorbildfunktion und muss sich sichtbar zu ihrer Verantwortung bekennen, alle vorgegebenen Sicherheitsregeln beachten und selbst an Schulungsveranstaltungen teilnehmen.

Die Verwaltungsspitze hat die Aufgabe, den Sicherheitsprozess zu initiieren, zu steuern und zu überwachen. Auch wenn die operative Umsetzung eines *Informationssicherheitsmanagementsystems* typischerweise an Informationssicherheitsbeauftragte (ISB) delegiert wird: **Die Gesamtverantwortung für die Informationssicherheit bleibt immer bei der Verwaltungsspitze.**[35]

Weiterführende Literatur:

Informationssicherheit für die Verwaltungsspitzen von Städten und Gemeinden
DST, DStGB, BSI, 2022
[DST22] (→ *Anhang 2*)

Informationssicherheit für Landrätinnen und Landräte – IT-Grundschutz in den Landkreisen
DLT, BSI, 2021
[DLT21] (→ *Anhang 2*)

[31] Siehe [ITV.SH24] (→ *Anhang 2*).

[32] Siehe [IBK24] (→ *Anhang 2*).

[33] Siehe [VdS24] (→ *Anhang 2*).

[34] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Alternative-IT-Grundschutztools/IT-Grundschutztools.html

[35] Siehe BSI-Standard 200-1, https://www.bsi.bund.de/dok/6603458.

5.1.3 Die Rolle von Informationssicherheitsbeauftragten (ISB)

Ungeachtet der Gesamtverantwortung der Verwaltungsspitze sollte in jeder Kommunalverwaltung eine oder ein ISB bestellt und ihr oder ihm die zur Erfüllung dieser Aufgabe notwendigen personellen und finanziellen Ressourcen bereitgestellt werden.

Es ist empfehlenswert, die Position der oder des ISB direkt der obersten Leitungsebene zuzuordnen (z. B. als Stabsstelle). Es sollte vermieden werden, Mitarbeitende aus dem *IT-Betrieb* zusätzlich mit dieser Aufgabe zu betrauen, da es hierbei zu Rollenkonflikten kommen kann. Die oder der ISB muss nicht zwingend eine ausgebildete IT-Fachkraft sein. Eine Person mit Koordinationsfähigkeit, Engagement, Durchsetzungsvermögen und Interesse für das Thema kann mit entsprechenden Schulungen diese Rolle wahrnehmen.

Die Informationssicherheitsbeauftragten sind für den Aufbau und die Aufrechterhaltung des Informationssicherheitsmanagements der Kommune zuständig. Sie prüfen daher anhand einer der oben aufgelisteten Standards oder Modelle, welche Sicherheitsanforderungen bereits erfüllt sind, und koordinieren die Umsetzung derjenigen Anforderungen, die noch nicht umgesetzt sind (bspw. durch den *IT-Betrieb).* Die Informationssicherheitsbeauftragen beraten die Leitung in allen Fragen der Informationssicherheit und unterrichten sie regelmäßig und anlassbezogen über den Stand der Informationssicherheit innerhalb der Kommune. Darüber hinaus sind die ISB bei allen Vorhaben der Kommune zu beteiligen, die die Informationssicherheit betreffen, auch bei Beteiligung von Dienstleistern. Die oder der ISB sollte ein unmittelbares Vortragsrecht bei der jeweiligen Leitung haben.

Exkurs zu Datenschutzerfordernissen:

Das Thema Datenschutz kann nach einem Cyberangriff erheblichen zeitlichen Aufwand bedeuten. Steht die Möglichkeit eines Datenabflusses im Raum, muss möglicherweise ad hoc und aus dem Gedächtnis rekonstruiert werden, welche Arten von Daten auf welchen Dateiverzeichnissen lagen und betroffen sein könnten.

Durch eine Zusammenarbeit mit den Datenschutzbeauftragten können sinnvolle vorbereitende Maßnahmen unter Berücksichtigung der landesspezifischen Datenschutzvorgaben identifiziert werden. Dazu können bspw. eine Erfassung der Speicherorte für personenbezogene Daten oder das regelmäßige Löschen nicht mehr benötigter Daten zählen. So kann der Umfang der potenziell abfließenden Datenmengen und damit der Aufwand im Ereignisfall erheblich gesenkt werden (siehe auch → *Anhang 4.5*).

Weiterführende Literatur:

BSI Online-Kurs IT-Grundschutz, Lerneinheit 2.4: Der Informationssicherheitsbeauftragte
BSI, 2024
https://www.bsi.bund.de/dok/10990432

5.1.4 Technische Maßnahmen

Es hätte in unserer fiktiven Stadt Rodenburg auch anders laufen können. Erinnern Sie sich zurück an den Tag, an dem Herr Schmidt, der Bürosachbearbeiter für Personalangelegenheiten, die Probleme mit seiner Arbeitsplatz-IT bemerkt (→ Kapitel 2.1):

„Der schmeißt mich ständig aus der Verbindung raus", beschwert sich Herr Schmidt am Telefon bei Frau Christina Seiler, Anwendungsbetreuerin aus dem IT-Bereich. In der Tat erscheinen Frau Seiler die Anmeldungen auf dem Konto von Herrn Schmidt merkwürdig. Auch das Intrusion Detection System meldet vermehrt fehlerhafte Loginversuche mit diesem Account und blockiert in der Firewall automatisiert die auffälligen IP-Adressen. Dank Zwei-Faktor-Authentisierung bleibt es jedoch beim Versuch, die Angreifer konnten sich mit Herrn Schmidts Nutzernamen und (wohl recht einfachem) Passwort keinen Zugriff auf das kommunale Netzwerk verschaffen.

Die Erfahrungen aus den vergangenen Vorfällen haben gezeigt, dass es neben den organisatorischen Maßnahmen zur Verbesserung der Informationssicherheit auch essenziell wichtige technische Maßnahmen und Best Practices gibt, durch deren Umsetzung die Informationssicherheit maßgeblich gesteigert und die Auswirkung eines Vorfalls gemindert werden kann.

Als besonders wertvoll für die Schadensbegrenzung haben sich regelmäßige Backups erwiesen. Wichtig ist, dass die Backups nicht nur erstellt, sondern auch getestet werden. Ein Backup, das sich nicht wieder einspielen lässt, ist leider nutzlos bei einem Datenverlust. Neben den aktuell weitverbreiteten Online-Backups sollten Backups auch offline vorgehalten werden, um eine Verschlüsselung der Backups im Falle eines *Ransomware*-Angriffs zu vermeiden.

Im besten Fall jedoch schaffen es die Angreifer gar nicht erst in das System einzudringen. Um hier die Hürden so hoch wie möglich zu legen, ist z. B. aktuelle Software mit den aktuellsten *Patches* unabdingbar.[36] So können Sicherheitslücken möglichst schnell geschlossen werden. Gleiches gilt auch für eine gut durchdachte Netzinfrastruktur mit *Netzsegmentierung* und durch *Firewalls* abgesicherte externe Zugänge sowie Netzüberwachung.

Arbeitshilfen und Checklisten zu den wichtigsten technischen Maßnahmen sind z. B. im Produkt WiBA des BSI zu finden.[37]

Aus der Praxis:
Was sollten Sie überprüfen, um es Angreifern schwer zu machen?

- Berechtigungs- und Passwortmanagement
- Mehrfaktor-Authentisierung
- *Patch*-Management
- Härtung von Systemen
- Backups
- *Netzsegmentierung*
- Protokollierung
- Ereigniserkennung (IDS)

5.1.5 Sensibilisierung der Mitarbeitenden

Die Mitarbeitenden sind ein Schlüsselfaktor in der Informationssicherheit, denn E-Mails oder manipulierte Webseiten stellen nach wie vor die häufigsten Infektionswege dar. **Die Sensibilisierung der Mitarbeitenden für einen angemessenen Umgang mit Gefährdungen ist elementar. Sie sollte allerdings niemals die einzige Maßnahme sein, sondern andere Maßnahmen ergänzen.** Dabei muss nicht gleich eine umfangreiche Sensibilisierungskampagne geplant werden. Bereits kleine Maßnahmen wie z. B. Rundmails, die in konkreten Gefährdungslagen auf spezifische *Phishing*-Mails hinweisen, ein Gespräch im Rahmen des Onboardings neuer Mitarbeitender

[36] Siehe [ACS18a] (→ *Anhang 2*).

[37] https://www.bsi.bund.de/dok/WIBA

oder ein TOP Informationssicherheit im Rahmen einer regelmäßigen Besprechung helfen schon weiter. Zur Sensibilisierung der Mitarbeitenden der Kommune stehen verschiedene **kostenfreie Angebote** zur Verfügung.

Die **BSI-Kampagne „einfach aBSIchern“** ist eine nationale Kampagne des Bundesamts für Sicherheit in der Informationstechnik und des Bundesministeriums des Innern und für Heimat (BMI) zur Steigerung der Informationssicherheit. Auf der Website der Kampagne[38] werden typische digitale Nutzungsszenarien aus der alltäglichen Lebenswelt thematisiert. Hierfür werden verschiedene Materialien (bspw. Bildmotive oder Webbanner) sowie Erklärvideos und Hilfsdokumente zum Download zur Verfügung gestellt (bspw. zum Thema Homeoffice). Die Kampagne richtet sich primär an Verbraucherinnen und Verbraucher, kann jedoch auch sehr gut behördenintern zur niedrigschwelligen Sensibilisierung der Mitarbeitenden genutzt werden.

Der **Werkzeugkasten Sensibilisierung** der Bundesakademie für öffentliche Verwaltung (BAköV) bietet einen Leitfaden zur Sensibilisierung in der öffentlichen Verwaltung, der grundsätzliche Informationen zur Entwicklung und Durchführung von Sensibilisierungskampagnen und -veranstaltungen enthält. Zudem enthält der Werkzeugkasten frei abrufbare Vorlagen, die in Kommunen zur Erstsensibilisierung genutzt werden können, bspw. Plakate, Flyer oder Schulungskonzepte. Weiterhin können die von der BAköV bereitgestellten Inhalte einfach und einsatzfertig in bereits bestehende oder noch einzuführende E-Learning-Plattformen importiert werden. Die Produkte des Werkzeugkastens werden im internen Bereich der BSI-Sicherheitsberatung bereitgestellt.[39]

Mit der 2012 gegründeten **Allianz für Cyber-Sicherheit** (ACS) steht Unternehmen, Verbänden, Behörden und Organisationen eine kooperative Plattform zur Verfügung, über die Informationen zu aktuellen Bedrohungslagen und praxisnahe Cybersicherheitsmaßnahmen ausgetauscht werden. Teilnehmende erhalten kostenfreien Zugang zu umfangreichen Materialien, Informationen und Angeboten der anderen Mitglieder, u. a. auch zur Sensibilisierung, und können so den Schutz der eigenen IT-Infrastruktur deutlich verbessern. Die Mitgliedschaft ist kostenlos.[40]

Die **Cyberfibel** wird vom BSI in Zusammenarbeit mit „Deutschland sicher im Netz“ (DsiN) herausgegeben und richtet sich primär an Verbraucherinnen und Verbraucher, kann aber aufgrund des Umfangs und der Methodik auch für eine niedrigschwellige behördeninterne Sensibilisierung genutzt werden. Die Cyberfibel ist ein leicht verständliches Handbuch und Nachschlagewerk zur Wissensaneignung und -vermittlung rund um das Thema Cybersicherheit.[41]

Das **„Behörden-IT-Sicherheitstraining“** (BITS) ist ein kostenloses Web-Training zur Information und Sensibilisierung von Mitarbeitenden an IT-Arbeitsplätzen in Verwaltungen. Es informiert zu neun verschiedenen Themenbereichen (z. B. E-Mail oder Passwörter) und stellt zum Kapitelabschluss jeweils entsprechende Quizfragen. Das BITS kann entweder direkt online genutzt[42] oder über die Plattform GitHub heruntergeladen und lokal im Intranet den Mitarbeitenden der Kommune zur Verfügung gestellt werden. Es wird von der Kommunal Agentur NRW GmbH und dem Landesbetrieb Verkehr, Hamburg, herausgegeben und steht unter der Schirmherrschaft des Städte- und Gemeindebundes NRW e. V.

Die **Forschungsgruppe Security, Usability, Society** (SECUSO) des Karlsruher Instituts für Technologie (KIT) stellt verschiedene Sensibilisierungsmaterialien und Tools für Bürgerinnen und Bürger sowie kleine und mittlere Unternehmen zur Verfügung, bspw. Flyer, Erklärvideos,

[38] https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/kampagne_node.html

[39] https://www.bsi.bund.de/DE/Intern/Sicherheitsberatung/LandKommune/Werkzeugkasten_Sensi_BAkoeV/erkzeugkasten_Sensi_BAkoeV_node.html Vorherige Anmeldung für den internen Bereich der Sicherheitsberatung für Länder und Kommunen unter https://www.bsi.bund.de/dok/SicherheitsberatungLK-Intern notwendig.

[40] Siehe [ACS] (→ *Anhang 2*).

[41] Siehe [DSiN21] (→ *Anhang 2*).

[42] Siehe [BITS24] (→ *Anhang 2*).

Online-Games/-Quiz, Add-ons für Browser oder Schulungsunterlagen.[43]

Im Projekt **„Dialog für Cyber-Sicherheit“** treten die organisierte Zivilgesellschaft[44], Vertreterinnen und Vertreter aus Wissenschaft, Kultur und Medien, Wirtschaft und Staat untereinander sowie mit dem BSI in einen intensiven Austausch. In verschiedenen Workstreams werden unterschiedliche Konzepte und Materialien erarbeitet. Unter anderem wurde der Leitfaden „Effektive IT-Security-Awareness: Wirksam ein Bewusstsein für Risiken schaffen“ erstellt[45]. Er bietet einen Fünf-Schritte-Plan für die Entwicklung und Evaluation von Sensibilisierungsmaßnahmen in einer Institution.

Auch in der allerersten Phase des Ransomware-Angriffs hätte es in der fiktiven Stadt Rodenburg anders laufen können – wenn Herr Schmidt beim Öffnen des Dialogfensters etwas skeptischer gewesen wäre (→ Kapitel 2.1):

Auf seinem Bildschirm erscheint ein Hinweis dort, wo eigentlich der Inhalt stehen sollte: „Dieses Dokument wurde mit einer älteren Programmversion erstellt, bitte klicken Sie auf Bearbeitung aktivieren, um den Kompatibilitätsmodus zu starten.“

Waren solche Meldungen nicht neulich in der IT-Sicherheitsschulung vorgekommen? Herr Schmidt ist sich unsicher und ruft lieber die Hotline an, um nachzufragen, ob er das nun wegklicken darf oder nicht. Dieses Vorgehen hatten sie doch explizit empfohlen, daran kann er sich deutlich erinnern.

Nach einer Prüfung des Dokuments meldet die IT zurück, dass es sich tatsächlich um Schadsoftware gehandelt habe. „Puh“, denkt sich Herr Schmidt. „Gut, dass ich daran gedacht habe …“

Weiterführende Literatur:

Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen
AG Handreichung ISLL, Version 3.0, 2024
[AGISLL24] (→ *Anhang 2*)

In dieser Handreichung werden neben konzeptionellen und inhaltlichen Vorschlägen zur Erstellung einer eigenen Informationssicherheitsleitlinie auch praxisnahe Empfehlungen zum Aufbau und Betrieb eines ISMS ausgearbeitet. Aufgrund des spezifischen Adressatenkreises stellt das Dokument eine hervorragende Grundlage für Kommunen zur initialen Befassung mit der Informationssicherheit dar.

[43] Siehe [KIT24] (→ *Anhang 2*).

[44] Die organisierte Zivilgesellschaft umfasst die Gesamtheit des Engagements der Bürgerinnen und Bürger eines Landes z. B. in Vereinen, Stiftungen, Verbänden, Initiativen oder sozialen Bewegungen. Dazu gehören alle Aktivitäten, die nicht profitorientiert und frei von parteipolitischen Interessen sind.

[45] Siehe [BSI24] (→ *Anhang 2*).

5.2 Planungen für den IT-Notfall

Es ist sicherlich die beste Option, wenn *IT-Notfälle* oder *-Krisen* gar nicht erst eintreten. Deren Eintrittswahrscheinlichkeit so weit wie möglich zu reduzieren, ist daher von zentraler Bedeutung (→ *Kapitel 5.1*). Dennoch verbleibt auch bei bester technischer Vorbereitung wie bei anderen Schadensereignissen ein Restrisiko, sodass man sich auch auf einen folgenreichen Cyberangriff oder andere große IT-Vorfälle vorbereiten muss. Dadurch kann die Schwere des Schadens bzw. die Dauer konkreter Beeinträchtigungen verringert werden. Es sollten organisatorische Vorbereitungen getroffen und die Bewältigung geplant sein, um einen schnellen Notbetrieb wiederherstellen zu können.

Vergangene Vorfälle zeigen, dass selbst bei einer rein präventiven Abschaltung des internen Netzwerks mindestens ein halber Tag für den Wiederanlauf eingerechnet werden muss. Bei einer vollständigen Kompromittierung inkl. Verschlüsselung ist von mehreren Monaten auszugehen, bis der *IT-Betrieb* zumindest weitgehend wiederhergestellt ist. Angesichts dessen ist jede Möglichkeit der Beschleunigung hilfreich.

Im folgenden Unterkapitel wird daher skizziert, welche Vorbereitungen getroffen werden können, um auch bei weitreichenden Ausfällen der IT die Aufrechterhaltung der wichtigsten Dienstleistungen gewährleisten und den Normalzustand schnellstmöglich wiederherstellen zu können. Dazu werden zunächst Aspekte der Bewältigungsorganisation behandelt (→ *Kapitel 5.2.1*), bevor die verschiedenen Eskalationsstufen *Störung, IT-Notfall und IT-Krise* und ein damit verbundenes Meldewesen näher beschrieben werden (→ *Kapitel 5.2.2*). Für kommunale Verwaltungen sind insbesondere die eingesetzten Fachanwendungen von großer Bedeutung, ohne die der Geschäftsbetrieb stark eingeschränkt wird. Deren Bestandsaufnahme und mögliche Priorisierungsansätze sind Gegenstand von → *Kapitel 5.2.3*. Da bei längerer Vorfalldauer zunächst ein Notbetrieb der wichtigsten Dienstleistungen etabliert werden muss, führt → *Kapitel 5.2.4* einige dafür im Vorfeld zu klärende Aspekte auf. Vorbereitungen in der Krisenkommunikation stellen sicher, dass die Öffentlichkeit zeitnah und korrekt über den IT-Vorfall in Kenntnis gesetzt wird (→ *Kapitel 5.2.5*). Schließlich wird die Wichtigkeit von Übungen hervorgehoben, die bei allen Beteiligten eine gewisse Routine für die Abläufe in den Ausnahmesituationen *IT-Notfall* oder *-Krise* schaffen (→ *Kapitel 5.2.6*).

Es werden in diesem Kapitel grundsätzlich Planungen für den *IT-Notfall* dargelegt. Diese sind jedoch gleichermaßen für *IT-Krisen* anwendbar. Durch das größere Ausmaß und die zumindest teilweise nicht ausreichenden Notfallpläne (Definitionen in → *Kapitel 5.2.2*) sind bei der *IT-Krise* Abweichungen bezüglich der Vorbereitungen insbesondere aufgrund der längeren Bewältigungsdauer (Durchhaltefähigkeit), des Ressourcenmehrbedarfs und größeren Kreises betroffener Stellen zu erwarten. Hinzu kommt eine größere Notwendigkeit, bei fehlenden Vorfestlegungen weitreichende Entscheidungen zu treffen.

5.2.1 Notfall- und Krisenorganisation

Kernpunkte:

- Enge Zusammenarbeit zwischen *kommunalem Verwaltungsstab* und *IT-Betrieb* ist essenziell.
- Die Rolle des IT-Dienstleisters bei größeren IT-Vorfällen muss ggf. im Vorfeld geklärt werden.
- In jedem Fall verbleibt die Verantwortung für die Notfallorganisation und das Etablieren von Einsatzstrukturen bzw. Verwaltungsstäben vollständig bei der Kommune.
- Eine aktuell gehaltene, netzunabhängige Verfügbarkeit der wichtigsten Informationen und Vorbereitungen ist entscheidend.

In Rodenburg konnte die IT-Krise nicht verhindert werden (→ Kapitel 2.1):

Sämtliche Arbeitsplätze und Fachanwendungen der Kommune stehen nicht mehr zur Verfügung. Bürgermeisterin Wirth ruft den Krisenstab zusammen, während Herr Jäger die Landesbehörden informiert.

Ohne existierenden Notfallplan muss nun unter Hochdruck und quasi ohne Informationen mit der Wiederherstellung zumindest der wichtigsten Dienstleistungen begonnen werden. Der Ausfall der IT-Systeme macht dabei nicht nur die eigentliche Arbeit der Mitarbeitenden unmöglich, sondern erschwert auch die Arbeit des Krisenstabs, da kein Zugriff auf bspw. Personallisten erfolgen kann und noch immer die Telefone nicht funktionieren. Glücklicherweise gelingt die Kommunikation der Führungsebene über dienstliche Handys oder private Erreichbarkeiten. Der Stab beginnt die Prozesse und Fachverfahren der Kommune zu priorisieren, um einen Notbetrieb der wichtigsten Dienstleistungen sicherzustellen.

Zur Vorbereitung auf Situationen, die mit der normalen Arbeits- und Ablauforganisation nicht mehr bewältigt werden können, sollten grundsätzlich Stabsstrukturen und Prozesse definiert und in einem Krisenmanagement- bzw. Notfallhandbuch festgehalten werden.

Oftmals sind entsprechende Strukturen lange etabliert, in Bezug auf andere Situationen wie Starkregen, Waldbrand oder größere Unfälle bereits eingeübt, weitere Szenarien zumindest vorgedacht (bspw. Stromausfall → *Anhang 4.1*). IT-Vorfälle hingegen fallen regelmäßig nicht in den Erfahrungsbereich der kommunalen Verwaltungsstäbe und Ansprechpersonen für das Notfall- bzw. behördliche Krisenmanagement.[46] Sie sollten aber unter der Maßgabe des *All-Gefahren-Ansatzes* in jedem Fall mitbedacht werden, schließlich können diese Situationen erhebliche Belastungen und Zeitdruck hervorrufen.[47] Sie müssen zudem in der Regel im Fokus der Öffentlichkeit bewältigt werden, denn die Auswirkungen bleiben nicht auf die Verwaltung beschränkt.

Cyberangriff – kein reines IT-Szenario

IT-Vorfälle sind ein spezifisches Szenario unter vielen, die im Rahmen der allgemeinen Notfallplanung adressiert werden. Es handelt sich mitnichten um ein „reines IT-Thema", sondern ist für die allgemeine Notfall- und Krisenorganisation der Kommune sehr relevant[48]: Bei einem größeren Cyberangriff geht es neben dem technischen IT-Notfallmanagement, das durch IT-Mitarbeitende bzw. den IT-Dienstleister umgesetzt wird, auch um allgemeinere Fragestellungen des Krisenmanagements (→ *Kapitel 3.1*). Diese reichen von der Priorisierung einzelner Bereiche und Aufgaben für Notbetrieb und Wiederherstellung bis hin zur Gesundheitsfürsorge für das Personal. Gerade dieser Punkt ist nicht zu unterschätzen: Die Mitarbeitenden werden möglicherweise Konflikten im direkten Kontakt mit der Bevölkerung und lokal ansässigen Unternehmen ausgesetzt. Je nach Arbeitsbereich kommt es zu extremer Mehrarbeit und Stress bis hin zur völligen Erschöpfung – oder aber zu signifikanter Unterbeschäftigung aufgrund wegfallender Arbeitsmittel. Erzwungene Untätigkeit auf der einen, sichtbare Überlastung auf der anderen Seite, gepaart mit kritischer Berichterstattung und offensiver Suche nach Schuldigen kann individuell und auf organisatorisch-institutioneller Ebene extreme Belastungen hervorrufen. Problematisch sind bei einem solchen Vorfall vor allem die erwartbar langen Ausfallzeiten, auf die sich alle einstellen müssen. Die Bewältigung ist also nicht allein eine Aufgabe der IT-Mitarbeitenden oder

[46] Hiermit ist die Person oder zentrale Stelle gemeint, die sich um die Vorplanung und das In-Übung-Halten für Notfälle und Krisen kümmert. In der Regel sind hierfür auch die Bezeichnungen *BCM*-Beauftragte oder Krisenmanagement-Beauftragte gebräuchlich.

[47] Der Sprachgebrauch im Hinblick auf allgemeine Regelungen für physische Gefahren und IT-spezifisch gebräuchliche Vorkehrungen (bspw. nach BSI-Standard 200-4) unterscheidet sich oft. Die notwendige gesamtheitliche Resilienz einer Kommunalverwaltung nach einem *All-Gefahren-Ansatz* kann allerdings nur durch ein gutes Zusammenspiel zwischen Zivil- und Katastrophenschutz, Notfall- bzw. behördlichem Krisenmanagement und Informationssicherheit gelingen. Die unterschiedlichen Wordings dürfen dem nicht im Wege stehen. Daher sollten alle Beteiligten mit der nötigen Sensibilität für dieses Thema vorgehen!

[48] Dies gilt insbesondere für die Ansprechpersonen für das Notfall- bzw. behördliche Krisenmanagement.

gar des IT-Dienstleisters. All diese nicht technischen Aspekte müssen im Sinne eines ganzheitlichen Resilienzansatzes schon in der Vorbereitung bedacht werden, um im Ereignisfall schnell und umfassend handlungsfähig zu sein.

Die Bewältigung erfordert ein Zusammenspiel vieler verschiedener Akteure, die mit ihren fachlichen Hintergründen jeweils eigene Aufgabenpakete zu erledigen haben: Neben der Verwaltungsspitze, regelmäßigen Mitgliedern des *Verwaltungsstabes* und Ansprechpersonen für das Notfall- bzw. behördliche Krisenmanagement gehören dazu auch IT-Verantwortliche bzw. der *IT-Betrieb* sowie ggf. weitere *Stakeholder* wie Dienstleister oder Landesbehörden. Oft gibt es unterschiedliche Vorstellungen oder sogar Missverständnisse bezüglich der Aufgabenverteilung und wechselseitigen Verantwortlichkeiten, Fähigkeiten und Bedarfe im *IT-Notfall*. Diese können durch aktive, szenariobezogene Notfallplanungen im Vorfeld abgebaut und dadurch im *IT-Notfall* vermieden werden. In diesem Rahmen können sowohl bei Ansprechpersonen für das Notfall- bzw. behördliche Krisenmanagement als auch im *IT-Betrieb* Personen identifiziert werden, die sich der Verantwortung für die Verzahnung von IT-Notfallmanagement und allgemeiner Notfallplanung aktiv annehmen.

Stabsstrukturen in IT-Notfällen

Im besten Fall kann man in *IT-Notfällen* auf bereits bestehende Krisenmanagementstrukturen des *Verwaltungsstabes* als administrativ-organisatorische Komponente zurückgreifen. Diese sind geeignet, umfassende verwaltungstypische Entscheidungen schnell, ausgewogen und unter Beachtung aller notwendigen Gesichtspunkte zu treffen. Mit dem Einberufen des *Verwaltungsstabs* wird sowohl der Zeitdringlichkeit als auch dem ungewöhnlichen Maß an Koordinations- und Entscheidungsbedarf in der Aufgabenerledigung Rechnung getragen. Gerade wenn verschiedene Ämter bzw. Behörden betroffen sind und koordiniert zusammenarbeiten müssen oder wenn eine Vielzahl unterschiedlicher Informationen zu bewerten sind, um auf ihrer Grundlage zu abgestimmten Entscheidungen zu kommen, ist der Einsatz eines *Verwaltungsstabes* zweckmäßig.[49,50] Bei der Festlegung ereignisspezifischer Mitglieder für den *Verwaltungsstab* ist auf eine angemessene Einbindung von *IT-Betrieb* sowie ggf. IT-Dienstleistern oder IT-Fachberatern zu achten. Aus einer Bestandsaufnahme der Fachanwendungen (→ *Kapitel 5.2.3*) können sich weitere ereignisspezifisch einzubindende Mitglieder für den *Verwaltungsstab* ableiten lassen.

Eine besondere Schwierigkeit bei *IT-Notfällen* ist die Fülle und Vielfalt sehr technischer Fragestellungen. Sowohl ein direkter Austausch des Fachpersonals untereinander als auch eine direkte Anbindung an die Amtsleitungen mit entsprechender Entscheidungskompetenz sind notwendig und müssen in den Arbeitsstrukturen abgebildet werden. Grundsätzlich widmet sich der *Verwaltungsstab* auf Basis geeigneter Vorlagen ausschließlich strategischen Entscheidungen, z. B. zur Priorisierung von Fachverfahren (→ *Kapitel 5.2.3*) oder zur Auswahl der IT-Sicherheitsdienstleister. Der Stab führt **keine** Detaildiskussionen. Das bedeutet: Die Lösungen bzw. ggf. mehrere Optionen, über die zu entscheiden ist, müssen bereits bei der Erstellung der Beschlussvorlagen für die Stabsbesprechung durch die fachlich zuständigen Bearbeitenden formuliert werden.

Die Einbindung der verschiedenen Stellen sollte in Übungen getestet werden (→ *Kapitel 5.2.6*).

Social-Media-Monitoring als Informationsquelle

Es ist fest davon auszugehen, dass die Folgen eines schweren IT-Vorfalls auch außerhalb der Verwaltung nicht unbemerkt bleiben: Die Schnittstellen nach außen sind vielfältig und wenn etwas nicht funktioniert, fällt es auf. Schnell finden die Informationen darüber auch den Weg in eine größere Öffentlichkeit. Noch bevor die Lokalpresse berichtet, sind die ersten

[49] Siehe AK V der Innenministerkonferenz: „Hinweise zur Bildung von Stäben der administrativ-organisatorischen Komponente (Verwaltungsstäbe – VwS)“ (2004), https://lernplattform-babz-bund.de/goto.php?target=file_110653_download&client_id=BBKILIAS.

[50] Auch kleinere Verwaltungsstrukturen, die oftmals über keine besonderen Aufbauorganisationen oder Stäbe im Not- bzw. Krisenfall verfügen, sollten sich ihren Kapazitäten entsprechend bemühen, Krisenmanagementstrukturen zu etablieren und im Rahmen der jeweiligen Organisationsstruktur Möglichkeiten zu schaffen, um in solchen Fällen adäquat reagieren zu können.

Posts in den sozialen Netzwerken zu finden. Generell kommt daher dem Monitoring von Informationskanälen Dritter, insbesondere von Social Media, eine stetig steigende Bedeutung zu. Dieses findet in der Regel im Bereich der Pressestäbe statt (→ *Kapitel 5.2.5*), denn oft muss die Verwaltung in ihrer eigenen Krisenkommunikation auf das Geschehen in unterschiedlichen Social-Media-Kanälen reagieren, nutzt hierzu eben diese Kanäle und greift in öffentliche Debatten ein. Hierdurch kann zum einen die Hoheit über kursierende Informationen behalten oder zurückerlangt und eine größere Öffentlichkeit erreicht werden.

Allerdings können die geposteten Nachrichten auch wichtige Erkenntnisse für die Arbeit des *Verwaltungsstabes* liefern: Wurde vielleicht eine Problemstellung übersehen, die nun zutage getreten ist? Wo muss nachgesteuert werden? Die Meldungen in den sozialen Netzwerken sind damit nicht ausschließlich für die Presse- und Öffentlichkeitsarbeit relevant, sondern auch eine Informationsquelle für die Stabsarbeit. Eine enge Einbindung des Social-Media-Monitorings in die Stabsstruktur ist daher essenziell.

Einbindung der IT-Dienstleister

Die verbreitete Übertragung von Aufgaben im *IT-Betrieb* an IT-Dienstleister – sei es lediglich die Betreuung einzelner Fachanwendungen oder der vollständige Betrieb mit Wartung und Aufrechterhaltung – ersetzt nicht die eigene kommunale Planung für *IT-Notfälle*. Die Verantwortung für die Notfallorganisation und das Etablieren von Einsatzstrukturen bzw. Verwaltungsstäben verbleibt vollständig bei der Kommune. Auch Entscheidungen zu Finanzierung und Priorisierung im Ereignisfall können nicht an den IT-Dienstleister abgegeben werden.

Um diese Entscheidungen vorzubereiten, bedarf es einer engen Abstimmung mit dem IT-Dienstleister. Die wechselseitigen Verantwortlichkeiten, Fähigkeiten und Bedarfe müssen im Vorfeld geklärt werden. Selbst Aufgaben des unmittelbaren IT-Notfallmanagements werden nicht unbedingt vom IT-Dienstleister übernommen. Verträge, die verpflichtende Hilfe des IT-Dienstleisters bei Cybernotfällen enthalten, sind eher selten und relativ kostenintensiv. Dennoch halten manche IT-Dienstleister Räume und IT-Infrastruktur für ihre Kundenkommunen vor, die im Falle eines möglichen vollständigen Systemausfalls genutzt werden können. Andere unterstützen auch durch ein eigenes *Computer Emergency Response Team (CERT)*. Die Möglichkeiten und Limitationen der Unterstützung durch den IT-Dienstleister in der Ereignisbewältigung müssen im Vorfeld abgeklärt werden, um in einer Akutphase keine zusätzlichen Stolpersteine durch falsche Erwartungshaltungen zu generieren.

Das in der Regel vorhandene IT-Notfallmanagement der jeweiligen IT-Dienstleister sollte strukturell eng an die politisch-administrative Entscheidungsebene angebunden werden. Häufig empfiehlt sich hier eine direkte Einbindung über Fachberater bzw. Verbindungspersonen in die kommunalen Stabsstrukturen. So kann der Stab eine zielgerichtete Steuerung der IT-Dienstleister gewährleisten und den Fortschritt der getroffenen Maßnahmen besser nachverfolgen.

Das Handbuch IT-Notfallmanagement

Sind Verantwortlichkeiten, Bedarfe und Fähigkeiten auch für IT-Vorfälle geklärt, müssen daraus geeignete Krisenbewältigungsstrukturen abgeleitet werden. Alles zusammen wird in einem Handbuch IT-Notfallmanagement oder einem Anhang zum allgemeineren Handbuch Krisenmanagement bzw. Notfallhandbuch festgehalten. Diese Schritte obliegen den Ansprechpersonen für das Notfall- bzw. behördliche Krisenmanagement. So befinden sich alle Informationen zur Notfallbewältigung an einer zentralen Stelle und können bei einem IT-Vorfall schnell aufgefunden und eingesehen werden.

Das Handbuch sollte darüber hinaus noch Informationen zu den weiteren Vorplanungen enthalten, bspw.:

- die konkret in *IT-Notfällen* notwendige Besetzung des *Verwaltungsstabes*,
- Kontakt- und Alarmierungslisten (Mitarbeitende, Dienstleister, mögliche externe Unterstützung),

- für den *Notfall* vorbereitete Infrastruktur und Ressourcen (→ *Kapitel 5.2.4*)[51],
- Meldepflichten samt Mustern für Meldebögen oder Lageberichte,
- Vorlagen für die Krisenkommunikation (mindestens für Erstmeldungen, → *Kapitel 5.2.5*),
- Wiederanlaufplan ggf. inkl. einer Priorisierung (→ *Kapitel 4* und → *Kapitel 5.2.3*),
- ggf. Vorlagen zur analogen Durchführung von Fachverfahren.

In den bisherigen Ausführungen wurde ein Cyberangriff auf die Kommunalverwaltung selbst zugrunde gelegt. Es ist allerdings auch wichtig, das Szenario eines möglicherweise kompromittierten Kommunikationspartners mitzudenken und in das Handbuch zu integrieren: Kommunen haben bei vielen Fachverfahren technische Schnittstellen zu Partnern. Es werden – teils automatisiert – Daten angefragt, abgeglichen und ausgetauscht, Übersichten oder Sachstände gemeldet oder entgegengenommen. Ist ein solcher Partner von einem Cyberangriff betroffen, müssen Maßnahmen zum Eigenschutz erfolgen. In der Regel werden in einem solchen Fall Kommunikationsverbindungen gekappt. Es sollte daher festgehalten werden, welche Verbindungen zu den jeweiligen Partnern ganz konkret bestehen. Dazu sollte im Handbuch auch formuliert werden, welche Bedingungen durch einen betroffenen Partner konkret zu erfüllen sind, bevor die direkte Kommunikation auf den zuvor etablierten Kanälen wieder aufgenommen wird.

Ganz wichtig: Es muss eine vom internen Netzwerk unabhängige Version des Handbuchs IT-Notfallmanagement sowie ggf. mitgeltender Unterlagen existieren. Sonst können die Mitarbeitenden in dem Moment, wenn es am dringendsten gebraucht wird, nicht darauf zugreifen. Gehen Sie davon aus, dass in einem solchen Moment die an das Netzwerk angeschlossene IT vollständig abgeschaltet werden muss! Die wichtigsten Informationen sollten in einem Notfallordner entweder auf Papier oder auf einem nicht im internen Netz befindlichen („Stand-alone"-)Notfallnotebook vorgehalten werden. Neben den spezifisch für den *Notfall* vorbereiteten Unterlagen sind dabei insbesondere grundlegende Informationen zur IT selbst vonnöten: der Netzwerkplan und ein technisches Wiki bzw. Anleitungen, IT-Konfigurationen und Hardwareanforderungen für die Wiederherstellung. Dabei wird zwingend ein geeigneter Prozess benötigt, um diese netzwerkunabhängig vorgehaltenen Informationen auf dem aktuellsten Stand zu halten.

Denken wir zurück an unsere fiktive Stadt Rodenburg (→ Kapitel 2.1), bei der die technische Vorbereitung eine vollständige Verschlüsselung der IT-Systeme nicht verhindern konnte. Sämtliche Arbeitsplätze und Fachanwendungen der Kommune stehen nicht mehr zur Verfügung.

Eine gute Vorbereitung auf eine mögliche Krisenbewältigung macht jetzt den entscheidenden Unterschied und ändert den weiteren Verlauf:

Bürgermeisterin Wirth ruft den Krisenstab zusammen, während Herr Jäger die Landesbehörden informiert.

Dank des aktuell gehaltenen Notfallnotebooks können die vorbereiteten Alarmierungslisten abgearbeitet werden. Fachberater für den Krisenstab werden einberufen, Kontakt zum IT-Dienstleister wird hergestellt. Während der IT-Betrieb den Vorfall analysiert, werden die vorbereiteten Notfallarbeitsplätze in Betrieb genommen. So können Wiederanlaufplan und Priorisierungen überprüft, vorbereitete Pressemeldungen befüllt und Hinweiszettel für die Bevölkerung hergestellt werden. Zum Dienstbeginn am Montag herrscht hektischer, aber sortierter Betrieb im Krisenstab und das Anlaufen eines Notbetriebes ist bereits auf den Weg gebracht.

[51] Es ist ratsam, mehrere vom Netz abgetrennte Notebooks oder Laptops und Handys als Arbeitsmittel für den *IT-Notfall* vorzuhalten und die Räumlichkeiten für die Arbeit im *IT-Notfall* zu bestimmen. Im Handbuch sollten sowohl der Standort der Geräte mit Zugangsdaten als auch die Räumlichkeiten festgehalten werden. So ist gewährleistet, dass die Infrastruktur in der ersten Bewältigungsphase direkt vorhanden ist.

Weiterführende Informationen:

Lernplattform Krisenmanagement
BBK (BABZ), 2021
https://lernplattform-babz-bund.de/goto.php?target=cat_110277&client_id=BBKILIAS

Die Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung (BABZ) bietet im Rahmen des kostenfreien, jederzeit online verfügbaren Lernangebots ein Modul zum Krisenmanagement an. Dieses vermittelt einen Überblick über Organisationsformen, Strukturen und Prozesse im Krisenmanagement. Es enthält zudem ein Muster-Krisenmanagement-Handbuch, das unter Beachtung der örtlichen Gegebenheiten und der lokalen bzw. landesrechtlichen Regelungen als Grundlage für eigene Planungen dienen kann.

Veranstaltungsangebot der BABZ
https://www.bbk.bund.de/DE/Themen/Akademie-BABZ/BABZ-Angebot/Veranstaltungen/veranstaltungen_node.html

Die BABZ bietet zusätzlich zum jederzeit online verfügbaren Lernangebot Seminare zum Risiko- und Krisenmanagement für kreisangehörige Städte und Gemeinden, für Kreise bzw. kreisfreie Städte, für Regierungsbezirke und auch für Landes- und Bundesbehörden an. Ziel ist die Förderung der Handlungskompetenz im Krisenmanagement sowie die Identifizierung des Handlungsbedarfs der jeweiligen Gebietskörperschaft. Die Kosten für Veranstaltungen der BABZ werden weitestgehend vom Bund getragen.

Weiterführende Literatur:

Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement
BMI, 2011
https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi-schutz-kritis-risiko-und-krisenmanagement.pdf?__blob=publicationFile&v=12
Dieser Leitfaden bietet das Handwerkszeug, um ein Risiko- und Krisenmanagement in Einrichtungen aufzubauen oder bestehende Planungen und Strukturen zu ergänzen. Er ist auch auf (insbesondere größere) Kommunalverwaltungen anwendbar.
Einmal jährlich wird an der BABZ eine Schulung zu diesem Leitfaden angeboten.

Hilfsmittel zum BSI-Standard 200-4
BSI, 2023
https://www.bsi.bund.de/dok/200-4-hilfsmittel

Der modernisierte BSI-Standard 200-4 bietet verschiedene Hilfsmittel und Dokumentvorlagen an, die bei der effektiven Umsetzung unterstützen sollen. Sie können teilweise losgelöst vom BSI-Standard 200-4 eingesetzt werden. Es finden sich dort bspw. eine Vorlage eines Notfallhandbuchs inkl. Beispieltexten als auch die „Weiterführenden Aspekte zur Bewältigung“, die sich insbesondere mit Stabsarbeit, aber auch dem Sonderfall IT-Krisenmanagement befassen.

5.2.2 Meldewege und Eskalationsstufen

Der folgende Abschnitt skizziert die Eskalationsstufen eines Vorfalls – von der *Störung* bis hin zur *IT-Krise*. Für jede Stufe werden mögliche Meldewege und organisatorische Maßnahmen aufgelistet, die selbstverständlich um weitere, den örtlichen Gegebenheiten angepasste Punkte erweitert werden sollten (z. B. um landesrechtlich vorgegebene Meldewege).

Einrichtung einer Meldestelle

Für die erfolgreiche Bewältigung eines Vorfalls ist ein schneller und geeigneter Informationsfluss essenziell: Melde- und Alarmierungswege sollten eindeutig festgelegt, in das Handbuch IT-Notfallmanagement (→ *Kapitel 5.2.1*) aufgenommen und entsprechend kommuniziert werden.

Wir empfehlen die Einrichtung einer zentralen Meldestelle, die rund um die Uhr erreichbar ist. In Kommunen könnte dies bspw. über ein Bereitschaftshandy organisiert werden, das von Mitarbeitenden des *IT-Betriebs* mitgeführt oder – nach einer spezifischen Schulung – an bereits etablierte Bereitschaftsdienste übergeben werden könnte. Die Meldungen sollten in einem zuvor festgelegten Format erfolgen, um sicherzustellen, dass alle für die Erstbewertung erforderlichen Informationen enthalten sind. Dazu gehören:

- Zeitpunkt und Ort des Ereignisses,
- meldende Person oder Stelle,
- eventuell betroffene Personen, Bereiche oder Prozesse,
- mögliche Ursache oder Auslöser sowie
- die aktuellen Auswirkungen.

Dazu kann bspw. eine IT-Notfallkarte (Abbildung 3), die an den Arbeitsplätzen aushängt oder im Homeoffice mitgeführt wird, herangezogen werden. Sie benennt die ständig erreichbare Meldestelle und gibt Hinweise zu benötigten Informationen sowie sinnvollen weiteren Schritten.

Abbildung 3: Vorlage für die IT-Notfallkarte des BSI[52]

Definition von Eskalationsstufen

Der *IT-Betrieb* bzw. die Meldestelle kann dann basierend auf den übermittelten Informationen eine erste Lageeinschätzung vornehmen. Auf Basis von im Vorhinein festgelegten Schwellwerten sollte der Vorfall eindeutig eingestuft werden, um im weiteren Verlauf die notwendigen Eskalations- und Meldewege ableiten zu können. Je nach Qualifikation sollten der Meldestelle entsprechend eindeutige Entscheidungshilfen an die Hand gegeben werden, um zu bestimmen, welche Eskalationsstufe vorliegt. Hierfür eignen sich Checklisten mit Kriterien, auf deren Basis eine nachvollziehbare und gut dokumentierbare Entscheidung zur Einstufung des Ereignisses getroffen werden kann.

Ein beispielhaftes Eskalationsstufenmodell ist in Tabelle 1 dargestellt. Es orientiert sich am

[52] Siehe https://www.bsi.bund.de/dok/13035678.

BSI-Standard 200-4[53]. Im Rahmen dieses Wegweisers werden die Begrifflichkeiten *Störung, IT-Notfall* und *IT-Krise* durchgängig im nachfolgend erläuterten Sinne verwendet. Diese **Festlegung auf Begriffe ist notwendig**, weil viele abweichende Begriffe und Definitionen gebräuchlich sind. In unterschiedlichen Fachcommunitys hat sich für verwandte und teils sehr ähnliche Sachverhalte oft ein spezifisches Vokabular etabliert. Umgekehrt werden zuweilen dieselben Begriffe verwendet, um unterschiedliche Sachverhalte zu beschreiben – der „Notfall" bedeutet z. B. im Rettungswesen etwas vollkommen anderes als im IT-Bereich. In der Kommunalverwaltung arbeiten Menschen mit ganz unterschiedlichen Hintergründen in vielfältigen Arbeitsbereichen. Im Alltag ist das selten ein Problem, aber es gilt zu verhindern, dass sie in der Lagebewältigung aneinander vorbeireden und Missverständnisse entstehen. Es ist daher sehr wichtig, dass die Begrifflichkeiten unabhängig vom konkreten Szenario einheitlich definiert und verwendet werden. Dabei sind die lokalen Gegebenheiten und insbesondere der Kontext landesrechtlicher Festlegungen maßgeblich.

Tabelle 1: Beispielhaftes Eskalationsstufenmodell nach BSI-Standard 200-4

Eskalationsstufe			Definition
1	Grau	Normalbetrieb	–
2	Gelb	Störung	Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen. Sie kann in der Regel innerhalb des Normalbetriebs behoben werden.
3	Orange	IT-Notfall	Nicht tolerable Unterbrechung mindestens eines zeitkritischen Geschäftsprozesses, für deren Bewältigung geeignete Notfallpläne vorliegen oder adaptiert werden können.
4	Rot	IT-Krise	Erhebliche Unterbrechung mindestens eines (zeit-)kritischen Geschäftsprozesses, für deren Bewältigung keine Notfallpläne vorliegen bzw. nicht ausreichend greifen.

Wie sieht der Eskalationsweg in unserer fiktiven Stadt Rodenburg aus? Zu Beginn der Entwicklungen ist noch nicht viel zu ahnen:

Bürosachbearbeiter Schmidt aus dem Personalbereich ruft die Hotline an, um wiederholte Verbindungsabbrüche zu melden. Dies ist für den IT-Betrieb der erste Hinweis, dass überhaupt ein Problem vorliegen könnte.

Als *Störung* wird ein unerwartetes Ereignis oder eine Abweichung vom Normalzustand des Systems bezeichnet. Allgemein verursachen diese *Störungen* keine bis sehr geringe Auswirkungen, bleiben z. B. auf einen Benutzer begrenzt oder zumindest ohne Folgen für den Geschäftsbetrieb. Es gehört zum täglichen *IT-Betrieb*, Störungsmeldungen zu sichten, zu prüfen und deren Ursachen zu beheben. Dabei wird auf reguläre Prozesse zur Störungsbeseitigung zurückgegriffen. Die wenigsten IT-Vorfälle sind auf einen Cyberangriff zurückzuführen. Fehler in Softwareprogrammen, Hardwaredefekte oder falsche Nutzereingaben sind viel häufiger dafür verantwortlich. Aber auch Angriffe werden initial durch Supportanfragen von Endbenutzern oder Meldungen von Systemen zur Angriffserkennung (engl. *Intrusion Detection System*, IDS) entdeckt. Werden solche Betriebsanomalien richtig eingeordnet und hinreichend ernst genommen, ist das für eine frühzeitige Reaktion entscheidend. Wird eine schwerwiegende Fehlfunktion oder ein Angriff

[53] Siehe 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.

vermutet, kann auf eine höhere Stufe eskaliert werden.

Könnte eine *Störung* perspektivisch zur Beeinträchtigung eines Geschäftsprozesses führen, lohnt es sich, frühzeitig zusätzliche Ressourcen bereitzustellen und die *Notfall- oder Krisenstrukturen* über eine (Vor-)Alarmierung in Bereitschaft zu versetzen. Wichtig ist, dass die zentrale Meldestelle frühzeitig alle relevanten Informationen erhält. Deren Mitarbeitende sollten mit dem Ablauf bei schwerwiegenden Systemausfällen vertraut sein und die Situation durch regelmäßige Übungen aus der Praxis kennen (→ *Kapitel 5.2.6*). Nicht immer muss vor Ort etwas vorgefallen sein: Warnungen von externen Stellen können umfassendere Maßnahmen notwendig machen, um ein anderenorts erkanntes Risiko zu minimieren. Auch diese Situationen fallen unter das Störungsmanagement bzw. müssen ggf. von hier ausgehend eskaliert werden.

Zurück in Rodenburg ist die Situation zunächst nicht zu höheren Eskalationsstufen eskaliert worden. Der IT-Betrieb hat mit den Verbindungsabbrüchen von Herrn Schmidt einen Standardanruf bearbeitet und das Problem scheinbar behoben.

Nun erhält IT-Leiter Jäger die Mitteilung, dass im Fachbereich Öffentliche Sicherheit und Ordnung keine Computer und keine Telefone mehr funktionieren. Innerlich flucht er. Arbeitsunfähigkeit im Ordnungsamt wird schnell zeitkritisch – und was, wenn die Feuerwehr auch betroffen ist?

Findet er ein relativ schnell zu behebendes Problem, kann er es vielleicht noch bei einer Störung belassen, sonst muss er aufgrund der fehlenden Arbeitsfähigkeit mindestens zu einem IT-Notfall eskalieren. Eine frühzeitige Information aller relevanten Stellen ist in jedem Fall notwendig.

Wird durch eine Fehlfunktion der IT der Geschäftsbetrieb stark beeinträchtigt und betrifft dies mindestens einen zeitkritischen Geschäftsprozess, der absehbar nicht innerhalb der maximal tolerierbaren Ausfallzeit wiederhergestellt werden kann, handelt es sich um einen *IT-Notfall*. Es wird davon ausgegangen, dass zur Bewältigung von *IT-Notfällen* bereits geeignete Pläne vorliegen oder die bestehenden Pläne adaptiert werden können. Auch wenn aufgrund einer Warnung von außen die risikoreduzierenden Ad-hoc-Maßnahmen deutliche Auswirkungen auf den Geschäftsbetrieb haben oder ein nicht mit normalen Ressourcen bewältigbarer Aufwand entsteht, muss ggf. von einem *IT-Notfall* ausgegangen werden.

In Rodenburg stellt IT-Leiter Jäger nach Prüfung der Situation fest, dass sämtliche Dateien verschlüsselt sind. Er schaltet alle Server ab oder trennt sie vom Netzwerk, die gesamte Kommunalverwaltung ist quasi nicht mehr arbeitsfähig und ihm ist klar, dass dies nicht in wenigen Stunden zu beheben ist, sondern deutlich in die Arbeitswoche hinein andauern wird.

Damit ist der Worst Case eingetreten und er muss die IT-Krise ausrufen.

Sobald mit erheblichen negativen Auswirkungen auf die Verwaltung und ihre Dienstleistungen zu rechnen ist, die nicht mit normalen Strukturen und Ressourcen bewältigt werden können, wird die Situation als ***IT-Krise*** aufgefasst. Zu deren Bewältigung liegen typischerweise keine spezifischen Notfallpläne vor, die vorhandenen Pläne können nicht hinreichend adaptiert werden oder sie greifen schlicht nicht. Dass für die Bewältigung daher kreative Ad-hoc-Lösungswege gefunden werden müssen, ist also charakteristisch für eine solche Situation. Die *IT-Krise* ist zudem von einem großen Schadensausmaß und erwartungsgemäß auch langen Ausfallzeiten gekennzeichnet, bspw. dem übergreifenden Erliegen des Geschäftsbetriebs einschließlich der Bereitstellung kritischer Dienstleistungen, einer starken Außenwirkung, hohen Bewältigungskosten, größeren rechtlichen Folgen oder sogar der Gefährdung von Menschen.

Eskalationsstufen in der Gefahrenabwehr:

IT und Gefahrenabwehr nutzen grundsätzlich unterschiedliche Begriffswelten. Dies kann auch in Form anders benannter Eskalationsstufen bei einem großen IT-Vorfall aufeinanderprallen. Im IT-Bereich wird oft auf die Definitionen des BSI-Standards 200-4 zurückgegriffen, wie sie auch diesem Wegweiser zugrunde gelegt wurden. Eine Krise ist demnach eine erhebliche Unterbrechung mindestens eines (zeit-)kritischen Geschäftsprozesses, für deren Bewältigung keine Notfallpläne vorliegen bzw. nicht ausreichend greifen.

In der Gefahrenabwehr hingegen handelt es sich bei einer **Krise** um eine vom Normalzustand abweichende Situation mit dem Potenzial für oder mit bereits eingetretenen Schäden an Schutzgütern, die mit der normalen Aufbau- und Ablauforganisation nicht mehr bewältigt werden kann (BBK-Glossar, https://www.bbk.bund.de/DE/Infothek/Glossar/_functions/glossar.html).

Bei sehr weitreichender Beeinträchtigung der Verwaltung eines (Land-)Kreises oder einer kreisfreien Stadt, die ggf. auch weitere *Kritische Infrastrukturen* im verwalteten Gebiet betrifft, und wenn hierdurch unmittelbare negative Auswirkungen auf die Bevölkerung bestehen, kann in der Gefahrenabwehr gemäß jeweils geltendem Katastrophenschutzgesetz des Landes eventuell eine **Katastrophe** oder **besondere Einsatzlage** (oder eine andere Bezeichnung gemäß der landesrechtlichen Regelung) festgestellt werden.

Das Ausrufen einer solchen Eskalationsstufe aus dem Bereich der Gefahrenabwehr aufgrund einer IT-Krise ist in der Vergangenheit bereits vorgekommen, es ist jedoch nicht die Regel. Ob vor Ort im Einzelfall so entschieden wird bzw. werden sollte, hängt von den jeweiligen Gegebenheiten ab. Man muss sich im Vorfeld in jedem Fall die Konsequenzen bewusst machen. Das Ausrufen einer solchen Eskalationsstufe kann je nach Ländergesetzgebung geänderte Zuständigkeiten oder Meldeverpflichtungen mit sich bringen. Zudem steigt in der Regel die Aufmerksamkeit der Öffentlichkeit und auch der überregionalen Medien.

Die Bewältigung von *IT-Notfall* oder *IT-Krise* erfordert in der Regel eine übergeordnete, strategische Koordinierung unter Einbindung vieler verschiedener *Stakeholder* auch außerhalb des eigentlichen *IT-Betriebs*.

Definition von Melde- und Eskalationswegen

Für jede Eskalationsstufe ist jeweils zu definieren, welche weiteren Stellen die Meldestelle informieren, alarmieren und hinzuziehen muss. Dazu müssen die Erreichbarkeiten und die Kommunikationskanäle festgelegt werden, und zwar einschließlich einer Redundanzlösung und möglicher Abweichungen außerhalb der üblichen Geschäftszeiten.

Bei einer *Störung* verbleibt die Bewältigung regelmäßig beim *IT-Betrieb* (ggf. IT-Abteilung oder IT-Dienstleister), während bei den höheren Stufen zusätzlich IT-Leitung, ISB und ggf. weitere Stellen bedacht werden müssen. Frühzeitig sollten kurze Informationen an die Verwaltungsspitze und die Presse-/Öffentlichkeitsarbeit gegeben werden, insbesondere wenn im weiteren Verlauf auch eine Außenwirkung zu erwarten ist.

Spätestens bei einem *IT-Notfall* schließen die internen Meldewege dann regelmäßig folgende Stellen ein:

- Verwaltungsspitze (Landrätin/Landrat bzw. (Ober-)Bürgermeisterin/(Ober-)Bürgermeister bzw. Ratsvorsitzende),
- *IT-Betrieb* und ggf. IT-Dienstleister,
- IT-Leiterin bzw. IT-Leiter,
- Informationssicherheitsbeauftragte bzw. Informationssicherheitsbeauftragter,
- Datenschutzbeauftragte bzw. Datenschutzbeauftragter,

- Pressesprecherin bzw. Pressesprecher,
- ggf. weitere interne Stellen (→ *Kapitel 5.2.5*).

Wie laufen die Meldewege in unserer fiktiven Stadt Rodenburg (→ Kapitel 2.1)?

Der Mitarbeiter des Fachbereichs Öffentliche Sicherheit und Ordnung reagiert richtig, als er am frühen Sonntagmorgen IT-Leiter Jäger über die umfangreichen IT-Probleme informiert. Nach einer ersten Einschätzung der Lage eskaliert dieser die Problematik sofort an Bürgermeisterin Wirth und informiert natürlich weitere IT-Mitarbeitende, um die Vorfallbewältigung schnellstmöglich anstoßen zu können. Noch am gleichen Tag wird ein Stab eingerichtet, um die Krisensituation der Kommune zu steuern. Damit sind auch die weiteren relevanten Stellen mit im Boot.

Spätestens bei Eintritt einer *IT-Krise* sollte zur administrativ-organisatorischen Bewältigung ein Stab einberufen werden. Hierzu sollten die Krisenmanagementstrukturen des *Verwaltungsstabes* als administrativ-organisatorische Komponente genutzt werden (→ *Kapitel 5.2.1*).

Abhängig vom Schadensausmaß stehen in einer Kommune eventuell nicht ausreichend interne Expertise und Ressourcen für die erfolgreiche Bewältigung des Vorfalls zur Verfügung. Es empfiehlt sich, in solchen Fällen frühzeitig **externe Unterstützung** hinzuzuziehen (→ *Kapitel 3.2* bzw. → *Kapitel 5.3*).

Berücksichtigung externer Meldepflichten und Adressaten

Neben der Festlegung der internen Meldewege muss immer mitgedacht werden, welche externen Stellen informiert werden müssen. Besonders wichtig ist die Beachtung etwaiger Meldepflichten, etwa nach DS-GVO (bei Betroffenheit persönlicher Daten), nach § 8b Abs. 4 BSIG (bei Betroffenheit *Kritischer Infrastruktur* nach BSI-KritisV) oder auf Basis länderspezifischer Regelungen (z. B. bei Bevölkerungsschutzlagen). Hinzu können noch Pflichtmeldungen kommen, die sich aus Verträgen ergeben, bspw. aus Zugängen zu kommunalen Datennetzverbünden oder möglicherweise abgeschlossenen Cyberversicherungspolicen.

Nach § 33 DS-GVO sind Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden der zuständigen Aufsichtsbehörde zu melden. Für Kommunen ist dies regelmäßig die/der jeweilige Landesbeauftragte für den Datenschutz. Gleichzeitig muss der Vorfall dokumentiert (§ 33 Abs. 5 DS-GVO) und geeignete Maßnahmen zur Behebung getroffen werden. Unter Umständen sind auch die betroffenen Personen über der Verletzung des Datenschutzes zeitnah in Kenntnis zu setzen (§ 34 DS-GVO). Wie dies aussehen kann, ist → *Abbildung 4* zu entnehmen. Selbst wenn ein Angriff relativ früh entdeckt wird, ist die Wahrscheinlichkeit groß, dass bereits Daten abgeflossen sind.

Zusätzlich zu verpflichtenden Meldungen sollte überlegt werden, welche externen Adressaten über die Situation in Kenntnis gesetzt werden sollten. Dies betrifft in erster Linie direkte Geschäftspartner mit bestehenden digitalen Kommunikationsbeziehungen, die ggf. eigene Maßnahmen ergreifen müssen. Das können neben den externen Partnern, die Fachanwendungen bereitstellen oder warten und somit für den Wiederanlauf benötigt werden (→ *Kapitel 5.2.3*), auch z. B. Dienstleister oder externe Stellen sein, die entweder eigene Schutzmaßnahmen ergreifen sollten oder den Ausfall der kommunalen Dienstleistungen zu spüren bekommen (→ *Kapitel 5.2.5*). Hinzu kommen all jene, die bei der Bewältigung des Vorfalls unterstützen können (→ *Kapitel 3.2* sowie → *Kapitel 5.3*).

Grundsätzlich wird zudem empfohlen, für alle Cyberangriffe bei der Polizei Strafanzeige zu erstatten. Nur so kann die Polizei die Strafverfolgung aufnehmen, die Bekämpfungsstrategien optimieren und gesicherte Fallzahlen erheben. Bei einem Angriff auf IT-Systeme werden in der Regel mehrere Straftaten nach Strafgesetzbuch (StGB) begangen, insbesondere nach:

- § 202a Ausspähen von Daten,
- § 202b Abfangen von Daten,

- § 202c Vorbereiten des Ausspähens und Abfangens von Daten,
- § 202d Datenhehlerei,
- § 303a Datenveränderung,
- § 303b Computersabotage.

Für Betroffene haben das Bundeskriminalamt bzw. die zuständigen Landeskriminalämter spezialisierte Anlaufstellen eingerichtet, die Zentralen Ansprechstellen Cybercrime (ZAC)[54]. Sie stehen den Opfern von Cyberstraftaten beratend zur Seite und unterstützen beim Erstatten einer Anzeige. Wird eine Straftat angezeigt, müssen Beweise gerichtsfest erhoben und alle Vorgänge entsprechend dokumentiert werden. In einigen Aspekten kann die Polizei auch direkt bei der Bewältigung unterstützen, bspw. indem sie Lösegeldverhandlungen übernimmt oder Log-Dateien bereitstellt, die für das *Incident Response Team* nicht leicht zugänglich sind.

Auch für die Landesämter für Verfassungsschutz können Meldungen von betroffenen Kommunen von Interesse sein: Fremde Nachrichtendienste sind in erster Linie an Informationen interessiert, die bei staatlichen Institutionen abgeschöpft werden können. Kommunen verwalten sensible Informationen, deren „Wertigkeit“ aus nachrichtendienstlicher Sicht sie selbst oft gar nicht abschließend beurteilen können. Steht bei einem Cyberangriff im Raum, dass Unbefugte auf personenbezogene Daten oder vertrauliche, möglicherweise auch offiziell als Verschlusssachen eingestufte Informationen Zugriff hatten, sollte der Verfassungsschutz in Kenntnis gesetzt werden. Das Bundesamt für Verfassungsschutz hält eine Liste der Ansprechpartner für den Spionageschutz bereit.[55]

Weiterführende Literatur:

Es hat Sie erwischt!
BKA und Zentrale Ansprechstellen Cybercrime der Polizeien, 2022 [BKA22a] (→ *Anhang 2*)

Informationen der Strafverfolgungsbehörden bei einem Cyberangriff auf Unternehmen, Behörden und Institutionen

[54] Kontaktdaten unter: [BKA24] (→ *Anhang 2*).

[55] Ansprechpartner: [BFV24] (→ *Anhang 2*).

5.2.3 Bestandsaufnahme von Fachanwendungen

Kernpunkte:

- Eine Bestandsaufnahme der genutzten Fachanwendungen und Systeme muss im Vorfeld durchgeführt und aktuell gehalten werden.
- Eine transparente, gut kommunizierte Priorisierung sorgt für Rückhalt.
- Ein Wiederanlaufplan verkürzt die Zeit bis zur vollständigen Wiederherstellung der Systeme entscheidend.

Nach dem Cyberangriff gegen unsere fiktive Stadt Rodenburg (→ Kapitel 2.1) muss schnellstmöglich zumindest ein rudimentärer Betrieb wiederhergestellt werden.

Die Systeme wurden durch die Angreifer verschlüsselt und durch den IT-Leiter vom Netz getrennt. Der IT-Betrieb verschafft sich nun einen Überblick, welche Fachverfahren von dem Cyberangriff betroffen sind und ob eine kurzfristige Wiederherstellung einzelner Fachanwendungen möglich ist. Der Krisenstab und die Pressestelle sind auf diese Informationen angewiesen, um die Mitarbeitenden und die Bevölkerung zu informieren, welche Dienstleistungen die Kommune jetzt noch anbieten kann. Zusätzlich muss der Krisenstab die Reihenfolge der Wiederherstellung in den nächsten Wochen überlegen.

Warum vorbereiten?

Cyberangriffe können Kommunen unterschiedlich schwer treffen. Im schlimmsten Fall kommt es zu einem kompletten Ausfall der IT. Dann sind zunächst sämtliche Aufgaben und Dienstleistungen einer Kommune massiv gestört oder gänzlich unterbrochen. Beim Wiederaufbau des Systems stellt die hohe Anzahl und breite Vielfalt an unterschiedlichen genutzten Fachverfahren eine große Herausforderung dar. Es kann nicht gleichzeitig mit der Wiederherstellung aller Fachverfahren begonnen werden. Die Fachverfahren hängen zudem teilweise voneinander ab, sodass die eine Anwendung technisch nicht ohne die vorherige Wiederherstellung der anderen funktioniert. Es braucht also eine definierte Reihenfolge des Wiederanlaufs.

Hat man im Vorfeld keine zentrale Gesamtübersicht der eingesetzten Fachverfahren erstellt und dabei erfasst, für welche Dienstleistungen diese notwendig sind, wie diese technisch konfiguriert sind und wie die einzelnen Anwendungen miteinander in Verbindung stehen, so verstreicht zu Beginn einer Vorfallbewältigung erst einmal viel Zeit, um diesen Schritt nachzuholen. Sobald der Zugriff auf die IT nicht mehr gewährleistet ist, muss zudem unter erschwerten Bedingungen gearbeitet werden. Vieles muss aus dem Kopf rekonstruiert werden und das Ergebnis bliebe vermutlich unvollständig. **Die Übersicht vorher zu erstellen, ist daher absolut essenziell für die Krisenbewältigung.**

Idealerweise werden diese Vorbereitungen im Rahmen eines vollständigen *Business Continuity Managements (BCM)* z. B. nach BSI-Standard 200-4[56] erarbeitet. Dann erfolgt zunächst eine *Business Impact Analyse (BIA)*, die die Kritikalität und benötigte Wiederanlaufzeit der einzelnen Geschäftsprozesse bestimmt und die für die Prozesse benötigten Ressourcen (nicht nur im Bereich IT) erfasst. Darauf aufbauend können dann die für die einzelnen Geschäftsprozesse konkret benötigten Fachanwendungen betrachtet werden. Eine Priorisierung erfolgt auf der Ebene der Geschäftsprozesse, sodass auch Abhängigkeiten

[56] Siehe 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.

zwischen Fachanwendungen erkannt werden können, die allein dadurch entstehen, dass sie der Durchführung desselben Geschäftsprozesses dienen.

Die Einführung eines BCM führt zu den vollständigsten Ergebnissen in der Vorbereitung und stellt daher den Goldstandard dar. Falls bspw. aufgrund der Aufgabenfülle jedoch nur wenige Ressourcen zur Verfügung stehen, kann man sich dem Ziel auch schrittweise nähern, indem man von den Fachanwendungen ausgeht. Dies wird im Folgenden näher erläutert und stellt eine pragmatische Vorgehensweise dar, da sich die Fachanwendungen oft einfacher zentral ermitteln lassen als die Geschäftsprozesse.

Wenn dann erst einmal bekannt ist, welche Fachanwendungen für welche besonders kritischen Aufgaben erforderlich sind, kann darauf aufbauend deren Wiederherstellung priorisiert werden. Das wiederum erlaubt eine klarere Kommunikation nach außen: Die Bürgerinnen und Bürger können gezielter auf bestehende Einschränkungen und ggf. auf analoge Alternativen für die Zwischenzeit hingewiesen werden.

Welche Systeme und Fachanwendungen können betroffen sein?

Startpunkt ist eine Liste aller in einer Kommune genutzten Fachanwendungen (und der darunter liegenden IT-Systeme). Bei über 300 genutzten Fachanwendungen im Bereich größerer Kommunalverwaltungen ist es nicht möglich, diese hier mustergültig aufzulisten. Eine solche Liste kann nur durch die IT-Verantwortlichen vor Ort erstellt werden. Neben ihrem Nutzen für die Krisenbewältigung kann eine solche Liste übrigens auch verwendet werden, um bei Sicherheitswarnungen schnell zu entscheiden, ob eine eigene Betroffenheit vorliegt und dringend *Patches* eingespielt werden müssen.

Häufig liegen bereits (Teil-)Verzeichnisse bei den IT-Verantwortlichen vor. Zudem können die Verzeichnisse von Verarbeitungstätigkeiten aus dem Datenschutz als gute zusätzliche Quelle fungieren, da sie, sofern gut erhoben, einen guten Überblick über die genutzten Fachanwendungen bieten.

Eine Anmerkung zur Vorgehensweise: Grundsätzlich ist es lohnenswert, auch im Vorgriff auf ein vollständiges BCM zu einem späteren Zeitpunkt, die Erfassung und Dokumentation von Aufgaben, Verfahren und IT-spezifischen Aspekten zentral zu handhaben. Einerseits werden so Personalressourcen entlastet: Die Notwendigkeit für Fachabteilungen, eine Vielzahl von einzelnen, inhaltlich aber überlappenden Erfassungen durchzuführen, wird dadurch reduziert. Andererseits wird eine Gesamtübersicht für das Krisenmanagement und andere Angelegenheiten (z. B. Datenschutz, Geheimschutz, BCM, IT-Risikoabschätzungen) geschaffen. Im Krisenfall sind somit alle relevanten Daten zentral verfügbar und können aus dem Informationspool bezogen werden.

Nun muss die Gesamtliste noch mit weiteren relevanten Informationen angereichert werden. Diese bilden zum einen die technischen Rahmenbedingungen ab, wie bspw. konkrete Hardwareanforderungen oder Konfigurationen. Zum anderen muss jeweils der Zusammenhang zu den Geschäftsprozessen bzw. Aufgaben hergestellt werden.

Viele Fachanwendungen werden zudem nicht auf den lokalen Systemen der Kommunen, sondern über externe Rechenzentren zur Verfügung gestellt. Dies hat Einfluss darauf, wie bzw. wo und durch wen die Wiederherstellung erfolgen muss. Diese Informationen müssen daher ebenfalls in der Gesamtübersicht vermerkt sein.

Welche Auswirkungen hätte ein Ausfall?

Damit auch die möglichen Folgen eines Ausfalls aus der Gesamtliste direkt hervorgehen, sollten nicht nur die von den jeweiligen Fachanwendungen abhängigen Dienstleistungen und Aufgaben festgehalten werden. Relevant sind auch die ggf. eintretenden rechtlichen, finanziellen oder sonstigen Konsequenzen der Nichterfüllung dieser Dienstleistung oder Aufgabe sowie die möglicherweise existierenden Alternativen – von händischer Aufgabenerledigung über Workarounds bis hin zu einer Übernahme der Aufgabe durch Außenstellen oder Dritte wie bspw. andere Kommunen.

Nachdem identifiziert wurde, welche Fachverfahren für die jeweilige Aufgabenerledigung genutzt und durch wen diese zur Verfügung gestellt werden, ergibt sich – in Zusammenarbeit mit den Nutzenden der jeweiligen Fachanwendungen – ein besseres Bild davon, welche Auswirkungen ihr Ausfall auf die Handlungsfähigkeit einer Kommunalverwaltung hätte. Denkbar sind hier bspw. fehlende Auszahlungsmöglichkeiten von Gehältern oder Sozialleistungen bei *Störungen* der Software des Kassenwesens, *Störungen* bei der Anmeldung von Fahrzeugen bei Ausfällen der Fachanwendungen für die Kfz-Zulassung bis hin zu fehlenden Zugangsmöglichkeiten ins Gebäude bei Einschränkungen der Software zur Schließanlagenverwaltung.

Zusammenfassend helfen die folgenden Prüffragen beim Erstellen der Gesamtübersicht:

- Welche Software von welchem Hersteller ist im Einsatz?
- Welche Geschäftsprozesse bzw. Aufgaben stützen sich auf die jeweilige Software?
- Gibt es Workarounds, wenn die Standardanwendung nicht funktioniert?
- Gibt es Wartungsverträge für das Fachverfahren? Mit welchem *Service-Level-Agreement* (SLA) und welchen Notfallerreichbarkeiten?
- Gibt es Schnittstellen zu anderen Fachverfahren/anderen Behörden oder Kommunikationspartnern? Wann kappen diese ggf. bestehende Kommunikationsverbindungen und unter welchen Bedingungen werden diese wiederhergestellt (z. B. Zugang zu kommunalen Datennetzverbünden)?
- Wer ist für das Verfahren verantwortlich? Gibt es dafür Dienstleister? Wenn ja, mit welchen SLA? Mit welchen Notfallerreichbarkeiten? Wie schnell wird eine Wiederherstellung ermöglicht und welche Unterstützung kann der Dienstleister im Schadensfall leisten? Welche Art von Notbetrieb ist im SLA beschrieben?
- Welche sind die konkreten technischen bzw. Hardwareanforderungen für das Fachverfahren (z. B. andere Softwaredienste, Portfreigaben)? Welche Softwareversion, welcher *Patch*stand und welche individuelle Konfiguration sind im Einsatz?
- Welche Zugangsdaten werden benötigt? Wie können Zugangsdaten wiederhergestellt werden? Gibt es eine Zwei-Faktor-Authentisierung?
- Gibt es eine Möglichkeit, die jeweils benötigten Daten neu einzulesen oder quer einzuspielen? Wird hierbei Revisionssicherheit benötigt? Könnte man die benötigten Daten ggf. anderweitig wiederbekommen, falls auch Backups betroffen sein sollten (externe Standorte/Firmen/Dienstleister/Auftragnehmer)?
- Gibt es eine Übersicht von relevanten internen und externen Sicherheitsexperten, die zusätzlich zu den oben genannten Wartungsverträgen bei Sicherheitsvorfällen unterstützen können?

Warum priorisieren?

Wie eingangs bereits erwähnt, ist es aufgrund der Komplexität und Vielzahl von Fachverfahren und gleichzeitig begrenzter Ressourcen bei der Schadensbeseitigung nicht möglich, alle Fachanwendungen gleichzeitig wiederherzustellen. Die Wiederherstellung der vollständigen Arbeitsfähigkeit einer Kommunalverwaltung kann nach einem Cyberangriff zwischen wenigen Tagen bis hin zu vielen Monaten dauern. Es muss daher entschieden werden, womit im Rahmen der Wiederherstellung begonnen werden soll. In diesen Entscheidungsprozess sollten nach Möglichkeit auch die Verantwortlichen für die Fachanwendungen einbezogen werden.

Grundlage für die Priorisierung ist die vorherige Identifizierung aller genutzten Fachanwendungen. Nur wenn bekannt ist, welche Fachanwendungen im Haus wofür genutzt werden und wovon sie abhängen, können bei einer Wiederherstellung des Systems auch einzelne Verfahren priorisiert und vorrangig entstört werden. Steht dies schon fest, beschleunigt und erleichtert es den Aufbau eines Notbetriebes, kann somit Ausfälle vorrangiger Dienstleistungen verkürzen und ermöglicht auch die Vorbereitung alternativer Handlungspläne für besonders dringende Dienstleistungen.

Relevante Kriterien/Prüffragen bei einer Priorisierung sind:

- Wichtigkeit der Dienstleistung für die Bevölkerung (z. B. Sozialleistungen)
- Wichtigkeit der Dienstleistung für ansässige, insbesondere kleinere Wirtschaftsunternehmen (z. B. Zahlungen für Dienstleistungen, Arbeitsfähigkeit)
- Wichtigkeit der Dienstleistung für die Kommunalverwaltung (Aufrechterhaltung der eigenen Arbeitsfähigkeit, Kommunikationsfähigkeiten wie bspw. Telefon, E-Mail oder besonderes elektronisches Behördenpostfach, Regressansprüche, Zeiterfassung[57] etc.)
- Gibt es Alternativen zu der digitalen Bearbeitung? Sollten z. B. Papiervordrucke genutzt werden können, könnte die Wiederherstellung der entsprechenden Dienstleistung herunterpriorisiert werden.
- Wichtigkeit der Anwendung als technische Grundlage für andere Fachanwendungen (Abhängigkeiten beachten)
- Für das Fachverfahren benötigtes Kommunikationsnetz (intern, befreundetes Netz (z. B. des Landes), Internet)
- Ggf. weitere lagebedingte Anforderungen (z. B. Corona-Meldezahlen)
- Ggf. auch Einfachheit/Schnelligkeit der Wiederherstellung, Erreichbarkeit der wichtigen technischen Ansprechpartner, Machbarkeit

Analoge Fragestellungen liegen auch der BIA zugrunde, der man sich mit diesem Vorgehen auf Basis der Fachverfahren langsam angenähert hat. Bewähren kann sich in diesem Kontext auch die Schutzbedarfsanalyse aus der Informationssicherheit kombiniert mit Aspekten einer BIA (*Recovery Point Objective RPO/Recovery Time Objective RTO*) beim Schutzziel der Verfügbarkeit. Durch die konkreten Zeitangaben für noch tolerierbare Verfügbarkeitsausfälle und tolerierbare Datenverluste wird die hierfür notwendige Zuarbeit der Fachbereiche erleichtert. Obwohl die Schutzbedarfsanalyse bspw. im Weg in die Basis-Absicherung (WiBA) und im IT-Grundschutz-Profil Kommunalverwaltung nicht explizit vorgesehen ist, kann man diese aggregiert auf die Verwaltungsleistungen anwenden und daraus ebenfalls eine Priorisierung ableiten.

Aufgrund der Heterogenität der Kommunen ist es nicht möglich, eine konkrete Priorisierung zentral vorzuschlagen. Die Erfahrung vergangener IT-Vorfälle zeigt, dass die folgenden Fachverfahren recht hoch priorisiert und schnell wiederhergestellt wurden. Die Auflistung gibt daher einen ersten Anhaltspunkt, erhebt jedoch keinen Anspruch auf Vollständigkeit:

- Fachanwendungen für Meldewesen (Ausstellen von Personalausweisen, Reisepässen, Ummeldungen),
- Fachanwendungen für Standesämter (Beurkundung von Geburten, Todesfällen, Eheschließungen),
- Melderegister-Schnittstelle (Informationsfluss zwischen Standesamt und Einwohnermeldeamt),
- Fachanwendung für Ausländer- und Staatsangehörigkeitswesen,
- Dokumentenmanagementsystem (eAkte),
- Websites/Internet/Public-Key-Infrastruktur der Verwaltung,
- Fachanwendung Rechnungswesen (Haushaltsplanung und Budgetierung),
- Finanzsoftware,
- Kassensystem,
- Software für die Personalverwaltung,
- Sitzungsmanagement-Software,
- Software zur Schließanlagenverwaltung,
- Fachanwendung für Arbeit, Jugend, Soziales,
- Fachanwendung für das Sozialamt,
- Fachanwendung Wohngeld,
- Fachanwendung Kfz-Zulassung,
- Fachanwendung für Ordnungswidrigkeiten,
- Fachanwendung Abfall- oder Abwasserwirtschaft,
- Software für die Notfallrettung,
- Fachanwendungen für Gewerbe- und Bauaufsicht,
- Software für Liegenschaftskataster,
- Bibliothekssoftware.

Im Anschluss an die Priorisierung – ob sie vorbereitet wird oder leider erst im Ereignisfall ad hoc

[57] Eine Erfahrung früherer Vorfälle ist, dass eine funktionierende Zeiterfassung psychologisch wichtig für die überlasteten Mitarbeitenden ist: Sie führt zu einem sichtbaren Nachhalten der teilweise signifikanten Mehrarbeit. So wird der Eindruck vermieden, diese könne nach erfolgreicher Bewältigung unberücksichtigt bleiben.

erfolgen muss – sollte auch die interne Kommunikation (→ *Kapitel 5.2.5*) mit den Mitarbeitenden stattfinden. Jeder Bereich hat seine wichtigen Aufgaben. Werden diese ohne Erklärung herunterpriorisiert, kann dies zu Unmut führen. Sind die angewendeten Kriterien hingegen transparent und fühlen sich die Mitarbeitenden mitgenommen, reduziert dies ggf. Nachfragen und Änderungswünsche im weiteren Verlauf. Auch bei einem nur teilweisen Ausfall von Fachanwendungen kann durch eine im Vorfeld erfolgte Identifizierung und Priorisierung schnell überprüft werden, welche Dienstleistungen der Kommunalverwaltung betroffen sind. Dies hilft insbesondere bei der Erstellung einer schnellen Erstinformation für die Bevölkerung.

Die fertiggestellte Übersicht mit der Priorisierung sollte dann in einer vom internen Netzwerk unabhängigen Version (bspw. im Notfallnotebook oder als Papierausdruck, → *Kapitel 5.2.1*: Das Handbuch IT-Notfallmanagement) festgehalten werden, damit sie auch in Notfall und Krise zur Verfügung steht.

Von der Priorisierung zum Wiederanlaufplan

Die in diesem Kapitel beschriebenen Schritte werden für den Wiederanlauf in den Notbetrieb und für die Wiederherstellung der Systeme zwingend benötigt. Idealerweise verfügt man jedoch nicht nur über eine Priorisierung, sondern über einen aktuellen und vollständigen Wiederanlaufplan, der im Ereignisfall direkt abgearbeitet werden kann. Die darin enthaltenen Voraussetzungen und Abläufe sollten dann unbedingt im Vorfeld nicht nur ermittelt, sondern auch getestet werden.

Ein wichtiger Aspekt muss in Vorbereitung des Wiederanlaufplans zusätzlich zur beschriebenen Priorisierung geklärt werden: Welche Schritte müssen unternommen werden, um die Anbindung an externe Rechenzentren oder eine automatisierte Schnittstelle zu Dritten im Rahmen von Fachverfahren wieder einrichten zu können? Häufig führt ein Schadensereignis in einer Kommune unmittelbar dazu, dass sämtliche Schnittstellen zur Kommune bei externen Rechenzentren oder Softwareanbietern sicherheitshalber unterbrochen werden, damit sich die Schadsoftware nicht auf weitere Systeme ausbreiten kann. Daher muss nicht nur geklärt werden, welche Systeme rein technisch aufeinander aufbauen, sondern auch welche Dienste zur Bedingung für eine Wiederanbindung gemacht werden. Es kann z. B. sein, dass ein Fachverfahren an sich zwar keine E-Mail-Funktionalität benötigt, eine Passwortänderung und Wiederaufnahme der Schnittstelle jedoch nur von der bekannten kommunalen E-Mail-Adresse aus möglich sind.

Es ist also in der Praxis durchaus möglich, dass eine im Vorfeld überlegte Priorisierung von Fachanwendungen in bestimmten Punkten durch externe Anforderungen erschwert werden kann. Die Wiederanbindung durch Dritte erfolgt in der Regel erst, wenn ein sicherer Zustand wiederhergestellt werden konnte, um einen erneuten Ausfall durch noch nicht bereinigte Systeme zu verhindern. Hier sind genaue Absprachen der Verantwortlichen für Bereinigung und Wiederanlauf notwendig.

Weiterführende Literatur:

Business Impact Analyse – Ersteinschätzung
Stadt Essen, 2023
[ESS23] (→ *Anhang 2*)

Über den Landkreistag ist hier eine unterstützende Unterlage der Stadt Essen zwecks Ersteinschätzung im Rahmen einer Business Impact Analyse erhältlich.

Dokumentenvorlage Wiederanlauf-/Wiederherstellungsplan
BSI, 2023

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Vorlage_Wiederanlaufplan.docx

Die Wiederanlauf- und Wiederherstellungsplanung gemäß BSI-Standard 200-4, Kapitel 6.10, wird durch die entwickelte Dokumentenvorlage unterstützt.

5.2.4 Vorkehrungen für einen Notbetrieb

Kernpunkte:

- Ideal: Einrichtung eines vollständigen *BCM*-Systems
- Beschaffung einer Notfallinfrastruktur beschleunigt den Übergang in einen Notbetrieb.
- Gesonderte Sicherung der wichtigsten Daten stellt die Basis für einen funktionierenden Notbetrieb dar.

Stehen durch einen IT-Vorfall erst einmal sämtliche Systeme nicht mehr zur Verfügung, kann es Wochen bis Monate dauern, um die tatsächliche Wiederherstellung zu bewältigen. Da in der Regel zumindest einige zeitkritische Dienstleistungen nicht so lange ausfallen dürfen, wird für die Zwischenzeit ein Notbetrieb notwendig. Um diesen zu ermöglichen, werden sowohl organisatorische als auch (ressourcen-)technische Vorbereitungen benötigt.

Idealerweise folgen die Vorbereitungen dem Vorgehen des *Business Continuity Managements (BCM)*[58]. Dann können, aufbauend auf einer *Business Impact Analyse (BIA)*, Notfallhandbuch und Notfallvorsorgekonzepte, Geschäftsfortführungspläne, technische Wiederanlaufpläne für einen Notbetrieb sowie Wiederherstellungspläne für die Rückkehr in den Normalbetrieb erstellt werden. Damit liegen dann auch Bedarfsplanungen vor, die konkret notwendige Vorbereitungen und Beschaffungen begründen, um auf einen IT-Vorfall bestmöglich vorbereitet zu sein.

Es können jedoch auch ohne eine solch detaillierte Analyse und Vorgehensweise einige wichtige Vorbereitungen getroffen werden. Die schrittweise Annäherung an einen Wiederanlaufplan durch Erstellen einer Gesamtübersicht der Fachanwendungen, Anreichern mit weiteren notwendigen Informationen für den Wiederanlauf und Priorisierung wurde in → *Kapitel 5.2.3* detailliert beschrieben. Zusätzlich sollten für den Notbetrieb weitere Vorbereitungen getroffen werden:

Für einen Notbetrieb wird **Hardware** benötigt, die auf keinen Fall durch den Vorfall kompromittiert ist. Es lohnt sich, neben dem Notfallnotebook (→ *Kapitel 5.2.1* Handbuch IT-Notfallmanagement) weitere Laptops oder mobile Endgeräte, die nicht an das Netzwerk angeschlossen sind, in Reserve zu halten. Sollten die zeitkritischen und zwingend aufrechtzuerhaltenden Dienstleistungen (→ *Kapitel 5.2.3*) bereits erhoben worden sein, sollten sie darauf überprüft werden, ob sie mit mobiler Ausstattung (Laptop, mobiler Hotspot, Handy) prinzipiell erbringbar sind[59] und wie viele Arbeitsplätze im Minimum gleichzeitig benötigt werden. So kann daraus das benötigte Mengengerüst präziser abgeleitet werden.[60]

Ein Konzept für die Kommunikation per **Telefon** ist eine weitere Vorbereitungsmaßnahme (→ *Anhang 4.2*). Insbesondere wenn die interne Telefoninfrastruktur ausschließlich IP-basiert oder sogar auf Basis von *Unified Communication-Clients* aufgebaut ist, ist die Wahrscheinlichkeit hoch,

[58] Für eine detaillierte Beschreibung der Vorgehensweise siehe BSI Standard 200-4, 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.

[59] Dies sind die Bereiche, bei denen die eingesetzten Softwaresysteme entweder rein clientseitig funktionieren oder die externe Serverkomponente über das Internet erreichbar ist.

[60] Ggf. kann die für den Notbetrieb beschaffte Hardware dann im Ereignisfall noch ergänzt werden um Geräte von Mitarbeitenden, die z. B. urlaubs- oder krankheitsbedingt bereits längere Zeit nicht im Betrieb waren. Darauf sollte man sich bei der Planung jedoch nicht verlassen. Es muss insbesondere beachtet werden, dass zwischen einem ersten Eindringen von Tätergruppierungen in ein Netzwerk und dem Entdecken ein längerer Zeitraum vergeht. **Sinnvollerweise wird für eine solche Ergänzung das Ergebnis forensischer Untersuchungen abgewartet (→ *Kapitel 3.2*), um eine Kompromittierung der Notbetriebinfrastruktur möglichst auszuschließen.**

dass zunächst keine Telekommunikation mehr möglich ist. Für diesen Fall werden Notfallhandys oder eine strikte Regelung für den Einsatz von Privatgeräten[61] benötigt. Die Telefonnummern müssen auch offline vorgehalten werden, allen relevanten Mitarbeitenden bekannt sein und den externen Kommunikationspartnern bekannt gemacht werden.

Für die Kommunikation mit Externen werden zudem **Notfall-E-Mail-Adressen** benötigt. Diese müssen vom eigenen Netzwerk losgelöst eingerichtet sein. Idealerweise sind diese Adressen den wichtigsten Kommunikationspartnern bereits im Vorfeld bekannt, damit sie den darüber versendeten Nachrichten vertrauen und ihnen Beachtung schenken. Zumindest für die zentralen Fachverfahren und wichtigsten Kommunikationspartner sollte eine solche E-Mail-Adresse bereits im Vorfeld hinterlegt sein, damit die Wiederherstellung der ursprünglichen E-Mail-Kommunikationsinfrastruktur keine zwingende Voraussetzung zur Wiederanbindung darstellt (→ *Kapitel 5.2.3*).

Mit einer **Notfall-Website** kann die Kommunikation in der Krise deutlich verbessert und beschleunigt werden (→ *Kapitel 5.2.5*). Diese Website sollte für den Fall einer vollständigen Kompromittierung des eigenen Netzwerks bei einem externen Hoster liegen und – zumindest rudimentär – vorbefüllt werden. Sie kann dann im *Notfall* oder in der *Krise* direkt freigeschaltet und damit öffentlich zugänglich gemacht werden (sogenannte Darksite).

Schließlich werden für die Erbringung von Dienstleistungen diverse **Dateien und Informationen** benötigt. Das können Formulare und Merkblätter sein, aber eben auch nachschlagbare Informationen wie Baupläne oder aktuelle Sachstände der Bearbeitung. Vergangene Vorfälle haben gezeigt, dass hier eine analoge Datensicherung oder auch ältere, nicht kompromittierte Backups einen entscheidenden Vorteil bedeuten. Je nach betroffener Dienstleistung kann ggf. auch eine Datenwiederherstellung durch ein „Zurückholen" der ausgetauschten Daten von nicht kompromittierten Dienstleistern oder anderen Kommunikationspartnern eine Option darstellen.

Dies muss allerdings vorbereitet werden, um im Ereignisfall möglichst zeitnah umgesetzt werden zu können.

Eventuell können für die Dauer eines Notbetriebs auch einige Dienstleistungen von anderen – bspw. benachbarten Kommunen – übernommen werden (→ *Kapitel 5.3*). Kontinuierlich oder sehr regelmäßig ablaufende Prozesse können zudem möglicherweise durch Partner zunächst

Weiterführende Literatur:

BSI-Standard 200-4
BSI, 2024
https://www.bsi.bund.de/dok/6603458

Hilfsmittel zum BSI-Standard 200-4
BSI, 2023
https://www.bsi.bund.de/dok/200-4-hilfsmittel

Der modernisierte BSI-Standard 200-4 bietet verschiedene Hilfsmittel und Dokumentvorlagen an, die bei der effektiven Umsetzung unterstützen sollen. Sie können teilweise losgelöst vom BSI-Standard 200-4 eingesetzt werden. Es finden sich dort bspw. Vorlagen eines Notfallhandbuchs und Notfallvorsorgekonzepts sowie von Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungsplan. Auch ein BIA-Auswertungsbogen mit Hinweisen wird dort zur Verfügung gestellt.

Erste Hilfe bei einem schweren IT-Sicherheitsvorfall
BSI, 2020
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html

Dieses Papier dient als Notfalldokument für Informationssicherheitsbeauftrage, CISOs und Systemadministratoren von KMU und kleineren Behörden für den Fall eines schweren IT-Sicherheitsvorfalls.

[61] Auf private Accounts bspw. bei Messengerdiensten sollte nur im äußersten Notfall zurückgegriffen werden.

unverändert fortgeführt werden. Bei vergangenen Vorfällen sind z. B. monatliche Zahlungen in Absprache mit dem ausführenden Bankinstitut unter Vorbehalt weiter getätigt worden. Diese beiden Möglichkeiten erfordern Absprachen im Vorfeld und eine gründliche Dokumentation während des Notbetriebs, um eine Kontrolle und Bereinigung der Daten sowie Rückübergabe im Rahmen der Wiederherstellung zu gewährleisten.

Die für den Notbetrieb durchgeführten Vorbereitungen sollten sorgfältig im Handbuch IT-Notfallmanagement (→ *Kapitel 5.2.1*) hinterlegt werden, um im Ereignisfall sofort griffbereit zu sein.

5.2.5 Kommunikation während Vorfällen

Kernpunkte:

- Schnelle, ehrliche, verständliche und konsistente Information ist essenziell.
- Eine Vorbereitung wichtiger Inhalte und alternativer Erreichbarkeiten wird benötigt.
- Verschiedene Kanäle und Zielgruppen (z. B. Mitarbeitende, Medien, Bevölkerung) müssen berücksichtigt werden.

Warum kommunizieren?

Bei einem größeren IT-Vorfall in einer Kommunalverwaltung kommt es in der Regel zu Auswirkungen, die für Bürgerinnen und Bürger, mindestens aber für die Mitarbeitenden deutlich zu spüren sind – von ausfallenden Erreichbarkeiten bis zu Benachrichtigungen über Datenabflüsse. Bei *Ransomware*-Angriffen liegt es zudem im Interesse von Angreifergruppierungen, dass ein solcher Vorfall publik wird. Dadurch soll der Druck auf die Verwaltung aufgebaut und die Zahlungsbereitschaft erhöht werden. Insofern ist es weitgehend unvermeidlich, dass Informationen über einen Vorfall an die Öffentlichkeit dringen. Kommunen müssen sich mit einer entsprechenden Kommunikationsstrategie gut aufstellen und auf mögliche Fragen vorbereiten. Um diese Aufgabe erfüllen zu können, bedarf es einer im Vorfeld etablierten Struktur im Bereich der Kommunikation, die auch die starke Belastung im Ereignisfall bewältigen kann.

Der Cyberangriff in unserer fiktiven Stadt Rodenburg (→ Kapitel 2.1) war erfolgreich und die IT ist nicht mehr funktionsfähig.

Der Bürgermeisterin ist klar, dass spätestens bei Dienstbeginn am nächsten Tag kein Arbeitsablauf normal funktionieren wird. Bürgerinnen und Bürger, Lieferanten und Dienstleister, ansässige Unternehmen, aber auch die eigenen Mitarbeitenden werden wissen wollen, was los ist. Erfahren sie es nicht zeitnah, stehen sie z. B. unverhofft und ohne Erklärung vor verschlossenen Türen oder erreichen trotz normaler Geschäftszeiten niemanden über die bekannte Servicenummer. So wird sich Unmut ausbreiten und die Gerüchteküche wird angeheizt. Viele von ihnen haben zudem dringende Anliegen, eine Verschiebung auf unbestimmte Zeit durch die Kommune kann existenzgefährdend sein.

Ziel sollte es für jede Kommune sein, die Deutungshoheit über die Situation zu bewahren und durch glaubwürdige Kommunikation einen Reputationsverlust zu verhindern. Eine ehrliche, proaktive und frühzeitige Information (offensive Kommunikationsstrategie) führt in den meisten Fällen zu Verständnis für eventuelle Einschränkungen und kann mögliche Auswirkungen für die einzelnen Bürgerinnen und Bürger reduzieren, indem sie Alternativen aufzeigt („niemanden allein im Regen stehen lassen“). Wird das Ausmaß eines Vorfalls hingegen zunächst nicht kommuniziert und Kontakt mit den Medien vermieden, ist damit zu rechnen, dass

dennoch Informationen an die Öffentlichkeit gelangen. Eine defensive Kommunikationsstrategie, die sich auf die Beantwortung von Nachfragen beschränkt und lediglich auf öffentlich bekanntgewordene Informationen reagiert, bietet mehr Raum für Spekulationen. Das führt nicht nur zu Unsicherheiten bei den Betroffenen, sondern lässt die Behörden auch hilflos, dadurch nicht vertrauenswürdig und im schlimmsten Fall unaufrichtig erscheinen. Ein solches Vorgehen führt regelmäßig zu negativer Berichterstattung, kann Konflikte mit den betroffenen Bürgerinnen und Bürgern schüren und die Vertrauenswürdigkeit der staatlichen Institutionen massiv beschädigen.

Warum vorbereiten?

Bereitgestellte Informationen sollten so verständlich und klar formuliert und so umfassend wie möglich sein. In der Erstphase eines größeren Vorfalls stellt dies eine erhebliche Herausforderung dar, die unter hohem Zeit- und Erfolgsdruck zu bewältigen ist. Grundsätzlich ist es daher ratsam, im Vorfeld einen szenarienübergreifenden Krisenkommunikationsplan zu erstellen, der auch Spezifika von IT-Sicherheitsvorfällen enthält.

Im Krisenkommunikationsplan sollte zunächst die Einbindung der Kommunikation in die Notfall- und Krisenorganisation (→ *Kapitel 5.2.1*) beschrieben sein. Darüber hinaus sollte die aufbau- und ablauforganisatorische Vorbereitung im Fokus stehen: Grundsätze, Zuständigkeiten und Verantwortlichkeiten für die Kommunikation, die Definition von Zielgruppen und Kommunikationskanälen sowie die Ressourcenplanung (Personal, Technik, Räumlichkeiten). Der Krisenkommunikationsplan sollte um szenariotypische Aspekte von IT-Vorfällen ergänzt werden (z. B. Mustertexte, Sprachregelungen, Checklisten). Die Fokussierung auf strukturelle Aspekte dient dazu, bei unterschiedlichen Vorfällen handlungsfähig zu bleiben und leistungsfähige Kommunikationsstrukturen für die Bewältigung zahlreicher, in der *Krise* parallel und unter teils hohem Zeitdruck anfallender Kommunikationsaufgaben zu entwickeln. Die Planungen sollten – gerade mit Blick auf IT-Vorfälle – auch den Ausfall von Kommunikationskanälen (Website, E-Mail, Telefon) und IT-Systemen mitdenken. Hier sind bspw. eine Vorbereitung technischer Alternativwege, aber auch eine netzwerkunabhängige Speicherung von Zugangsdaten (u. a. bei Social-Media-Konten, falls genutzt) notwendig.

Ergänzend kommen einer Kommune in einer solchen Situation bereits aufgebaute Kontakte zu relevanten Medien und etablierte Kommunikationskanäle (bspw. Soziale Medien, Website) zugute. Werden diese im Regelbetrieb kontinuierlich bedient, entsteht bestenfalls ein Vertrauensverhältnis zwischen der Kommune einerseits und andererseits den Kommunikationspartnern bei den klassischen Medien (bspw. Lokaljournalismus) sowie der Nutzerbasis von Sozialen Medien. Zudem werden organisatorische und technische Hürden bereits im Normalbetrieb abgebaut und treten nicht erst unvorhergesehen bei einem dann möglicherweise notwendigen Ad-hoc-Wechsel des Kommunikationskanals im Rahmen eines Vorfalls auf.

Welche Zielgruppen?

Die Zielgruppen, an die sich die Krisenkommunikation richten wird, müssen zielgruppenspezifisch auf den passenden Kanälen angesprochen werden. Dabei sollte ein One-Message-Ansatz im Sinne einheitlicher Kernbotschaften verfolgt werden. Diese Kernbotschaften können eine kanal- und zielgruppenspezifisch angepasste Form annehmen, müssen aber insgesamt konsistent transportiert werden.

Grundsätzlich gilt: interne Kommunikation vor externer Kommunikation. Daher sind die **eigenen Mitarbeitenden die erste Zielgruppe.** Es ist zu bedenken, dass, neben einem gewissen Grundstock an allgemeinen Informationen zur Situation für alle Mitarbeitenden, für viele Kolleginnen und Kollegen jeweils spezifische Zusatzinformationen notwendig sein können, bspw. für:

- Presse/Öffentlichkeitsarbeit,
- Verwaltungsspitze,
- Bürgerservice,
- Pforte/Sicherheitsleitstelle,
- ggf. Rechtsabteilung,
- Informationssicherheitsbeauftragte,
- Datenschutzbeauftragte,
- Personalvertretung.

Die Zusatzinformationen für diese spezifischen Bereiche werden in der Regel über die Stabsstruktur in *Notfällen* und *Krisen* (→ *Kapitel 5.2.1*) im Rahmen der entsprechenden Stabsbesprechungen weitergegeben.

Darüber hinaus gibt es eine ganze Reihe von **externen Zielgruppen** mit jeweils eigenen Bedarfen:

- Bevölkerung:
  - sowohl direkt Betroffene (z. B. über Sozialamt, Jugendamt) als auch lediglich räumlich betroffene oder interessierte Personen,
  - verschiedene Altersgruppen,
  - Menschen mit Einschränkungen,
  - nicht deutschsprachige Personen,
- Medien,
- ansässige Wirtschaftsunternehmen,
- kommunale Eigenbetriebe,
- andere Behörden (insbesondere mit bestehender Zusammenarbeit) und Dienstleistende, die Dienstleistungen liefern oder mit einer Dienstleistung beliefert werden.

Sonderfall: Zusätzlich gibt es ggf. explizite Meldeverpflichtungen bei Vorfällen sowie direkt benötigte oder hilfreiche Einrichtungen für die unmittelbare Bewältigung (z. B. Polizei oder externe Dienstleister), mit denen kommuniziert werden muss. Auf diese Aspekte wird im → *Kapitel 5.2.2* näher eingegangen.

Welche Kanäle?

Es sollten möglichst alle von der Bevölkerung für den Kontakt mit der Kommunalverwaltung genutzten Kommunikationswege mit einem Hinweis auf die aktuelle Situation und ggf. einem Verweis auf weiterführende Informationen versehen werden:

- eigene Website: Sofern noch verfügbar, erstaufgerufene Seite mit auffälligem Hinweis versehen oder Overlay einblenden[62], falls nicht mehr verfügbar, Notfall-Webseite bei externem Webhoster anlegen[63],
- andere Websites bspw. von kommunalen Unternehmen,
- soziale Medien (soweit bereits genutzt),
- Pressemitteilung,
- lokale Medien (Radio, Zeitung, Fernsehen, ggf. inkl. der Regionalbüros der Landessender),
- Aushang auf Eingangstüren mit Publikumsverkehr,
- Telefonbandansage,
- ggf. Faltblätter mit Erreichbarkeiten an zentralen Anlaufpunkten in der Kommune.

Die Fülle der Informationen und der andauernde Aktualisierungsbedarf sind herausfordernd. Es sollte daher eine Konzentration auf einige wenige Kanäle erfolgen, auf denen umfassend und aktuell informiert wird, während an anderer Stelle lediglich auf diese Informationsquellen verwiesen wird. Bei der Auswahl der aktiv befüllten Kanäle müssen verschiedene Aspekte berücksichtigt werden, z. B. Schnelligkeit und Aufwand der Befüllung (welche Kanäle können selbst bedient werden, bei welchen wird ein Mittler benötigt?), Reichweite, verschiedene Zielgruppen, Ausfallsicherheit und Nutzbarkeit bei einem eigenen IT-Vorfall.

Welche Inhalte?

Vorrangig sollten folgende Grundprinzipien für die Kommunikation gelten:

- schnell (aktiv und frühzeitig),
- wahr (sachlich, transparent und korrekt),
- verständlich (kurz, einfach, unkompliziert, bildhaft),
- konsistent (einheitlich, koordiniert und kontinuierlich).

Dabei gilt der Grundsatz: Schnelligkeit geht vor Vollständigkeit. Das bedeutet nicht, dass Schnelligkeit grundsätzlich vor Richtigkeit gehen sollte, aber selbst bei einer unsicheren Faktenlage sollte das bereits Bekannte kommuniziert werden. Jedes Zögern oder Warten auf die letzte Datenlage bietet Raum für Spekulationen von Medien, Gegnern eines transparenten Prozesses

[62] Hierbei handelt es sich um eine Seiteneinblendung, die über die eigentlichen Inhalte gelegt wird und in jedem Fall wahrgenommen und aktiv entfernt werden muss. Ein Beispiel findet sich in → *Abbildung 5* am Ende dieses Unterkapitels.

[63] Es empfiehlt sich ggf. auch die Vorbereitung einer sogenannten Darksite. Dabei handelt es sich um bereits vorbefüllte Webseiten, die erst in *Notfall* oder *Krise* freigeschaltet und damit öffentlich zugänglich werden, ggf. auch bei einem externen Webhoster.

und möglicherweise auch Profiteuren der vermeintlich unsicheren Lage. Das kann unterschiedliche Formen annehmen, z. B. ein gezieltes Streuen falscher Informationen oder das Anpreisen angeblich jetzt erforderlicher „Katastrophenüberlebenspakete". Die Kommune droht dann die Deutungshoheit über die Situation zu verlieren. Anerkannt ist mittlerweile, dass man auch Unsicherheit über die Faktenlage bzw. noch offene Fragen kommunizieren kann, solange weiterhin mitgeteilt wird, was man tun möchte, um genau diese unsichere Faktenlage zu beseitigen (Kommunikation der im *Verwaltungsstab* getroffenen Maßnahmen, bspw. „Erkundungsteam", „*Krisenstab*", „externe Expertenteams", „Dienstleister", „weitere folgende Maßnahmen").

Sind mehrere Stellen mit der Vorfallbewältigung betraut (z. B. Ermittlungsbehörden, Einrichtungen des Landes, externe Dienstleister), dann muss sichergestellt sein, dass die Kommunikation nach außen dennoch konsistent erfolgt. Entweder nur eine Stelle kommuniziert, oder es findet eine enge Abstimmung zwischen den Stellen statt. Vor Veröffentlichung von technischen Details eines Angriffs und Informationen zu einer Angreifergruppierung ist eine Absprache mit den Ermittlungsbehörden unabdingbar.

Wie die Lagebewältigung insgesamt ist auch die Kommunikation darüber ein Dauerlauf mit unterschiedlichen Phasen:

Sehr schnelle Erstinformation
Hier geht es um einen schnellstmöglichen Hinweis auf auftretende Einschränkungen samt kurzer Begründung. Im besten Fall können zu diesem Zeitpunkt schon Auswirkungen für die Bevölkerung grob skizziert sowie erste Notfallerreichbarkeiten und Hinweise auf die für weiterführende Informationen gewählten Kanäle gegeben werden. Eine kommunikative Überspitzung in der Lagedarstellung sollte vermieden werden (Kommunikationsgrundsatz: „wahr").

Weiterführende Informationen/FAQ
Einige Stunden nach der Erstmeldung erfolgt idealerweise die nächste Meldung mit weiteren Details und Auskünften. Zügige bzw. im weiteren Verlauf regelmäßig erfolgende Aktualisierungen der Informationen sind von großer Bedeutung:

So wird auch nach außen transportiert, dass die Vorfallbewältigung stetig und aktiv weitergetrieben wird. Beginnend mit der Erstinformation ergibt sich so eine aufeinander aufbauende, sachliche und stets aktuelle Berichterstattung aus erster Hand.

Zu den relevanten Inhalten gehören typischerweise:

- Beschreibung und Erklärung der Situation,
- Umfang der Gefahren und Folgeschäden (z. B. Kategorien betroffener Daten, möglicher Datenabfluss),
- Schilderung der Gegenmaßnahmen (Nennung von Namen beteiligter Behörden und Unternehmen nur nach Abstimmung),
- Zeitabschätzung für die Wiederherstellung von Dienstleistungen,
- weitere, detailliertere Erreichbarkeiten,
- geänderte Orte oder Abläufe (z. B. manuelle Bearbeitungsstellen, Spezialbehandlung in Härtefällen),
- Empfehlungen/Hinweise für Bevölkerung und betroffene Unternehmen (z. B.: Woran kann erkannt werden, dass eine Kommunikation der Kommunalverwaltung authentisch ist? Wie sollte man sich verhalten, wenn Unregelmäßigkeiten im Zusammenhang mit den eigenen Daten vermutet werden?).

Bei vergangenen größeren Vorfällen hat sich im weiteren Verlauf die Veröffentlichung von Frequently Asked Questions (FAQ) bewährt, also einer Zusammenstellung von häufig gestellten Fragen sowie der zugehörigen Antworten. Diese Fragen und Antworten sollten übersichtlich strukturiert zur Verfügung gestellt werden, damit sie das Auffinden jeweils benötigter Detailinformationen ermöglichen. Ein Beispiel für FAQ findet sich in → *Abbildung 6* am Ende dieses Unterkapitels.

Es ist sehr empfehlenswert, die Veröffentlichungen Dritter (Medien, Social Media etc.) über den Vorfall sowie die sich dazu entwickelnden Online-Diskussionen zu beobachten. Hier können sich unter Umständen falsche Informationen rasch und weit verbreiten. Durch die Beobachtung kann bei Bedarf zeitnah mit Präzisierungen oder Korrekturen reagiert werden. Diese Art

des moderierenden Eingriffs stellt einen Mehraufwand dar, ist allerdings auch notwendig, um die Hoheit über die Lagedarstellung zu behalten. Ein solches Monitoring ist zusätzlich für den *Verwaltungsstab* notwendig (→ *Kapitel 5.2.1*), da daraus bspw. Erkenntnisse über Nachsteuerungsbedarf bei Bewältigungsmaßnahmen gewonnen werden können. Beide Bedarfe sollten, schon um Ressourcen zu sparen, aus einer Hand adressiert werden.

Umgang mit großem Medieninteresse

Während eines *IT-Notfalls* oder einer *IT-Krise* kann ein ggf. sehr großes Medieninteresse zu erheblichem Handlungsdruck führen. Dies gilt insbesondere dann, wenn der Vorfall auch die überregionalen Medien erreicht und sich die Anzahl der Anfragen entsprechend potenziert. Der damit einhergehende Aufwand muss im Vorfeld einkalkuliert werden.

Erste hilfreiche Schritte sind das Etablieren und Einüben der Kommunikationsstrukturen im Vorfeld sowie im Ereignisfall die Vorwegnahme und Bündelung möglicher Anfragen in Form weiterführender Informationen bzw. FAQ sowie Pressestatements oder Pressekonferenzen.

Sinnvoll ist darüber hinaus, für (externe) Unterstützung zu sorgen. Können Mitarbeitende anderer Bereiche aufgrund des IT-Vorfalls ihrer regulären Tätigkeit nicht nachgehen, so könnten sie als Verstärkungskräfte eingesetzt werden. Mit einer geeigneten Sprachregelung und den FAQ lässt sich auf diesem Weg die telefonische Erreichbarkeit für Nachfragen verbessern. Eventuell besteht für kreisangehörige Städte und Gemeinden auch die Möglichkeit einer gegenseitigen Unterstützung der Pressestellen innerhalb des Kreises. Im Aufgabenfeld des Monitorings von Social Media stellt möglicherweise die Einbindung spezialisierter Strukturen, z. B. der Hilfsorganisationen, des Technischen Hilfswerks (THW) oder der Berufsfeuerwehren, etwa im Sinne eines „VOST“ (Virtual Operation Support Team), eine Option dar. Bestehen gute und vertrauensvolle Kontakte zu lokalen Journalistinnen und Journalisten, geben diese möglicherweise erlangte offizielle Informationen in Online-Diskussionen weiter oder weisen die kommunale Pressestelle auf kritische Debatten in Social-Media-Gruppen hin. In jedem Fall ist es hilfreich, die Möglichkeiten bereits im Vorfeld durchzudenken und Absprachen zu treffen. Dabei sollten bereits etablierte Konstrukte und Kontakte vorrangig eingeplant und genutzt werden, um einen möglichst reibungsfreien Ablauf zu erlauben.

Spezielle Inhalte für die interne Kommunikation

Bei der Kommunikation gilt grundsätzlich „intern“ vor „extern“: Die eigenen Mitarbeitenden sollten die Informationen nicht aus den Medien erhalten, sondern sie vorher oder zeitgleich zur Verfügung gestellt bekommen. Es ist nicht zu vermeiden, dass sie auf den Vorfall angesprochen und nach Informationen gefragt werden. So können sie dann informiert als Multiplikatoren fungieren, anstatt mit ihrer Unsicherheit alleingelassen zu werden.

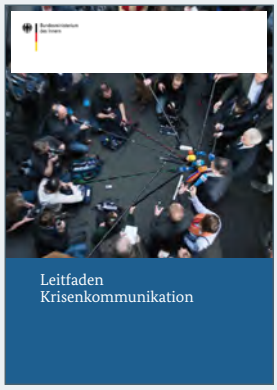
Mitarbeitende sollten gezielt darauf vorbereitet werden, dass sie unter Umständen auf die aktuellen Vorgänge in der Kommune angesprochen werden. Es wird daher eine Sprachregelung für die Außenkommunikation benötigt. Die Mitarbeitenden sollten gegenüber Medienvertretern grundsätzlich auf die offiziellen Ansprechpartnerinnen und -partner der Institution verweisen. Zudem sollte darauf geachtet werden, dass die Informationen, die den Mitarbeitenden an die Hand gegeben werden, für die Öffentlichkeit geeignet sind oder bei internen Informationen klar kommuniziert wird, wie damit umzugehen ist.

Bei einem Cyberangriff steht immer auch die Schuldfrage im Raum. Mitarbeitende werden nervös und fahrig, wenn sie Angst haben, dass sie die Situation verursacht haben könnten. Möglicherweise wird sogar nach Sündenböcken gesucht oder bereits existierende Konflikte wachsen sich in der Stresssituation zum Mobbing Einzelner aus. Dem muss offensiv begegnet werden. Schon die deutliche Botschaft, dass Fehler gerade in Stresssituationen jedem passieren können und nun die gemeinsame Bewältigung im Fokus steht, kann entschärfend wirken. Auch Entscheidungen zu Priorisierungen im Rahmen des Wiederanlaufens eines Netzwerks müssen offen kommuniziert werden. Schließlich haben alle Mitarbeitenden ihre eigenen wichtigen

Aufgaben – werden diese vom *Verwaltungsstab* ohne weiteren Kommentar augenscheinlich nicht als wichtig wahrgenommen, kann dies zu Unmut führen.

Die Gestaltung der internen Kommunikation bleibt über die Dauer der Lagebewältigung eine anhaltende Aufgabe. Die Mitarbeitenden müssen Geduld für monatelange Arbeitseinschränkungen und Provisorien aufbringen. Es braucht Verständnis für das schnell überlastete Schlüsselpersonal, das nicht alle Anliegen direkt abarbeiten kann. Verschärfte Sicherheitsregeln müssen immer wieder erklärt und in Erinnerung gerufen werden, damit sie nicht zu schnell wieder aufgeweicht werden.

Weiterführende Literatur:



Leitfaden Krisenkommunikation
BMI, 2014
[BMI14] (→ *Anhang 2*)

Der Leitfaden klärt die Schlüsselbegriffe und enthält eine Übersicht über Prozesse und Strukturen sowie Grundregeln der Risiko- und Krisenkommunikation. Hinzu kommen Arbeitshilfen und Checklisten zur Vor- und Nachbereitung von Krisenkommunikation sowie ein Muster für den Aufbau eines Krisenkommunikationsplanes.

Weiterführende Informationen:

Seminarangebot der BABZ
BBK (BABZ), 2024
https://www.bbk.bund.de/DE/Themen/Akademie-BABZ/BABZ-Angebot/Veranstaltungen/veranstaltungen_node.html

Die Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung (BABZ) bietet im Rahmen ihres Lernangebots Seminare zu Grundlagen und Strukturen der Risiko- und Krisenkommunikation an. Die Kosten für Veranstaltungen der BABZ werden dabei weitestgehend vom Bund getragen.

Aus der Praxis: Positivbeispiele der Krisenkommunikation

Hier werden als Ergänzung zum Kapitel 5.2.5 einige Beispiele für Krisenkommunikation durch Kommunen bei vergangenen IT-Vorfällen aufgeführt. Es handelt sich um Teile der Krisenkommunikation, die sich im Einzelfall als durchaus wirksam herausgestellt haben. Sie sind jedoch nicht als rundum empfohlene Musterbeispiele zu verstehen. Vielmehr wurden sie als Ideengeber und Ausgangspunkt für Überlegungen zur Erstellung eigener Vorlagen hier aufgeführt.

HINWEIS ZUM CYBERANGRIFF

auf Stadtverwaltung, Stadtwerke und Sozialstation der Stadt Rodgau

STADTRODGAU

Benachrichtigung über eine Verletzung des Schutzes von personenbezogenen Daten gemäß Art. 34 Abs. 1 DSGVO i.V.m. § 61 HDSIG.

Was ist passiert?

Am 23.02.2023 drangen bislang unbekannte Akteure von außen in unsere Netzwerke ein und verschafften sich Zugang zu internen Informationen.

Was haben wir getan?

- Unmittelbar nach Bekanntwerden des Cyberangriffs wurden die zuständigen Behörden über den Vorfall informiert.
- Der Hessische Beauftragte für Datenschutz und Informationsfreiheit wurde unverzüglich im gleichen Zuge durch eine entsprechende Erstmeldung benachrichtigt. Zum aktuellen Zeitpunkt stehen wir in ständigem Austausch mit den zentralen Ermittlungsbehörden sowie der hessischen Datenschutzbehörde.

Woran arbeiten wir?

- Gegenwärtig arbeiten wir mit mehreren Unternehmen aus dem Bereich der IT-Sicherheit, die auf Cyberangriffe sowie Krisenmanagement spezialisiert sind, zusammen.
- Die IT-Abteilung der Stadtverwaltung und Stadtwerke arbeiten mit Hochdruck an umfangreichen Schutzmaßnahmen, um weitere Schäden zu verhindern und Systeme sowie Datenbestände abzusichern. Zusätzlich wird das Informationssicherheitsniveau der Stadt nach dem erfolgreichen Cyberangriff dem Risiko entsprechend angepasst, um den Angriff bestmöglich aufzuarbeiten und zukünftige Angriffe besser abwehren zu können.

Was bedeutet das für Sie?

- Zum aktuellen Zeitpunkt ist der Stadt Rodgau kein Datenabfluss bekannt, jedoch ist dieser nicht gänzlich auszuschließen. Sollten wir zu einem späteren Zeitpunkt feststellen, dass ein Datenabfluss stattgefunden hat, werden wir Sie unverzüglich gesondert darüber informieren.
- Wir bitten Sie im Augenblick der Lage um erhöhte Wachsamkeit im Kontext der Kommunikation mit der Stadt Rodgau. Darunter fallen insbesondere gefälschte E-Mails (Phishing), gefälschte Telefonanrufe oder verdächtige E-Mail-Anhänge mit Schadcode, die ggf. durch Dritte im Kontext der Stadt versendet werden könnten.

Vielen Dank für Ihr Verständnis und Ihr Vertrauen.

Abbildung 4: Zeitungsannonce der Stadt Rodgau zur Information über einen möglichen Abfluss personenbezogener Daten (Quelle: Stadt Rodgau)

Erstinformationen (Stadt Rodgau)

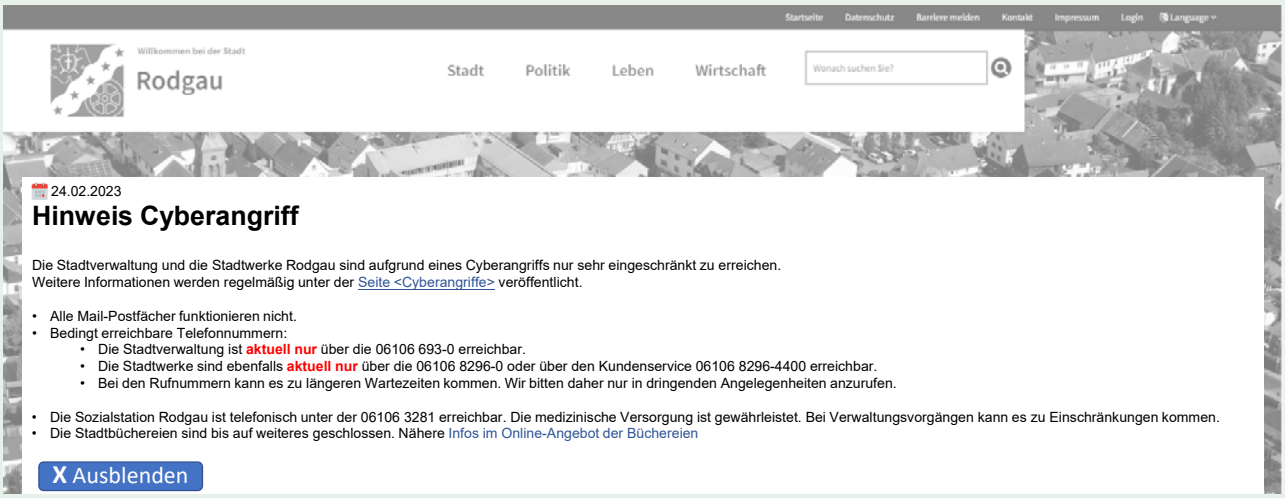


Abbildung 5: Website Overlay der Stadt Rodgau, [ROD23] (→ *Anhang 2*)

FAQ (Rhein-Pfalz-Kreis)

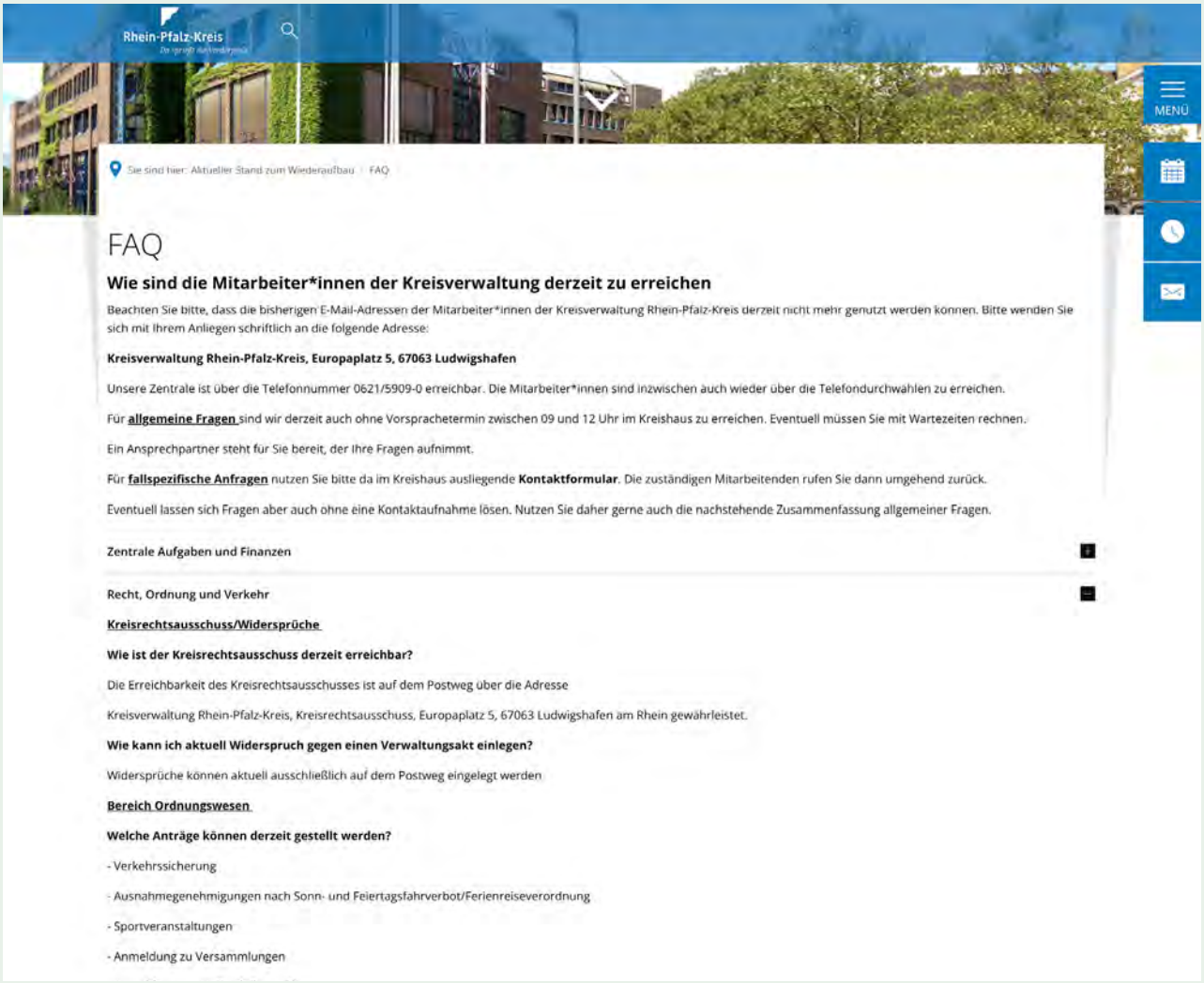


Abbildung 6: Auszug der FAQ des Rhein-Pfalz-Kreises, [RPK23] (→ *Anhang 2*)

5.2.6 Übung macht den Meister

Kernpunkte:

- Übungen als Chance sehen, aus Fehlern zu lernen
- Denk- und Planungslücken aufzeigen
- In Krisen Köpfe kennen – Akteure im Krisenmanagement kennenlernen
- IT-Systeme und Backup-Möglichkeiten testen

Die Cyberangriffe auf Kommunen der vergangenen Zeit führen deutlich vor Augen, wie sehr kommunale IT durch Angriffe von außen beeinträchtigt und geschädigt werden kann. Die Handlungsabläufe in Cyberkrisensituationen regelmäßig zu üben, hilft, diesem Risiko zu begegnen und die möglichen Auswirkungen eines Cyberangriffs zu reduzieren.

Dabei können einerseits Tests durchgeführt werden, um spezifische technische und organisatorische Maßnahmen zunächst zu überprüfen und praxisnah zu erproben und zu optimieren. Dies kann das erstmalige Wiedereinspielen eines Backups umfassen, das Testen der technischen Notfallausstattung oder auch eine erste Krisensitzung in einer neu zusammengesetzten Stabsstruktur. Übungen im engeren Sinne dienen auf der anderen Seite dazu, die bereits fertig ausdefinierten und im Vorfeld den handelnden Personen in einer Ausbildungsveranstaltung beigebrachten Prozesse des Krisenmanagements zu festigen und die Handlungssicherheit zu stärken. In der Ausführung sind Tests und Übungen im engeren Sinne sehr ähnlich, sodass sie häufig auch vermischt zum Einsatz kommen. Im Folgenden wird daher nicht explizit zwischen diesen beiden Formen unterschieden, sondern auf den Nutzen und die verschiedenen möglichen Formate von Übungen im weiteren Sinne (einschließlich Tests) eingegangen.

Wirksames Krisenmanagement

Übergreifendes Ziel von Krisenmanagementübungen ist die Optimierung von Abläufen. Dies kann Tests der vorab festgelegten Zuständigkeiten und Notfallpläne ebenso umfassen wie das Einüben des Handelns in den verschiedenen festgelegten Eskalationsstufen. Übungen können zudem mögliche Denklücken, z. B. fehlende Berücksichtigung von Interdependenzen, aufzeigen und somit die Folgen eines realen Cyberangriffs reduzieren. Die gewonnenen Erfahrungen und die Verbesserung von festgestellten Defiziten können in einer realen Schadenslage zu einer besseren Bewältigung führen.

Übungen im engeren Sinne dürfen jedoch nicht dazu führen, dass Übungsteilnehmende überfordert und damit verunsichert werden. Sie müssen immer das Ziel der Förderung der Handlungskompetenz haben. Eine falsche, überfordernde Übungssteuerung könnte hierfür kontraproduktiv sein.

Handelnde Personen kennenlernen und gemeinsames Verständnis schaffen

Krisenmanagementübungen erfordern – genau wie eine Lagebewältigung es auch täte – die Zusammenarbeit verschiedener Fachbereiche bzw. Organisationen, die im Alltag nur wenige Berührungspunkte haben. Unterschiedliche Erwartungshaltungen, spezifische Sichtweisen sowie die Bedeutung von (Fach-)Begriffen können in gesicherter Übungsumgebung abgeglichen und geklärt werden. So schaffen Übungen ein gemeinsames Verständnis für Probleme, die unterschiedliche Schwerpunktsetzung der Beteiligten sowie Lösungswege und helfen im Ereignisfall, das Zusammenwirken zu vereinfachen. Wer „in Krisen Köpfe kennt“, also alle relevanten Akteure bereits vor Eintritt eines Vorfalls kennengelernt hat, kann im Rahmen einer Lagebewältigung schneller agieren und somit mögliche Schäden

reduzieren. Übungen können eine sehr gute Gelegenheit sein, die entsprechenden Netzwerke innerhalb der Kommunalverwaltung und mit externen Partnern wie bspw. IT-Dienstleistern zu knüpfen.

Die Vorteile persönlicher Netzwerkbildung dürfen allerdings nicht dazu führen, dass die Ereignisbewältigung personenabhängig gedacht wird! Die Strukturen und Prozesse müssen auch dann funktionieren, wenn sich die beteiligten „Köpfe" im konkreten Fall noch nicht kennen.

Wissen

Kommunale Akteure, die sich regelmäßig mit der Sicherheit ihrer IT-Systeme auseinandersetzen, werden mögliche Schäden eines Cyberangriffs besser bewältigen. Die Sensibilisierung des *IT-Betriebs*, aber auch der Verwaltungsspitze sowie aller Mitarbeitenden kann die Durchführung von Angriffen erschweren. Erkenntnisse, die aus Übungen oder realen Cyberangriffen auf andere Kommunen oder Unternehmen gewonnen werden, helfen dabei, Schwachstellen zu identifizieren, die Sicherheit der eigenen IT zu erhöhen sowie das Krisenmanagement zu verbessern. Regelmäßiger Austausch zu „lessons learned" bietet die Gelegenheit, neue Lösungsansätze kennenzulernen, darüber zu diskutieren und so voneinander zu lernen. Der Blick „über den Tellerrand" und auf kreative Lösungen, die anderenorts funktioniert haben, kann dabei helfen, auch bei eigener Betroffenheit neue, unkonventionelle Wege zu beschreiten, z. B. um Dienstleistungen provisorisch wieder anzubieten.

Berührungsängste abbauen

Besonders bei Mitarbeitenden, die in ihrem beruflichen Alltag kaum tiefer gehende Berührungspunkte damit haben, entstehen oft Hemmungen, sich mit dem fremden und unüberschaubaren Thema „Cybersicherheit" zu beschäftigen. Schulungsveranstaltungen und gut gesteuerte Übungen helfen, diese Berührungsängste abzubauen. Durch das Auseinandersetzen mit den unbequemen Themen gewinnen die Mitübenden an Klarheit und Handlungssicherheit in realen Gefahrenlagen.

Übungskonzepte

Übungen können grundsätzlich mit sehr unterschiedlichen Zielsetzungen organisiert werden. Daher müssen vor der Auswahl eines Übungskonzepts zunächst die Ziele konkretisiert werden.

Übungen zur Bewältigung von Cyberangriffen können dann bspw. als theoretische Planbesprechungen, Stabsübungen, technische Tests oder praktische Vollübungen durchgeführt werden (für nähere Erläuterungen der verschiedenen Übungskonzepte siehe weiterführende Literatur am Ende des Unterkapitels). Vorbereitung, Aufwand und Schwierigkeit der Übungen müssen dabei individuell an die Gegebenheiten vor Ort angepasst werden. Bei Bedarf können externe Dienstleister hinzugezogen werden, um bei der Konzeption von Übungen zu beraten, diese vorzubereiten und durchzuführen oder sie zu beobachten und zu evaluieren.

Ist bislang noch keine Übung zu diesen Themen durchgeführt worden, empfiehlt sich ein Einstieg in zunächst begrenztem Umfang. Im technischen Bereich kann dies bspw. das testweise Zurückspielen eines Backups in geschützter Umgebung sein (Restore-Übung). Zur ersten Überprüfung der Krisenmanagement-Strukturen und -Prozesse lässt sich mit geringem Vorbereitungsaufwand der *Verwaltungs- bzw. Krisenstab* (ggf. inkl. IT-Dienstleister) zusammenrufen. Mittels eines kurzen Lagevortrags kann der Stab dann mit der Situation eines vollständigen Serverausfalls für mindestens zwei Wochen konfrontiert werden und die notwendigen Schritte in einer ersten Übungssitzung durchsprechen. So kann auf einer noch recht simplen ersten Übung über einen längeren Zeitraum modulweise aufgebaut werden. Dabei können weitere Tests und Übungen mit spezifischem ergänzendem Fokus gewählt werden, bevor perspektivisch tatsächlich auch eine praktische Vollübung angesetzt werden kann.

Weiterführende Literatur:

Übungsbaukasten des UP KRITIS
TAK Übungen des UP KRITIS, 2022
https://www.bsi.bund.de/dok/upk-uebungsbaukasten

Der Themenarbeitskreis (TAK) Übungen des UP KRITIS hat zur Unterstützung von Betreibern Kritischer Infrastrukturen bei der Planung, Durchführung und Nachbereitung von Übungen einen Übungsbaukasten erstellt. Er dient als praxisorientierte Hilfestellung, um Übungen systematisch und effektiv durch alle Phasen zu begleiten. Hierfür stehen Übersichten über Übungsarten, Anleitungen, Hilfsmittel und Vorlagen zur Verfügung.

Trainingskoffer
BSI
https://www.bsi.bund.de/dok/Trainingskoffer

Zur niedrigschwelligen Sensibilisierung der Mitarbeitenden bietet das BSI eine kostenfreie Spielesammlung an. Mit dieser kann die Bewältigung eines Cyberangriffs spielerisch trainiert werden.

5.3 Externe Unterstützungsmöglichkeiten

Kernpunkte:

- Proaktiv Kontakte knüpfen, noch bevor ein IT-Vorfall eintritt
- In vielen Bundesländern bieten die zuständigen Landeseinrichtungen Unterstützung an.
- Austausch in Fachkreisen: IT-SiBe-Forum, Allianz für Cyber-Sicherheit, Jahrestagungen
- Kooperationsvereinbarungen mit umliegenden Kommunen für den Fall der Fälle

Einzelkämpfer haben es oft schwer, so auch bei der Informationssicherheit. Gerade kleinen Kommunen fehlt es eventuell an den entsprechenden Fachkräften, um sich ausführlich mit der Absicherung ihrer technischen Infrastruktur zu beschäftigen. Die Fülle der Aufgaben erschwert zudem eine detaillierte Vorbereitung. Doch es existieren zahlreiche Unterstützungsangebote der Spitzenverbände, Einrichtungen auf Landesebene und von Bundesbehörden. Idealerweise sollten sich die zuständigen Personen in Kommunen damit externer Hilfe bedienen und im Vorfeld ein Netzwerk aus Verbündeten aufbauen. Denn wird ein Sicherheitsvorfall medienwirksam bekannt, gehen eventuell nicht nur seriöse Hilfsangebote ein.

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) erstellt Handreichungen und Arbeitshilfen und engagiert sich in Arbeitskreisen, bspw. bei der Entwicklung des speziell an kommunale Verwaltungen angepassten IT-Grundschutz-Profils. Mitgliedern der Allianz für Cyber-Sicherheit beim BSI stehen zahlreiche Handlungsempfehlungen und Austauschformate zur Verfügung. Bestimmte Betroffene (vor allem KRITIS-Betreiber, Stellen des Bundes) kann das BSI im Rahmen seines gesetzlichen Auftrags auch bei der Bewältigung von IT-Sicherheitsvorfällen tatkräftig unterstützen.

Schulungen für die Wahrnehmung der Aufgaben als ISB werden von der Bundesakademie für öffentliche Verwaltung (BAköV) in enger Zusammenarbeit mit dem BSI angeboten. Die Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung (BABZ) des BBK bietet verschiedene Seminare zum Risiko- und Krisenmanagement (→ *Kapitel 5.2.1*) an. Ziel ist die Kompetenzförderung im Krisenmanagement, die Beratungen zum Aufbau entsprechender Strukturen sowie die Identifizierung von individuellem Handlungsbedarf.

Auch Einrichtungen auf Länderebene bieten mehr und mehr Unterstützungsmöglichkeiten an, die teilweise auch Kommunen anderer Länder offenstehen. Eine zentrale Rolle spielen dabei die *Computer Emergency Response Teams* (CERTs), die bspw. einen zielgruppengerechten Informations- und Warndienst oder automatisierte Leak-Checker zur Verfügung stellen. Das hessische Cyber Competence Center (H3C) schult z. B. im Cyberabwehr-Ausbildungszentrum für Kommunen die Erarbeitung und nachhaltige Implementierung von Notfallplänen für die Betriebsfortführung im Falle eines Ausfalls der IT-Systeme (*Business Continuity Management)*. Die Cybersicherheitsagentur Baden-Württemberg (CSBW) bietet eine rund um die Uhr besetzte Hotline zur Cyber-Ersthilfe an. Das Bayerische Landesamt für Sicherheit in der Informationstechnik (LSI) gibt Kommunen auch beim Aufbau des Notfallmanagements Hilfestellung. Als Kommune lohnt es sich damit in jedem Fall, mit einem bestimmten Bedarf auf die eigenen Landesbehörden zuzugehen.

Zum Thema Spionageabwehr bzw. Cyberkriminalität stehen die Landesbehörden für Verfassungsschutz (LfV) und Landeskriminalämter (LKÄ) als Ansprechpartner zur Verfügung. Zur Beratung und Prävention können Kommunen auf vielfältiges Informationsmaterial und Angebote für individuelle Vortragsveranstaltungen zurückgreifen. Bei einem Cyberangriff empfiehlt

es sich, diese Stellen frühzeitig für forensische Zwecke mit einzubinden (→ *Kapitel 5.2.2*).

Eine Mitgliedschaft in Netzwerken von Fachexperten kann ein weiterer Weg sein, den Austausch von Wissen bei der Umsetzung von Informationssicherheit in Theorie und Praxis zu fördern. Das vom Deutschen Landkreistag getragene und vom Deutschen Städtetag, dem Deutschen Städte- und Gemeindebund sowie dem BSI unterstützte Forum der IT-Sicherheitsbeauftragten von Kommunen und Ländern (IT-SiBe-Forum[64]) dient explizit dem Erfahrungsaustausch. Auch regelmäßige Veranstaltungen kommunaler Spitzenverbände, wie bspw. der „Kommunale IT-Sicherheitskongress" der Kommunalen Spitzenverbände oder das Onlineformat „Digital.Kommunal.Sicher – Informationssicherheit in der Kommunalverwaltung" der kommunalen Spitzenverbände Nordrhein-Westfalens und des Dachverbandes kommunaler IT-Dienstleister in NRW (KDN), sind ein guter Ansatzpunkt.

Hilfreich kann es auch sein, sich einen Überblick über den Markt für Incident-Response-Dienstleister zu verschaffen, die bei der Forensik und dem Wiederaufbau als Externe unterstützen. Das BSI pflegt eine Liste qualifizierter Dienstleister, die bei gezielten Angriffen durch APT-Angreifer helfen können.[65] Mit den so gewonnenen Informationen können Kontaktdaten im Handbuch IT-Notfallmanagement hinterlegt werden, und die Vergabe im Ereignisfall wird entscheidend beschleunigt. Cyberversicherungen können zumindest Teile der Kosten für Betriebsausfall und Wiederaufbau nach Cyberangriffen decken. Teil dieser Policen ist nicht selten auch die Bereitstellung externer Dienstleister zur Unterstützung im Schadensfall. Allerdings wird häufig bereits ein relativ hoher Umsetzungsstand der Informationssicherheit zum Abschluss einer Police verlangt (→ *Kapitel 5.1*).

Zuletzt lohnt sich die Vernetzung vor Ort. Hier gibt es möglicherweise ansässige Unternehmen, oder lokale Verbände der Hilfsorganisationen (bspw. → *Kapitel 5.2.5*), die bei der Bewältigung eines Cyberangriffs unterstützen könnten. Insbesondere ist eine Kooperation mit den Nachbarkommunen sinnvoll. Gerade für den Fall eines kompletten IT-Ausfalls können einige der kritischen Dienstleistungen eventuell in Amtshilfe von den umliegenden Kommunen erbracht werden. Idealerweise existieren dafür bereits im Vorfeld verschriftlichte Absprachen. Diese können ebenfalls bei anderweitigen Katastrophenlagen für die Verwaltung (bspw. Stromausfall, Hochwasser) zum Einsatz kommen.

Übersicht der Ansprechpartner

- Standards, Handreichungen, zielgruppenspezifische Arbeitshilfen: Bundesamt für Sicherheit in der Informationstechnik (BSI), Kommunale Spitzenverbände, ggf. Landeseinrichtungen für IT-Sicherheit
- Wissensaustausch: Allianz für Cyber-Sicherheit, IT-SiBe-Forum, Kommunale Spitzenverbände
- Schulungen & Weiterbildung: BAköV, BABZ, Landeseinrichtungen für IT-Sicherheit
- Warn- und Informationsdienst: Landeseinrichtungen für IT-Sicherheit/CERTs
- Prävention Cybercrime: Landeskriminalämter, Zentral- und Ansprechstelle Cybercrime (ZAC)
- Spionageabwehr: Landesämter für Verfassungsschutz, Bundesamt für Verfassungsschutz
- Forensik, Wiederaufbau: Externe IT-Dienstleister (ggf. Zertifizierung durch BSI)
- Amtshilfe: Nachbarkommunen

[64] [IT-SiBe-Forum] (→ *Anhang 2*).

[65] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

Weiterführende Links:

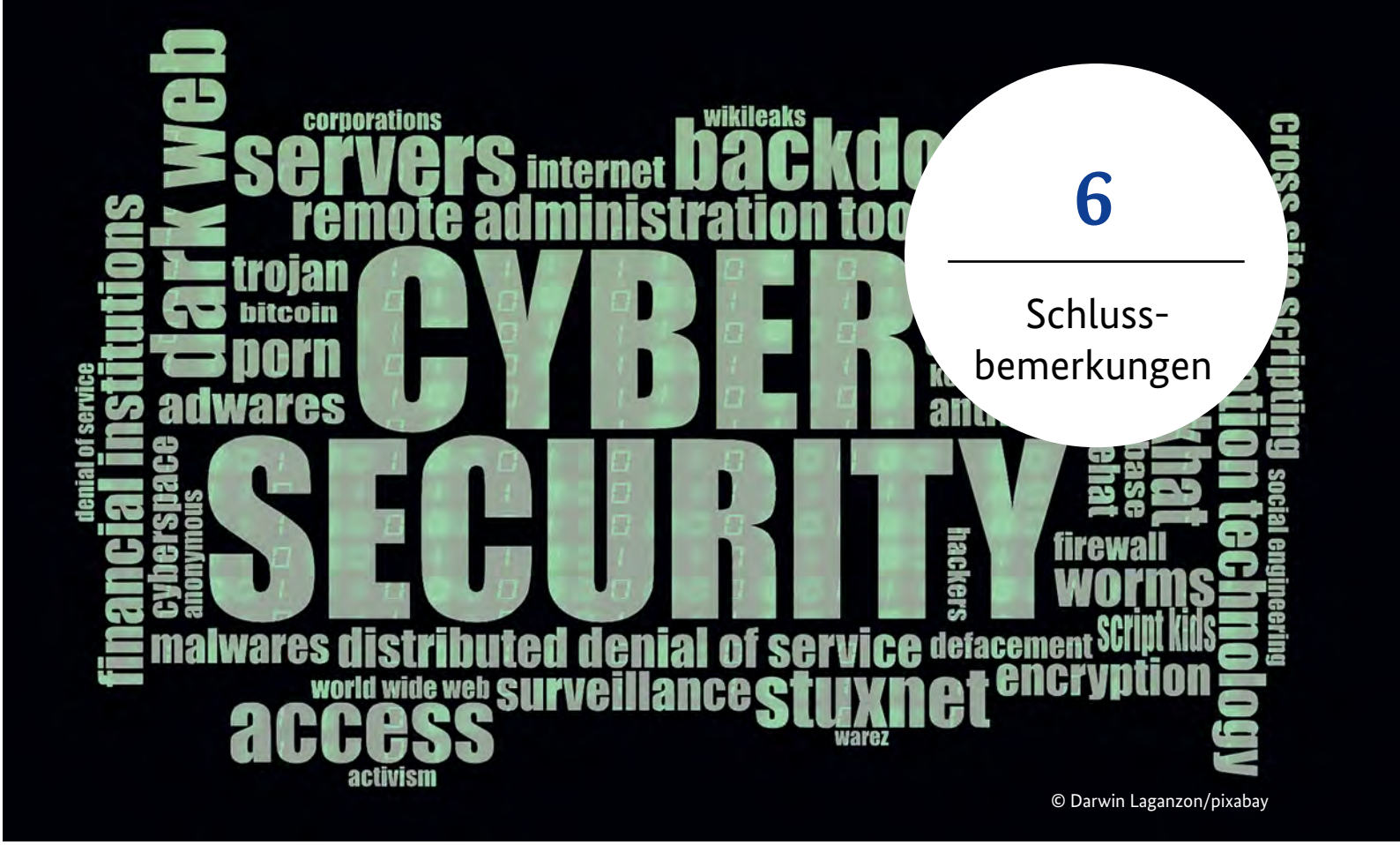
Forum der IT-Sicherheitsbeauftragen
[IT-Sibe-Forum] (→ *Anhang 2*)

Allianz für Cyber-Sicherheit
[ACS] (→ *Anhang 2*)

BSI-Sicherheitsberatung für Länder und Kommunen
https://www.bsi.bund.de/dok/SicherheitsberatungLK

BfV-Kontaktmöglichkeiten
Prävention: wirtschaftsschutz@bfv.bund.de, Tel.: 030-18-792-3322
Spionageabwehr (Hinweise): hinweise@bfv.bund.de, Tel.: 030-18-792-6000

Übersicht der Leistungen von Bund und Ländern (Stiftung Neue Verantwortung)
[SNV23] (→ *Anhang 2*)



Schlussbemerkungen

Informationssicherheit kostet Zeit und Geld. Doch ein Totalausfall der Informationstechnik zieht einen längeren Ausfall wichtiger Dienstleistungen nach sich und verursacht damit nicht nur finanziellen Schaden für die betroffene Kommune. Der Ausfall kann vielmehr existenzbedrohend für die betroffenen Bürgerinnen und Bürger sowie lokalen Unternehmen sein und auch gegen geltendes Recht verstoßen. Vertrauliche Informationen bzw. personenbezogene Daten können abfließen und veröffentlicht werden. Der Verwaltung droht ein Image- und Vertrauensverlust in der Bevölkerung.

Dieser Wegweiser soll dabei unterstützen, das Bewusstsein für Cybergefahren zu schärfen und eine Auseinandersetzung mit der Thematik zu initiieren. Informationssicherheit ist dabei niemals als Zustand, sondern als laufender Prozess zu verstehen. Insbesondere ein Managementsystem für Informationssicherheit (ISMS) kann diese Entwicklung sinnvoll unterstützen und in die richtigen Bahnen lenken. Präventive und reaktive Maßnahmen, zusammen mit Möglichkeiten zur Detektion, bilden das Grundgerüst für eine solide aufgestellte Informationssicherheit. Und sollte es doch einmal zu einem Vorfall kommen, kann die Bewältigung durch eine adäquate Vorbereitung und das Einüben von Strukturen, Prozessen und Notfallmaßnahmen entscheidend beschleunigt werden.

Eine wirksame Vorsorge für Cybergefahren und ein effizienter Umgang mit *IT-Krisen* wird von der öffentlichen Verwaltung erwartet – gerade vor dem Hintergrund der aktuellen sicherheitspolitischen Lage. Dieser Wegweiser erleichtert Ihnen die Auseinandersetzung mit der Thematik. Sollte Ihnen das Thema noch neu sein, nutzen Sie den Wegweiser als Einstieg. Wenn Sie schon weiter fortgeschritten sind, reflektieren Sie mithilfe des Wegweisers den erreichten Stand und schärfen Sie bei Bedarf noch einmal nach. Wichtig ist, dass Sie anfangen und dranbleiben.

Daher: Nehmen Sie sich direkt einen Baustein des Wegweisers vor und machen Sie den wichtigen nächsten Schritt!

Anhang 1

Abkürzungsverzeichnis und Glossar

Anhang 1.1 Abkürzungsverzeichnis

Erklärungen für kursiv aufgeführte Begriffe finden sich im Glossar.

APT	*Advanced Persistent Threat*
BABZ	Bundesakademie für Bevölkerungsschutz und Zivile Verteidigung
BAköV	Bundesakademie für öffentliche Verwaltung
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BCM	*Business Continuity Management*
BDSG	Bundesdatenschutzgesetz
BIA	*Business Impact Analyse*
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung *Kritischer Infrastrukturen* nach dem BSI-Gesetz
CERT	*Computer Emergency Response Team*
CISO	Chief Information Security Officer
(D)DoS	*(Distributed) Denial of Service*
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
IDS	*Intrusion Detection System*
ISB	Informationssicherheitsbeauftragte/Informationssicherheitsbeauftragter
ISMS	*Information Security Management System*
KMU	Kleine und mittlere Unternehmen
KRITIS	*Kritische Infrastrukturen*
RaaS	*Ransomware-as-a-Service*
RPO	*Recovery Point Objective*
RTO	*Recovery Time Objective*
SLA	*Service-Level-Agreement*
VPN	*Virtual Private Network*
WiBA	Weg in die Basisabsicherung (→ *Kapitel 5.1.1*)

Anhang 1.2 Glossar

Advanced Persistent Threat (APT)	Ein Advanced Persistent Threat (APT) liegt dann vor, wenn ein gut ausgebildeter, typischerweise staatlich gesteuerter Angreifender zum Zweck der Spionage oder Sabotage über einen längeren Zeitraum hinweg gezielt ein Netz oder System angreift, sich unter Umständen darin bewegt und/oder ausbreitet und so Informationen sammelt oder Manipulationen vornimmt.
All-Gefahren-Ansatz	Berücksichtigung aller Gefahrenarten (zum Beispiel Naturgefahren, technologische Gefahren) im Rahmen des Risiko- und Krisenmanagements.
Attribuierung/ Attribution	Attribuierung bezeichnet den Vorgang, den Urheber eines Cyberangriffs zu benennen. (Quelle: [BMI21] (→ *Anhang 2*))
Business Impact Analyse	Eine Business Impact Analyse ist eine strukturierte Untersuchung mit dem Ziel, (zeit-)kritische Geschäftsprozesse und Ressourcen zu identifizieren.
Business Continuity Management (BCM)	Business Continuity Management bezeichnet die Steuerung sämtlicher Aktivitäten, die eine geordnete Geschäftsfortführung nach Schadensereignissen zum Ziel haben.
Computer Emergency Response Team (CERT)	Ein Computer Emergency Response Team (CERT) ist die zentrale Anlaufstelle einer Organisation oder eines Landes für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen.
Defacement	Bei einem Defacement wird eine Webseite durch einen Angreifer unter Ausnutzung von Schwachstellen oder ausgespähten bzw. erratenen Zugangsdaten mutwillig verändert.
(Distributed) Denial of Service ((D)DoS)	Wenn Dienste, die eigentlich über das Internet erreichbar sein sollten, nicht verfügbar sind, spricht man von einem Denial of Service (DoS). Eine mutwillige Überlastung wird meist unter Zuhilfenahme eines Botnetzes hervorgerufen. Dabei werden vom Täter vorher gekaperte IT-Systeme zusammengeschlossen und zeitgleich auf das Ziel losgelassen. Dies bezeichnet man als (D)DoS ((Distributed) Denial of Service).
Double Extortion	Vorgehensweise von vielen *Ransomware*-Gruppierungen, bei der im Vorfeld der Verschlüsselung sensible Daten gestohlen werden. Dann wird versucht, zusätzlich „Schweigegeld“ zu erpressen, also Geld dafür zu verlangen, diese Daten nicht zu veröffentlichen oder zu verkaufen.
Firewall	Die Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert.

Hybride Bedrohungen	Hybride Bedrohungen bezeichnen verschiedene Formen illegitimer Einflussnahme auf Staaten durch fremde Staaten. Dabei versuchen diese fremden Staaten, auch mittels nicht-staatlicher Akteure, durch den koordinierten Einsatz verschiedener Instrumente ihre Ziele gegen unsere Interessen und Werte offen oder verdeckt durchzusetzen. Sie beabsichtigen hierbei, unsere Demokratie zu schwächen und zu destabilisieren. Zu den eingesetzten Instrumenten gehören bspw. Desinformation, Cyberangriffe auf staatliche Stellen und Unternehmen, Spionage, wirtschaftliche Einflussnahme, zum Beispiel durch gezielte Investition in Schlüsselindustrien und Sabotage von Kritischen Infrastrukturen.
Intrusion Detection System (IDS)	Als Intrusion Detection wird die aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch bezeichnet. Das Ziel von Intrusion Detection besteht darin, aus allen im Überwachungsbereich stattfindenden Ereignissen diejenigen herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten, um diese anschließend vertieft zu untersuchen. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden.
Informationssicherheitsmanagementsystem (ISMS)	Das ISMS ist ein Managementsystem für Informationssicherheit. Es umfasst alle Regelungen, die für die Steuerung und Lenkung des Schutzes von Informationen in der Institution nötig sind. Es legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).
IT-Betrieb	Sammelbegriff für die Personen, die verantwortlich für den Betrieb der IT der Kommunalverwaltung sind (z. B. IT-Mitarbeitende, IT-Team, IT-Abteilung ...).
(IT-)Krise	Erhebliche Unterbrechung mindestens eines (zeit)kritischen Geschäftsprozesses, für deren Bewältigung keine Notfallpläne vorliegen bzw. diese nicht ausreichend greifen
Krisenstab/ Verwaltungsstab	Krisenstab/Verwaltungsstab beschreibt eine administrativ-organisatorische Komponente mit operativ-taktischer Funktion. Er kann auch als Stab für außergewöhnliche Ereignisse bezeichnet werden.
Kritische Infrastrukturen (KRITIS)	Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
Low-hanging Fruits	Als „Low-hanging Fruits“ (englisch für „tiefhängende Früchte“) bezeichnet man schnell und einfach erreichbare Ziele.

Makro	Ein Makro ist eine Funktion innerhalb der Microsoft-Office-Programme Word und Excel, mit der Arbeitsschritte innerhalb des Dokuments oder Tabellenblatts aufgezeichnet und im Anschluss beliebig oft abgespielt werden können, um wiederkehrende und zeitaufwändige Aufgaben zu erleichtern. (Quelle: [ITSN24] (→ *Anhang 2*))
(IT-)Notfall	Nicht tolerable Unterbrechung mindestens eines zeitkritischen Geschäftsprozesses, für deren Bewältigung geeignete Notfallpläne vorliegen oder adaptiert werden können.
Netzsegmentierung	Die Netzsegmentierung ist ein Architekturansatz, mit dem ein Netzwerk in mehrere Segmente oder Subnetze unterteilt wird, die jeweils als ein eigenes kleines Netzwerk fungieren. Dadurch können Netzwerkadministratoren den Datenverkehr zwischen Subnetzen mit detaillierten Richtlinien steuern. (Quelle: [PAN24] (→ *Anhang 2*))
Patch	Ein Patch (aus dem Englischen für „Flicken“) ist eine Aktualisierung für Software, die Korrekturen vornimmt und/oder Sicherheitslücken schließt. Software-Patches werden gelegentlich auch ohne explizite Inkenntnissetzung des Benutzers durchgeführt oder als notwendige Aktualisierungen ausgewiesen. Beim Patch-Management wird die Durchführung von Patches extern gesteuert. (Quelle: [ITSN24] (→ *Anhang 2*))
(Spear-)Phishing	Unter dem Begriff Phishing (Neologismus abgeleitet von „fishing“, englisch für ‚Angeln‘) versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. Das sogenannte Spear-Phishing (englisch spear = Speer) richtet sich gezielt gegen bestimmte Firmen oder Organisationen.
Ransomware	Bei einem Ransomware-Angriff werden die Daten auf einem IT-System verschlüsselt und eine Entschlüsselung erst gegen Zahlung eines Lösegeldes (englisch Ransom) in Aussicht gestellt.
Ransomware-as-a-Service	Das Bereitstellen von Schadsoftware wird als Malware-as-a-Service (MaaS) bezeichnet. Auf *Ransomware* spezialisierte MaaS werden *Ransomware*-as-a-Service (RaaS) genannt.
Recovery Point Objective (RPO)	Unter Recovery Point Objective ist der im Rahmen einer *BIA* ermittelte maximal zulässige Datenverlust zu verstehen. Dieser bedingt direkt die notwendige Häufigkeit von Datensicherungen, da das System im Ereignisfall auf die letzte verfügbare Datensicherung zurückfällt und alle neueren Daten nicht mehr verfügbar sind.

Risikomanagement	Kontinuierlich ablaufendes, systematisches Verfahren zum zielgerichteten Umgang mit Risiken, das die Analyse und Bewertung von Risiken sowie die Planung und Umsetzung von Maßnahmen insbesondere zur Risikovermeidung/-minimierung und -akzeptanz beinhaltet.
Recovery Time Objective	Unter Recovery Time Objective wird die im Rahmen der *BIA* ermittelte geforderte Wiederanlaufzeit verstanden. Diese beschreibt den maximal zulässigen Zeitraum vom Ausrufen des Notfalls bis zum Zeitpunkt der Inbetriebnahme einer Notfalllösung.
Service-Level-Agreement (SLA)	Ein Service-Level-Agreement (SLA, deutsch Dienstleistungs-Güte-Vereinbarung) bezeichnet einen Rahmenvertrag bzw. die Schnittstelle zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen. (Quelle: [WIKI24] (→ *Anhang 2*))
Social Engineering	Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Cyberkriminelle verleiten das Opfer auf diese Weise bspw. dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.
Stakeholder	Als Stakeholder (deutsch „Teilhaber“, Interessengruppe, Interessenvertreter oder Anspruchsberechtigter) wird eine Person oder Gruppe bezeichnet, die ein berechtigtes Interesse am Verlauf oder Ergebnis eines Prozesses oder Projektes hat. (Quelle: [WIKI24] (→ *Anhang 2*))
Spyware	Unter dem Begriff Spyware (auch Spähprogramme oder Spionage-Software) wird Schadsoftware zusammengefasst, die IT-Systeme wie Computer ohne Befugnis aufzeichnen und die Aufzeichnungen an Dritte weitergeben. (Quelle: [ITSN24] (→ *Anhang 2*))
Störung	Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen. Diese kann in der Regel innerhalb des Normalbetriebs behoben werden.
Triple Extortion	Vorgehensweise von *Ransomware*-Gruppierungen, bei der zusätzlich zur *Double Extortion* in einem nächsten Schritt zusätzliche Maßnahmen angedroht werden, um den Zahlungsdruck weiter zu erhöhen. Dies können etwa Angriffe gegen die Verfügbarkeit von Systemen (*(D)DoS-Angriffe*) sein oder weitere Erpressungen gegen Kunden des *Ransomware*-Opfers, deren Daten ebenfalls betroffen sind.
Unified Communication-Clients	Als Unified Communication-Client bezeichnet man eine Benutzeroberfläche, über die mehrere Kommunikationsdienste wie z. B. Telefonie, E-Mail oder Instant Messaging zentral genutzt werden können.

Verwaltungsstab	Siehe *Krisenstab*
Virtual Private Network (VPN)	Bei einem Virtual Private Network, kurz VPN, handelt es sich um ein virtuelles, nicht-öffentliches Netzwerk. „Virtuell“ bedeutet, dass die verschiedenen Endgeräte in diesem Netzwerk nicht direkt physisch miteinander oder mit einem zentralen Router verbunden sind. Eine VPN-Verbindung dient dazu, über das ungeschützte Internet eine geschützte (verschlüsselte) Verbindung zwischen zwei Endpunkten herzustellen.
Zero-Day-Schwachstelle	Eine Zero-Day-Schwachstelle ist eine dem Hersteller unbekannte Schwachstelle in informationstechnischen Systemen. (Quelle: [BMI21] (→ *Anhang 2*))

Anhang 2

Quellenverzeichnis externer Links

Die in diesem Anhang enthaltenen Links zu Inhalten von Internet-Seiten Dritter („fremden Inhalten“) wurden durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach bestem Wissen und unter Beachtung größtmöglicher Sorgfalt zusammengestellt und vermitteln lediglich den Zugang zu „fremden Inhalten“. Dabei wurde auf die Vertrauenswürdigkeit dritter Anbieter und die Fehlerfreiheit sowie Rechtmäßigkeit der „fremden Inhalte“ besonders geachtet.

Da jedoch der Inhalt von Internetseiten dynamisch ist und sich jederzeit ändern kann, ist eine stetige Einzelfallprüfung sämtlicher Inhalte, auf die ein hier aufgeführter Link verweist, nicht in jedem Fall möglich. Das BBK und das BSI machen sich deshalb den Inhalt von Internet-Seiten Dritter, die mit den Inhalten des vorliegenden Wegweisers verlinkt sind, insoweit ausdrücklich nicht zu eigen. Für Schäden aus der Nutzung oder Nichtnutzung „fremder Inhalte“ haftet ausschließlich der jeweilige Anbieter der Seite, auf die verwiesen wurde.

[ACS] Allianz für Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html [letzter Zugriff: 01.10.2024]

[ACS18a] Bundesamt für Sicherheit in der Informationstechnik: *Empfehlung: IT im Unternehmen: BSI-Veröffentlichungen zur Cybersicherheit. Management von Schwachstellen und Sicherheitsupdates*, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_093.pdf [letzter Zugriff: 01.10.2024]

[ACS18b] Bundesamt für Sicherheit in der Informationstechnik: *Handhabung von Schwachstellen. Empfehlungen für Hersteller*, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf [letzter Zugriff: 01.10.2024]

[ACS24] Allianz für Cyber-Sicherheit: *Ich habe einen Vorfall – Checkliste Technik*, https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html?cms_pos=3 [letzter Zugriff: 01.10.2024]

[AGISLL24] AG Handreichung ISLL: *Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, Version 3.0*, https://www.staedtetag.de/files/dst/docs/Themen/2024/Handreichung-ISLL-2024.pdf [letzter Zugriff: 24.10.2024]

[BITS24] Kommunal Agentur GmbH: *Behörden IT-Sicherheitstraining*, https://bits-training.de/ [letzter Zugriff: 01.10.2024]

[BKA22a] Bundeskriminalamt: *Es hat Sie erwischt!*, https://www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/Cybercrime/062022_flyer_cybercrime.pdf [letzter Zugriff: 01.10.2024]

[BKA22b] Bundeskriminalamt: *BKA verzeichnet neuen Höchstwert bei Cyber-Straftaten – Bundeslagebild Cybercrime 2021 veröffentlicht*, https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220509_PM_CybercrimeBLB.html [letzter Zugriff: 01.10.2024]

[BKA23] Bundeskriminalamt: *Im Fokus: Bundeslagebild Cybercrime 2023*, https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html [letzter Zugriff: 01.10.2024]

[BKA24] Bundeskriminalamt: *Zentrale Ansprechstellen Cybercrime der Polizeien*, https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html, [letzter Zugriff: 01.10.2024]

[BFV22] Bundesamt für Verfassungsschutz: *Informationsblätter*, https://www.verfassungsschutz.de/DE/themen/wirtschafts-wissenschaftsschutz/unsere-produkte/unsere-produkte_artikel.html [letzter Zugriff: 01.10.2024]

[BFV23] Bundesamt für Verfassungsschutz: *Informationsblatt „Schutz vor Sabotage“*, https://www.verfassungsschutz.de/DE/themen/wirtschafts-wissenschaftsschutz/unsere-produkte/unsere-produkte_artikel.html [letzter Zugriff: 01.10.2024]

[BFV24] Bundesamt für Verfassungsschutz: *Ansprechpartner Spionage/Sabotage*, https://www.wirtschaftsschutz.info/DE/Themenfelder_Arbeitsordner/Gefahren_Akteure_und_Methoden/Spionage_Sabotage/ansprechpartner_node.html [letzter Zugriff: 01.10.2024]

[BMI09] Bundesministerium des Innern: *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html [letzter Zugriff: 01.10.2024]

[BMI14] Bundesministerium des Innern: *Leitfaden Krisenkommunikation*, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.html [letzter Zugriff: 01.10.2024]

[BMI21] Bundesministerium des Innern, für Bau und Heimat: *Cybersicherheitsstrategie für Deutschland 2021*, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf [letzter Zugriff: 01.10.2024]

[BMI23] Bundesministerium des Innern und für Heimat: *Sensibilisierung im Umgang mit hybriden Bedrohungen einschließlich Desinformation (BLoAG)*, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/heimat-integration/wehrhafte-demokratie/BMI24013.html [letzter Zugriff: 01.10.2024]

[BMI24a] Bundesministerium des Innern und für Heimat: *Hybride Bedrohungen und Desinformation*, https://www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html [letzter Zugriff: 01.10.2024]

[BMI24b] Bundesministerium des Innern und für Heimat: *Desinformation als hybride Bedrohung*, https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/artikel-desinformation-hybride-bedrohung.html [letzter Zugriff: 01.10.2024]

[BMI24c] Bundesministerium des Innern und für Heimat: *Weltweite Ermittlungserfolge gegen Cyberkriminalität*, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2024/05/endgame.html [letzter Zugriff: 01.10.2024]

[BREG22] Bundesregierung: *Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen*, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI22017-resilienz-katastrophen.pdf [letzter Zugriff: 01.10.2024]

[BSI23] Bundesamt für Sicherheit in der Informationstechnik: *Unterstützung bei der Vorfallsbearbeitung*, https://www.wirtschaftsschutz.info/SharedDocs/Kurzmeldungen/DE/Ini_WiS/Flyer_BSI_April_23.html [letzter Zugriff: 01.10.2024]

[BSI24] Bundesamt für Sicherheit in der Informationstechnik: *Dialog für Cybersicherheit*, https://www.dialog-cybersicherheit.de/ [letzter Zugriff: 01.10.2024]

[BW14] Regierungspräsidium Karlsruhe, *Musternotfallplan Stromausfall,* https://rp.baden-wuerttemberg.de/fileadmin/RP-Internet/Themenportal/Sicherheit/_DocumentLibraries/Documents/MusternotfallplanStromausfall.pdf [letzter Zugriff: 01.10.2024]

[CP21] Nicola Rupp: *Redundante Kommunikation an der Schnittstelle zwischen BOS & KRITIS, in: Crisis Prevention 2/2021*, https://crisis-prevention.de/kommunikation-it/redundante-kommunikation-an-der-schnittstelle-zwischen-bos-kritis-nicola-rupp.html [letzter Zugriff: 01.10.2024]

[DSiN21] Bundesamt für Sicherheit in der Informationstechnik, Deutschland sicher im Netz e. V.: *Cyberfibel*, https://www.cyberfibel.de/ [letzter Zugriff: 01.10.2024]

[DLT21] Deutscher Landkreistag, Bundesamt für Sicherheit in der Informationstechnik: *Informationssicherheit für Landrätinnen und Landräte – IT-Grundschutz in den Landkreisen*, https://www.landkreistag.de/images/stories/themen/IT-Sicherheit/211217_Handlungsleitfaden_IT-Grundschutz.pdf [letzter Zugriff: 01.10.2024]

[DST22] Bundesamt für Sicherheit in der Informationstechnik, Deutscher Städtetag, Deutscher Städte- und Gemeindebund: *Informationssicherheit für die Verwaltungsspitzen von Städten und Gemeinden*, https://www.staedtetag.de/files/dst/docs/Publikationen/Weitere-Publikationen/2022/papier-rolle-der-verwaltungsspitze-in-der-Informationssicherheit.pdf [letzter Zugriff: 01.10.2024]

[ESS23] Stadt Essen: *Anlage zur DA Informationssicherheit: Business Impact Analyse – Ersteinschätzung*, https://www.landkreistag.de/images/stories/themen/IT-Sicherheit/achterKongress/IT-SiRi_BIA-Ersteinschaetzung_FB-Umfrage.pdf [letzter Zugriff: 01.10.2024]

[EU16] Europäisches Parlament und Europäischer Rat: *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679, [letzter Zugriff: 01.10.2024]

[HybridCoE24] https://www.hybridcoe.fi [letzter Zugriff: 01.10.2024]

[IBK24] Innovationsstiftung Bayerische Kommune: *ISK V 4.0*, https://www.bay-innovationsstiftung.de [letzter Zugriff: 01.10.2024]

[ITP18] IT-Planungsrat: *Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung (Stand 06.12.2018, Version 2.0)*, https://docs.fitko.de/arc/policies/informationssicherheitsleitlinie/ [letzter Zugriff: 01.10.2024]

[IT-Sibe-Forum] Forum der IT-Sicherheitsbeauftragten, https://info.it-sibe-forum.de/ [letzter Zugriff: 01.10.2024]

[ITSN24] ITService.Network: *Lexikon*, https://it-service.network/it-lexikon/ [letzter Zugriff: 01.10.2024]

[ITV.SH24] ITV.SH: *Sicherheit für Kommunen in Schleswig-Holstein (SiKoSH),* https://itvsh.de/sikosh/ [letzter Zugriff: 01.10.2024]

[KIT24] Karlsruher Institut für Technologie: *Materialien und Tools für Bürger:innen und KMUs*, https://secuso.aifb.kit.edu/642.php [letzter Zugriff: 01.10.2024]

[Lange24] Jens Lange: *Kommunaler Notbetrieb*, https://kommunaler-notbetrieb.de/ [letzter Zugriff: 01.10.2024]

[PAN24] paloalto Networks: *Was ist Netzwerksegmentierung?*, https://www.paloaltonetworks.de/cyberpedia/what-is-network-segmentation [letzter Zugriff: 01.10.2024]

[RFC22] RFC-Editor: RFC 9116: *A File Format to Aid in Security Vulnerability Disclosure*, https://www.rfc-editor.org/rfc/rfc9116.html [letzter Zugriff: 01.10.2024]

[ROD23] Stadt Rodgau: *Website Overlay*, https://www.rodgau.de [letzter Zugriff: 08.03.2023]

[RPK23] Rhein-Pfalz-Kreis: *FAQ*, https://www.rhein-pfalz-kreis.de/stoerung/faq [letzter Zugriff: 01.10.2024]

[SNV23] Stiftung Neue Verantwortung: *Übersicht der Leistungen von Bund und Ländern*, https://cybersicherheitskompass.de/ [letzter Zugriff: 01.10.2024]

[SWI24] SWI-Informationssicherheit für den Mittelstand GmbH/IT-Sicherheitscluster e. V.: *CISIS12®*, https://cisis12.de/ [letzter Zugriff: 01.10.2024]

[UNDRR23a] United Nations Office for Disaster Risk Reduction: *Resilienz gegenüber Katastrophen – Selbstbewertungsleitfaden für Kommunen*, https://mcr2030.undrr.org/sites/default/files/2023-03/UNDRR_Disaster%20resilience%20scorecard%20for%20cities_Detailed_German_Mar2023.pdf [letzter Zugriff: 01.10.2024]

[UNDRR23b] United Nations Office for Disaster Risk Reduction: *Resilienz gegenüber Katastrophen – Selbstbewertungsleitfaden für Kommunen (Excel-Tool)*, https://mcr2030.undrr.org/sites/default/files/2023-08/undrr_disaster-resilience-scorecard-for-cities_detailed_excel-tool_german_aug2023.xlsm [letzter Zugriff: 01.10.2024]

[VdS24] VdS Schadensverhütung GmbH: *Richtlinie VdS 10000*, https://vds.de/kompetenzen/cyber-security/zertifizierungen/informations-sicherheits-und-datenschutzmanagement/vds-10000-informationssicherheit-fuer-kmu [letzter Zugriff: 01.10.2024]

[WIKI24] Wikimedia Foundation Inc.: *Wikipedia®*, https://de.wikipedia.org/wiki/[letzter Zugriff: 01.10.2024]

Anhang 3

Übersicht weiterführender Quellen

In diesem Anhang werden die in den einzelnen Kapiteln bereits angefügten weiterführenden Literaturquellen und Informationen noch einmal gebündelt aufgeführt und durch einige weitere Quellen ergänzt.

Anhang 3.1 Übergreifende Quellen

Top 10 Ransomware-Maßnahmen
https://www.bsi.bund.de/dok/Top10-Ransomware

Top 10 Ransomware-Maßnahmen (Detektion)
https://www.bsi.bund.de/dok/Top10-Ransomware-Detektion

Maßnahmenkatalog Ransomware
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.html

Anhang 3.2 Bedrohungslage

Ransomware – Fakten und Abwehrstrategien BSI, 2024
https://www.bsi.bund.de/dok/ransomware-links
Die Webseite liefert eine Übersicht der zur Verfügung gestellten Materialien rund um das Thema *Ransomware* – von Erläuterungen zu Bedrohungslage und Entwicklung von Ransomware im Detail zu Maßnahmen bei Prävention und Reaktion.

Anhang 3.3 Handeln in der Lage

Erste Hilfe bei einem schweren IT-Sicherheitsvorfall
BSI, 2020
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html
Dieses Papier dient als Notfalldokument für Informationssicherheitsbeauftrage, CISOs und Systemadministratoren von KMU und kleineren Behörden für den Fall eines schweren IT-Sicherheitsvorfalls.

TOP 12 Maßnahmen bei Cyber-Angriffen
Allianz für Cyber-Sicherheit, 2019
https://www.bsi.bund.de/dok/notfallkarte-massnahmen
Die Übersicht richtet sich an IT-Verantwortliche und Administratoren. Sie ist nicht abschließend und nicht maßgeschneidert auf alle Adressaten zugeschnitten, liefert allerdings erste Impulse und Hilfestellungen bei der Reaktion auf einen Vorfall.

Umgang mit Lösegeldforderungen bei Angriffen mit Verschlüsselungstrojanern auf Kommunalverwaltungen
DST, DLT, DStGB, BKA, BSI, 2020
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/Ransomware-Kommunen-Empfehlung.html
Empfehlungen der Bundesvereinigung der kommunalen Spitzenverbände, des Bundeskriminalamtes und des Bundesamtes für Sicherheit in der Informationstechnik

Listen zertifizierter Dienstleister und Experten
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.html

Unterstützung bei der Vorfallsbearbeitung
BSI, 2023
[BSI23] (→ *Anhang 2*)
Meldeformular: https://mip2.bsi.bund.de/meldungen/meldung-ohne-registrierung-erstellen/?meldestelle=10&formular=32

Anhang 3.4 Vorbereitung: Prävention und Detektion vor Reaktion

BSI IT-Grundschutz-Standards 200-1 bis 200-4
BSI, 2024
https://www.bsi.bund.de/dok/6603458

Informationssicherheit für die Verwaltungsspitzen von Städten und Gemeinden
DST, DStGB, BSI, 2022
[DST22] (→ *Anhang 2*)

Informationssicherheit für Landrätinnen und Landräte – IT-Grundschutz in den Landkreisen
DLT, BSI, 2021
[DLT21] (→ *Anhang 2*)

Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen
DST, DLT, DStGB, VITAKO, 2017
AG Handreichung ISLL, 2024
[AGISLL24] (→ *Anhang 2*)
In dieser Handreichung werden neben konzeptionellen und inhaltlichen Vorschlägen zur Erstellung einer eigenen Informationssicherheitsleitlinie auch praxisnahe Empfehlungen zum Aufbau und Betrieb eines ISMS ausgearbeitet.

BSI Online-Kurs IT-Grundschutz, Lerneinheit 2.4: Der Informationssicherheitsbeauftragte
BSI, 2024
https://www.bsi.bund.de/dok/10990432

Es hat Sie erwischt!
BKA und Zentrale Ansprechstellen Cybercrime der Polizeien, 2022
[BKA22a] (→ *Anhang 2*)
Informationen der Strafverfolgungsbehörden bei einem Cyberangriff

Dokumentenvorlage Wiederanlauf-/Wiederherstellungsplan
BSI, 2023
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Vorlage_Wiederanlaufplan.docx
Die Wiederanlauf- und Wiederherstellungsplanung gemäß BSI-Standard 200-4, Kapitel 6.10, wird durch die entwickelte Dokumentenvorlage unterstützt.

Leitfaden Krisenkommunikation
BMI, 2014
[BMI14] (→ *Anhang 2*)
Der Leitfaden klärt die Schlüsselbegriffe und enthält eine Übersicht über Prozesse und Strukturen sowie Grundregeln der Risiko- und Krisenkommunikation. Hinzu kommen Arbeitshilfen und Checklisten zur Vor- und Nachbereitung von Krisenkommunikation sowie ein Muster für den Aufbau eines Krisenkommunikationsplanes.

Übungsbaukasten des UP KRITIS
TAK Übungen des UP KRITIS, 2022
https://www.bsi.bund.de/dok/upk-uebungsbaukasten
Der Themenarbeitskreis (TAK) Übungen des UP KRITIS hat zur Unterstützung von Betreibern Kritischer Infrastrukturen bei der Planung, Durchführung und Nachbereitung von Übungen einen Übungsbaukasten erstellt. Er dient als praxisorientierte Hilfestellung, um Übungen systematisch und effektiv durch alle Phasen zu begleiten. Hierfür stehen Übersichten über Übungsarten, Anleitungen, Hilfsmittel und Vorlagen zur Verfügung.

Trainingskoffer
BSI
https://www.bsi.bund.de/dok/Trainingskoffer
Zur niedrigschwelligen Sensibilisierung der Mitarbeiterinnen und Mitarbeiter bietet das BSI eine kostenfreie Spielesammlung, mit der spielerisch die Bewältigung eines Cyberangriffs trainiert werden kann.

Forum der IT-Sicherheitsbeauftragen
[IT-Sibe-Forum] (→ *Anhang 2*)

Allianz für Cyber-Sicherheit
[ACS] (→ *Anhang 2*)
Sicherheitsberatung für Länder und Kommunen
https://www.bsi.bund.de/dok/SicherheitsberatungLK

Übersicht der Leistungen von Bund und Ländern (Stiftung Neue Verantwortung)
[SNV23] (→ *Anhang 2*)

Anhang 4

Wegweiser zu verwandten Themen

Bei der Vorbereitung auf Cybervorfälle stellen sich mitunter Fragen, denen im Schwerpunkt andere Szenarien zugrunde liegen. Zudem werden Themenkomplexe und Fragestellungen berührt, die ganz grundsätzlich im Rahmen eines kommunalen *Risikomanagement*-Prozesses zu klären, aber auch vor dem Hintergrund möglicher Cybervorfälle relevant sind.

Das folgende Kapitel soll daher als Wegweiser zu weiteren Quellen dienen, die einen ganzheitlicheren *Risikomanagement*-Prozess unterstützen können oder bei der Beantwortung von weiterführenden, aus der Betrachtung von Cybergefahren heraus entstandenen Fragen helfen.

Anhang 4.1 Stromausfall

Größere IT-Ausfälle können nicht nur durch Cyberangriffe, sondern u. a. auch durch Stromausfälle entstehen. Um bei einem plötzlichen Ausfall der Stromversorgung physische Schäden an IT-Hardware zu vermeiden, kommt bei Servern oder in Rechenzentren häufig eine unterbrechungsfreie Stromversorgung (USV) zum Einsatz, die zumindest ein geordnetes Herunterfahren ermöglicht. Soll darüber hinaus die Arbeitsfähigkeit bei Stromausfall aufrechterhalten werden, müssen weiter gehende Vorkehrungen getroffen werden. Diese kommen insbesondere dann zum Tragen, wenn man sich auf einen länger andauernden Stromausfall vorbereiten möchte. Auch wenn Deutschland über eine sehr sichere Stromversorgung verfügt, sind gravierende Versorgungsstörungen, auch über einen längeren Zeitraum, nicht auszuschließen.

Bezüglich der Vorbereitung von Städten, Gemeinden und Kreisen auf Großeinsatzlagen und Katastrophen, wie großflächigere Stromausfälle sie nach sich zögen, finden sich die einschlägigen Regelungen in den Brand- und Katastrophenschutzgesetzen der Länder. In der Regel haben Städte, Gemeinden und Kreise Pläne für solche Situationen aufzustellen. Zu Stromausfallszenarien wurden häufig bereits Planungen durchgeführt, auf die speziell mit Blick auf die IT-spezifischen Aspekte aufgebaut werden kann.

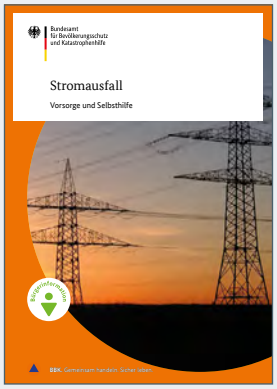
Weiterführende Literatur:

Musternotfallplan Stromausfall
Regierungspräsidium Karlsruhe, 2014
[BW14] (→ *Anhang 2*)

Beispiel eines Notfallplans, der vielfach von anderen Kommunen in ihren Planungen aufgegriffen wird.

Notstromversorgung in Unternehmen und Behörden
BBK, 2024
https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-13-notstromversorgung-unternehmen-behoerden.pdf?__blob=publicationFile&v=12

Dieser Leitfaden unterstützt bei der Konzeption, der Planung und dem Betrieb einer Notstromversorgung. Neben grundlegenden Informationen bietet er auch einfach zu handhabende Checklisten, mit denen der Status quo in einer Einrichtung schnell erfasst werden kann. Auf dieser Basis kann eine robuste Notstromversorgung auf- bzw. ausgebaut werden.



Stromausfall Vorsorge und Selbsthilfe
BBK, 2019
https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/Buergerinformationen/stromausfall-vorsorge-selbsthilfe.pdf?__blob=publicationFile&v=11

Der Leitfaden gibt Hinweise und Empfehlungen für die private Vorsorge bei einem Stromausfall.

Neue Erkenntnisse zur Lagerfähigkeit von Brennstoffen für Netzersatzanlagen
BSI, 2015
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Lagerfaehigkeit_Brennstoff_NEA/Lagerfaehigkeit_Brennstoff_NEA.pdf

Der Begriff „Dieselpest“ fällt immer wieder, wenn es um die Frage geht, wie lange Dieselkraftstoff in Tanks von Netzersatzanlagen gelagert werden kann, bevor er unbrauchbar wird, und welchen Anteil die vom Gesetzgeber gewollte Beimischung von Fettsäuremethylester (FAME, auch Biodiesel genannt) an Problemen mit der Langzeitlagerung hat. Um diese Frage zu klären, hat das Bundesministerium des Inneren beim „Institut für Wärme und Oeltechnik e. V.“ (IWO) in Hamburg die Durchführung einer entsprechenden Studie zur Brennstoffqualität in Netzersatzanlagen (NEA) initiiert, die in diesem Dokument zusammengefasst dargestellt wird.

Anhang 4.2 Telekommunikationsausfall

Telekommunikation ist unverzichtbar für die Handlungsfähigkeit von Verwaltungen. Ein Ausfall von Telekommunikationsmitteln (Festnetz-Telefon, Mobilfunk, Internetanbindung) kann neben technischem Versagen auch durch gezielte Cyberangriffe verursacht werden. Zudem geht das Abschalten der IT nach einem Angriff häufig auch mit dem Verlust der an die IT gekoppelten Kommunikationsmittel einher. Es handelt sich demzufolge um ein mögliches Folgeszenario von *IT-Krisen*, für das vorgesorgt werden sollte. Redundante Kommunikationsmittel können Ausfälle kompensieren.

Für eine funktionierende Kommunikation auch über Notfallkanäle sind immer mindestens zwei Kommunikationspartner relevant. Daher ist eine schnelle, einseitige Festlegung auf bestimmte technische Wege nicht erfolgversprechend, sondern riskiert ein Fehlschlagen des Verbindungsaufbaus im Krisenfall. Die Planung von redundanten Kommunikationskanälen muss vielmehr einem geordneten Prozess in Abstimmung mit den Partnern folgen (Abbildung 7).

Um die Einführung einer tatsächlich funktionierenden Lösung sicherzustellen, müssen insbesondere folgende Fragen beantwortet werden:

- Mit wem/welchen Akteuren muss/will ich in der Krise über dieses Kommunikationsmittel kommunizieren?
  - Daraus folgt: Haben meine Partner bereits redundante/alternative Kommunikationsmittel? Wenn ja, entsprechen diese meinen Anforderungen an das Kommunikationsmittel? (siehe nächsten Punkt)
  - Wie viele Einheiten des Kommunikationsmittels benötige ich?

- Welche (technischen/organisatorischen) Anforderungen habe ich an das Kommunikationsmittel? Dabei sind insbesondere die folgenden Aspekte relevant:
  - Interoperabilität
  - Verfügbarkeit (räumlich/zeitlich)[66]
  - Latenz (Sprachübertragung)
  - Datenbandbreite (reine Sprach- oder auch Datenübertragung)
  - Kosten (Anschaffung/Betrieb)
  - Reichweite

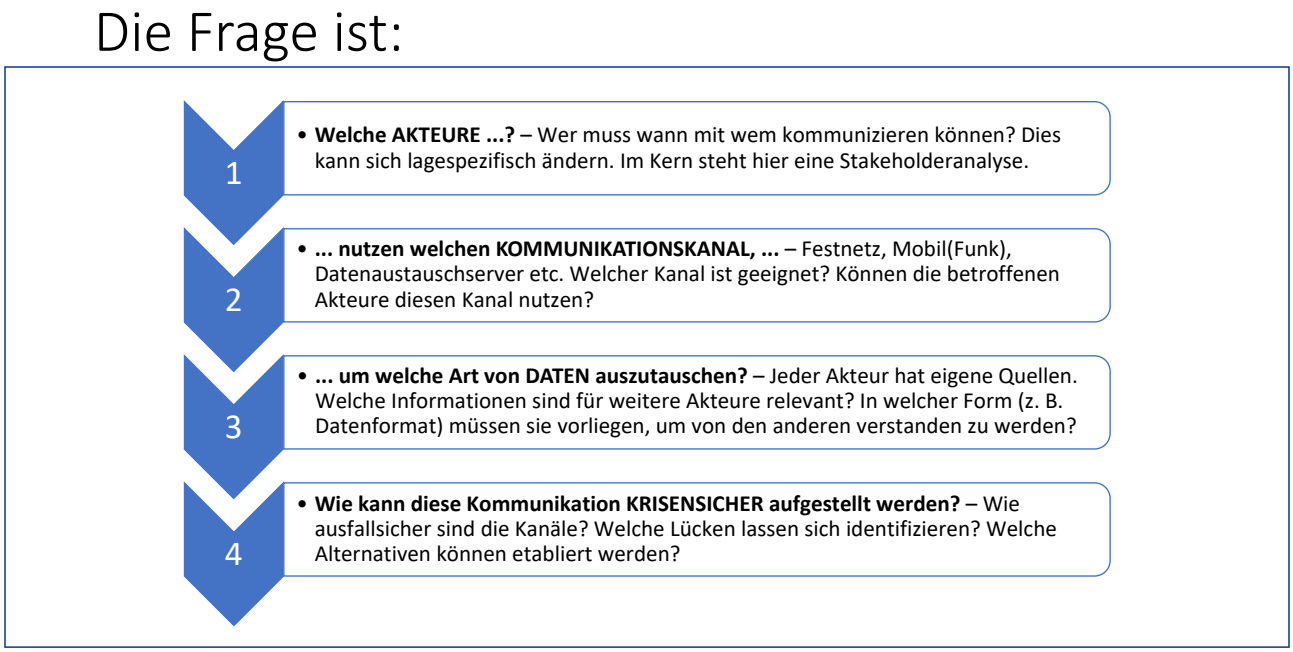


Abbildung 7: Prozess zur Einführung redundanter Kommunikationskanäle (Quelle: [CP21], (→ *Anhang 2*))

[66] Hier lohnt ein Verifizieren der Signalstärke am gewünschten Einsatzort insbesondere bei Satellitenkommunikation.

Anhang 4.3 Hybride Bedrohungen

Cyberangriffe können als Teil einer hybriden Angriffskampagne eingesetzt werden. Der Begriff *hybride Bedrohungen* bezeichnet verschiedene Formen illegitimer Einflussnahme auf Staaten durch fremde Staaten. Hierzu setzen staatliche sowie staatlich beauftragte Akteure koordiniert unterschiedliche Instrumente ein, um den gesellschaftlichen Zusammenhalt in einem Staat zu schwächen und sein Handeln zu erschweren. Auf diese Weise soll die Demokratie geschwächt und destabilisiert werden. Zu den eingesetzten Instrumenten gehören bspw. Desinformation, Cyberangriffe auf staatliche Stellen und Unternehmen, Spionage, wirtschaftliche Einflussnahme z. B. durch Investition in Schlüsselindustrien, Sabotage von Kritischen Infrastrukturen und Einflussnahme auf freie Wahlen.

Eine oft verwendete Form hybrider Bedrohungen ist Desinformation. Darunter werden falsche oder irreführende Informationen verstanden, die durch fremde Staaten mit Täuschungsabsicht und mit dem Ziel der Beeinflussung der öffentlichen Meinungs- und Willensbildung verbreitet werden. Eine solche Kampagne kann auch auf lokaler Ebene auf eine Diskreditierung der Verwaltung abzielen.

Kommunen als unterste Verwaltungsebene sind für die Stabilität des politischen Systems und für die öffentliche Sicherheit von besonderer Bedeutung. Durch die Erbringung des Großteils der bürgernahen staatlichen Dienstleistungen sowie vielfach auch das Unterhalten von Infrastruktur der täglichen Daseinsvorsorge haben sie vielfältigen, direkten Kontakt mit Bürgerinnen und Bürgern und verfügen über viele persönliche und andere sensible Daten. Im Zusammenhang mit Cyberangriffen auf Kommunalverwaltungen können zusätzliche Manipulationen (z. B. *Defacement* von Webseiten oder Desinformation) sowie brandmarkende Kommentare in sozialen Medien genutzt werden, um die öffentliche Meinung zu beeinflussen. Kommunalverwaltungen müssen sich dementsprechend darauf einstellen, dass sie bei der Bewältigung der Lage zusätzlichen Herausforderungen begegnen. Dadurch kommt insbesondere einer guten eigenen Krisenkommunikation eine besondere Bedeutung zu (→ *Kapitel 5.2.5*).

Die große Herausforderung hybrider Bedrohungen besteht darin, sie zu erkennen und abzuwehren. Dafür ist ein gutes Zusammenspiel aller relevanten Akteure essenziell (→ *Kapitel 5.2.2*).

Weiterführende Literatur und Informationen:

Sensibilisierung im Umgang mit hybriden Bedrohungen einschließlich Desinformation
Empfehlungen der BLoAG Hybrid, BMI, 2023
[BMI23] (→ *Anhang 2*)

Die dargestellten Maßnahmen für die kommunale Ebene dienen dazu, hybride Bedrohungen zu erkennen und abzuwehren, Maßnahmen zu koordinieren sowie die Resilienz von Staat und Gesellschaft zu stärken.

Hybride Bedrohungen und Desinformation
BMI, 2024
[BMI24a] (→ *Anhang 2*)
[BMI24b] (→ *Anhang 2*)

Auf den Webseiten des BMI wird ausführlich auf die Themen hybride Bedrohungen und Desinformation eingegangen – insbesondere zu Letzterem werden zudem einige Maßnahmenmöglichkeiten vorgestellt.

Hybrid CoE
[HybridCoE24] (→ *Anhang 2*)

Auf der internationalen Ebene wirkt unter der Schirmherrschaft der Europäischen Union und der NATO das European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) als netzwerkbasiertes, internationales und unabhängiges Zentrum zur Bekämpfung hybrider Bedrohungen.

Anhang 4.4 Personal

Die Notwendigkeit einer Sensibilisierung aller Mitarbeitenden für einen angemessenen Umgang mit IT-Sicherheitsgefährdungen wird in → *Kapitel 5.1.5* thematisiert.

Im IT-Bereich ergibt sich bei der Umsetzung von Sicherheitsmaßnahmen darüber hinaus die Schwierigkeit eines eklatanten Fachkräftemangels. Häufig ist das existierende IT-Personal überlastet und es gibt nicht genug geschultes und geübtes Personal, um eine adäquate Abwesenheitsvertretung zu gewährleisten. Hinzu kommen mögliche Interessenskonflikte zwischen *IT-Betrieb* und IT-Sicherheitsfragen, wenn diese Aufgaben durch den Fachkräftemangel in Personalunion wahrgenommen werden müssen.

Für diese sehr verbreiteten Probleme werden an verschiedenen Stellen bereits Lösungsansätze auch abseits einer verstärkten Personalgewinnung erprobt. Um gegenseitig von den anderenorts gesammelten Erfahrungen und Ideen profitieren zu können, lohnt sich die Teilnahme an Austauschformaten (bspw. am IT-SiBe-Forum oder an anderen Veranstaltungsreihen der kommunalen Spitzenverbände, am Runden Tisch des Landes o. Ä.).

Als Denkanstöße, um nach Lösungen zu suchen, könnten die folgenden Fragen behilflich sein:

- Lassen sich aus den Reihen des existierenden Personals IT-affine Personen für eine entsprechende (ggf. berufsbegleitende) Aus- oder Weiterbildung rekrutieren?
- Lässt sich eine entsprechende Aus- oder Weiterbildung fördern (ggf. mit Bedingungen an die anschließende Verweildauer in der Kommunalverwaltung bzw. an die Rückzahlung von Ausbildungssummen bei vorzeitigem Verlassen der Kommunalverwaltung)?
- Teilweise werden Informationssicherheitsinhalte bereits in relevante Aus- oder Fortbildungen integriert, bspw. in Verwaltungsstudiengänge. Gibt es evtl. bereits entsprechende Studiengänge oder Initiativen der zuständigen Landesebene, die bevorzugt ausgewählt werden könnten?

Aufgrund der Bedeutung der Kommunalverwaltungen als unterste Verwaltungsebene und der dort vorliegenden Vielzahl sensibler Daten sollte zudem auf eine sicherheitsorientierte Personalauswahl geachtet werden. Auch wenn ohnehin nur wenige Bewerbungen eingehen, dürfen Überlegungen hinsichtlich der Verlässlichkeit der Kandidatinnen und Kandidaten nicht vernachlässigt werden. IT-Sicherheitspersonal ist in kritischen Funktionen tätig, sodass die Möglichkeit der Innentäterschaft oder der Anwerbung durch ausländische Nachrichtendienste grundsätzlich gegeben ist. Bei Fragen oder Zweifeln lohnt sich eine Kontaktaufnahme mit dem zuständigen Landesamt für Verfassungsschutz.

Weiterführende Literatur:

Informationsblätter des Bundesamtes für Verfassungsschutz
BfV, 2022
[BFV22] (→ *Anhang 2*)

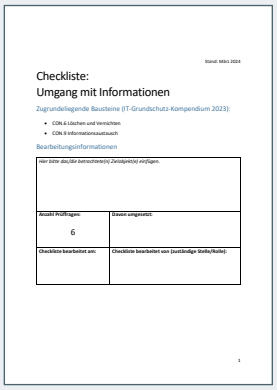
Die Informationsblätter „Pre-Employment Screening“, „Bedrohung durch Innentäter“ und „Methoden der Spionage: HUMINT“ erläutern Sicherheitsrisiken im größeren Kontext einer möglichen Innentäterschaft des eigenen Personals und liefern Prüffragen und Hinweise zur Reduzierung des Risikos während der Personalgewinnung und im weiteren Verlauf. Es lohnt grundsätzlich ein regelmäßiger Blick auf das Angebot der Seite, da das BfV die Informationsblätter zum Wirtschaftsschutz in regelmäßigen Abständen aktualisiert und um weitere Themen ergänzt.

Anhang 4.5 Präventiver Informationsschutz

Kommunalverwaltungen verfügen über eine große Menge sensibler Daten, die eines besonderen Schutzes bedürfen. Relevant ist nicht nur der Schutz personenbezogener Daten, zu dem Kommunalverwaltungen nach DS-GVO bzw. BDSG gesetzlich verpflichtet sind. Auch detaillierte Informationen zu Kontakten, Vorgehensweisen im Verwaltungshandeln und standardmäßig verwendeten Vorlagen, aber auch über Liegenschaften und Sicherheitspläne erleichtern Angreifern die Vorbereitung von Cyberangriffen, z. B. mithilfe besonders schwer zu entdeckenden *Spear-Phishings*, sowie von anderen Sabotagehandlungen. Unachtsam öffentlich zur Verfügung gestellte Daten oder ein Datenabfluss – auch durch einen Cyberangriff – können von geneigten Akteuren grundsätzlich für ihre Zwecke genutzt werden: Sei es die Behinderung von Arbeitsabläufen und Kommunikation in Politik und Verwaltung, aber auch die Beeinflussung von Entscheidungsträgern und öffentlicher Meinung oder die Aufstachelung politischer Gruppierungen.

Neben einer effizienten Kommunikation im Ernstfall (→ *Kapitel 5.2.5*) ist daher auch ein präventiver Informationsschutz essenziell.

Weiterführende Literatur:


Stand: März 2024

Checkliste:
Umgang mit Informationen

Zugrundeliegende Bausteine (IT-Grundschutz-Kompendium 2023):

- CON.6 Löschen und Vernichten
- CON.9 Informationsaustausch

Bearbeitungsinformationen

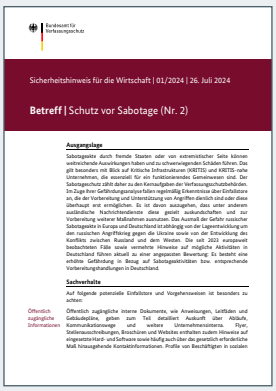
Hier bitte das/die benutzerkonto(s) Zutreffende(s) eintragen.

Anzahl Prüffragen:	Etwaig umgesetzt:
6	
Checkliste bearbeitet am:	Checkliste bearbeitet von (zuständige Stelle/Rolle):

1

Checkliste Umgang mit Informationen
BSI, 2023
https://www.bsi.bund.de/dok/WIBA

Die Checkliste „Umgang mit Informationen“ des BSI-Produkts „Weg in die Basis-Absicherung“ (WiBA) bietet gezielte Prüffragen und Hinweise rund um den Austausch von Informationen auf verschiedenen technischen Wegen, aber auch zum Thema Löschen und Vernichten von Informationen.


Bundesamt für Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 01/2024 | 26. Juli 2024

Betreff | Schutz vor Sabotage (Nr. 2)

Ausgangslage

Sabotageakte durch fremde Staaten oder von extremistischer Seite können weitreichende Auswirkungen haben und zu schwerwiegenden Schäden führen. Das gilt besonders mit Blick auf Kritische Infrastrukturen (KRITIS) und KRITIS-nahe Unternehmen, die essenziell für ein funktionierendes Gemeinwesen sind. Der Sabotageschutz zählt daher zu den Kernaufgaben der Verfassungsschutzbehörden. Im Zuge ihrer Gefährdungsanalysen haben regelmäßig Erkenntnisse über Einflussnahmen, die der Vorbereitung und Unterstützung von Angriffen dienlich sind oder diese überhaupt erst ermöglichen. Es ist davon auszugehen, dass unter anderem ausländische Nachrichtendienste diese gezielt auskundschaften und zur Vorbereitung weiterer Maßnahmen ausnutzen. Das Ausmaß der Gefahr russischer Sabotageakte in Europa und Deutschland ist abhängig von der Lageentwicklung um den russischen Angriffskrieg gegen die Ukraine sowie von der Entwicklung des Konflikts zwischen Russland und dem Westen. Die seit 2023 europaweit beobachteten Fälle sowie vermutete Hinweise auf mögliche Aktivitäten in Deutschland führen aktuell zu einer angespannten Bewertung. Es besteht eine erhöhte Gefährdung in Bezug auf Sabotageaktivitäten bzw. entsprechende Vorbereitungshandlungen in Deutschland.

Sachverhalte

Auf folgende potenzielle Einfallstore und Vorgehensweisen ist besonders zu achten:

Öffentlich zugängliche Informationen

Öffentlich zugängliche interne Dokumente, wie Anweisungen, Leitfäden und Gebäudepläne, geben zum Teil detailliert Auskunft über Abläufe, Kommunikationswege und weitere Unternehmensinterna. Flyer, Stellenausschreibungen, Broschüren und Websites enthalten zudem Hinweise auf eingesetzte Hard- und Software sowie häufig auch über das gesetzlich erforderliche Maß hinausgehende Kontaktinformationen. Profile von Beschäftigten in sozialen

Schutz vor Sabotage
BfV, 2022/2023
[BFV23] (→ *Anhang 2*)

Der Sicherheitshinweis für die Wirtschaft sowie das Informationsblatt „Schutz vor Sabotage“ geben einen kurzen Überblick über die datenbasierten Sabotagerisiken. Sie liefern Hinweise auf die verschiedenen Bereiche, in denen auf Datensparsamkeit geachtet werden sollte, sowie zu möglichen Maßnahmen der Risikominderung.

Anhang 4.6 Integriertes Risikomanagement

Um die Bevölkerung effektiv vor Krisen und Katastrophen schützen zu können, ist eine erfolgreiche Zusammenarbeit von staatlichen Stellen (z. B. Gefahrenabwehr und Katastrophenschutz) und Betreibern Kritischer Infrastrukturen (KRITIS-Betreiber) unerlässlich.

Das Integrierte Risikomanagement (IRM) für den Schutz der Bevölkerung bietet einen Ansatz, wie das (bestehende oder im Aufbau befindliche) *Risikomanagement* der betroffenen Akteure miteinander verknüpft werden kann, um sich z. B. zu identifizierten Risiken auszutauschen oder auch um vorhandene Ressourcen und Fähigkeiten im Ereignisfall optimal nutzen zu können.

Das IRM bietet hierfür ein strukturiertes Verfahren für die Zusammenarbeit zwischen unterschiedlichen Akteuren und bringt alle Verantwortlichen an einen Tisch. Dieser Austausch fördert das gegenseitige Verständnis von Strukturen und Zuständigkeiten und ermöglicht allen Beteiligten, sich ein Bild von den Ressourcen und Fähigkeiten der jeweils anderen Akteure zu machen. Durch diese koordinierte Vorgehensweise können Synergieeffekte genutzt und die Weichen für ein erfolgreiches gemeinsames Risiko- und Krisenmanagement gestellt werden.

Im Verlauf des Integrierten Risikomanagements (Abbildung 8) werden Erkenntnisse, Pläne und Maßnahmen von staatlicher Seite und von KRITIS-Betreibern immer wieder in den Austausch gebracht.

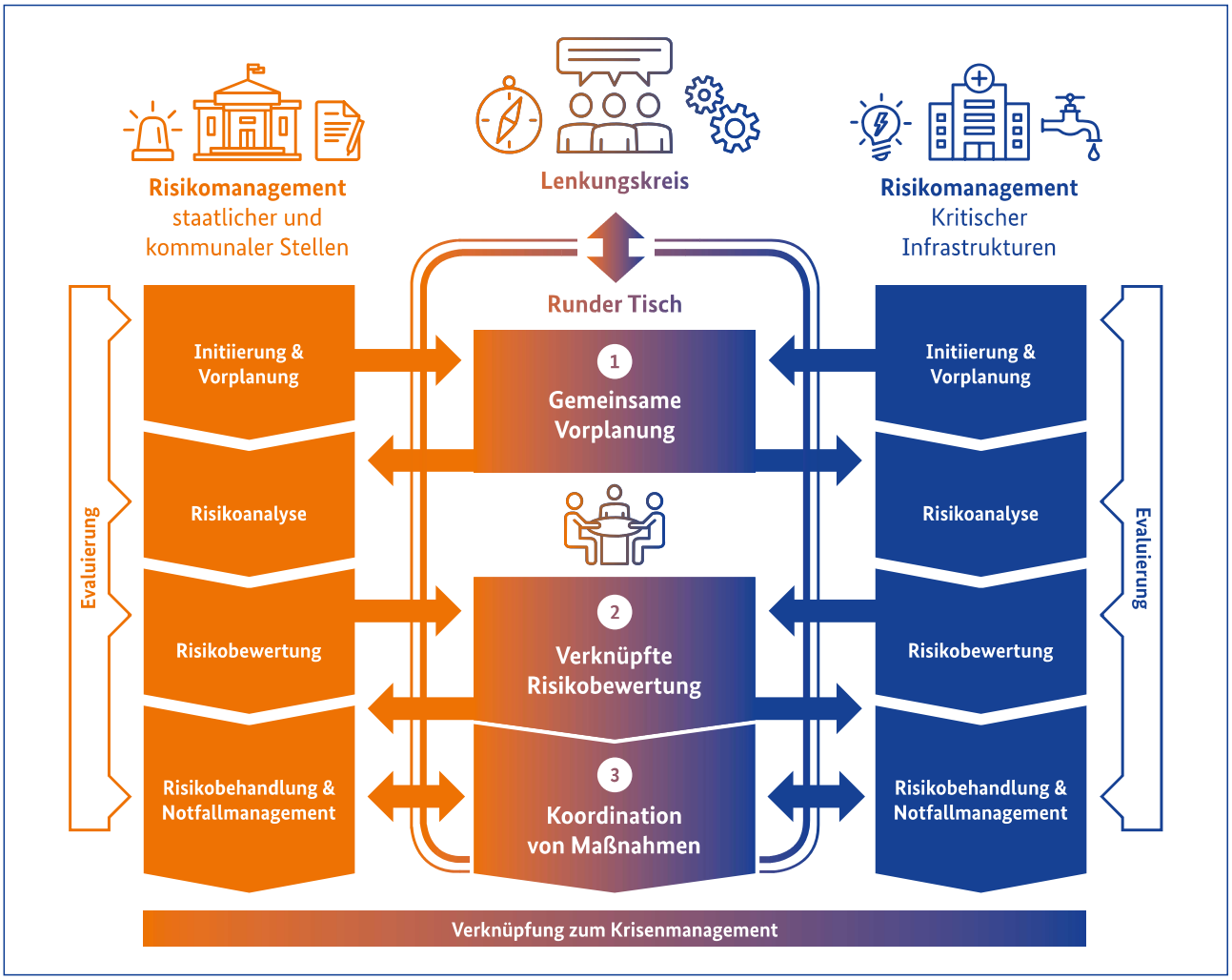


Abbildung 8: Zusammenarbeit staatlicher Akteure und KRITIS-Betreiber im Integrierten Risikomanagement für den Schutz der Bevölkerung (Quelle: BBK)

Weiterführende Literatur:

Integriertes Risikomanagement
BBK, 2024
https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Schutzkonzepte-KRITIS/Integriertes-Risikomanagement/integriertes-risikomanagement_node.html

Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement Leitfaden für Unternehmen und Behörden
BMI, 2011
https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi-schutz-kritis-risiko-und-krisenmanagement.pdf?__blob=publicationFile&v=12

Der Leitfaden stellt ein Managementkonzept für solche Einrichtungen vor, die von staatlicher Seite als Kritische Infrastrukturen bezeichnet werden. Das Konzept unterstützt die Betreiber Kritischer Infrastrukturen bei der strukturierten Ermittlung von Risiken, der darauf basierenden Umsetzung vorbeugender Maßnahmen sowie dem effektiven und effizienten Umgang mit Krisen.

Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten Arbeitshilfe für die Anwendung im Bevölkerungsschutz
BBK, 2019, Praxis im Bevölkerungsschutz – Band 20
https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-20-schutz-infrastrukturen-identifizierung.pdf?__blob=publicationFile

Die vorliegende Empfehlung ist eine Arbeitshilfe zur Benennung der Bestandteile von KRITIS, deren Ausfall aus Sicht von Staat und Kommune die Leistungserbringung der Infrastruktur erheblich beeinträchtigen könnte. Sie fußt auf einer Methode zur Identifizierung Kritischer Infrastrukturen, die vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt wurde.

Impressum

Herausgeber
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Referat N.II.2 – KRITIS Sektoren 1, Cyber-Sicherheit u. Cyber-AZ
Emil-Nolde-Str. 7
53113 Bonn

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

Bezugsquelle | Kontakt
NII2@bbk.bund.de
www.bbk.bund.de

sicherheitsberatung-regional@bsi.bund.de
www.bsi.bund.de

Stand
Oktober 2024

Druck
strohmeyer dialog.druck GmbH

MIX
Papier | Fördert gute Waldnutzung
FSC® C111446
FSC www.fsc.org

Gestaltung
familie redlich AG – Agentur für Marken und Kommunikation
KOMPAKTMEDIEN – Agentur für Kommunikation GmbH

Bildnachweise
Titelbild AdobeStock©Levin; S. 2, 10, 22, 28 Gerd Altmann/pixabay; S. 2, 6 Nurdin Bekkeldieva/pixabay; S. 2, 31 Cliff Hang/pixabay; S. 2, 73 Darwin Laganzon/pixabay
Abb. 1, 2, 3 BSI; Abb. 4, 5 Stadt Rodgau; Abb. 6 Rhein-Pfalz-Kreis; Abb. 7 [CP21]; Abb. 8 BBK

ISBN 978-3-949117-30-5

www.bbk.bund.de
www.bsi.bund.de