Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe

BBK

Risikoanalyse Tunnelleitzentrale

Empfehlungen für eine einrichtungsbezogene Risikoanalyse

Fachinformation

Praxis im Bevölkerungsschutz

Band 14

BBK. Gemeinsam handeln. Sicher leben.

Praxis im Bevölkerungsschutz

Band 14

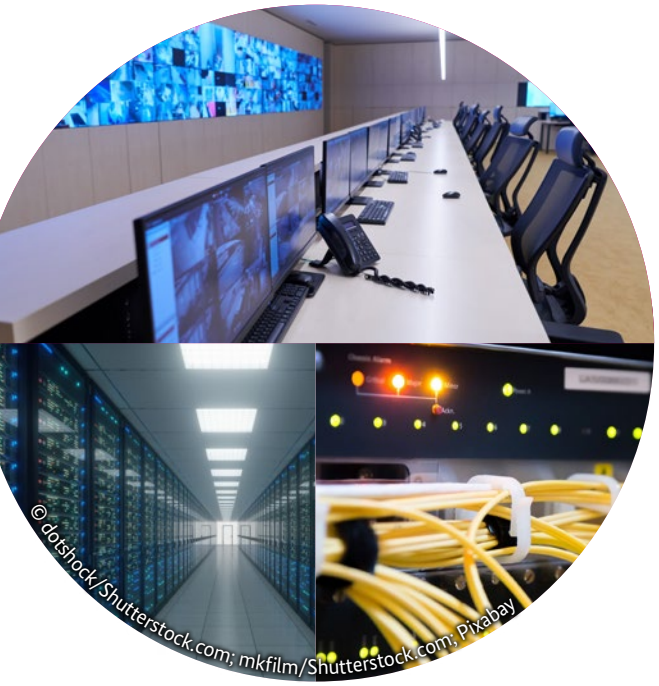
Bildnachweis
Titelseite © dotshock/Shutterstock.com

Risikoanalyse Tunnelleitzentrale

Empfehlungen für eine einrichtungsbezogene Risikoanalyse

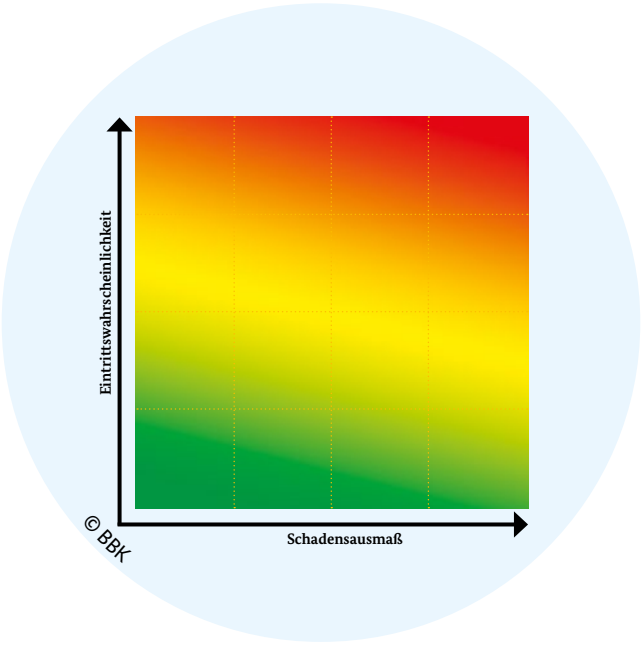
Band 14 · Praxis im Bevölkerungsschutz

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe


© dotshock/Shutterstock.com; mkfilm/Shutterstock.com; Pixabay


© WHYFRAME/Shutterstock.com


© Riccardo Piccinini/Shutterstock.com


Eintrittswahrscheinlichkeit
Schadensausmaß
© BBK

Inhalt

Vorwort

Christoph Unger
Präsident des Bundesamtes für
Bevölkerungsschutz und Katastrophenhilfe

Liebe Leserinnen und Leser,

Die Sicherstellung der Mobilität und die Versorgung der Bevölkerung setzen leistungsfähige Verkehrsinfrastrukturen voraus. Wie selbstverständlich nutzen wir täglich diese Infrastrukturen, zu denen neben Straßen und Brücken auch Tunnelbauwerke verschiedenster Art gehören. Bei der Durchfahrt sehen wir Betonwände, Beleuchtung und Notausgänge, doch wie die Sicherheitstechnik aussieht und wie sie funktioniert, ist uns in der Regel unbekannt.

Die Tunnel zu überwachen, einen reibungslosen Tunnelbetrieb zu gewährleisten und im Ereignisfall die notwendigen Maßnahmen zur Rettung von Personen einzuleiten und die Einsatzleitung zu unterstützen, gehört zu den wesentlichen Aufgaben einer Tunnelleitzentrale. Nicht erst Störungen in einem Tunnel, sondern schon der Ausfall einer Tunnelleitzentrale würde somit nicht nur die Sicherheit im Tunnel beeinträchtigen, sondern – sofern Tunnel gesperrt werden müssen – auch verkehrliche Auswirkungen nach sich ziehen.

Um die Funktionsfähigkeit der Tunnelleitzentralen zu erhalten, ist es wichtig, die jeweiligen Gefahren zu kennen, die zum Ausfall der Einrichtung führen können, die Risiken zu bewerten und, darauf aufbauend, zielgerichtet Schutzmaßnahmen umzusetzen. Dies gilt insbesondere für alle Prozesse, die durch die IT unterstützt werden. Ohne IT-Unterstützung sind heutzutage viele Prozesse gar nicht mehr denkbar; allerdings bergen sie auch neue Risiken, denen im Rahmen eines Risikomanagements entsprechend begegnet werden muss.

Die vorliegenden Empfehlungen zur Durchführung einer Risikoanalyse wurden im Rahmen des Forschungsprojekts SKRIBTPlus „Schutz kritischer Brücken und Tunnel“ erarbeitet. In diesem Projekt, das innerhalb des Programms „Forschung für die zivile Sicherheit“ durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert und von der Bundesanstalt für Straßenwesen (BASt) als Konsortialführer geleitet wurde, wurden Brücken und Tunnel als die kritischen Bauwerke im Zuge von Straßen aus der aktuellen Perspektive der zivilen Sicherheitsforschung untersucht und Maßnahmen zur Erhöhung ihrer Verfügbarkeit entwickelt. Für die Förderung des Projektes durch das Bundesministerium für Bildung und Forschung und die Begleitung durch den Projektträger VDI sei an dieser Stelle ebenso herzlich gedankt wie unseren Projektpartnern für die konstruktive und fruchtbare Zusammenarbeit.

Mit dieser Broschüre wollen wir Ergebnisse unserer Projektarbeiten präsentieren, um die Betreiber von Tunnelbauwerken anzuregen, ein Risikomanagement für Tunnelleitzentralen zu etablieren oder um neue Aspekte zu ergänzen. Die hier vorgestellte Methodik, mit der sowohl Fragen der IT-Sicherheit als auch allgemeine Sicherheitsaspekte zusammengeführt werden, wurde zwar mit dem Fokus Tunnelleitzentralen erarbeitet, sie ist aber grundsätzlich auch für andere vergleichbare Einrichtungen, die Überwachungs- und Steuerungsfunktionen wahrnehmen, also z. B. Verkehrsleitzentralen oder Leitstellen von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) anwendbar.

An dieser Stelle bedanken wir uns auch bei den Straßenbauverwaltungen der Länder für ihre Unterstützung und Begleitung bei der Bearbeitung dieser Thematik und würden uns freuen, wenn wir sie mit diesen Empfehlungen bei ihrer Arbeit unterstützen und so einen Beitrag zur Erhöhung der Sicherheit in Tunneln leisten könnten.

Christoph Unger

Präsident
Bundesamtes für Bevölkerungsschutz
und Katastrophenhilfe

Verbundprojekt SKRIBTPlus

Schutz kritischer Brücken und Tunnel

https://www.sifo.de/sifo/de/projekte/schutz-kritischer-infrastrukturen/schutz-von-verkehrsinfrastrukturen/skribt/skribt-schutz-kritischer-bruec-nd-tunnel-im-zuge-von-strassen.html

Um die zivile Sicherheit von Verkehrsteilnehmern auf Brücken und in Tunneln zu erhöhen, startete das Bundesministerium für Bildung und Forschung (BMBF) im Programm „Forschung für die zivile Sicherheit“ für den Themenschwerpunkt „Schutz von Verkehrsinfrastrukturen“ im März 2008 das Projekt „Schutz kritischer Brücken und Tunnel im Zuge von Straßen (SKRIBT)“.

Ausgehend von einer umfassenden Bedrohungsanalyse wurden im Projekt relevante Szenarien wie Brand, Explosion, Kontamination, Überflutung sowie Sturm hinsichtlich ihrer Wirkungen auf Bauwerke und Nutzer berechnet. Untersucht wurde auch der Faktor Mensch und sein Verhalten in Gefahrensituationen sowie das Vorgehen der Betriebs- und Einsatzdienste bei Schadensereignissen. Auf dieser Basis wurden Schutzmaßnahmen und Sicherheitslösungen entwickelt, die vom Bauwerksschutz, neuen Detektionstechnologien bis hin zu speziellen Schulungen der Verkehrsteilnehmer und Empfehlungen zur Optimierung der Notfallkonzepte reichen. Die entwickelten Maßnahmen sind das Ergebnis einer engen Zusammenarbeit von zehn interdisziplinären Partnern, bestehend aus Bundesbehörden, öffentlichen Forschungseinrichtungen sowie der Privatwirtschaft. Das Projekt SKRIBT wurde nach dreieinhalb Jahren Laufzeit im Juli 2011 abgeschlossen.

Im Nachfolgeprojekt SKRIBTPlus, das im Dezember 2014 abgeschlossen wurde, wurden, aufbauend auf den Erkenntnissen und Innovationen aus SKRIBT, neue bauliche, betriebliche sowie organisatorische Maßnahmen entwickelt und bereits betrachtete Maßnahmen im Hinblick auf ihre Schutzwirkung optimiert. Darüber hinaus wurden Verfahren zur Identifizierung kritischer Bauwerke und zur Bewertung der Maßnahmenwirksamkeiten weiterentwickelt sowie praxisfreundliche Anwendungshilfen für Bauwerkseigentümer, -betreiber, Nutzer sowie die Betriebs- und Einsatzdienste erarbeitet.

Mit den vorliegenden Empfehlungen zur Durchführung einer Risikoanalyse sollen die Tunnelbetreiber angeregt werden, ein betriebliches Risikomanagement zu etablieren, um die Betriebsabläufe in einer Tunnelleitzentrale ausfallsicherer zu gestalten, Schäden an Menschen und Umwelt zu vermeiden sowie rechtliche oder vertragliche Anforderungen zu erfüllen.

Partner im Verbundprojekt SKRIBT Plus

Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe

Julius-Maximilians-Universität
Würzburg

Universität Stuttgart

Siemens

Fraunhofer EMI

Bundesanstalt für
Strassenwesen

Ruhr-Universität Bochum

Hochtief Solutions AG

Schüssler-Plan

PTV Group

Quelle: © dotshock/Shutterstock.com

A

Einleitung

Quelle: © mkfilm/Shutterstock.com

Quelle: © Pixabay

Einleitung

Für die Aufrechterhaltung des Betriebs in Straßentunneln sind die Tunnelleitzentralen (TLZ) zuständig. Sie übernehmen die Überwachung, Steuerung und Sicherung des Verkehrs sowie die Steuerung der technischen Betriebseinrichtungen im Normal-, Störungs- und im Ereignisfall. Dabei ist gemäß den Richtlinien für die Ausstattung und den Betrieb von Straßentunneln (RABT) bei Tunneln ab 400 m Länge eine 24-stündige Überwachung sicherzustellen [1]. Auch wenn der Tunnelbetrieb grundsätzlich automatisch gesteuert wird, ist die ständige Überwachung der Tunnel eine wesentliche Voraussetzung, um das Sicherheitsniveau für die Tunnelnutzer zu gewährleisten. Im Sinne der Aufrechterhaltung eines zuverlässigen Verkehrssystems „Straße" können Straßentunnel und die zugehörigen Tunnelleitzentralen je nach ihrer Bedeutung Kritische Infrastrukturen darstellen.

In vielen Bundesländern nehmen die Leitzentralen neben der Tunnelüberwachung auch weitere Aufgaben wahr. Zu diesen Aufgaben gehören z. B. die Verkehrsüberwachung und -steuerung auf Bundesautobahnen, die Koordinierung von Winterdiensteinsätzen, die Überwachung der Fernmeldetechnik/Telekommunikationstechnik, die Überwachung der Windwarnanlagen von Brückenbauwerken. Sie fungieren auch als Meldestellen des jeweiligen Bundeslandes für die Anforderungen von Autobahnmeistereien oder die An- und Abmeldung von Tagesbaustellen von Autobahnabschnitten.

Bei Ereignissen im Tunnel sind die Operatoren in der Tunnelleitzentrale bis zum Eintreffen der Einsatzkräfte für die Erstmaßnahmen im Tunnel zuständig. Unmittelbar nach der Alarm- bzw. Notrufauslösung ist es ihre Aufgabe, die Selbstrettungsphase der Tunnelnutzer zu unterstützen, d. h. den Tunnel zu sperren, die Beleuchtung einzuschalten, die Belüftung zu steuern und die Nutzer durch Lautsprecherdurchsagen zu informieren, soweit dieses nicht durch automatisierte Prozesse erfolgt. In jedem Fall ist eine Überwachung dieser Prozesse durch die Operatoren erforderlich.

Eine wesentliche Aufgabe der TLZ besteht auch darin, den Einsatzkräften die notwendigen Lageinformationen (z. B. Richtung der Rauchausbreitung im Brandfall, Personenströme etc.) zu übermitteln. Je nach Konzeption der TLZ können die Operatoren auch weitere Aufgaben übernehmen, wie z. B. die Disposition der Einsatzkräfte und Einsatzmittel im Ereignisfall. In der zweiten Phase, nach dem Eintreffen der Einsatzkräfte, wirkt die TLZ unterstützend und beratend. Sie hat eine Mitwirkungspflicht, handelt aber auf Anweisung der Feuerwehr oder der Polizei. Die Einsatzleitung liegt grundsätzlich bei der Feuerwehr oder der Polizei.

Der Ausfall der TLZ hätte erhebliche Konsequenzen für den Betrieb der überwachten Tunnel. Um diesen Betrieb zu gewährleisten, müssen insbesondere die für den Betrieb erforderlichen Infrastrukturen (Energieversorgung, Informations- und Kommunikationstechnik) dauerhaft und zuverlässig zur Verfügung stehen. Zwar hat der Ausfall der TLZ – sei es durch Fehlfunktionen der technischen Komponenten, physische Einflüsse, wie z. B. Naturereignisse, oder durch vorsätzliche Handlungen etwa in Form von Hackerangriffen auf die Überwachungssoftware – je nach Ausmaß nicht zwingend eine Sperrung der überwachten Tunnel zur Folge. Dennoch hat eine möglichst kurzfristige Wiederherstellung der Funktionsfähigkeit der TLZ allein aus betrieblicher bzw. Ressourcensicht hohe Priorität, da die Tunnel bei Ausfall der TLZ vor Ort mit Personal besetzt werden müssen.

In den vorliegenden Empfehlungen wird eine methodische Vorgehensweise zur Durchführung einer Risikoanalyse für Tunnelleitzentralen aufgezeigt. Im Rahmen der Risikoanalyse gilt es, kritische Prozesse bzw. Prozesselemente in den TLZ, die für die Funktion und die Verlässlichkeit des Betriebs erforderlich bzw. unabdingbar sind, zu identifizieren, mögliche Gefährdungen, die zu einem Betriebsausfall führen können, zu analysieren, Verwundbarkeiten der Prozesse und der Prozesselemente gegenüber den betrachteten Gefahren abzuschätzen und daraus Maßnahmenempfehlungen für ein im Vorfeld definiertes Schutzniveau abzuleiten. Die Risikoanalyse ist eine wesentliche Voraussetzung für ein effektives betriebliches Risikomanagement mit dem Ziel, Betriebsabläufe ausfallsicherer zu gestalten, Schäden an Menschen und Umwelt zu vermeiden sowie rechtliche oder vertragliche Anforderungen zu erfüllen.

B

Rahmen-
bedingungen

Quelle: Natalia Klenova/EyeEm/Getty Images

Rahmenbedingungen

In verschiedenen Bereichen wie etwa im Bankenbereich, im Telekommunikationsbereich oder generell in Aktiengesellschaften oder großen GmbH's besteht die Verpflichtung, Risikoanalysen durchzuführen oder ein Risikomanagementsystem einzurichten. Für Tunnelleitzentralen existieren keine vergleichbaren rechtlichen Regelungen.

Allerdings gibt es eine Reihe von nationalen und internationalen Standards, die das Vorgehen für eine Risikoanalyse aufzeigen.

Zudem geben verschiedene Empfehlungen Hinweise für die Einführung und Umsetzung eines Risiko- und Informationssicherheitsmanagements. Insbesondere die Frage der IT-Sicherheit nimmt angesichts verschiedener Vorfälle in den vergangenen Jahren an Bedeutung zu und steht zunehmend im Fokus der Politik und der Betreiber Kritischer Infrastrukturen. Nicht zuletzt das im Juni 2015 vom Bundestag verabschiedete IT-Sicherheitsgesetz stellt höhere Anforderungen an die informationstechnischen Systeme Kritischer Infrastrukturen und adressiert auch den Sektor Transport und Verkehr.

1. Norm DIN EN 50518 – Alarmempfangsstelle (AES)

Für die Einrichtung und den Betrieb von Sicherheitszentralen und Leitstellen hat es bis 2011 auf nationaler Ebene keine Normung gegeben. Mit der Veröffentlichung der Europäischen Normenreihe DIN EN 50518, die durch das Technische Komitee CENELEC[1] / TC 79 „Alarmanlagen" erarbeitet wurde, ist diese seit September 2011 in Deutschland anzuwenden.

Der Geltungsbereich dieser Europäischen Norm erstreckt sich auf „[...] Alarmempfangsstellen, welche Signale überwachen und/oder empfangen und/oder verarbeiten, die eine umgehende Reaktion auf Notfälle erfordern" [2]. Betroffen sind nicht nur Meldungen bzw. Signale aus Einbruch- und Überfallmeldeanlagen, vielmehr schließt die Norm alle Alarmanlagen der Normenreihe DIN EN 50131 ff. mit ein:

- Zutrittskontrollanlagen (EN 50133)
- Videoüberwachungsanlagen (EN 50132)
- Audio- und Video-Hauskommunikations-Systeme
- Personen-Hilferuf-Anlagen (Hausnotrufanlagen/Aufzugsnotrufanlagen) (EN 50134)

sowie

- Brandmeldeanlagen
- (Fahrzeug-) Ortungs- und Verfolgungsanlagen
- Überwachungssysteme für Wachpersonal (Arbeitsplatzabsicherung/Ortung)
- Überwachungssysteme für Telekommunikationsnetze

Alle zentralen Stellen, die Informationen aus solchen Anlagen empfangen, verarbeiten und (personelle) Interventionen einleiten, sollten den Anforderungen dieser Norm entsprechen [2]. Dies können Werkschutzzentralen, Sicherheitszentralen oder Leitstellen der Behörden und Organisationen für Sicherheitsaufgaben (BOS) sein.

Die DIN EN 50518 ist in drei Teile gegliedert und regelt im ersten Teil die örtlichen Voraussetzungen sowie die baulichen Anforderungen an die Alarmempfangsstelle. Es werden z. B. Mindestwandstärken für die Außenhaut der AES definiert, die Angriffen mit mechanischen Mitteln standhalten sollen. Der Zugang zu einer AES ist mit einer baulichen Personenschleuse zu versehen. Lüftungseingänge und -ausgänge müssen sich von innen luftdicht verriegeln lassen. Auch sind die AES mit Alarmanlagen auszustatten, die Einbruch, Feuer, Gas-Konzentrationen, Zutritt/Austritt etc. optisch sowie akustisch signalisieren. Darüber hinaus ist die Kapazität der Notstromversorgung für alle relevanten Betriebsfunktionen für die Zeitdauer von 24 Stunden auszurichten.

[1] Europäisches Komitee für Elektrotechnische Normung (Comité Européen de normalisation Electrotechnique).

Der zweite Teil der Norm [3] behandelt die technischen Anforderungen an eine AES. Gefordert wird u. a. die Aufzeichnung und Dokumentation der Daten aus dem Betrieb, wozu Meldungen, eingeleitete Maßnahmen sowie Kommunikationsdaten gehören. Darüber hinaus sind die Einrichtungen der AES regelmäßig zu prüfen und Ersatzeinrichtungen bzw. Ersatzverfahren für Komponenten des Alarmempfangs und der Weiterleitung der Alarmsignale bei Störungen vorzusehen. Für alle außerplanmäßigen Vorkommnisse, die den Betrieb der AES einschränken und alle unvorhersehbaren Ereignisse, die zum Ausfall der AES führen, ist ein schriftlicher Plan zu erstellen, in dem die Tätigkeiten bzw. die zu ergreifenden Maßnahmen für das jeweilige Ereignis klar definiert sind. Beispiele für außergewöhnliche Vorkommnisse sind im Abschnitt 11.2 der Norm aufgeführt und umfassen:

- Ausfall von Verarbeitungseinheiten, die den bestimmungsgemäßen Betrieb beeinträchtigen
- Fehler, Störungen oder Schäden an örtlichen Einrichtungen, Kommunikationseinrichtungen oder Kommunikationsleitungen
- Feuer, einschließlich Feuer in angrenzenden und benachbarten Objekten
- Überschwemmung oder andere Wassereinbrüche
- Sturm- und Blitzschäden, Überspannungen mit Wirkung auf das Stromversorgungsnetz und Telefonleitungen
- Fahrzeug-Aufprall, einschließlich Schienenfahrzeuge und Flugzeuge
- mutwillige Beschädigung
- kriminelle Angriffe und Bombendrohung oder andere Bedrohungssituationen

Für betriebliche Abläufe wird im dritten Teil der Norm [4] gefordert, dass die AES mit mindestens zwei Personen besetzt sein muss und die Mitarbeiter eine behördliche Sicherheitsüberprüfung vorweisen müssen. Für die Mitarbeiter der AES muss es ein Aus- und Weiterbildungskonzept geben, das alle theoretischen und praktischen Anforderungen an die Tätigkeit abdeckt.

Darüber hinaus sollen dokumentierte Verfahren etabliert werden, die den Zutritt und das Verlassen der AES regeln sowie den sicheren Umgang mit vertraulichen Informationen, zu denen die Mitarbeiter Zugang haben, gewährleisten. Dies gilt auch für die Bearbeitung von Meldungen und Daten. Notfallpläne sollen sicherstellen, wie im Fall des Ausfalls der AES zu verfahren ist. So müssen u. a. für Gefahren wie Angriffe von außerhalb (Einbruch), Überfälle, Feuer und Wasser entsprechende Notfallverfahren vorhanden sein. Ebenso muss ein Reaktionsplan erstellt werden, der eine Teilevakuierung sowie die vollständige Evakuierung der AES beinhaltet.

Die Einhaltung der Anforderungen der Normen der Reihe EN 50518 ist in Form eines jährlich wiederkehrenden Audits durch eine akkreditierte Stelle zu bescheinigen. Hierfür hat die VdS Schadenverhütung GmbH einen Zertifizierungsleitfaden erstellt [5].

Neben den baulichen, technischen und betrieblichen Anforderungen ist in der Norm die Durchführung einer Risikoanalyse vorgesehen, die alle für eine AES relevanten Risiken prüfen soll. In einem ersten Schritt ist eine Risikobeurteilung für den Standort der AES zu erstellen (Abschnitt 4.1, 4.2). Dabei muss die Standortwahl insbesondere Gefahren wie Feuer, Explosion, Überflutung, Vandalismus und Gefahren, die aus der Umgebung resultieren, Rechnung tragen.

Eine Risikobewertung wird auch bei der Planung einer Einbruchmeldeanlage nach EN 50131-1 gefordert (Abschnitt 6.1). Ebenso sind gegen die Auswirkungen von Blitzschlägen Vorkehrungen zu treffen und es ist eine Risikoanalyse in Übereinstimmung mit EN 62305-2 (Blitzschutz – Teil 2: Risiko-Management) durchzuführen.

Konsequenzen für Tunnelleitzentralen

Gemäß der Definition des weitgefassten Anwendungsbereichs der AES ist diese Norm auch für Tunnelleitzentralen anwendbar. Gleichwohl wird in der Fachwelt kontrovers diskutiert, ob die Norm, die mit dem Fokus auf private

Sicherheitsdienstleister entstanden ist, auch die Leitstellen der öffentlichen Betreiber anwenden sollen [6]. Kritik finden insbesondere die in einigen Bereichen formulierten hohen baulichen und technischen Sicherheitsanforderungen, die insbesondere für kleinere Leitstellen unter Berücksichtigung von Kosten-Nutzen Aspekten nicht als zweckmäßig erachtet werden. Grundsätzlich besteht keine gesetzliche Verpflichtung, die Norm anzuwenden. Gleichwohl spiegeln die Anforderungen der Norm den Stand der Technik wider, was bei entsprechenden Anpassungen die Haftungsrisiken minimiert.

Auch die (öffentlichen) Betreiber von Tunnelleitzentralen sollten prüfen, ob die Notwendigkeit zur Umsetzung dieser Norm gegeben ist, also haftungsrechtliche Gründe hierfür sprechen. Auf Basis einer Risikoanalyse ist dann zu ermitteln, welche Anforderungen dieser Norm angemessen sind und umgesetzt werden sollen und welche Vorgaben nicht zielführend sind oder durch andere kostengünstigere Maßnahmen mit vergleichbarem Effekt ersetzt werden können.

2. Methodische Ansätze zur Durchführung einer Risikoanalyse

Es existiert eine Reihe von methodischen Ansätzen zur Durchführung einer Risikoanalyse. Grundsätzlich unterscheiden sich die Methoden darin, ob eine quantitative oder qualitative Risikobewertung aus den Parametern Eintrittswahrscheinlichkeit und Schadensausmaß vorgenommen wird. Quantitative Berechnungen setzen allerdings voraus, dass entsprechendes Datenmaterial zur Verfügung steht. In aller Regel fehlen aber die erforderlichen Daten und Statistiken, auf deren Basis Eintrittswahrscheinlichkeiten für Gefahren oder auch das zu erwartende Schadensausmaß berechnet werden können.

Unabhängig davon, ob ein quantitativer oder qualitativer Ansatz für die Risikobewertung gewählt wird, ist die Durchführung einer Risikoanalyse mit Arbeitsaufwand und folglich auch mit Kosten verbunden. Um diesen Aufwand zu begrenzen, bietet sich für die Durchführung einer Risikoanalyse für TLZ eine zweistufige Vorgehensweise an, die auf bewährten Methoden beruht:

1. Erstellung/Überprüfung des Sicherheitskonzepts auf Basis von IT-Grundschutz

2. Durchführung einer detaillierten Risikoanalyse

Die Betriebsabläufe bzw. die einzelnen Prozesse in der TLZ werden maßgeblich durch die Informationstechnologie unterstützt. Daher ist die Gewährleistung der Informationssicherheit, die auf den Grundwerten Verfügbarkeit, Vertraulichkeit und Integrität beruht, ein ganz wesentlicher Bestandteil der Risikoanalyse und des darauf aufbauenden Sicherheitskonzepts für Tunnelleitzentralen. Der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bietet eine praxiserprobte qualitative Methode zur Risikobewertung in der Informationssicherheit, welche in einem **ersten Schritt** zur Überprüfung des vorhandenen Schutzniveaus angewendet werden sollte. Die Methodik ist eingebunden in ein ganzheitliches Konzept eines Informationssicherheitsmanagements, das als Bestandteil eines allgemeinen Risikomanagements im BSI-Standard 100-1 „Managementsysteme für die Informationssicherheit (ISMS)“ [7] ausführlich erläutert wird.

Die Methode des IT-Grundschutzes basiert auf dem BSI-Standard 100-2 [8], der die Vorgehensweise zur Anwendung des IT-Grundschutzes beschreibt, und den IT-Grundschutzkatalogen. In den nach dem Baukastenprinzip aufgebauten Grundschutzkatalogen, bestehend aus Baustein-, Gefährdungs- und Maßnahmenkatalogen, werden für IT-Systeme, Anwendungen, Netze, *aber auch für die Bereiche der Infrastruktur, Organisation, Personal und Notfallvorsorge,* wie es im Basisschutzkonzept des Bundesministeriums des Inneren (BMI) 2005 veröffentlicht wurde [9], Standardsicherheitsmaßnahmen empfohlen. Folglich deckt der IT-Grundschutz nicht nur Aspekte der Informationssicherheit ab, sondern bezieht auch andere Werte, wie z. B. Gebäude, technische Versorgungsinfrastruktur etc., mit ein. Dabei werden typische Gefährdungen betrachtet (z. B. Feuer, Überflutung, Computer-Viren etc.), die eine hohe Eintrittswahrscheinlichkeit haben oder erheblichen Schaden anrichten können, die Schutzmaßnahmen erfordern. Da es sich bei den Maßnahmen um einen Basisschutz handelt, der mögliche Verwundbarkeiten bzw. Schwachstellen sowie die Eintrittswahrscheinlichkeiten mit berücksichtigt,

bedarf es bei der IT-Grundschutz-Vorgehensweise ohne weiteren Analyseaufwand zunächst nur eines Soll-Ist-Abgleichs zwischen den in den IT-Grundschutzkatalogen empfohlenen und den bereits realisierten Maßnahmen. Auf diese Weise soll eine Basis-Sicherheit gegenüber Standard-Gefährdungen erreicht werden.

Der IT-Grundschutz konkretisiert die allgemein gehaltenen Anforderungen der ISO-Standards 27001 [10] und 27002 [11] und hat sich als ganzheitliches Konzept für Informationssicherheit als Standard etabliert. Eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz erfolgt durch das BSI.

Die Durchführung einer detaillierten Risikoanalyse in einem **zweiten Schritt** erweist sich dann als sinnvoll, wenn es sehr kritische Bereiche/Systeme gibt, die im IT-Grundschutz nicht behandelt werden, d. h. zusätzliche Maßnahmen zu ergreifen sind. Dies gilt vor allem, wenn Szenarien herangezogen werden, die in ihrer Intensität über den ggf. realisierten Schutz gegenüber der betrachteten Gefahr deutlich hinausgehen. Dabei orientiert sich die Risikoanalyse-Methodik sowohl am Leitfaden zum Risiko- und Krisenmanagement für Unternehmen und Behörden des Bundesministeriums des Innern [12] als auch an der Methode für die Risikoanalyse im Bevölkerungsschutz des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe [13].

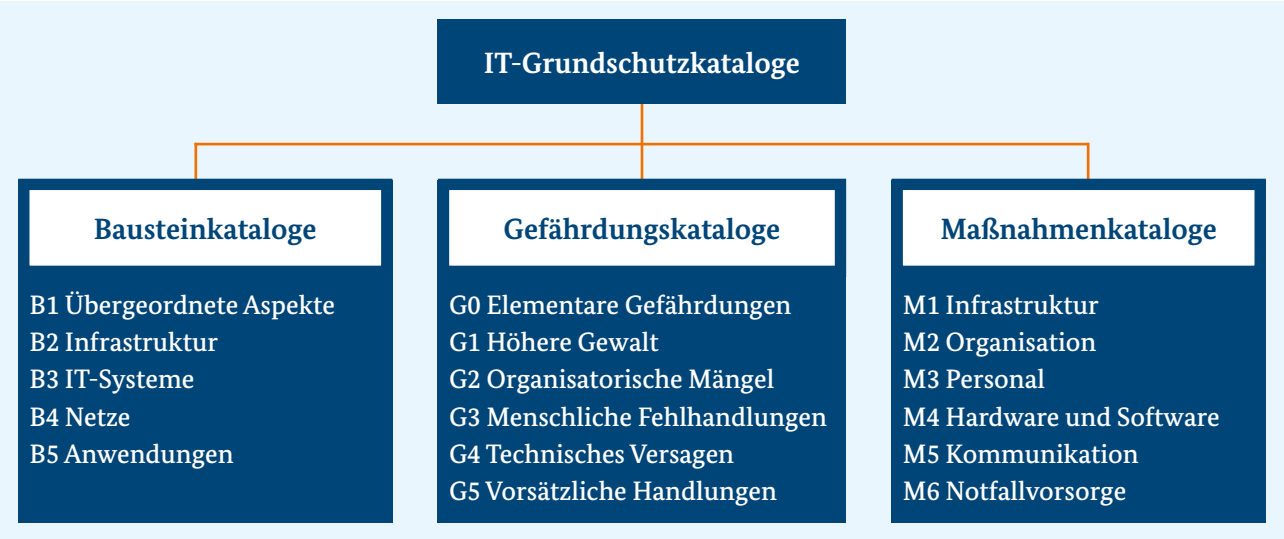


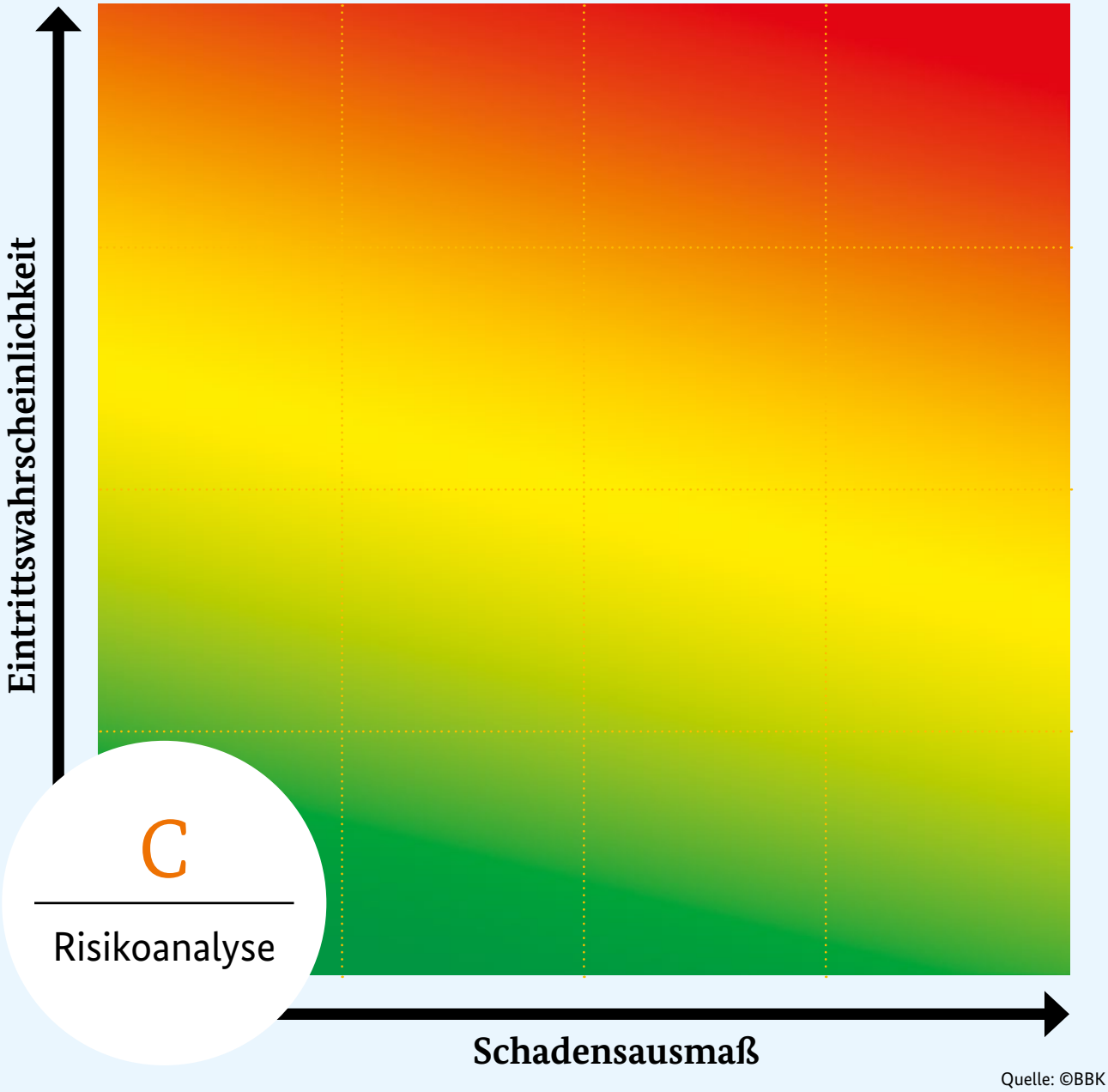
Abbildung 1: Systematik der IT-Grundschutzkataloge; Quelle BBK

Standards zur Informationssicherheit, Risikomanagement

- Bundesamt für Sicherheit in der Informationstechnik (BSI 2008):
  BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS). Bonn.
- Bundesamt für Sicherheit in der Informationstechnik (BSI 2008):
  BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise. Bonn.
- Bundesamt für Sicherheit in der Informationstechnik (BSI 2008):
  BSI-Standard 100-3 Risikoanalyse auf Basis von IT-Grundschutz. Bonn.
- Bundesamt für Sicherheit in der Informationstechnik (BSI 2008):
  BSI-Standard 100-4 Notfallmanagement. Bonn.
- Bundesamt für Sicherheit in der Informationstechnik (BSI 2011):
  Ergänzung zum BSI-Standard 100-3 Verwendung der elementaren Gefährdungen aus den IT-Grundschutz-Katalogen zur Durchführung von Risikoanalysen. Bonn.
- ISO/IEC 27001:2015-03 Information technology – Security techniques – Information security management systems requirements specification.
- ISO/IEC 27002:2014-02 Information technology – Security techniques – Code of practice for information security management.
- ISO/IEC 27005:2011-06 Information technology – Security techniques – Information security risk management.
- ISO 31000:2009-11 Risk management – principles and guidelines.
- ISO/IEC 31010:2009-11 Risikomanagement Verfahren zur Risikobeurteilung.

Empfehlungen und branchenbezogene Leitfäden zum Risikomanagement und Risikoanalyse

- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK 2010) (Hrsg.):
  Methode für die Risikoanalyse im Bevölkerungsschutz (= Reihe Wissenschaftsforum, Band 8). Bonn.
- Bundesministerium des Innern (BMI 2011) (Hrsg.):
  Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. Berlin.
- Bundesministerium des Innern (BMI 2005) (Hrsg.):
  Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Empfehlungen für Unternehmen. Berlin.
- Bundesamt für Sicherheit in der Informationstechnik (BSI 2013) (Hrsg.):
  Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Leitfaden. Bonn.
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK 2008) (Hrsg.):
  Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens. Bonn.



Quelle: ©BBK

Risikoanalyse

Die im Folgenden vorgestellte Vorgehensweise zur Durchführung einer Risikoanalyse für Tunnelleitzentralen besteht aus mehreren systematisch aufgebauten Schritten, die in der nachstehenden Abbildung aufgeführt sind. Grundsätzlich lässt sich diese Vorgehensweise anhand der folgenden Fragestellungen erläutern:

- *Vorbereitung:* Woran muss man denken, wenn man eine Risikoanalyse durchführen möchte?
- *Kritikalitätsanalyse/Schutzbedarfsfeststellung:* Welche Bereiche der Einrichtung sind für den Betriebsablauf besonders wichtig und folglich kritisch?
- *Gefahrenanalyse und Szenarienentwicklung:* Welche Gefahren drohen?
- *IT-Grundschutzanalyse:* Welche Schutzmaßnahmen gibt es bereits?
- *Detaillierte Risikoanalyse:* Reichen diese Maßnahmen gegenüber den betrachtete Szenarien aus?
  - Wie wahrscheinlich sind diese Szenarien?
  - Gibt es besonders verwundbare Bereiche?
  - Wie hoch ist der Schaden beim Ausfall bestimmter Prozesselemente?
  - Wie hoch ist das Risiko?

Abbildung 2: Vorgehensweise der Risikoanalyse; Quelle: BBK

1. Vorbereitung

1.1 Implementierung des Risikomanagements

Die Durchführung einer Risikoanalyse muss gut vorbereitet sein, indem im Vorfeld grundsätzliche Fragen zur Etablierung eines Risikomanagements in der Einrichtung geklärt und die erforderlichen organisatorischen Voraussetzungen geschaffen werden. Hierzu zählen insbesondere

- die Implementierung des Projekts durch die Leitungsebene in die bestehenden Strukturen,
- die Festlegung der Zuständigkeiten im Rahmen der Umsetzung,
- die Bereitstellung notwendiger Ressourcen,
- eine Definition der Schutzziele für die Einrichtung, die den generellen Maßstab für die spätere Bewertung der Risiken bilden [12].

Dabei sind für eine erfolgreiche Umsetzung des Risikomanagements folgende Punkte relevant:

- Die Durchführung einer Risikoanalyse in einer TLZ sollte durch die zuständige Verwaltungsbehörde für Straßentunnel, in der Regel durch die Straßenbauverwaltung der Länder, initiiert und getragen werden. Es liegt in der Verantwortung der zuständigen Verwaltungsbehörde, den Untersuchungsbereich im Rahmen der Risikoanalyse festzulegen, die Ziele des Risikomanagements zu definieren sowie grundlegende Entscheidungen über zu ergreifende Schutzmaßnahmen zu treffen. Darüber hinaus sind die Rahmenbedingungen zur Durchführung der Risikoanalyse zu schaffen (z. B. personelle und finanzielle Ressourcen).
- Es sollte eine Projektgruppe eingerichtet werden, die die Risikoanalyse durchführt und geeignete Maßnahmenvorschläge erarbeitet. Beteiligte in der Projektgruppe können Mitarbeiter der TLZ sein, die sich mit den Abläufen und Strukturen der TLZ gut auskennen, des Weiteren IT-Administratoren sowie Sicherheitsbeauftragte für Straßentunnel. Nach Bedarf können auch weitere Institutionen, die eine entsprechende Expertise für die Risikoanalyse liefern können, einbezogen werden. Dies können z. B. kommunale Ämter sein, die erforderliches Datenmaterial zur Verfügung stellen. Idealerweise sollte aber auch jener Personenkreis aus Feuerwehr, Polizei und den Rettungsdiensten eingebunden werden, der an der Erstellung und Abstimmung der Alarm- und Gefahrenabwehrpläne für Straßentunnel beteiligt ist. Die Moderation bzw. die Steuerung der Projektgruppe könnte der Leiter der TLZ oder der Sicherheitsbeauftragte für Straßentunnel wahrnehmen.
- Eine erfolgreiche Umsetzung der Risikoanalyse setzt ebenso voraus, dass eine enge Kommunikation zwischen der zuständigen Verwaltungsbehörde und der Projektgruppe stattfindet, d. h. die Verwaltungsbehörde in regelmäßigen Abständen über die Arbeit der Projektgruppe informiert und diese möglichst in alle wichtigen Planungs- und Entscheidungsprozesse eingebunden wird.
- Alle Entscheidungen, Begründungen und Ergebnisse im Verlauf des Risikoanalyse-Prozesses sind sorgfältig zu dokumentieren, um die Nachvollziehbarkeit von Vorgängen und getroffenen Maßnahmen für alle Beteiligten zu gewährleisten. Da die Risikoanalyse nicht statisch ist, sondern ein dynamischer Prozess, der wiederholt werden muss, ist die Dokumentation von Entscheidungen z. B. über Schwellenwerte oder Definition von Kriterien außerordentlich wichtig. Auf diese Weise wird sichergestellt, dass im Rahmen einer Fortschreibung der Risikoanalyse die Risikoidentifikation und -bewertung auf einer nachvollziehbaren Basis erfolgt.

1.2 Definition der Ziele zum Schutz der Tunnelleitzentrale

Im Vorfeld der Risikoanalyse sind zunächst die Ziele festzulegen, die das erwünschte Schutzniveau bzw. den Sollzustand für die Einrichtung bzw. für die zu schützenden Bereiche der Einrichtung beschreiben und an denen sich die Untersuchung orientieren kann. Anhand dieser Ziele lassen sich kritische Prozesse und die zugehörigen Elemente ermitteln sowie die identifizierten Risiken bewerten. Sie bilden somit die Entschei-

dungsgrundlage, ob zusätzliche Maßnahmen im Rahmen des Risikomanagements zu ergreifen sind.

Die ständige Tunnelüberwachung durch eine Tunnelleitzentrale ist ein wesentlicher Baustein des Sicherheitssystems für Straßentunnel. Zwar hat der Ausfall der TLZ nicht zwingend eine Sperrung der überwachten Tunnel mit den entsprechenden verkehrlichen Auswirkungen zur Folge, solange die Überwachung der Tunnel vor Ort gewährleistet ist. Dies wird jedoch umso kritischer, je mehr Tunnel von einer Stelle aus überwacht werden. Deshalb hat eine möglichst kurzfristige Wiederherstellung der Funktionsfähigkeit der TLZ allein aus betrieblicher bzw. Ressourcensicht hohe Priorität.

Daraus lässt sich als **übergeordnetes Ziel** ableiten, dass für die Gewährleistung des Sicherheitsniveaus im Tunnel – auch im Fall von extremen Ereignissen / Extremsituationen – die **Funktionsfähigkeit der TLZ** aufrechterhalten werden soll. Dieses Ziel zum Schutz der Einrichtung lässt sich weiter konkretisieren, z. B.

- Vermeidung eines Totalausfalls der TLZ (ggf. Definition der maximal tolerierbaren Ausfallzeit)
- Aufrechterhaltung der Funktionalität besonders kritischer Systeme (z. B. Steuerung, Kommunikation)
- Reduzierung der Wiederanlaufzeiten

Je nach Ausrichtung des Risikomanagements und der Risikoanalyse – All-Gefahrenansatz oder die Betrachtung nur bestimmter Gefahren? Gesamtbetrachtung der Einrichtung oder Begrenzung des Analysebereichs auf einzelne Ressourcen und Systeme? – können spezielle Ziele, z. B. Schutz der Einrichtung vor Angriffen (physischer Schutz), Schutz des Personals oder Sicherheit der Informations- und Kommunikationstechnik Grundlage für das Risikomanagement sein.

1.3 Festlegung des Analysebereichs

Es ist erforderlich, vor Beginn der Risikoanalyse den zu analysierenden Bereich festzulegen. Die Analyse kann sich auf die gesamte Einrichtung beziehen oder – je nach Zielsetzung – sich allein auf den Standort der TLZ, d. h. die baulich-physische Infrastruktur und die mit diesem Standort verbundenen Risiken beschränken. Ferner kann sich die Analyse auf einzelne Organisationseinheiten und somit nur auf bestimmte Prozesse, beispielsweise die Kernaufgaben der Einrichtung, wie Überwachung, Steuerung der Betriebstechnik sowie Einsatzunterstützung beziehen oder auch alle Aufgaben der Einrichtung, einschließlich der jeweiligen Unterstützungsprozesse (vgl. → Kapitel C.1.4.1), umfassen.

Wichtig ist, dass in der Risikoanalyse dann alle Elemente betrachtet werden, die zur Erfüllung dieser Aufgaben beitragen, also nicht nur die IT-Infrastruktur, auf die sich die meisten Prozesse in einer TLZ stützen, sondern auch Personal und physische Objekte wie Gebäude und die technische Versorgungsinfrastruktur. In der Informationsverarbeitung wird z. B. zur Abgrenzung des Geltungsbereichs für ein auf Basis von IT-Grundschutz zu erstellendes IT-Sicherheitskonzept der Begriff „Informationsverbund“ verwendet. Demnach umfasst der *„Informationsverbund die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen“* [8].

Bei einer Gesamtbetrachtung der Einrichtung muss auch das Übertragungsnetz zu den Tunneln mit den jeweiligen Datenübergabepunkten sowie auch weitere Kommunikationsverbindungen nach außen, z. B. zu den Leitstellen der Feuerwehr, der Polizei sowie den Verkehrszentralen einschließlich der Schnittstellen in die Risikoanalyse einbezogen werden (vgl.→ Kapitel C.1.4.2).

1.4 Bestandsaufnahme der Prozesse und der Prozesselemente

1.4.1 Prozesse

Ausgangspunkt der Risikoanalyse ist eine Bestandsaufnahme der Prozesse und der jeweiligen Ressourcen, die diese Prozesse ermöglichen bzw. unterstützen (vgl. → Kapitel C.1.4.2). Ein Prozess beschreibt die Summe der Tätigkeiten und Bearbeitungsschritte im Laufe der Leistungserbringung.

Prozesse lassen sich unterteilen in Management- bzw. Führungsprozesse, Kernprozesse sowie Unterstützungsprozesse. Führungsprozesse enthalten die leitenden Aufgaben einer Einrichtung. Kernprozesse beschreiben die eigentlichen (operativen) Aufgaben der Einrichtung, in einer TLZ sind es die die Tunnelüberwachung, Beseitigung von Störungen einschließlich Betreuung der Wartungs- und Instandsetzungsarbeiten im Tunnel und im Ereignisfall die Einleitung von Hilfsmaßnahmen sowie die Unterstützung der Einsatzkräfte. Unterstützungsprozesse sichern die Arbeitsfähigkeit der Einrichtung, indem sie alle erforderlichen Ressourcen (Personal, Technik, Informationen) für die Führungs- und Kernprozesse bereitstellen sowie die Umsetzung administrativer Aufgaben begleiten. Zu den Unterstützungsprozessen zählen neben den allgemeinen Verwaltungsaufgaben u. a. auch

- Aus- und Fortbildung der Mitarbeiter
- Übungen und Funktionstests
- Informations- und Wissensmanagement
- Risikomanagement
- Störungs- und Notfallmanagement (bezieht sich auf Ereignisse, die die TLZ betreffen)
- Instandhaltung der TLZ-Infrastruktur

In der folgenden → Tabelle 1 sind Kern- und Unterstützungsprozesse für die TLZ beispielhaft aufgeführt, ohne Anspruch auf Vollständigkeit zu erheben. Die → Abbildung 3 verdeutlicht die Prozessablaufkette für den Prozess „Notrufannahme/Alarmierung/Einsatzunterstützung“, die sich in weitere Prozessschritte unterteilt. Je nachdem, auf welchem Wege eine Ereignismeldung erfolgt (Notrufstation, Notruf über Mobiltelefon an Leitstellen der Feuerwehr oder der Polizei oder Meldungen mittels Detektion), ergeben sich in der Prozessablaufkette bzgl. der Reihenfolge der Kommunikationsabläufe der Einsatzdienste und bei den einzelnen Prozessschritten geringfügige Änderungen. Die exemplarisch in der Abbildung dargestellte Prozesskette muss nicht in Gänze durchlaufen werden und kann z. B. nach der Notrufannahme mit der Beratung des Anrufenden enden. In ähnlicher Weise lassen sich auch die in der → Tabelle 1 aufgeführten Kern- und Unterstützungsprozesse in weitere Teilprozesse oder Prozessschritte unterteilen.

Quelle: © Miha Creative/Shutterstock

Tabelle 1: Beispiel für Kern- und Unterstützungsprozesse einer Tunnelleitzentrale
Kernprozesse
Im Regelbetrieb
Prozess: Überwachung und Steuerung des Verkehrs und der Tunneltechnik
Prozess: Betreuung der Wartungs- und Instandsetzungsarbeiten im Tunnel
Im Ereignisfall/Störfall
Prozess: Notrufannahme/Alarmierung/Einsatzunterstützung
Notrufannahme
Weiterleiten der Informationen (Alarmierung)
Erstmaßnahmen
Einsatzunterstützung
Einsatzende
Prozess: Störungsbeseitigung
Fehlermeldung/Alarm optisch/akustisch
Kenntnisnahme Störung / Quittieren
Zeitliche Priorisierung der zu ergreifenden Maßnahmen
Einleitung Maßnahmen / Eröffnung Protokoll
Durchführung Maßnahmen
Ende/Schließen Protokoll
Unterstützungsprozesse
Organisation der TLZ
Haushalt und Verwaltung
Aus- und Fortbildung der Mitarbeiter
Übungen und Funktionstests
Informations- und Wissensmanagement (Daten- und Dokumentpflege, Bereitstellung notwendiger Informationen)
Risikomanagement
Störungs- und Notfallmanagement (Ereignisse die TLZ betreffend)
Instandhaltung der (TLZ-) Infrastruktur (bauliche und technische Anlagen, IT-Systeme)
Beschaffung

Hinweis:
Wurde für die TLZ ein Qualitätsmanagementsystem erstellt, können die dort beschriebenen Prozesse auch der Risikoanalyse zugrunde gelegt werden.

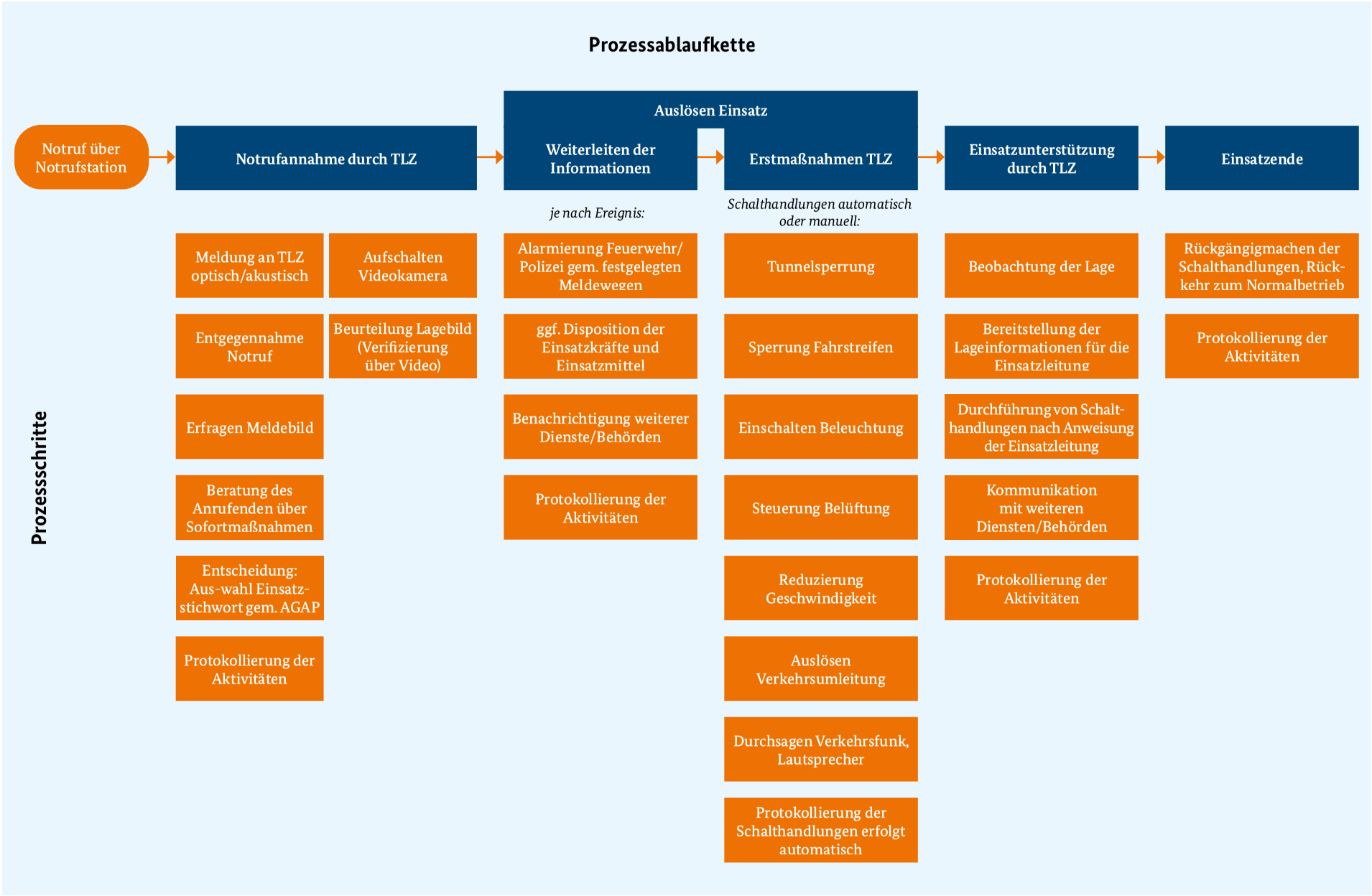


Abbildung 3: Protessablaufkette „Notrufannahme/Alarmierung/Einsatzunzterstützung“; Quelle BBK

1.4.2 Prozesselemente

In einem weiteren Schritt der Vorbereitung der Risikoanalyse werden alle Prozesselemente[2] erfasst, die zur Erfüllung der Prozesse benötigt werden. Es sind sowohl physische als auch virtuelle Elemente (z. B. Software, Daten), die ausfallen oder beschädigt werden und folglich auch die betrachteten Prozesse beeinträchtigen können. Dabei handelt es sich grundsätzlich um folgende Elemente [12]:

- Fachpersonal
- Gebäude und Gelände
- Allgemeine technische Anlagen und Geräte (interne Versorgungsnetze/Haustechnik, Informations- und Kommunikationstechnik)
- Einrichtungsspezifische technische Anlagen und Geräte
- Daten und Unterlagen (alle elektronisch und in Papierform vorgehaltenen Informationen, die für die Aufrechterhaltung von Prozessen notwendig sind)
- Betriebsmittel (z. B. Ersatzteile, Dieselvorrat für Notstromaggregat)

Eine Übersicht der Prozesselemente für die Tunnelleitzentrale ist beispielhaft in → Tabelle 2 dargestellt.

Gegenstand der weiteren Risikobetrachtung sind nicht die Prozesse selbst, sondern die den Prozess tragenden jeweiligen Elemente, deren Bedeutung für die Aufrechterhaltung von Prozessen im Rahmen einer Kritikalitätsanalyse/Schutzbedarfsfeststellung (vgl. → Kapitel C.2) festzulegen ist.

Es ist sinnvoll und angebracht, im Zuge der Bestandsaufnahme der Prozesselemente diese nach zusammenhängenden Einheiten und ähnlichen Objekten zu gruppieren und somit auch die Zahl der in der Risikoanalyse zu berücksichtigenden Elemente und der technischen Komponenten zu reduzieren. Dies gilt vor allem für die IT-Anwendungen und IT-Systeme, die an eine oder auch mehrere Hardwarekomponenten gebunden sein können und folglich im weiteren Verlauf der Risikoidentifikation als ein (Ziel-) Objekt zu betrachten sind. Voraussetzung für eine Gruppenbildung in der IT ist allerdings, dass die Elemente

- vom gleichen Typ sind,
- eine ähnliche Konfiguration aufweisen,
- ähnlich in das Netz eingebunden sind,
- ähnliche Anwendungen bedienen,
- ähnlichen Sicherheitsmechanismen unterliegen,
- bzgl. der Kritikalität der Dienste, die von ihnen unterstützt werden bzw. in ihrem Schutzbedarf übereinstimmen [8].

In einer Gruppe können z. B. mehrere Clients oder auch Server, welche die gleichen Aufgaben wahrnehmen, zusammengefasst sein.

Für die Erfassung der Prozesselemente im Bereich der Informationssicherheit wird beispielhaft die IT-Grundschutz-Vorgehensweise herangezogen, deren Schritte nachfolgend kurz erläutert werden[3]:

[2] Zur Vereinheitlichung der Terminologie werden in diesem Leitfaden die Begriffe „Elemente“ bzw. „Prozesselemente“ verwendet. Dies schließt die IT-Anwendungen und IT-Systeme ein, die im Rahmen der IT-Grundschutzanalyse als „Zielobjekte“ bezeichnet werden.

[3] ausführliche Beschreibung für eine Strukturanalyse des Informationsverbundes siehe BSI Standard 100-2.

Schritt 1: Erfassung der Anwendungen[4] und der zugehörigen Informationen

- Bei der Dokumentation der Anwendungen ist es wichtig, dass die Prozesse, die diese Anwendungen unterstützen, sowie die Art der Information, die diese verarbeiten (Messdaten, personenbezogene Daten, verwaltungsspezifische Daten etc.), vermerkt werden. Denn der in einem weiteren Schritt (vgl. → Kapitel C.2) festzulegende Schutzbedarf der Anwendungen korrespondiert mit dem Schutzbedarf der damit verarbeiteten Informationen.
- Neben den Anwendungen werden auch Datenträger und Dokumente, welche schützenswerte Informationen beinhalten und ggf. auch als Redundanz im Stör- oder Ereignisfall vorgehalten werden (z. B. Archiv- und Backup-Datenträger, Notfallhandbücher, Alarm- und Gefahrenabwehrpläne der überwachten Tunnel oder wichtige Vertragsdokumente) wie Anwendungen behandelt und mit erfasst.

Schritt 2: Erhebung von IT-Systemen[5] und ähnlichen Objekten

- Bei den IT-Systemen werden sowohl die vernetzten als auch die nicht vernetzten Systeme aufgenommen. Erfasst wird nur das System als solches und nicht dessen Einzelbestandteile (Rechner, Tastatur, Bildschirm). Dabei werden gleichgeartete Systeme, z. B. mehrere Einzelplatz-PCs, die die bereits genannten Voraussetzungen hinsichtlich Typ, Konfiguration etc. erfüllen, in einer Gruppe zusammengefasst.
- Es ist anzunehmen, dass in den meisten Einrichtungen ein Netzplan mit Darstellung der IT-Systemarchitektur existiert, der ggf. aktualisiert als Ausgangsbasis für die Bestandsaufnahme der IT-Systeme dienen kann.

Abweichend von dieser Reihenfolge kann es auch hilfreich sein, zuerst die IT-Systeme zu erheben und anschließend die Anwendungen orientiert an den IT-Systemen zusammenzutragen.

Im Anschluss an die Bestandsaufnahme werden die Anwendungen den IT-Systemen zugeordnet, die für die Ausführung dieser Anwendungen benötigt werden.

Schritt 3: Erfassung der Räume und der Kommunikationsverbindungen

- Im letzten Schritt wird vermerkt, in welchem Gebäude bzw. Räumlichkeiten der Liegenschaft die IT-Systeme untergebracht sind. Es sind Räume, die ausschließlich dem IT-Betrieb dienen (z. B. Serverraum) sowie Räume, in denen die IT-Systeme betrieben werden (Büroräume, Leitstellenraum). Auch Räume, in denen schützenswerte Informationen in Form von Datenträgern oder in Papierform aufbewahrt werden, sind aufzuführen.
- Neben den Räumen werden auch die Wegstrecken erfasst, über die die Kommunikationsverbindungen laufen.

Analog dieser Systematik sind auch die weiteren Elemente der physischen Infrastruktur technische Anlagen wie Kühlung, Lüftung, Verteiler interner Versorgungsnetze etc.) sowie die notwendigen Betriebsmittel (Ersatzteile, Dieseltank) nach Standort aufzulisten.

[4] unter Anwendungen werden Verfahren verstanden, die zur Unterstützung von Geschäftsprozessen und Fachaufgaben dienen [8], (vgl. → Tabelle 2).

[5] der Begriff IT-System umfasst die IT-Hardwarekomponenten, also Computer, aktive Netzkomponenten, TK-Anlagen etc. [8].

Hinweis:
Im Zuge des weiteren Vorgehens kann es durchaus sinnvoll sein, eine tabellarische Übersicht der Prozesse mit Zuordnung der an diesen Prozessen beteiligten Anwendungen und IT-Systemen, weiteren Einzelelementen (z. B. eingesetztes Fachpersonal, erforderliche Betriebsmittel) sowie auch den technischen Komponenten der physischen Infrastruktur zu erstellen. Auf diese Weise könnten alle Prozesse ermittelt werden, die durch den Ausfall eines bestimmten Elements betroffen wären.

Tabelle 2: Prozesselemente einer Tunnelleitzentrale (Beispiel)

Fachpersonal	Gebäude/Gelände	Technische Anlagen/Geräte	Relevante Betriebsmittel	Sonstige schützenswerte Dokumente
• Operator • Systemadministrator (intern oder extern) • Techniker (intern oder extern) • Verwaltungspersonal ...	*Hauptgebäude* • Leitstellenraum • Technikräume • Büroräume *Weitere Gebäude/Anlagen auf dem Betriebsgelände* • Netzersatzanlage/ Generatoren • Dieseltank ...	• Interne Versorgungs-netze/Haustechnik • Strom • Wasser • Heizung/Lüftung • Kühlung • Brandmeldeanlage • Gebäudeüberwachung ...	• Ersatzteile • Dieselvorrat für Notstromversorgung ...	• Verträge • Betriebshandbücher • Gebäudepläne • Netzplan ...

Technische Anlagen und Geräte: Informations- und Kommunikationstechnik			
Anwendungen	**IT-Systeme**	**Datenträger**	**Kommunikationsverbindungen**
• Videomanagementsystem • Bedien- und Beobachtungs-software • Einsatzleitsystem • Betriebssysteme • Standard-Anwendungssoftware • Internet-Anwendungen • Sicherheitssoftware ...	• Zentralrechner • Kommunikationsserver • Datenbankserver • Netzdrucker • TK-Anlage • Client • Großbildmonitorwand • Netz ...	• Stationäre und mobile Datenträger • Externe Datenspeicher ...	• Interne und externe Kommunikations-verbindungenn • Schnittstellen zu Tunneln, anderen Leitstellen, Fernwartung ...

2. Kritikalitätsanalyse / Feststellung des Schutzbedarfs

Eine Kritikalitätsbetrachtung der Prozesse und der dazugehörigen Prozesselemente im Vorfeld der eigentlichen Risikoanalyse hat das Ziel, die kritischen und unverzichtbaren Bereiche zu identifizieren, deren Funktionieren für die Einrichtung von existenzieller Bedeutung ist (s. Definition). Durch eine Priorisierung der kritischen Prozesse und Elemente kann der Untersuchungsaufwand der in einem zweiten Schritt durchzuführenden Risikoanalyse (vgl. → Kapitel C.5) begrenzt werden, indem nur die als kritisch angesehenen Bereiche einer Risikoidentifikation unterzogen und die aus der Risikobewertung abgeleiteten vorbeugenden Maßnahmen zur Risikominimierung auf jene Bereiche konzentriert werden.

Definition des Begriffs „Kritikalität“

„Kritikalität ist das Maß für die Bedeutsamkeit eines Prozesses / einer Aufgabe in Bezug auf die Konsequenzen, die eine Störung oder ein Ausfall des Prozesses / der Aufgabe für die Funktionsfähigkeit einer Einrichtung/Dienstleistung hat“ [12]

Für die Festlegung der Kritikalität der Prozesse können verschiedene Kriterien herangezogen werden, die sich auch an den formulierten Schutzzielen (vgl. → Kapitel C.1.2) orientieren können. Im Leitfaden des Bundesministeriums des Innern werden beispielsweise folgende Kriterien genannt

- Die Auswirkungen des Prozessausfalls auf Leben und Gesundheit
- Der Umfang der Dienstleistung, der durch den Prozessausfall betroffen ist
- Der Zeitraum, innerhalb dessen die Auswirkungen des Prozessausfalls als kritisch anzusehen sind
- Die vertragliche, ordnungspolitische oder gesetzliche Relevanz der Ausfallfolgen
- Die mit dem Ausfall verbundenen wirtschaftlichen Schäden
- Die möglichen Auswirkungen eines Ausfalls auf die Umwelt

Um die Auswirkungen eines Prozessausfalls abzuschätzen, wird die „Zeit“, d. h. wie lange darf ein Prozess ausfallen, ohne nennenswerten Schaden anzurichten, als das entscheidende Kriterium für die Kritikalitätsbewertung herangezogen. Dabei kann die Prozesskritikalität durch Ja/Nein-Entscheidung bestimmt oder auch mehreren Kritikalitätskategorien von „unkritisch“ bis „hoch kritisch“ zugeordnet werden (siehe z. B. BSI-Standard 100-4 „Notfallmanagement“, Business-Impact-Analyse [14]).

Kritikalitätsbetrachtungen können im ersten Schritt auf der Prozessebene und im zweiten auf der Ebene der Elemente durchgeführt werden. Wird ein Prozess als kritisch eingestuft, werden nachfolgend die zugehörigen Prozesselemente ermittelt und deren Kritikalität bestimmt (vgl. → Abbildung 4). Handelt es sich um eine überschaubare Anzahl von Prozessen, die ggf. größtenteils von den gleichen Prozesselementen getragen werden, so kann auf eine Priorisierung der Prozesse auch verzichtet werden.

Für die Bestimmung der Kritikalität der Prozesselemente wird die IT-Grundschutz-Vorgehensweise herangezogen. In der Terminologie des IT-Grundschutzes wird in Analogie an den Begriff „Kritikalität“ der Begriff „Schutzbedarf“ verwendet,der durch das Ausmaß der entstandenen Schäden definiert wird. Im Rahmen der Schutzbedarfsfeststellung wird ermittelt, welchen Schutzbedarf die Prozesselemente in Bezug auf die Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität besitzen.

Die Schadensauswirkungen, die bei Verlust der Vertraulichkeit und Integrität der Daten und der Verfügbarkeit von Anwendungen/IT-Systemen eintreten können, werden im IT-Grundschutz Schadensszenarien zugeordnet, die nahezu

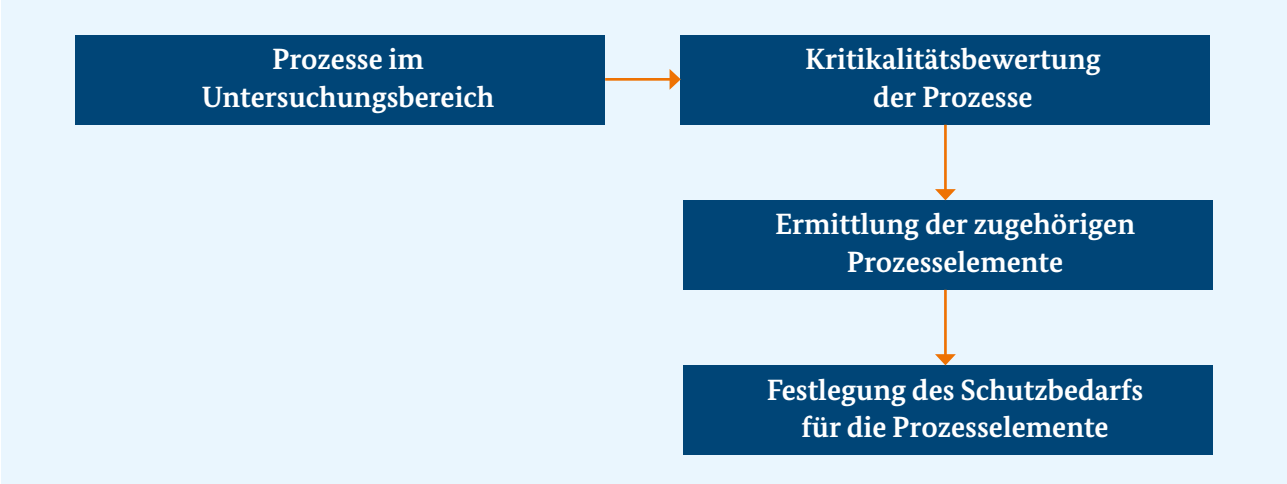


Abbildung 4: Ablauf der Kritikalitätsanalyse; Quelle BBK

deckungsgleich sind mit den im Leitfaden des Bundesministeriums des Innern genannten Kriterien zur Ermittlung der kritischen Prozesse:

- Verstoß gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung des informellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Innen- oder Außenwirkung
- Finanzielle Auswirkungen

Welche dieser Schadensszenarien (z. B. Beeinträchtigung der Aufgabenerfüllung und/oder finanzielle Schäden und/oder Vertragsverletzungen) bei Verlust der Verfügbarkeit, Vertraulichkeit und Integrität für die Einrichtung zutreffen, ist im Einzelnen zu untersuchen. Der BSI-Standard 100-2 beinhaltet einen Fragenkatalog, der es dem Anwender erleichtert, die möglichen Schäden der genannten Schadensszenarien zu ermitteln. Anzumerken ist, dass die Schadensauswirkungen nicht eindimensional zu betrachten sind. So kann der Ausfall einer Anwendung oder eines IT-Systems nicht nur die Aufgabenerfüllung beeinträchtigen, sondern gleichzeitig auch mit einem erheblichen finanziellen Investitionsaufwand zur Wiederherstellung der Funktionalität verbunden sein.

Im IT-Grundschutz werden drei Schutzkategorien definiert:

normal:	die Schadensauswirkungen sind begrenzt und überschaubar
hoch:	die Schadensauswirkungen können beträchtlich sein
sehr hoch:	die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen

Die Abgrenzungen zwischen den Kategorien muss jede Einrichtung für sich individuell festlegen. Eine mögliche Definition der Schutzbedarfskategorien ist in der nachfolgenden Tabelle beispielhaft aufgeführt.

Quelle: © engineerstory/Shutterstock.com

Tabelle 3: Beispiel für die Definition der Schutzbedarfskategorien

Schutzbedarfs-kategorie	Verfügbarkeit (max. tolerierbare Ausfallzeit)	Integrität der Daten und IT-Systeme	Vertraulichkeit der Daten
sehr hoch	max. 4 Stunden Ausfallzeit sind tolerierbar	Kompromittierung betrifft Daten, die die sicherheitsrelevanten Systeme sowie Steuerungssysteme beeinflussen	Vertraulichkeitsverluste betreffen Daten über interne Systeme und Strukturen, die dazu genutzt werden könnten, Angriffe (physisch oder virtuell) vorzubereiten Vertraulichkeitsverluste betreffen Daten, die die Persönlichkeitsrechte der Mitarbeiter beeinträchtigen oder auch sonstige negative Folgen (z. B. Vertragsverletzungen, finanzielle Schäden) für die Einrichtung haben
hoch	zwischen 4 und 24 Stunden Ausfallzeit sind tolerierbar	Kompromittierung betrifft sicherheitsrelevante Daten, die jedoch keine unmittelbaren Auswirkungen auf den Betrieb haben	Vertraulichkeitsverluste betreffen Daten, die unter Umständen negative Folgen für die Einrichtung oder das Personal haben könnten
normal	Ausfallzeiten von mehr als 24 Stunden sind tolerierbar	Kompromittierung betrifft allgemeine Daten ohne besondere Sicherheitsrelevanz	Vertraulichkeitsverluste betreffen allgemeine Daten, die keine weiteren Konsequenzen für die Einrichtung und keine negative Folgen für das Personal haben

Der Gesamtschutzbedarf ergibt sich durch den **maximalen** Schutzbedarf bezüglich der Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit.

Die Schutzbedarfsfeststellung wird, wie im Folgenden erläutert, in einer bestimmten Reihenfolge vorgenommen; Zunächst wird der Schutzbedarf für Anwendungen bestimmt und anschließend der Schutzbedarf für IT-Systeme, Räume sowie die Kommunikationssysteme abgeleitet.

Schritt 1: Schutzbedarfsfeststellung für Anwendungen

In einem ersten Schritt wird der Schutzbedarf für die Anwendungen ermittelt. Dazu gehören auch schützenswerte Dokumente und Datenträger, die im Rahmen der Bestandsaufnahme der Prozesselemente erfasst worden sind.

Schritt 2: Schutzbedarfsfeststellung für IT-Systeme

Aus dem Schutzbedarf der Anwendungen wird als nächstes der Schutzbedarf für die betroffenen IT-Systeme abgeleitet. Dabei werden die für das IT-System relevanten Anwendungen in ihrer Gesamtheit betrachtet und der Schutzbedarf des IT-Systems durch den Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen beim Ausfall dieser Anwendungen bestimmt (Maximumprinzip).

Dies bedeutet, dass der Schutzbedarf einer Anwendung nicht zwangsläufig mit dem des damit gekoppelten IT-Systems korrespondieren muss. Laufen nur unwesentliche Teile einer hochkritischen Anwendung auf einem bestimmten IT-System, so ist dessen Schutzbedarf auch niedriger einzustufen. Umgekehrt kann ein Server, auf dem mehrere weniger kritische Anwendungen laufen, durch die Kumulation der entstandenen Schäden beim Ausfall des Servers im Schutzbedarf höher eingestuft werden.

Der Gesamt-Schutzbedarf des IT-Systems wird nach dem Maximumprinzip durch den maximalen Schutzbedarf bezüglich der Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit bestimmt.

Schritt 3: Schutzbedarfsfeststellung für Räume

Der Schutzbedarf der Räume ist aus den in den jeweiligen Räumen installierten IT-Systemen oder den Dokumenten und Datenträgern, die in den Räumen aufbewahrt werden, ebenfalls nach dem Maximumprinzip abzuleiten.

Schritt 4: Schutzbedarfsfeststellung für Kommunikationsverbindungen

Die Schutzbedarfsfeststellung für sämtliche Kommunikationsverbindungen erfolgt nach folgendem Prinzip:

- Alle Kommunikationsverbindungen, die nach außen und über unkontrollierte Bereiche führen (Festverbindungen, drahtlose Verbindungen etc.) und die in verschiedener Weise manipuliert werden können, werden als kritisch eingestuft.
- Kritisch sind auch solche Verbindungen, die von IT-Systemen mit hohem oder sehr hohem Schutzbedarf ausgehen. Dabei werden zum einen diejenigen Verbindungen identifiziert, über die hochschutzbedürftige Informationen übertragen werden und zum anderen auch solche, über die derartige Informationen (z. B. sehr vertrauliche Informationen) nicht übertragen werden sollten.

Zwar bezieht sich die Schutzbedarfsermittlung in der IT-Grundschutz-Vorgehensweise auf die Informationssicherheit. Diese lässt sich aber hinsichtlich der Verfügbarkeitsanforderungen gleichermaßen auf andere technischen Elemente (z. B. Notstromversorgung, Kühlung etc.) außerhalb der IT-Infrastruktur übertragen.

Grundsätzlich gilt es, alle Ergebnisse der Schutzbedarfsfeststellung mit den jeweiligen Begründungen genau zu dokumentieren, um auch für spätere Überprüfungen die getroffenen Entscheidungen nachvollziehbar zu machen.

3. Gefahrenanalyse und Szenarienentwicklung

3.1 Gefahrenanalyse

In diesem Schritt der Risikoanalyse werden die relevanten Gefahren, die die Einrichtung in ihrer Funktionsfähigkeit beeinträchtigen oder gar zum Ausfall der gesamten Einrichtung führen können, ausgewählt. Nach dem All-Gefahren-Ansatz werden sowohl Naturgefahren, Gefahren, die aus menschlichem oder technischem Versagen resultieren, als auch vorsätzliche Handlungen, wie z. B. Cyberkriminalität oder Terrorismus, betrachtet.

Im Anhang 4 sind denkbare Gefahren, die eine Tunnelleitzentrale betreffen können, aufgeführt. Die Gefahrenliste enthält ebenso IT-spezifische Gefahren, die im BSI-Gefährdungskatalog „Elementare Gefährdungen“ [15] aufgeführt sind. In diesem Katalog sind die in den Gefährdungskatalogen G1 bis G5 des IT-Grundschutzes aufgeführten und teilweise sehr spezifischen Einzelgefahren auf 46 generische Gefährdungen zusammengefasst.

Die Gefahrenliste im Anhang erhebt keinen Anspruch auf Vollständigkeit und ist je nach Bedarf zu ergänzen bzw. zu modifizieren. Welche Gefahren am Standort bzw. für die Einrichtung relevant sein könnten, lässt sich u. a. mit Hilfe folgender Fragestellungen bestimmen:

- Wurde die Einrichtung in der Vergangenheit durch das Ereignis betroffen und könnte es sich wiederholen?
- Gibt es Ereignisbeispiele, die für die eigene Einrichtung herangezogen werden können?
- Gibt es Veränderungen im Umfeld der Einrichtung, die eine Gefahr darstellen können? (z. B. Ansiedlung von Störfallbetrieben)
- Welche natürlichen oder von Menschen gemachten Gefahren sind aufgrund der räumlichen Lage und Veränderungen der Rahmenbedingungen (z. B. klimatische Veränderungen, Entwicklungen in der IT-Technik, Entwicklung der sicherheitspolitischen Lage) möglich?

Die Basis für die Überprüfung des Sicherheitsniveaus der Einrichtung im Rahmen der IT-Grundschutzanalyse (vgl. → Kapitel C.4) bilden die Gefährdungskataloge. Dennoch wird darauf hingewiesen, dass es zusätzliche relevante Gefährdungen im Bereich der Informationssicherheit für einzelne betrachtete Elemente geben kann, die im IT-Grundschutz nicht berücksichtigt sind. Es handelt sich dabei um Gefährdungen, die

- durch eine besondere Technologie, ein spezielles Produkt oder einen besonderen Anwendungsfall bedingt sind oder
- bei den üblichen Szenarien nur unter sehr speziellen Voraussetzungen zum Schaden führen können oder
- sehr gute Fachkenntnisse, Gelegenheiten und Mittel eines Angreifers voraussetzen [16].

Die Ermittlung zusätzlicher IT-Gefahren soll für Prozesselemente mit hohem und sehr hohem Schutzbedarf erfolgen, da bei normalem Schutzbedarf die in den IT-Grundschutzkatalogen betrachteten Gefährdungen und die empfohlenen Sicherheitsmaßnahmen für diese Schutzkategorie in der Regel ausreichend sind. Ebenso kann es vorkommen, dass bestimmte Prozesselemente der Einrichtung nicht in den Bausteinen des IT-Grundschutzes abgebildet sind und für diese die relevanten Gefährdungen ermittelt werden müssen [16].

Die im Rahmen der Gefahrenanalyse zu erstellende Gefahrenliste sollte generell nicht nur Ereignisse aufnehmen, die mit hoher Wahrscheinlichkeit eintreten können und bei denen die zu erwartenden Schäden relativ gering sind (z. B. kurzer Stromausfall durch Kabelbeschädigung bei Bauarbeiten). Vielmehr sind in der Gefahrenanalyse auch jene Ereignisse zu betrachten, die zwar seltener auftreten, jedoch das Potenzial haben, aufgrund ihrer Intensität und/oder Dauer einen

erheblichen Schaden bzw. auch einen längerfristigen Ausfall der Einrichtung herbeizuführen (vgl. folgendes Kapitel).

Die Gefahrenanalyse sollte sinnvollerweise unter Beteiligung von allen sachverständigen Mitarbeitern, also IT-Sicherheitsbeauftragten, Administratoren, Anwendern oder auch externen Fachleuten erfolgen.

3.2 Szenarienentwicklung

Nach der Zusammenstellung der für den Standort / die Einrichtung relevanten Gefahren sind realistisch anzunehmende Szenarien zu entwickeln, die die Gefährdung näher erläutern. Ein Szenario beschreibt ein Ereignis im Detail bzw. zeigt auf, welche Entwicklung ein bestimmtes Ereignis nehmen könnte und mit welchen Auswirkungen zu rechnen ist. Somit sind Szenarien auch ein Instrument, um sich auf Ereignisse in Form von entsprechenden Notfallplänen vorzubereiten. Die Szenariobeschreibung sollte u. a. folgende Informationen umfassen [12][13]:

- Exposition: Welche Bereiche der Einrichtung bzw. Prozesse oder Prozesselemente können betroffen sein?
- Angenommene Intensität
- Zeitpunkt (Tageszeit und ggf. Jahreszeit)
- Dauer des Ereignisses
- Räumliche Ausdehnung
- Vorwarnzeit

Bei der Entwicklung eines Szenarios sollten, wenn möglich, Referenzereignisse herangezogen werden, um eine Vorstellung vom möglichen Ereignisablauf sowie den zu erwartenden Auswirkungen zu gewinnen. Der Schwerpunkt in der Szenariodarstellung liegt in der Beschreibung der Intensität bzw. den Auswirkungen für die Einrichtung, wohingegen die Ursache zunächst sekundär sein kann und erst für die spätere Ableitung von Schutzmaßnahmen im Rahmen der Notfallplanung Bedeutung erlangt. D. h. entscheidend für die Risikobetrachtung und die Maßnahmenauswahl ist, dass beispielsweise der Strom für mehrere Tage ausfällt und nicht das auslösende Ereignis (Schneesturm, Hochwasser oder Bombenanschlag auf Umspannwerke) [17].

Es sollten Szenarien erarbeitet werden, die in der Konsequenz eine erhebliche Beeinträchtigung des Standorts bzw. der Funktionsfähigkeit der Einrichtung beinhalten. Um die Bandbreite möglicher Entwicklungen im Rahmen eines Szenarios aufzuzeigen, ist es sinnvoll, Eskalationsstufen zu bilden, d. h. das Szenario hinsichtlich der Intensität und den zu erwartenden Auswirkungen zu variieren (z. B. Stromausfall über mehrere Stunden oder auch mehrere Tage).

Relevante Ereignisse, die zum Ausfall einer TLZ führen oder den Betriebsablauf erheblich beeinträchtigen können, sind z. B.:

- Stromausfall, z. B. durch extreme Wetterereignisse
- (Teil-) Ausfall des Standortes durch Naturereignisse oder Brand
- Zusammenbruch der Informationstechnik oder der Kommunikationsinfrastruktur, z. B. durch Hackerangriffe
- Ausfall einer kritischen Anzahl an Mitarbeitern
- Räumung der TLZ, z. B. aufgrund einer Bombendrohung
- Terroristischer Anschlag

In den folgenden Tabellen sind einige Beispiele für Szenarien aufgeführt.

Tabelle 4: Beispiele für Szenarien	
Flächendeckender langanhaltender Ausfall der Stromversorgung	
Ursache	Wintersturm und Niederschlag von besonders schwerem Schnee: Die Stromversorgung wird im Bereich der Hauptleitungen an mehreren wichtigen Stellen gleichzeitig unterbrochen.
Intensität	In Deutschland ist ein Ballungsraum mit mehreren Großstädten von dem Stromausfall betroffen. An verschiedenen Orten sind jeweils tausende Haushalte ohne Strom und Heizung, sodass THW, Feuerwehr und die Hilfsorganisationen ihre Ressourcen auf mehrere Einsatzgebiete verteilen müssen. Die deutschlandweit verfügbaren Notstromaggregate reichen nicht aus. Die Straßenverhältnisse sind schlecht, so dass die Versorgung nicht gesichert ist.
Räumliche Ausdehnung	Überregional
Dauer	Die Arbeiten zur Wiederherstellung der regulären Stromversorgung nehmen mehr als eine Woche in Anspruch
Referenzbeispiel	Stromausfall im Münsterland im November 2005
Ausfall von Informations- und Kommunikationstechnik	
Ursache	Über das Internet wird ein Computervirus verbreitet, der auch die Systeme der TLZ angreift.
Intensität	Sämtliche an das System angeschlossene Rechner fallen aus, es kommt zum Verlust großer Datenmengen.
Räumliche Ausdehnung	Weltweit
Dauer	Mehrere Tage
Referenzbeispiel	Der Computerwurm „Sasser“ infizierte Anfang 2004 etwa zwei Millionen Rechner und beeinträchtigte weltweit viele Unternehmen erheblich
Gezielter Cyber-Angriff auf die TLZ	
Ursache	Ein Angreifer (Innen- oder Außentäter) infiltriert Schadprogramme in die IT-Systeme der TLZ, die dazu verwendet werden, Steuerungssysteme anzugreifen und eine Fehlsteuerung der Prozesse herbeizuführen.
Intensität	Die Verfügbarkeit und die Integrität der Steuerungssysteme sind gestört. Kritische Prozesse können nicht mehr erbracht werden oder sind gestört.
Räumliche Ausdehnung	
Dauer	Mehrere Tage
Referenzbeispiel	STUXNET – gezielter Angriff auf iranische Nuklearanlagen 2010

Quelle: © Solarseven/Shutterstock.com

4. IT-Grundschutzanalyse

Nachdem die Informationen zur Kritikalität bzw. dem Schutzbedarf der betrachteten Prozesselemente vorliegen, gilt es zunächst zu prüfen, ob das realisierte Schutzniveau ausreichend ist oder insbesondere für Elemente mit hohem und sehr hohem Schutzbedarf in Anbetracht neuer Gefahren, die beispielsweise in den Gefährdungskatalogen nicht abgebildet sind sowie von extremen Ereignissen zusätzliche Maßnahmen erforderlich sind. Dann ist unter Umständen eine Risikoanalyse unter Berücksichtigung der Parameter Eintrittswahrscheinlichkeit, Verwundbarkeit der Elemente sowie der Schadensauswirkungen durchzuführen (vgl. → Kapitel C.5).

Da die Vorgehensweise einer Analyse des Schutzniveaus einer Einrichtung nach IT-Grundschutz im BSI-Standard 100-2 ausführlich beschrieben ist, wird an dieser Stelle lediglich das Prinzip und die wesentlichen Schritte vorgestellt.

Grundsätzlich wird davon ausgegangen, dass für Elemente mit normalem Schutzbedarf die Sicherheitsmaßnahmen des IT-Grundschutzes ausreichend sind und nur in den Schutzbedarfskategorien „hoch“ und „sehr hoch“ weitergehende individuelle Maßnahmen zu ergreifen sind, die auf einer ergänzenden Sicherheits- und Risikoanalyse beruhen sollen.

Der IT-Grundschutz geht von einer pauschalisierten Gefährdungslage aus und bietet einen Maßnahmenkatalog für die Bereiche Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation sowie die Notfallvorsorge an. Aufgebaut ist der Grundschutz nach dem Baukastenprinzip, das folgende Aspekte umfasst (vgl. auch → Abbildung 1):

Übergeordnete Aspekte und Infrastruktur, z. B.

- Sicherheitsmanagement
- Organisation
- Personal
- Notfallmanagement
- Datensicherungskonzept
- Datenschutz
- Gebäude
- Verkabelung
- Räume, Schutzschränke
- Häuslicher Arbeitsplatz

- IT-spezifische Bausteine, z. B.
  - Vernetzte und nicht vernetzte Systeme
  - Datenübertragungseinrichtungen
  - Telekommunikation
  - Anwendungen

Die Bearbeitung der IT-Grundschutzkataloge gliedert sich in mehrere Schritte:

Schritt 1: Abbildung des Informationsverbunds durch die vorhandenen Bausteine

Im ersten Schritt besteht die wesentliche Aufgabe darin, alle betrachteten Elemente, d. h. den gesamten Informationsverbund der Einrichtung durch die Bausteine möglichst genau abzubilden. Falls bereits ein Grundschutz-Konzept existiert, kann in diesem Schritt auch geprüft werden, ob neue Bausteine (diese werden vom BSI kontinuierlich aktualisiert) relevant sein können.

Schritt 2: Anpassung der Maßnahmen

Im zweiten Schritt sind die empfohlenen Maßnahmen hinsichtlich ihrer Anwendbarkeit zu prüfen. Es kann der Fall sein, dass manche Maßnahmen unter den konkreten Rahmenbedingungen entbehrlich sind oder manche Gefährdungen bereits durch anderweitige Maßnahmen abgedeckt sind. Grundsätzlich sollten alle im Baustein empfohlenen Maßnahmen für den Grundschutz umgesetzt werden. Etwaige Änderungen sind zu dokumentieren.

Schritt 3: Soll-Ist-Abgleich zwischen den vorhandenen und empfohlenen Maßnahmen (Basis-Sicherheitscheck)

In diesem Schritt wird der Umsetzungsstatus der empfohlenen Maßnahmen geprüft. Sinnvoll ist es, bereits beim Soll-Ist-Abgleich den Bedarf für eventuelle zusätzliche Sicherheitsmaßnahmen für besonders schützenswerte Elemente herauszuarbeiten und zu dokumentieren.

Im Anschluss an die Grundschutzanalyse ist eine ergänzende Sicherheitsanalyse durchzuführen, die in Form eines Management-Reports begründen bzw. dokumentieren soll, ob für bestimmte Prozesselemente weitergehende Risikobetrachtungen erforderlich sind. Demnach sind es Elemente, die

- einen hohen oder sehr hohen Schutzbedarf haben,
- mit den vorhandenen Bausteinen der IT-Grundschutz-Kataloge nicht hinreichend abgebildet werden können,
- in Umgebungen oder mit Anwendungen betrieben werden, die im IT-Grundschutz nicht vorgesehen sind.

5. Detaillierte Risikoanalyse

Bei der Durchführung einer detaillierten Risikoanalyse steht die Frage im Vordergrund, ob die schützenswerten Elemente durch die Standardsicherheitsmaßnahmen, so wie der IT-Grundschutz sie empfiehlt, in Anbetracht der (Extrem-) Szenarien und ggf. neuer Gefahren ausreichend geschützt sind oder nicht. Die potenziellen Risiken sollen unter Berücksichtigung der Eintrittswahrscheinlichkeiten, der Verwundbarkeiten sowie des Schadensausmaßes bewertet werden, um darauf aufbauend Maßnahmen gezielt einzusetzen. Das Vorgehen für eine detaillierte Risikoanalyse wird im Folgenden beschrieben.

5.1 Abschätzung der Eintrittswahrscheinlichkeit/Plausibilität

Die Eintrittswahrscheinlichkeit eines Szenarios kann quantitativ oder qualitativ bestimmt werden. Allerdings lassen sich statistisch exakt belegbare Eintrittswahrscheinlichkeiten nur für wenige Szenarien (z. B. Hochwasser) ermitteln. Sofern für das betrachtete Szenario keine statistischen Erkenntnisse vorliegen, gilt es eine Abschätzung vorzunehmen, die sich auf begründete Annahmen, auf Erfahrungswerte oder Expertenmeinungen stützt [13]. Eine Hilfestellung kann die Analyse der jeweiligen Rahmenbedingungen sein, z. B. Häufigkeit der Ereignisse aufgrund klimatischer Veränderungen, Referenzereignisse oder die Betroffenheit der eigenen Einrichtung durch ein Szenario in der Vergangenheit.

Bei der Bestimmung der Eintrittswahrscheinlichkeit ist zu berücksichtigen, dass die Einschätzung der Eintrittswahrscheinlichkeit die aktuelle Lage widerspiegelt. Ändern sich die Rahmenbedingungen, so ist auch die Eintrittswahrscheinlichkeit neu zu bewerten.

Im folgenden Beispiel (vgl. → Tabelle 5) wird die Klassifizierung der Eintrittswahrscheinlichkeit in vier Stufen vorgenommen. Es ist wichtig, die Herleitung der Klassifizierung zu beschreiben und die Annahmen sowie Begründungen für die Eintrittswahrscheinlichkeit eines Szenarios zu dokumentieren. Damit können die Ergebnisse bei einer Aktualisierung/Überprüfung der Risikoanalyse nachvollzogen und entsprechend angepasst werden [13].

Tabelle 5: Beispiel für die Klassifizierung der Eintrittswahrscheinlichkeit

Kategorie		Beschreibung
IV	sehr hoch	Das Szenario kann häufig eintreten (z. B. mehrmals im Jahr)
III	hoch	Das Szenario kann relativ häufig eintreten (unter Umständen jährlich)
II	mittel	Das Szenario kann gelegentlich und in größeren Zeitabständen eintreten
I	gering	Wenn das Szenario eintreten sollte, dann selten oder äußerst selten (z. B. bezogen auf die Lebensdauer der TLZ nur einmal)

Im Zusammenhang mit Terrorismus oder anderen kriminellen Handlungen sind Wahrscheinlichkeitsbetrachtungen mit Zuordnung von Häufigkeiten eher schwierig. Zudem gibt es für solche Ereignisse (mit Ausnahme der Regionen mit kriegerischen Auseinandersetzungen) teilweise nur wenige Erfahrungen. So hat es z. B. in Deutschland noch keine erfolgreich durchgeführten, spektakulären terroristischen Anschläge auf Infrastruktureinrichtungen gegeben. Auch wenn eigentlich derartige Ereignisse unvorhersehbar sind und sich somit einer Wahrscheinlichkeitsbetrachtung entziehen, stellen sie eine latente Gefahr mit unabsehbaren Folgen dar. Um dennoch eine Risikoabschätzung vornehmen zu können, ist es daher sinnvoll, nicht die Eintrittswahrscheinlichkeit zu bestimmen, sondern sich auf Plausibilitätsüberlegungen zu stützen. Folgende Kriterien können u. a. hierfür herangezogen werden:

- Aktuelle sicherheitspolitische Lage[6]
- Bedeutung des betroffenen Ortes bzw. der Einrichtung (Motivation der Angreifer)
- Aufwand zur Durchführung des Anschlags:
    - Erforderliche Fähigkeiten und erforderliches Knowhow
    - Verfügbarkeit und Handhabbarkeit des Anschlagsmaterials
    - Lage der Einrichtung und Zugänglichkeit

Derartige Plausibilitätsüberlegungen beruhen auf der aktuellen Sicherheitslage. Ändert sich diese, so muss eine Neubewertung der Plausibilität vorgenommen werden. Analog der Skala für die Eintrittswahrscheinlichkeit wird die „Plausibilität“ von vorsätzlichen Handlungen ebenfalls in vier Stufen angegeben, wie die folgende Tabelle zeigt.

Im Bereich der Informationstechnik stellen Cyber-Angriffe eine ständige Gefahr dar, gegen die IT-Systeme entsprechend zu schützen sind. Informationen über besonders relevante und aktuelle Cyber-Gefährdungen bietet das Bundesamt für Sicherheit in der Informationstechnik [18].

Der Begriff „Eintrittswahrscheinlichkeit“ bezogen auf derartige Cyber-Bedrohungen ist allerdings ein wenig irreführend, da solche Angriffe zum heutigen Alltag gehören.

Im ursprünglichen Sinne bedeutet „Eintrittswahrscheinlichkeit“, ob ein Ereignis überhaupt bzw. wie häufig es eintreten kann. Ob dieses Ereignis zu einem Schaden führen kann, wird in einem weiteren Schritt der Risikoidentifikation, der Verwundbarkeitsanalyse, ermittelt. Hingegen bezieht sich in der Informationssicherheit die Wahrscheinlichkeitsbetrachtung darauf, ob ein Angriff unter Ausnutzung vorhandener Schwachstellen im IT-System erfolgreich durchgeführt werden und folglich zum Schaden führen kann. D. h. die Verwundbarkeit der Systeme wird in die Betrachtung der Wahrscheinlichkeit eines Ereignisses einbezogen.

[6] Für die Einschätzung der Bedrohungen durch politisch motivierte Anschläge können Informationen des Bundeskriminalamtes oder der jeweiligen Landeskriminalämter herangezogen werden.

Ob ein Grundschutz gegenüber Cyber-Gefahren vorhanden und ausreichend ist, wird im Rahmen des Soll-Ist-Maßnahmenabgleichs anhand der IT-Grundschutzkataloge geprüft (vgl. → Kapitel C.4).

Abgesehen von den alltäglichen, flächendeckenden Cyber-Angriffen stellt sich die Frage, ob speziell eine Tunnelleitzentrale ein ausgesuchtes Objekt für einen gezielten Cyber-Angriff sein kann[7]. Ein Motiv könnte sein, durch Manipulation der Software oder der IT-Systeme in der TLZ die Betriebstechnik in Tunneln zu stören oder gar außer Funktion zu setzen, so dass der Betrieb der überwachten Tunnel eingestellt werden muss.

Tabelle 6: Beispiel für die Klassifizierung der Plausibilität

Kategorie		Beschreibung
IV	relativ plausibel	• Die Einrichtung könnte ein Anschlagsziel darstellen • Die Beschaffung bzw. Herstellung des Anschlagsmaterials ist einfach zu bewerkstelligen • Die Einrichtung ist leicht zugänglich und unzureichend überwacht
III	eher unplausibel	• Die Einrichtung könnte ein Anschlagsziel darstellen • Die Beschaffung bzw. Herstellung des Anschlagsmaterials ist einfach zu bewerkstelligen • Die Einrichtung und das umliegende Gelände ist ausreichend gesichert und wird ständig überwacht
II	unplausibel	• Die Einrichtung könnte ein Anschlagsziel darstellen, hat aber geringere Bedeutung • Die Beschaffung des Anschlagsmaterials ist schwierig und die Durchführung des Anschlags mit einem hohen Aufwand verbunden
I	sehr unplausibel	• Als Anschlagsziel ist die Einrichtung eher unbedeutend • In Anbetracht der aktuellen sicherheitspolitischen Situation sind Anschläge außerdem eher auszuschließen

Dies würde beträchtliche verkehrliche Auswirkungen nach sich ziehen. Die Plausibilität eines solchen Szenarios sollte geprüft werden, wobei auch bei Cyber-Angriffen folgende Faktoren heranzuziehen sind:

- Mögliche Motive der Angreifer, sicherheitspolitische Lage
- Zeit- und Ressourcenaufwand, um den Angriff vorzubereiten
- Mögliche Schwachstellen im System: *Ist die Schwachstelle leicht zu identifizieren? Ist Spezialwissen erforderlich oder reichen leicht verfügbare Werkzeuge hierfür aus?*
- Erforderliche Fähigkeiten und Knowhow: *Sind tiefgehende Kenntnisse für den Angriff erforderlich oder reichen wenige technische Kenntnisse aus?*
- Angriffsentdeckung: *Wie schnell kann der Angriff entdeckt und somit der potenzielle Schaden vermieden bzw. minimiert werden (kurzfristig, mittel- oder langfristig?)*

[7] Mit dieser speziellen Thematik befasst sich das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Kooperationsprojekt „CyberSafe – Schutz von Verkehrs-, Tunnel und ÖPNVLeitzentralen vor CyberAngriffen“ (Laufzeit 2015 bis 2018).

5.2 Abschätzung der Verwundbarkeit

In der Verwundbarkeitsanalyse wird ermittelt, wie anfällig die Prozesselemente gegenüber einem bestimmten Szenario sind. Die Auswirkungen eines Szenarios auf die Prozessabläufe sind umso stärker, je höher die Verwundbarkeit der Prozesselemente ist. Betrachtet werden sollen diejenigen Elemente, die für die Aufrechterhaltung der Abläufe von besonderer Bedeutung sind, folglich einen hohen oder einen sehr hohen Schutzbedarf haben. Bereits umgesetzte Schutzmaßnahmen werden bei der Abschätzung der Vulnerabilität berücksichtigt. Im Mittelpunkt des Verfahrens steht die Überprüfung der Vulnerabilität der funktionsrelevanten Elemente.

Die Verwundbarkeit der Prozesselemente wird durch folgende Faktoren bestimmt:

- Exposition: *Ist das betrachtete Element dem Szenario ausgesetzt?*
- Funktionsanfälligkeit: *Würde das Element beim Eintritt des betrachteten Szenario weiter funktionieren?*
- Ersetzbarkeit: *Inwiefern kann die Funktion/ Leistung des Elements technisch oder organisatorisch ersetzt werden?*

Die Faktoren *Funktionsanfälligkeit* und *Ersetzbarkeit* beinhalten eine Reihe weiterer Kriterien, die in der → Tabelle 7 aufgeführt sind. Welche dieser Kriterien zur Abschätzung der Verwundbarkeit herangezogen werden, sollte einrichtungsspezifisch festgelegt werden. Zur Vereinfachung des Verfahrens werden die zugrunde gelegten Kriterien jedoch nicht einzeln bewertet. Demnach ist es zunächst nicht entscheidend, welcher Faktor zum Ausfall des Elements und somit zur Beeinträchtigung bzw. zum Ausfall des Prozesses geführt hat. Wichtig ist vielmehr, ob das Element gegenüber der Gefahr funktionsanfällig ist oder nicht bzw. ob im Fall des Funktionsausfalls die Leistung durch andere Elemente ersetzt werden kann [19].

Quelle: © Solarseven/Shutterstock.com

Tabelle 7: Verwundbarkeitsfaktoren und -Indikatoren

Verwundbarkeitsfaktor: Funktionsanfälligkeit	
Indikatoren	**Erläuterung**
Realisiertes Schutzniveau	Vorbeugende Maßnahmen zum Schutz der Elemente *(z. B. umgesetzte Maßnahmen im Rahmen des IT-Grundschutzes)*
Robustheit	Physische Robustheit insbesondere von Anlagen, Geräten, Gebäuden gegenüber den Einwirkungen aus dem Ereignis *z. B. verwendetes Material*
Pufferkapazität	Der Prozess oder seine Elemente können die Einwirkung eines Ereignisses in einem bestimmten Maß und über einen bestimmten Zeitraum verkraften, ohne beeinträchtigt zu werden *Während der Indikator „Robustheit" sich darauf bezieht, ob ein Element dem Ereignis standhält, beinhaltet der Indikator „Pufferkapazität" eine zeitliche Komponente und bezieht sich darauf, wie lange das Element dem Ereignis standhalten kann* *z. B. USV oder Netzersatzstromanlagen stellen einen Puffer dar, die die Funktion von Anlagen oder Geräten über einen bestimmten Zeitraum gewährleisten*
Abhängigkeit vom Fachpersonal	Für die meisten Betriebsabläufe ist Fachpersonal erforderlich. Zu berücksichtigen sind insbesondere die externen Diensleister, auf die die Einrichtung angewiesen ist
Abhängigkeit von internen Infrastrukturen	Ein Element ist für die Erbringung seiner Leistung auf eine interne Infrastruktur angewiesen *z. B. Notstromversorgung*
Abhängigkeit von externen Infrastrukturen	Ein Element ist für die Erbringung seiner Leistung auf eine externe Infrastruktur angewiesen *z. B. Abhängigkeit von der externen Stromversorgung*
Abhängigkeit von spezifischen Umweltbedingungen	Ist ein Element auf spezifische Umweltbedingungen angewiesen, dann ist es durch potenzielle Abweichungen der Bedingungen verwundbar *z. B. Beeinträchtigung der Funktionsfähigkeit der Computersysteme beim Ausfall der Klimaanlage*

Verwundbarkeitsfaktor: Ersetzbarkeit	
Redundanz, Ersatz	Parallele Strukturen, Systeme, die dieselbe Leistung wie die ausgefallenen Elemente erbringen *Die Ersetzbarkeit bezieht sich nicht ausschließlich auf die technische Redundanz; Betrachtet werden auch die organisatorischen Aspekte (z. B. geschultes Personal), die die Umsetzung der technischen Möglichkeiten zum Ersatz der ausgefallenen Leistung gewährleisten* *Überprüft wird die kurzfristige Ersetzbarkeit, langfristige Maßnahmen, die ein Element ersetzen, werden bei der Verwundbarkeitsabschätzung nicht betrachtet*
Substituierbarkeit	Die Leistung kann durch eine andere Infrastruktur ersetzt werden *z. B. Steuerung und Überwachung des Tunnels vor Ort beim Ausfall der TLZ; Übernahme der Überwachung durch eine andere TLZ*
Wiederherstellungsaufwand	Finanzieller, zeitlicher sowie personeller Aufwand für die Wiederherstellung des Elements (Phase nach dem Ereignis)
Transparenz	Die Zusammensetzung und die Funktionsweise des Elements sind leicht nachvollziehbar, was eine schnelle Reparatur ermöglicht

Quellen: [20][12]

Je nachdem, welche Prozesselemente betrachtet werden, können unterschiedliche Verwundbarkeitsindikatoren herangezogen werden. Bei IT-spezifischen Gefährdungen wird die Verwundbarkeit über Schwachstellen bei Hard- und Software, Netzwerk aber auch hinsichtlich Infrastruktur, Organisation und Personal definiert. Eine Liste möglicher Schwachstellen ist in der ISO/IEC 27005 [21] enthalten (vgl. → Tabelle 8). Da ständig neue Cyber-Bedrohungen auftreten, gilt es, die IT-Systemarchitektur laufend auf mögliche (neue) Schwachstellen zu prüfen.

Die Schwachstellen können zur Beschreibung der Verwundbarkeitsindikatoren in Bezug auf Funktionsanfälligkeit und Ersetzbarkeit (technisch und organisatorisch) der Elemente herangezogen und in die Systematik der Verwundbarkeitsabschätzung, die nachfolgend beschrieben wird, integriert werden.

Tabelle 8: Beispiele für Schwachstellen
Beispiel Schwachstellen Hardware
Unzureichende Instandhaltung / fehlerhafte Installation von Speichermedien
Empfindlichkeit gegenüber Feuchtigkeit, Staub oder Verunreinigung
Mangelnde Kontrolle über Konfigurationsänderungen
Mangelnde Klimatisierung
Beispiel Schwachstellen Software
Mangelhaftes Patch-Management
Mangelhafter Zugriffsschutz
Mangelhaftes Software Konfigurationsmanagement
Beispiel Schwachstellen Netzwerk
Mangelnde Mechanismen für Identifikation und Authentisierung
Mangelhaftes Netzwerkkonfigurationsmanagement
Fehlende Nachweismöglichkeit gesendeter und empfangener Nachrichten
Ungeschützte Kommunikationsverbindungen
Ungeschützter sensibler Datenverkehr
Mangelhafte Verkabelung
Single point of failure
Unsichere Netzwerkarchitektur
Übertragung von Passwörtern in Klartext
Unsachgemäßes Netzwerkmanagement (Routing Widerstandsfähigkeit gegen Störungen)
Ungeschützte Verbindungen in öffentliche Netze (insb. ungeschützte WLAN-Zugänge)
Beispiel Schwachstellen Personal
Mangelnde Sorgfalt bei der Personalauswahl; Anzahl/Verfügbarkeit des Personals
Unzureichende Anwenderschulung / Fehlerhafter Gebrauch von Hard- und Software
Unzureichendes Konzept für den Umgang mit Externen
Beispiel Schwachstellen Infrastruktur
Mangelnder Zutrittsschutz
Aufstellung in Wassersenke
Instabiles Stromversorgungsnetz (Spannungsschwankungen, Frequenzschwankungen)
Mangelnde Gebäudesicherheit
Ungeschützte Hardware
Beispiel Schwachstellen Organisation
Mangelndes Identitäts- und Berechtigungsmanagement (Identity and Access Management, IAM)
Fehlende regelmäßige Überprüfung/Audits (z. B. von Zugriffsrechten)
Mangelnde Berücksichtigung von Informationssicherheit in Verträgen mit Dienstleistern und Kunden
Mangelndes Logging und Monitoring
Mangelnde Instandhaltung
Mangelndes Dienstleister Management

Beispiel Schwachstellen Organisation
Unzureichende Notfallplanung
Unzureichendes Management System für Informationssicherheit (ISMS)
Mangelndes Hardware Lifecycle Management (von der Anschaffung bis zur Entsorgung)
Mangelndes Application Lifecycle Management (z. B. Tests, Dokumentation, Schulung)
Mangelndes Endgerätemanagement
Mangelndes Berechtigungsmanagement
Mangelndes Logging und Monitoring
Unzureichendes Security und Risiko Management
Fehlende Richtlinien für den Umgang mit Informations- und Kommunikationssystemen
Unzureichendes IT-Service Management

Quellen: [21]

Für die Abschätzung der Verwundbarkeit wird im Folgenden auf die Methode nach *Krings* [19] zurückgegriffen, die darauf beruht, dass die erforderlichen Informationen in einer bestimmten Reihenfolge eingeholt und zusammengeführt werden. Die vorgegebene Reihenfolge der Abfragen folgt einer Logik, die es ermöglicht, mit jedem Schritt den Gesamtaufwand der Verwundbarkeitsabschätzung zu minimieren.

In der → Abbildung 5 ist die Systematik zur Abschätzung der Verwundbarkeit dargestellt.

Die Einstufung in die Verwundbarkeitsklassen gemäß dem in der → Abbildung 5 dargestellten Ablaufschema wird in der → Tabelle 9 erläutert.

Quelle: © Dmitry Demidovich/Shutterstock.com

Erläuterung der Vorgehensweise:
Schritt 1:

- Festlegung, welche Elemente im Weiteren zu betrachten sind. Eine solche Liste der funktionsrelevanten Elemente ergibt sich aus dem vorangegangenen Schritt der Schutzbedarfsfeststellung.

Schritt 2:

- Überprüfung, welche Prozesselemente/Komponenten durch die betrachtete Gefahr betroffen sein könnte (Exposition)
- Nicht exponierte Prozesselemente werden der Verwundbarkeitsklasse I (nicht oder sehr gering verwundbar) zugeordnet und vom weiteren Verfahren wegen fehlender Exposition ausgeschlossen.

Schritt 3:

- Bestimmung der Funktionsanfälligkeit für die exponierten Prozesselemente.
- Prozesselemente, die im Fall des Szenarios nicht ausfallen würden, werden in die Verwundbarkeitsklasse II (gering verwundbar) eingestuft.

Schritt 4:

- Ermittlung, ob das Element bei einem Funktionsausfall durch andere technische Komponenten ersetzt werden kann. Ist dies nicht der Fall, so wird das Element der höchsten Verwundbarkeitsklasse V zugeordnet.
- Ist es jedoch vollständig oder auch nur teilweise technisch ersetzbar, so werden in einem weiteren Schritt die organisatorischen Rahmenbedingungen (Notfallpläne, Fachpersonal) betrachtet, die für die Umsetzung der Maßnahmen erforderlich wären.

Schritt 5:

- Prüfung, ob für die Gewährleistung der technischen Ersetzbarkeit das dafür erforderliche Personal vorhanden bzw. auch ausreichend geschult ist.

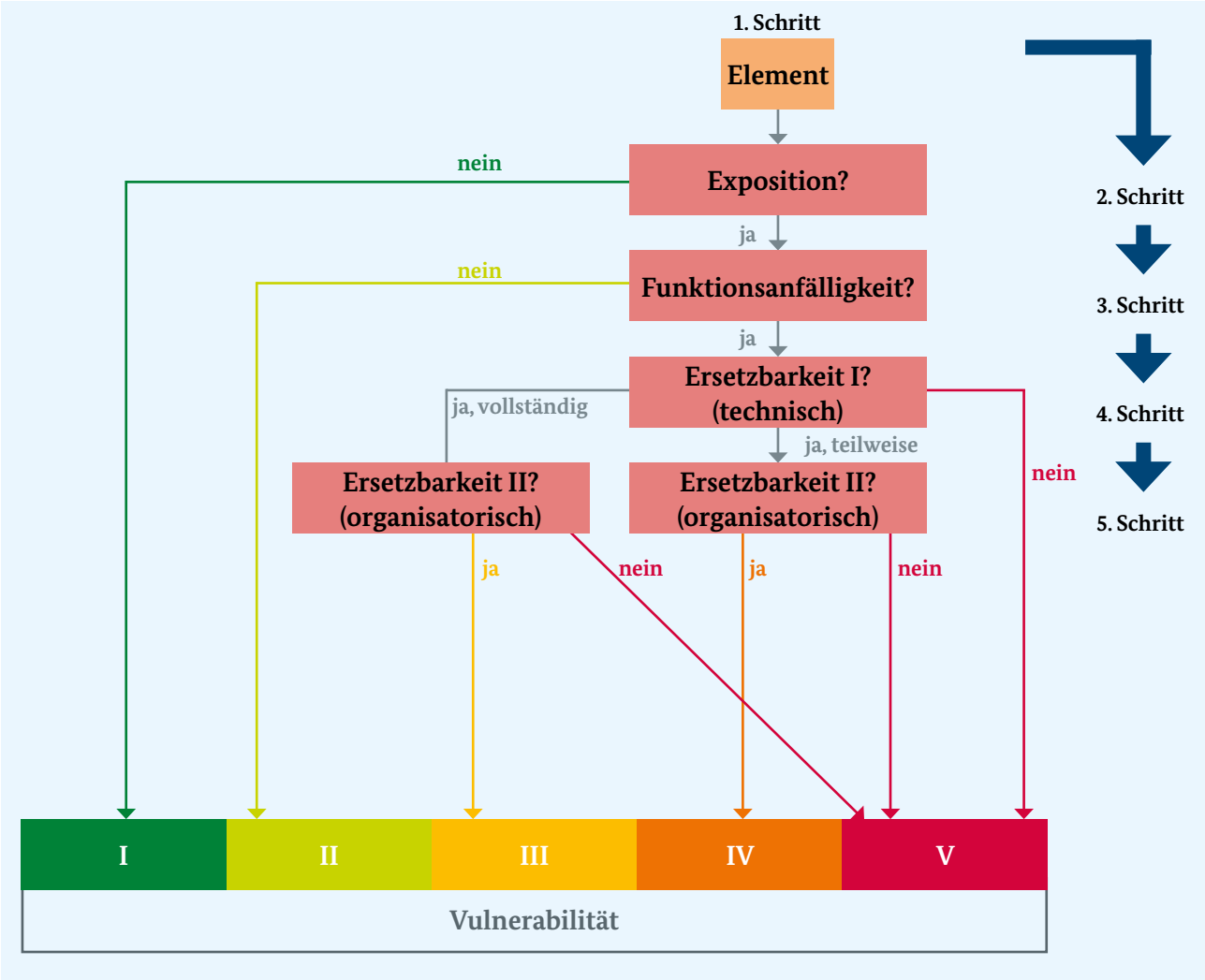


Abbildung 5: Systematik zur Abschätzung der Verwundbarkeit [19]; Quelle: BBK

Ergebnis der Verwundbarkeitsabschätzung ist eine Verwundbarkeitstabelle der betrachteten Prozesselemente. Elemente mit hohem oder sehr hohem Schutzbedarf und beispielsweise hoher Verwundbarkeit gegenüber dem Szenario geben Aufschluss über die mögliche Schwere der Auswirkungen auf die Prozesse und folglich auf das zu erwartende Schadensausmaß.

Tabelle 9: Zuordnung der Elemente zu Verwundbarkeitsklassen

Exposition	Funktions-anfälligkeit	Ersetzbarkeit		Verwundbarkeits-klasse	Erläuterung
		technisch	organisatorisch		
nicht exponiert				**Klasse I:** keine Verwundbarkeit	
exponiert	***nicht*** funktionsanfällig			**Klasse II:** geringe Verwundbarkeit	Das Element ist exponiert, aber in seiner Funktionsfähigkeit nicht beeinträchtigt. Durch die Exposition besteht dennoch immer noch Unsicherheit
	funktionsanfällig	***vollständig*** ersetzbar	Personal vorbereitet/geschult, um Maßnahmen umzusetzen	**Klasse III:** mittlere Verwundbarkeit	Aufgrund der Exposition und der Funktionsanfälligkeit fällt das Element aus, das technisch sowie organisatorisch vollständig ersetzt werden kann. Dennoch besteht ein vergleichsweise hohes Maß an Unsicherheit, dass es zu einer Beeinträchtigung der Leistung kommen kann
			kein (qualifiziertes) Personal	*Zuordnung zu Klasse V*	
		nur ***teilweise*** ersetzbar	Personal vorbereitet/geschult, um Maßnahmen umzusetzen	**Klasse IV:** hohe Verwundbarkeit	Es ist mit einem *teilweisen* Ausfall der Leistung zu rechnen
			kein (qualifiziertes) Personal	*Zuordnung zu Klasse V*	
		nicht ersetzbar		**Klasse V:** sehr hohe Verwundbarkeit	Es ist mit einem *vollständigen* Ausfall der Leistung zu rechnen

5.3 Bewertung der Schadensauswirkungen

Prinzipiell reicht eine Verwundbarkeitsabschätzung aus, um risikomindernde Maßnahmen ergreifen zu können. Will man jedoch – als Entscheidungsgrundlage für eine Maßnahmenpriorisierung – einen Risikovergleich der betrachteten Szenarien vornehmen, so ist zunächst das durch das jeweilige Szenario entstandene Risiko für die Einrichtung zu bestimmen.

Um Aussagen über das Risiko zu treffen, bieten sich zwei Möglichkeiten an:

1. Aus der Zusammenschau der im Rahmen der Verwundbarkeitsabschätzung ermittelten verwundbaren Elemente wird eine Gesamtverwundbarkeit für die Einrichtung bestimmt. Diese sollte durch Experten und Mitarbeiter, die mit den Prozessen der Einrichtung vertraut sind und die Konsequenzen des Ausfalls abschätzen können, vorgenommen werden. Aus den Parametern Eintrittswahrscheinlichkeit und Gesamtverwundbarkeit ergibt sich das Risiko durch das jeweilige Szenario. Dieses Verfahren bietet sich an, wenn Daten zur Quantifizierung von Schadensparametern nicht zur Verfügung stehen bzw. aufwendig zu ermitteln sind.

   Die → Tabelle 10 zeigt beispielhaft auf, wie die Schadensauswirkungen auf der Grundlage der Gesamtvulnerabilität beschrieben und klassifiziert werden können. Ausgehend von dem Schutzziel „Erhöhung der Ausfallsicherheit TLZ“ wird der Schaden durch die Schadensparameter Ausfalldauer und/oder Schweregrad der Beeinträchtigung des Betriebs und des damit verbundenen zeitlichen und finanziellen Wiederherstellungsaufwands beschrieben. Entscheidendes Kriterium ist, ob die Verfügbarkeit der Dienste der TLZ kurz-, mittel- oder langfristig eingeschränkt wird.

2. Ein gängiges Verfahren zur Ermittlung des Risikos besteht darin, das Schadensausmaß quantitativ zu bestimmen, etwa durch die entstandenen direkten Kosten für Sachwerte, Reparatur und Wiederherstellungsaufwand sowie den erhöhten Personalaufwand, wenn beim Ausfall der TLZ die überwachten Tunnel vor Ort mit Personal besetzt werden müssen. Führt der Ausfall einer TLZ zu einer mittel- oder längerfristigen Sperrung eines Tunnels, so könnten auch die indirekten volkswirtschaftlichen Kosten durch Umwegfahrten und die damit verbundenen Mehrreisezeiten bei der Bestimmung des Schadensausmaßes einbezogen werden.

   Sicherlich können konkrete Daten Verantwortliche und Entscheidungsträger eher überzeugen. Ob der Aufwand, der mit der Datenbeschaffung verbunden ist, gerechtfertigt ist und ob eine auf Basis von Verwundbarkeitsabschätzung vorgenommene Schadensermittlung nicht ebenso zum Ziel führen kann, ist abzuwägen.

Tabelle 10: Beispiel für die Klassifizierung und Beschreibung der Auswirkungen

Kategorie		Schadensausmaß	Erläuterung/Beispiele
IV	sehr hoch	Totalausfall der TLZ	• Physische Zerstörung des Gebäudes, der Gebäudeteile oder Anlagen der TLZ (Großbrand, Hochwasser, terroristischer Anschlag). Die Wiederinbetriebnahme dauert mehrere Wochen, ggf. ein bis zwei Jahre. Hoher finanzieller Wiederherstellungsaufwand. • Totalausfall über mehrer Tage, ggf. Wochen, etwa durch längerfristigen Stromausfall, Unterbrechnng der Kommunikationsverbindungen oder komplexe Systemausfälle der IT durch Hacker-Angriffe
III	hoch	Erhebliche Einschränkung des Betriebs	• Der Betrieb kann über mehrere Tage (oder Wochen) nur eingeschränkt aufrechterhalten werden, da mehrere kritische technische Komponenten betroffen sind und folglich einige sicherheitsrelevante Prozesse (z. B. Steuerung Betriebstechnik) nicht durchgeführt werden können. • Eingeschränkter Betrieb durch Ausfall einer kritischen Zahl von Mitarbeitern (internes und auch externes Personal).
II	mittel	Teilweise Einschränkung des Betriebs	• Die für den Betriebsablauf relevanten technischen Komponenten und Systeme sind nur kurzfristig betroffen und können innerhalb weniger Stunden (max. eines Tages) wieder in Betrieb genommen werden.
I	gering	Geringer Einfluss auf den Betriebsablauf	• Einige technische Komponenten und Systeme sind nur geringfügig in ihrem Funktionsumfang eingeschränkt, die wesentlichen Prozesse können auch weiterhin aufrechterhalten werden.

5.4 Risikovergleich und Risikobewertung

Im letzten Schritt der Risikoanalyse werden auf Basis der vorgenommenen Klasseneinteilung die Werte für die abgeschätzten Eintrittswahrscheinlichkeiten, die Verwundbarkeit oder die Schadensausmaße für die betrachteten Szenarien in eine Risikomatrix übertragen. Diese Darstellung ermöglicht einen einfachen Vergleich der von den Szenarien ausgehenden Risiken. Insbesondere bei qualitativen und semiquantitativen Analysen ist der Vergleich der Risiken in Relation zueinander sinnvoll, da die qualitativ ermittelten Ergebnisse keine absolute Aussagekraft besitzen. Mit Hilfe der Risikomatrix können somit diejenigen Szenarien erkannt werden, die das größte Risiko für die Einrichtung darstellen. Auf welchen Prozesselementen das jeweilige Risiko beruht, kann der Vulnerabilitätsanalyse entnommen werden.

Die in der Vulnerabilitätsanalyse vorgenommene Dokumentation der Schwachstellen bietet Ansatzpunkte für Maßnahmen zur Reduzierung der Anfälligkeit. Die Maßnahmen sollten vorrangig bei den Prozesselementen ansetzen, welche aufgrund ihrer hohen Kritikalität bzw. ihrer hohen Schutzbedarfe in dem betrachteten Szenario einem besonders hohen Risiko ausgesetzt sind. Letztlich ist es aber die Aufgabe der Leitung des Betreibers, Handlungsziele und Prioritäten in der Maßnahmenumsetzung festzulegen (vgl. → Kapitel D).

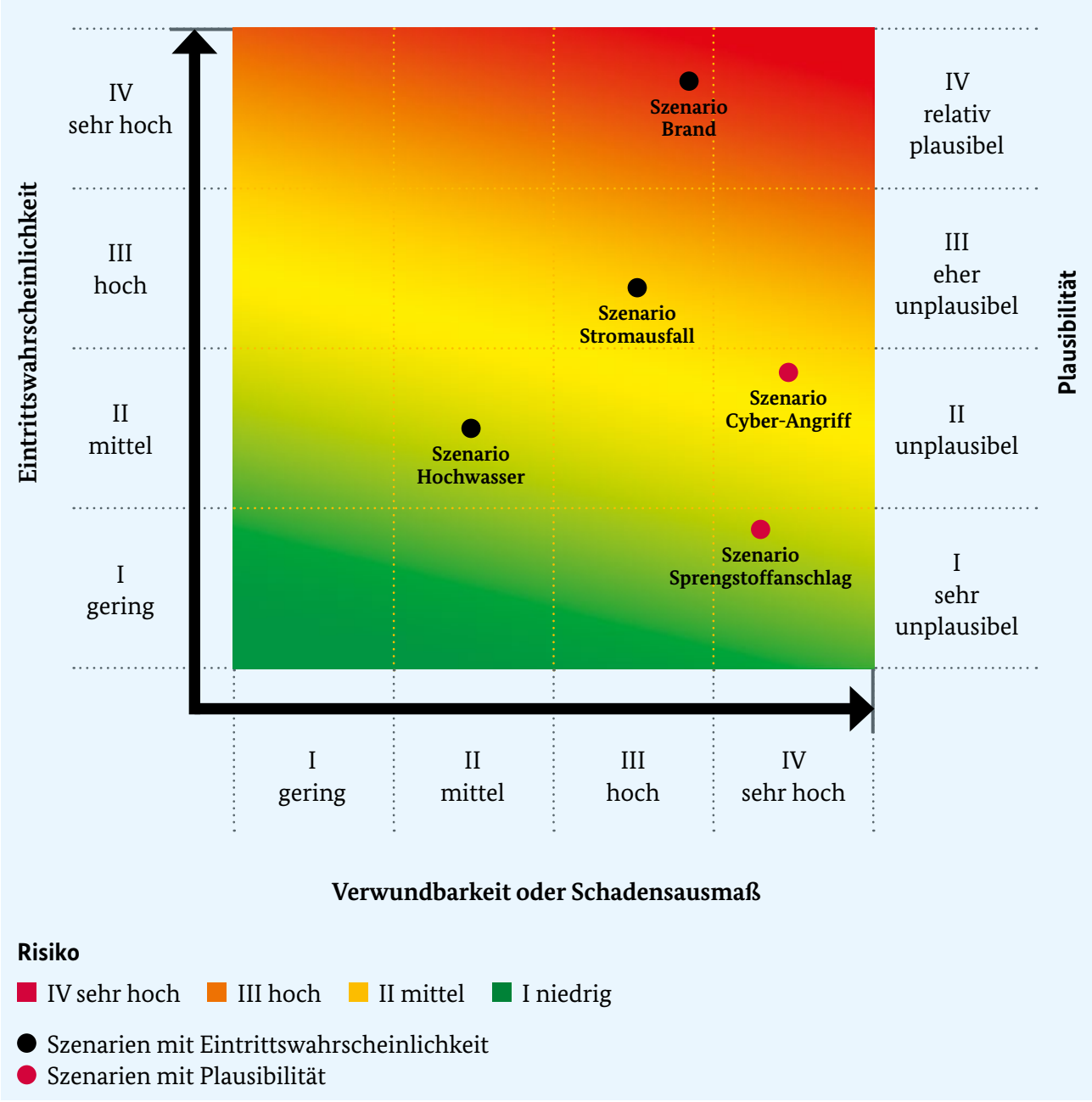


Abbildung 6: Risikomatrix; Quelle: BBK

Darstellung in Anlehnung an Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie Bundesamt für Bevölkerungsschutz (BABS), Schweiz [22]

D

Vorbeugende Maßnahmen

Quelle: Riccardo Piccinini/Shutterstock

Vorbeugende Maßnahmen und Strategien

Wurde aus der Risikobewertung ein Handlungsbedarf abgeleitet, so sind vorbeugende Maßnahmen zu erarbeiten, die zur Risikoreduzierung beitragen sollen. Dies können technische, organisatorische oder personelle Maßnahmen sein. Bei der Auswahl der Maßnahmen soll dem Kosten-Nutzen-Aspekt Rechnung getragen werden, indem die potenziellen Investitionen sowie die durch das Ereignis entstandenen direkten und indirekten Kosten gegenübergestellt werden. Neben Kosten-Nutzen-Aspekten sollten auch die rechtlichen Rahmenbedingungen sowie soziale Überlegungen in die Entscheidung über Schutzmaßnahmen einfließen.

Grundsätzlich gibt es mehrere Strategien für den Umgang mit den erkannten Risiken:

- **Risikovermeidung**
  Risiken können vermieden werden, indem man beispielsweise bei der Standortwahl für Gebäude oder Anlagen gefährdete Bereiche ausschließt. Ebenso können hochrisikobehaftete Prozesse eingestellt und durch andere Prozesse ersetzt oder riskante Technik außer Betrieb genommen werden.

- **Risikominimierung**
  Die meisten vorbeugenden Maßnahmen zielen darauf ab, die Verwundbarkeit der Prozesselemente gegenüber der Gefahr und somit das Schadensausmaß zu reduzieren sowie kritische Prozesse durch Schaffung redundanter Systeme aufrechtzuerhalten.

- **Risikotransfer**
  Risikotransfer bedeutet die Übertragung des Risikos auf eine andere Institution. So können finanzielle Schäden durch den Abschluss einer Versicherung gesenkt werden, da diese ganz oder teilweise ersetzt werden. Auch das Outsourcing von Aufgabenbereichen an vertrauenswürdige Dienstleister, die wirtschaftlich oder technisch besser in der Lage sind, die entsprechenden Risiken zu tragen, ist eine Form des Risikotransfers.

- **Risikoakzeptanz**
  Da nicht alle Risiken durch vorbeugende Maßnahmen gemindert oder ausgeschaltet werden können, weil z. B. die Abdeckung dieser Risiken wirtschaftlich nicht mehr vertretbar wäre, werden die verbleibenden Restrisiken akzeptiert. Risikoakzeptanz bedeutet aber, dass im Fall von (extremen) Ereignissen organisatorische Vorkehrungen für die Bewältigung einer solchen Lage getroffen werden müssen.

Welche der genannten Strategien zur Risikobehandlung zum Tragen kommt, hängt von der Bewertung der jeweiligen Risiken ab und ist eine Entscheidung, die auf der Leitungsebene getroffen und verantwortet werden sollte. Ziel muss es sein, durch wirtschaftlich angemessene Maßnahmen die vorhandenen Risiken auf ein vertretbares Maß zu senken.

Für risikomindernde Maßnahmen ergeben sich prinzipiell folgende Handlungsoptionen:

- Physischer Schutz von Gebäuden, Räumlichkeiten und sonstigen Anlagen (bauliche und sicherheitstechnische Maßnahmen)

- Spezielle Sicherheitsmaßnahmen zum Schutz der IT-Infrastruktur

- Schaffung von Redundanzen/Ersatzverfahren

  - Dopplung wichtiger IT-Systemkomponenten wie beispielsweise Server, Netzwerk, Kommunikationsverbindungen nach außen etc.)

  - Daten- oder Informationsredundanz durch Speicherung der Daten auf externen Speichermedien sowie Vorhalten der wichtigen Informationen auch in Papierform

  - Alternative Kommunikationswege

  - Redundanz TLZ, etwa durch Besetzung der Betriebsgebäude am Tunnel vor Ort oder durch Übernahme der Steuerung durch eine andere TLZ, wie dies z. B. in Nordrhein-Westfalen der Fall ist

- Standortplanung für die Technik
  - Verteilung der redundanten Systeme in mehreren Räumen
  - Auslagerung der Technik für Rückfallebenen (z. B. Einrichtungen einer USV bzw. Notstromversorgung) in andere Gebäude oder Gebäudeteile
- Notfallpläne
  - Einsatzpläne mit Festlegung der Meldewege, Zuständigkeiten und Verantwortlichkeiten für den Ereignisfall
  - Wiederanlaufpläne, um (IT)-Systeme und (IT)-Anwendungen möglichst schnell wieder in Betrieb nehmen zu können
  - Pläne zur Inbetriebnahme der Rückfallebenen (Besetzung der Betriebsgebäude am Tunnel vor Ort, Umschaltung der Steuerung auf eine andere TLZ)
  - Evakuierungspläne (z. B. im Fall einer Bombendrohung)
  - Pläne zur Aufrechterhaltung des Betriebs bei erheblichem Personalausfall

Damit die festgelegten Notfallverfahren im Ereignisfall auch funktionieren, sind Schulungen der Mitarbeiter sowie entsprechende Übungen durchzuführen.

- Maßnahmen zur Sicherung der organisatorischen Abläufe im Zusammenhang mit IT, z. B.
  - Regelungen zu Datensicherung, Datenschutz, Datenverarbeitung, Rechtezuweisungen etc.
  - Schulung und Sensibilisierung der Mitarbeiter zur Informationssicherheit
  - Verhaltensanweisungen bei Sicherheitsvorfällen
- Kommunikationskonzept nach außen für den Fall, dass die TLZ ausfällt, und sich in Folge dessen Störungen bzw. Verkehrsbehinderungen aufgrund eines eingeschränkten Tunnelbetriebs der überwachten Tunnel ergeben

Für die Auswahl der Maßnahmen insbesondere zur IT-Sicherheit können verschiedene Normen und IT-Grundschutz-Kataloge herangezogen werden:

- Die Norm DIN EN 50518 (vgl. → Kapitel B.1) definiert bauliche, technische und betriebliche Sicherheitsanforderungen zum Schutz der Alarmempfangsstellen.
- Die internationale Norm ISO 27002 [11] enthält insgesamt 135 generisch beschriebene technische und organisatorische Maßnahmen für die Gewährleistung der Informationssicherheit.
- Die IT-Grundschutz-Kataloge enthalten eine Vielzahl von Maßnahmen zu den Aspekten „Organisation“, „Personal“, „Notfallvorsorge“ (Übergreifende Aspekte), „Infrastruktur“, „IT-Systeme“, „Netze“ und „Anwendungen“. Auch diese Maßnahmen sind generisch beschrieben und bieten zunächst einen Basisschutz. Bei höheren Anforderungen in Bezug auf den Schutzbedarf müssen ggf. zusätzliche wirksamere Maßnahmen zur Erreichung der definierten Schutzziele ergriffen werden.
- Einen Überblick über die wichtigsten Sicherheitsmaßnahmen bietet der Leitfaden Informationssicherheit des BSI [23]. Im Fokus steht dabei die Darstellung der organisatorischen Maßnahmen, auf technische Details wird bewusst verzichtet.

Die Auswahl der Maßnahmen soll insbesondere unter Berücksichtigung der Kosten-Nutzen-Aspekte erfolgen. Gleichwohl müssen die Maßnahmen auch praxistauglich und den konkreten Gegebenheiten vor Ort angepasst sein. Auch die in den Regelwerken zur Informationssicherheit empfohlenen Maßnahmen sind generisch beschrieben, so dass diese bei der Planung an das konkrete Anwendungsumfeld angepasst werden müssen.

Für die Umsetzung der Maßnahmen sollte ein Umsetzungsplan erstellt werden, der Folgendes beinhaltet:

- **Priorisierung der Maßnahmen**
  Eine Priorisierung kann anhand des Kriteriums Schutzbedarf im Zusammenhang mit der Eintrittswahrscheinlichkeit und den Auswirkungen des Szenarios erfolgen. Darüber hinaus bietet es sich an, zunächst Maßnahmen umzusetzen, die sich im Rahmen des Soll-Ist-Abgleichs des IT-Grundschutzes als unzureichend oder als fehlend erwiesen haben (vgl. → Kapitel C.4). Es kann aber auch durchaus sinnvoll sein, ein Sofortprogramm mit Maßnahmen aufzustellen, die – unabhängig von der Dringlichkeit bzw. dem Schutzbedarf der jeweiligen Infrastrukturelemente – mit geringem finanziellen oder personellen Aufwand umgesetzt werden können.

- **Festlegung der Verantwortlichkeiten für die Umsetzung der einzelnen Maßnahmen**
  Während für die risikoanalytische Betrachtung eine Projektgruppe eingerichtet wird, die sich aus internen und externen Experten sehr unterschiedlicher Bereiche mit speziell definierten Verantwortlichkeiten für die Umsetzung der Risikoanalyse zusammensetzt, stehen im Zuge der Umsetzung der sich aus der Risikoanalyse ergebenden Maßnahmen die jeweils fachlich zuständigen Mitarbeiterinnen und Mitarbeiter in der Verantwortung.

- **Bereitstellung von Ressourcen**
  Bei der Bereitstellung der für die Umsetzung der Maßnahmen notwendigen Ressourcen sind nicht nur die Sachmittel zu berücksichtigen, sondern ggf. auch zusätzliche personelle Ressourcen einzustellen.

- **Planung der einzelnen Maßnahmen**
  Es empfiehlt sich, für die Umsetzung der einzelnen Maßnahmen Pläne zu erstellen, die den Ablauf inhaltlich und zeitlich strukturieren, etwa in Form eines Balkenplans, um auf diese Weise Einzelmaßnahmen besser aufeinander abstimmen, Überschneidungen zu erkennen und mögliche Doppelarbeit zu vermeiden.

Das auf Basis der Risikoanalyse entwickelte und umgesetzte Sicherheitskonzept bedarf einer fortwährenden Evaluierung und Aktualisierung. Dies ist beispielsweise der Fall, wenn

- im Zuge einer Umorganisation neue Prozesse bzw. Betriebsabläufe eingeführt werden, die hinsichtlich der Kritikalität neu bewertet werden müssen,

- neue IT-Systeme eingesetzt werden und sich ggf. neue Sicherheitslücken ergeben,

- sich die Gefährdungslage aufgrund neuer Gefahren oder Bedrohungen geändert hat und die Risikoanalyse entsprechend ergänzt werden muss,

- sich Mängel bei den vorhandenen Sicherheitsmaßnahmen während einer Übung, Störung bzw. während eines Ereignisses gezeigt haben.

Es sollte regelmäßig geprüft werden, ob die vorgesehenen Maßnahmen sowohl im Bereich technischer Sicherheitsmaßnahmen als auch organisatorischer Regelungen eingehalten werden. Darüber hinaus sind die Effizienz und die Praxistauglichkeit der eingesetzten Sicherheitsmaßnahmen, insbesondere der organisatorischen Regelungen, zu überprüfen. Gleichzeitig gilt es, den Stand der Technik und anderer Regularien (Normen, Vorschriften) zu verfolgen und in die Sicherheitskonzeption zu implementieren. Der BSI-Leitfaden IS-Revision bietet Hilfestellungen für die Durchführung solcher Überprüfungen [24].

E

Anhang

Quelle: © NuPenDekDee/Shutterstock

Anhang

Anhang 1: Literatur

[1] Richtlinien für die Ausstattung und den Betrieb von Straßentunneln RABT 2006. Forschungsgesellschaft für Straßen- und Verkehrswesen, Köln.

[2] DIN EN 50518-1 (VDE 0830-5-6-1):2010-12, Alarmempfangsstelle – Teil 1: Örtliche und bauliche Anforderungen.

[3] DIN EN 50518-2 (VDE 0830-5-6-2):2011-04, Alarmempfangsstelle – Teil 2: Technische Anforderungen.

[4] DIN EN 50518-3 (VDE 0830-5-6-3):2011-09, Alarmempfangsstelle – Teil 3: Abläufe und Anforderungen an den Betrieb.

[5] VdS 3137:2013-09 (2), Zertifizierung von Alarmempfangsstellen gemäß DIN EN 50518.

[6] Bierfert, Andreas (2013): DIN EN 50518 – die „Leitstellen"-Norm. Auswirkungen auf die deutschen Feuerwehren. In: BRANDSchutz. Heft 5. S. 360-362.

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI 2008): BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS). Bonn.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI 2008): BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise. Bonn.

[9] Bundesministerium des Innern (BMI 2005) (Hrsg.): Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Empfehlungen für Unternehmen. Berlin.

[10] ISO/IEC 27001:2015-03 Information technology – Security techniques – Information security management systems requirements specification.

[11] ISO/IEC 27002:2014-02 Information technology – Security techniques – Code of practice for information security management.

[12] Bundesministerium des Innern (BMI 2011) (Hrsg.): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. Berlin.

[13] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK 2010) (Hrsg.): Methode für die Risikoanalyse im Bevölkerungsschutz (= Reihe Wissenschaftsforum, Band 8). Bonn.

[14] Bundesamt für Sicherheit in der Informationstechnik (BSI 2008): BSI-Standard 100-4 Notfallmanagement. Bonn.

[15] Bundesamt für Sicherheit in der Informationstechnik (BSI 2011): Gefährdungskatalog G 0 „Elementare Gefährdungen". Bonn.

[16] Bundesamt für Sicherheit in der Informationstechnik (BSI 2008): BSIStandard 100-3 Risikoanalyse auf Basis von IT-Grundschutz. Bonn.

[17] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK 2008) (Hrsg.): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens. Bonn.

[18] Bundesamt für Sicherheit in der Informationstechnik (BSI 2012): Register aktueller Cyber-Gefährdungen und Angriffsformen. In: BSI- Analysen zur Cybersicherheit. Version 1.00.

[19] Krings, Susanne (2011): Verwundbarkeit Kritischer Infrastruktur gegenüber Hochwasserereignissen. In: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Indikatoren zur Abschätzung von Vulnerabilität und Bewältigungspotenzialen am Beispiel von wasserbezogenen Naturgefahren in urbanen Räumen. (= Schriftenreihe Forschung im Bevölkerungsschutz, Band 13). Bonn.

[20] Lenz, Susanne (2009): Vulnerabilität Kritischer Infrastrukturen. (= Schriftenreihe Forschung im Bevökerungsschutz, Band 4). Bonn.

[21] ISO/IEC 27005:2011-06 Information technology – Security techniques – Information security risk management.

[22] Bundesamt für Bevölkerungsschutz (BABS 2013) (Hrsg.): Katastrophen und Notlagen Schweiz. Risikobericht 2012. Bern.

[23] Bundesamt für Sicherheit in der Informationstechnik (BSI 2012) (Hrsg.): Leitfaden Informationssicherheit. IT-Grundschutz kompakt. Bonn.

[24] Bundesamt für Sicherheit in der Informationstechnik (BSI 2010): Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz. Bonn.

Abrufbar unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v4.pdf;jsessionid=6F431169220D6796A926F7E09DEC3421.internet481?__blob=publicationFile&v=2
Abgerufen am 08.04.2022

Anhang 2: Abbildungsverzeichnis und Tabellenverzeichnis

1. Abbildungsverzeichnis

2. Tabellenverzeichnis

Anhang 3: Abkürzungsverzeichnis

AES
Alarmempfangsstelle

BBK
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

BMBF
Bundesministerium für Bildung und Forschung

BMI
Bundesministerium des Innern

BOS
Behörden und Organisationen mit Sicherheitsaufgaben

BSI
Bundesamt für Sicherheit in der Informationstechnik

ISMS
Managementsystem für die Informationssicherheit

RABT
Richtlinien für die Ausstattung und den Betrieb von Straßentunneln

TLZ
Tunnelleitzentrale

Anhang 4: Gefahrenliste

Quellen: Bundesministerium des Innern (Hrsg.): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. Berlin, 2011; Bundesamt für Sicherheit in der Informationstechnik: Gefährdungskatalog G 0 „Elementare Gefährdungen“. 2011

Gefahr	Exposition	Mögliche Wirkung / gefährdete Bereiche
Natürliche Ereignisse / Höhere Gewalt		
Hochwasser	flussnahe und tiefliegende Bereiche	Funktionsbereiche in tiefliegenden Gebäudeteilen (Technikräume, Lagerräume)
Starkregen	deutschlandweit möglich	Beschädigung von Gebäuden und Anlagen; Aus- und Unterspülungen
Sturzflut	in Hanglagen	Beschädigung von Gebäuden und Anlagen; Aus- und Unterspülungen
Schneefall/ Schneeverwehungen/Hagel	deutschlandweit möglich	Beeinträchtigung von Personal, Dienstleistern und Lieferanten; Beschädigung von Gebäuden und Anlagen
Sturm/Tornado	deutschlandweit möglich	Ausfall von Mitarbeitern, Dienstleistern aufgrund von Verkehrsbehinderungen, Beschädigung von Gebäuden und Anlagen
Hitzewelle	deutschlandweit möglich	Gesundheitliche Beeinträchtigung der Mitrbeiter, eingeschränkte Leistungsfähigkeit; Auswirkungen auf die Haustechnik und Geräte (z. B. Kühlung)
Kältewelle	deutschlandweit möglich	Zerstörung der Versorgungsinfrastrukturen aufgrund von Eis- und Frostbildung; Ausfall der Mitarbeiter, Dienstleister aufgrund von Verkehrsbehinderungen
Erdbeben	Standorte in Erdbebengebieten: z. B. Rheingraben, Kölner Bucht, Vogtland, Schwäbische Alb	Zerstörung von Anlagen, Gebäuden, Versorgungsinfrastrukturen

Gefahr	Exposition	Mögliche Wirkung / gefährdete Bereiche
Natürliche Ereignisse / Höhere Gewalt		
Gravitative Massenbewegungen	kleinräumig, Standorte an Hängen, in Gebirgen	Zerstörung von Anlagen, Gebäuden, Versorgungsinfrastrukturen
Größere Epidemie/Pandemie	weltweit/deutschlandweit/ regional möglich	Ausfall von Mitarbeitern, externen Dienstleistern
Brand	--	Gefährdung des Personals, Zerstörung von Anlagen, Gebäuden
Massive Beeinträchtigung der externen Verkehrs- und Transportwege	deutschlandweit möglich	Beeinträchtigung von Personal, externen Dienstleistern und Lieferanten
Ausfall der externen Stromversorgung	deutschlandweit möglich	Beeinträchtigung von Anlagen und Geräten
Ausfall der externen Wasserversorgung	deutschlandweit möglich	Beeinträchtigung von Personal, Anlagen und Geräten
Ausfall und Störung von (internen) Versorgungsnetzen	--	Beeinträchtigung von Personal, Anlagen und Geräten
Ereignisse im Umfeld der Einrichtung		
Gefahrgutunfälle: Brand, Explosion, Freisetzung giftiger Substanzen oder Austreten gefährlicher Strahlung	im Umfeld von Gefahrgutstrecken (Straße, Schiene) sowie im Umfeld von Betrieben, Industrien, in denen Gefahrgut verwendet wird	Beeinträchtigung des Personals, der Gebäude (Kontamination)
Vorsätzliche Handlungen		
Bombendrohung	deutschlandweit möglich	Räumung der Einrichtung, Ausfall der Dienste
Bedrohung des Personals mit Schusswaffen	deutschlandweit möglich (abhängig von Zugänglichkeit)	--
Anschlag mit konventioneller Spreng- und Brandvorrichtung	deutschlandweit möglich (abhängig von Zugänglichkeit)	Gefährdung des Personals, Zerstörung von Anlagen, Gebäuden
Anschlg mit Freisetzung von CBRN-Agenzien	deutschlandweit möglich (abhängig von Zugänglichkeit)	Beeinträchtigung des Personals, der Gebäude und Anlagen (Kontamination)
Sabotage G 0.41[8]		Mutwillige Manipulation oder Beschädigung der Infrastruktur durch Innen- oder Außentäter. Besonders gefährdet sind nicht ausreichend geschützte gebäudetechnische oder kommunikationstechnische Infrastruktur oder zentrale Versorgungspunkte

[8] Nummer der „Elementaren Gefährdungen“ nach BSI

Gefahr	Beschreibung
Vorsätzliche Handlungen mit Hilfe oder auf Basis von IT	
Abfangen kompromittierender Strahlung G 0.13	Abfangen der durch elektromagnetische Wellen getragenen Informationen
Ausspähen von Informationen / Spionage G 0.14	Ausspähen von Daten auf optischen, akustischen oder elektronischem Weg
Abhören G 0.15	Gezielte Angriffe auf Kommunikationsverbindungen, Gespräche, Geräuschquellen aller Art oder IT-Systeme mit dem Ziel, Informationen zu sammeln
Diebstahl oder Verlust von Geräten, Datenträgern oder Dokumenten G 0.16/17	Erlangung/Offenlegung vertraulicher Informationen
Manipulation von Hard- oder Software oder Informationen G 0.21/22	Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen; Verfälschung von Informationen
Unbefugtes Eindringen in IT-Systeme G 0.23	Auslesen von Daten oder Einschleusen von Schadprogrammen über nicht oder unzureichend gesicherte Schnittstellen
Unberechtigte Nutzung oder Administration von Geräten und Systemen G0.30	Auch bei IT-Systemen mit einer starken Identifikations- und Authentisierungsfunktion ist die Gefahr der unberechtigten Nutzung gegeben, wenn Unbefugte an Zugangsdaten gelangen. Ausspähen von Informationen, Manipulation und Störungen können die Folge sein
Missbrauch von Berechtigungen G 0.32	Ein Missbrauch von Berechtigungen ist gegeben, wenn Mitarbeiter vorsätzlich recht- oder unrechtmäßig erworbene Zugangsrechte zu IT-Systemen außerhalb des ihnen vorgegebenen Rahmens nutzen und aus unterschiedlichen Motiven heraus der Einrichtung oder anderen Personen Schaden zufügen
Nötigung, Erpressung oder Korruption G 0.35	Durch Androhung von Gewalt, Nötigung oder Korruption der Mitarbeiter können Angreifer versuchen, an sicherheitsrelevante Informationen zu gelangen
Identitätsdiebstahl G 0.36	Unter Vortäuschung falscher Identität können Angreifer z. B. versuchen, an schützenswerte Informationen zu gelangen
Abstreiten von Handlungen G 0.37	Aus verschiedenen Gründen können Personen Handlungen (z. B. den Erhalt einer wichtigen Nachricht) abstreiten, z. B. weil diese gegen Sicherheitsvorschriften oder gegen Gesetze verstoßen

Gefahr	Beschreibung
Vorsätzliche Handlungen mit Hilfe oder auf Basis von IT	
Schadprogramme G 0.39	Verlust oder Verfälschung von Informationen oder Anwendungen, Ausspionieren von Daten und Passwörtern, Deaktivierung von Schutzsoftware oder Fernsteuerung von Systemen
Verhinderung von Diensten (Denial of Service) G 0.40	Die Nutzung bestimmter Dienstleistungen, Funktionen oder Geräten wird verhindert, indem z. B. die Dienste einer Ressource (z. B. Server) gezielt überlastet werden
Social Engineering G 0.42	Methode, durch Manipulation der Mitarbeiter einer Institution oder durch Aufbau von persönlichen Kontakten zu den Mitarbeitern, unberechtigten Zugang zu Informationen oder auch IT-Systemen zu gelangen
Einspielen von Nachrichten G 0.43	Eine Art der Sabotage, bei der speziell vorbereitete Nachrichten (z. B. Videosequenzen) in das System eingespeist werden, um falsche Informationen zu verbreiten
Unbefugtes Eindringen in Räumlichkeiten G 0.44	Diebstahl von Geräten, Ausspähen von Informationen, Manipulation der IT-Systeme
Menschliche Fehlhandlungen	
Software-Schwachstellen oder -Fehler G 0.28	Je komplexer die Software, desto fehleranfälliger ist sie. Sofern diese nicht rechtzeitig erkannt und behoben werden, führen diese zu Systemabstürzen oder auch fehlerhaften Darstellungen. Software-Schwachstellen können u. a. von Angreifern ausgenutzt werden, um Schadsoftware einzuschleusen, Daten auszulesen oder Manipulationen vorzunehmen
Fehlerhafte Nutzung oder Administration von Geräten und Systemen G 0.31	Fehlerhafte Nutzung (z. B. fehlerhafte Administration) kann sowohl die Sicherheit als auch die Funktionalität von Systemen beeinträchtigen und zu Datenverlust, Störungen oder Ausfällen der Systeme führen
Technisches Versagen	
Fehlfunktion von Geräten und Systemen G 0.26	Fehlfunktion z. B. aufgrund Materialermüdung, fehlender Wartung, konzeptionellen Schwächen oder nicht vorgesehenen Einsatzbedingungen
Verschiedene Ursachen	
Offenlegung schützenswerter Informationen G 0.19	Vertrauliche Informationen, wie Passwörter, personenbezogene Daten, Verträge oder Firmengeheimnisse können durch technisches Versagen, Unachtsamkeit oder vorsätzliche Handlungen an die Öffentlichkeit bzw. an unbefugte Personen gelangen

Gefahr	Beschreibung
Verschiedene Ursachen	
Informationen oder Produkte aus unzuverlässiger Quelle G 0.20	Beispielsweise kann das Einspielen von Updates oder Patches aus nicht vertrauenswürdigen Quellen zu Infizierung der IT-Systeme mit Schadprogrammen führen
Zerstörung von Geräten oder Datenträgern G 0.24	Mutwillige physische Zerstörung von Geräten, Datenträgern, Schriftstücken aus unterschiedlichen Motiven (Rache, Frust) durch Mitarbeiter oder Außentäter. Auch durch ungeschulten Umgang oder Fahrlässigkeit kann es zu Zerstörungen an Geräten und Datenträgern kommen
Ausfall von Geräten oder Systemen G 0.25	Ausfall zentraler Komponenten eines IT-Systems oder einzelner Komponenten der technischen Infrastruktur, die den Ausfall wichtiger Prozesse zur Folge haben. Die Ursachen können vielfältig sein und auf technisches Versagen, menschliche Fehlhandlungen, mangelnde Wartung oder auch vorsätzliche Handlungen zurückzuführen sein
Verstoß gegen Gesetze oder Regelungen G 0.29	Unzureichendes Sicherheitsmanagement in der Informationsbearbeitung kann gegen bestehende Rechtsvorschriften oder Verträge verstoßen
Missbrauch personenbezogener Daten G 0.38	Ein Missbrauch personenbezogener Daten kann beispielsweise dann vorliegen, wenn die An- und Abmeldung von Benutzern an IT-Systemen zur Anwesenheits- und Verhaltenskontrollen genutzt wird
Datenverlust G 0.45	Datenverlust durch Beschädigung, Verlust oder Diebstahl von Geräten oder Datenträgern sowie durch unbeabsichtigte oder auch beabsichtigte Löschung von Daten
Integritätsverlust schützenswerter Informationen G 0.46	Verlust der Integrität durch Übertragungsfehler, Fehleingaben oder Schadprogramme
Organisation/Personal	
Ausfall oder Störung von Dienstleistern G 0.11	Beeinträchtigung von Betriebsabläufen, wenn diese stark von Spezialdienstleistern (Systemadministration, Wartung) oder Zulieferern abhängig sind
Fehlplanung oder fehlende Anpassung G 0.18	Mängel in organisatorischen Abläufen, die direkt oder indirekt der Informationsverarbeitung dienen
Ressourcenmangel G 0.27	Beeinträchtigung der Betriebsabläufe aufgrund fehlender personeller, zeitlicher, finanzieller oder technischer Ressourcen
Personalausfall G 0.33	Beeinträchtigung der Betriebsabläufe insbesondere dann, wenn Schlüsselpersonal, das über besonderes Fachwissen verfügt und durch andere nicht ersetzt werden kann, ausfällt

Impressum

Herausgeber
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Provinzialstraße 93
53127 Bonn
Postfach 18 67
53008 Bonn

Telefon: +49 (0) 228 99 550-0
Telefax: +49 (0) 228 99 550-1620
E-Mail: BBK-abteilung-II@bbk.bund.de
Internet: www.bbk.bund.de

ISBN: 978-3-93947-65-1

Redaktion
Verfasserin:
Dipl. Geogr. Ingrid Mausa
BBK, Referat II.3, Strategie KRITIS, Cyber-Sicherheit KRITIS

Stand
Erstveröffentlichung 2015
Inhaltich unveränderte Neuauflage Mai 2022

Satz
ORCA Affairs GmbH, Schumannstraße 5, 10117 Berlin