



Bundesministerium
des Innern

Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement

Leitfaden für Unternehmen und Behörden



www.bmi.bund.de

Vorwort

Die Existenz unserer Gesellschaft ist abhängig von der Sicherstellung ihrer Versorgung mit verschiedensten Produkten, Funktionen und Dienstleistungen. Die Gewährleistung des Schutzes lebenswichtiger Einrichtungen ist deshalb eine Kernaufgabe staatlicher Sicherheitsvorsorge. Sowohl die Bedrohungssituation aufgrund des internationalen Terrorismus als auch die Zunahme natürlicher Extremereignisse stellen den Schutz dieser Kritischen Infrastrukturen vor wachsende Herausforderungen. Zusätzlich ergeben sich neue Gefährdungsmomente bei der Informationstechnik, die sämtliche Lebens- und Wirtschaftsbereiche durchdringt. Da die Mehrzahl der für unsere Gesellschaft als kritisch zu betrachtenden Infrastrukturen im Besitz privater Betreiber ist, arbeiten in Deutschland Staat und Wirtschaft Hand in Hand, um den wirkungsvollen Schutz dieser Anlagen, Einrichtungen und Systeme sicherzustellen. Dabei unterstützen die Sicherheitsbehörden die Unternehmen mit Beratung und Vernetzung, aber auch mit konkreten Handlungsempfehlungen. Die Wirtschaft selbst bringt ihren Sachverstand und ihre praktischen Erfahrungen in die Partnerschaft ein.

Der Leitfaden Risiko- und Krisenmanagement ist ein Ergebnis einer solchen Kooperation. Der Leitfaden richtet sich an die Betreiber Kritischer Infrastrukturen. Er soll ihnen Hilfestellungen beim Aufbau und der Weiterentwicklung ihres jeweiligen Risiko- und Krisenmanagements geben. Auf Grundlage der allgemeinen Empfehlungen des Basisschutzkonzeptes zum Schutz Kritischer Infrastrukturen (Bundesministerium des Innern, 2005) stellt er Methoden zur Umsetzung eines Risiko- und Krisenmanagements dar und ergänzt diese um praktische Handreichungen in Form von Beispielen und Checklisten. Bei der Entwicklung des Leitfadens wurden das Bundesministerium des Innern, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und das Bundesamt für Sicherheit in der Informationstechnik durch Experten der unternehmerischen Praxis unterstützt. Für ihre Mitarbeit während des gesamten Prozesses der Entstehung des Leitfadens dankt das Bundesministerium des Innern deshalb

- der Berufsgenossenschaft der Banken, Versicherungen, Verwaltungen, freien Berufe und besonderer Unternehmen – Verwaltungs-Berufsgenossenschaft –, Herrn Bernd Marquardt und Herrn Hans-Jürgen Penz,
 - der Commerzbank AG, Herrn Heinz-Peter Geil,
 - der Forschungszentrum Jülich GmbH, Frau Sonja Altstetter,
 - der Fraport AG, Herrn Friedhelm Jungbluth und Herrn Jens Sanner,
 - der Gelsenwasser AG, Herrn Uwe Marquardt,
 - der Infraprotect GmbH, Herrn Wolfgang Czerni,
 - der Trauboth Risk Management GmbH, Herrn Frank Tesch,
 - der VERISMO GmbH, Herrn Dr. Klaus Bockslaff,
- sowie ihren Mitarbeiterinnen und Mitarbeitern.

Der Dank gilt ferner folgenden Partnern, die sich mit Rat und Anregungen eingebracht haben: EnBW Regional AG, Gesamtverband der Deutschen Versicherungswirtschaft e. V. sowie Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V. Nach dem im Sommer 2007 vom Bundeskabinett verabschiedeten Umsetzungsplan KRITIS des Nationalen Plans zum Schutz Kritischer Informationsinfrastrukturen ist der Leitfaden Risiko- und Krisenmanagement ein weiterer Beitrag des Bundesministeriums des Innern zur Stärkung des Schutzes Kritischer Infrastrukturen. Zugleich wird damit die Bedeutung einer konstruktiven und vertrauensvollen Zusammenarbeit zwischen Staat und Wirtschaft in diesem wichtigen Bereich der Inneren Sicherheit unterstrichen.

Berlin im Januar 2008



COMMERZBANK



Ihre gesetzliche Unfallversicherung

T.R.M.
Trauboth Risk Management GmbH

VERISMO

INFRAPROTECT GmbH

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Inhalt

Vorwort	1
Zusammenfassung	7
1. Einleitung	9
2. Grundlagen zu Kritischen Infrastrukturen	10
2.1 Sektoren	10
2.2 Rahmenbedingungen und Eigenschaften Kritischer Infrastrukturen	10
2.2.1 Veränderung der Gefahrenlage	10
2.2.2 Sozioökonomische Rahmenbedingungen	11
2.2.3 Besondere Eigenschaften Kritischer Infrastrukturen	12
2.3 Rechtliche Vorgaben zum Risiko- und Krisenmanagement	13
3. Risiko- und Krisenmanagement zum Schutz Kritischer Infrastrukturen	14
3.1 Phase 1: Vorplanung in der Einrichtung	15
3.1.1 Etablierung des Risiko- und Krisenmanagements	15
3.1.2 Zuständigkeiten bei der Etablierung	15
3.1.3 Ressourcen zur Etablierung	15
3.1.4 Klärung der rechtlichen Verpflichtungen	15
3.1.5 Strategische Schutzziele	15
3.1.6 Risikokommunikation	16
3.2 Phase 2: Risikoanalyse	16
3.2.1 Kritikalitätsanalyse	17
3.2.2 Risikoidentifikation	18
3.2.2.1 Gefahrenanalyse und Szenarioentwicklung	18
3.2.2.2 Verwundbarkeitsanalyse	19
3.2.2.3 Risikoermittlung	20
3.2.2.4 Risikovergleich und Risikobewertung	21

3.3	Phase 3: Vorbeugende Maßnahmen und Strategien	21
3.3.1	Risikominderung	21
3.3.2	Risikovermeidung	22
3.3.3	Risikoüberwälzung	22
3.3.4	Akzeptanz von Risiken (Restrisiken)	22
3.3.5	Schadenerfahrungen der Sachversicherer	22
3.4	Phase 4: Krisenmanagement	22
3.4.1	Die Organisation des Krisenmanagements	24
3.4.1.1	Krisenplan	24
3.4.1.2	Aufbauorganisation	25
3.4.1.2.1	Krisenstab	25
3.4.1.2.2	Krisenstabsleiter	26
3.4.1.2.3	Krisenstabsteam	26
3.4.1.2.4	Fachberater im Krisenstab	26
3.4.1.3	Ablauforganisation	26
3.4.1.3.1	Meldewege und Alarmierung	27
3.4.1.3.2	Krisenkommunikation	29
3.4.1.4	Krisenstabsraum	30
3.4.2	Krisenbewältigung	30
3.4.2.1	Lagefeststellung	31
3.4.2.2	Lagebeurteilung, Entscheidung und Maßnahmenumsetzung	32
3.4.2.3	Kontrolle	32
3.4.2.4	Sicherstellung der betrieblichen und dienstlichen Kontinuität	32
3.4.2.5	Rückkehr zum Normalbetrieb	32
3.4.2.6	Dokumentation der Krisenbewältigung	32
3.4.3	Nachbereitung	33
3.4.4	Übungen	33
3.5	Phase 5: Evaluierung des Risiko- und Krisenmanagements	34

Anhang

I.	Literaturverzeichnis	36
II.	Abkürzungen	38
III.	Begriffe	39

IV. Gefahrenliste – Anhaltspunkte zu Art, Exposition, Intensität, Wirkungen und möglichen Ansprechpartnern 44

V. Checklisten 47

V.1	Vorbeugende Maßnahmen	48
V.1.1	Risiko- und Krisenmanagement – Allgemein	48
V.1.2	Gelände, Gebäude, Anlagen – Hochwasser	49
V.1.3	Gelände, Gebäude, Anlagen – Erdbeben	51
V.1.4	Gelände, Gebäude – Stürme	51
V.1.5	Gelände, Gebäude – Vorsätzliche Handlungen mit kriminellem und/oder terroristischem Hintergrund	52
V.1.6	Anlagen und Geräte – Stromversorgung	54
V.1.7	Anlagen und Geräte – Informationstechnologie	56
V.1.8	Anlagen und Geräte – Kommunikationstechnologie	57
V.2	Revision des Krisenmanagements	58
V.2.1	Allgemeine Organisation	58
V.2.2	Personal – Allgemein	62
V.2.3	Krisenmanagement – Pandemieplanung (insbesondere Influenzapandemie)	64
V.3	Krisenbewältigung	65
V.3.1	Allgemeine Verfahren in der Krise	65
V.3.2	Spezielle Verfahren in der Krise	68
V.4	Nachbereitung	72
V.5	Übungen	73
V.6	Auswahl und Ausstattung eines Krisenstabsraumes	75

VI. Beispiel Risikoanalyse 79

VI.1	Kritikalitätsanalyse	79
VI.2	Gefahrenanalyse und Szenarioentwicklung	80
VI.3	Verwundbarkeitsanalyse	81
VI.4	Risikoermittlung	82
VI.5	Risikovergleich	85

Zusammenfassung

Der Leitfaden stellt ein Managementkonzept vor, das Betreiber Kritischer Infrastrukturen, das heißt Unternehmen und Behörden, bei der strukturierten Ermittlung von Risiken, der darauf basierenden Umsetzung vorbeugender Maßnahmen sowie dem effektiven und effizienten Umgang mit Krisen unterstützt. Dabei werden Kritische Infrastrukturen als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“, verstanden.

Die jüngere Vergangenheit hat gezeigt, dass Infrastrukturen durchaus Schaden erleiden und Beeinträchtigungen kritischer Prozesse weitreichende soziale und ökonomische Folgen haben können.

Erhebliche Schäden können insbesondere durch

- Naturereignisse,
- technisches und/oder menschliches Versagen,
- vorsätzliche Handlungen mit terroristischem oder sonstigem kriminellen Hintergrund
- sowie Kriege hervorgerufen werden.

Für Betreiber Kritischer Infrastrukturen ist es wichtig, solche Ursachen zu erkennen und sich darauf einzustellen. Das bedeutet, Risiken im Vorfeld von Ereignissen so weit wie möglich zu erfassen, zu mindern und sich auf unvermeidbare Krisenfälle bestmöglich vorzubereiten. Eine solche Vorgehensweise trägt zur Sicherung der Existenz über das Krisenereignis hinaus bei und leistet damit für Unternehmen einen Beitrag zur Wertschöpfung sowie zur Einhaltung bestehender rechtlicher Bestimmungen und unterstützt Behörden im Rahmen ihrer Daseinsvorsorge.

Das in diesem Leitfaden vorgestellte Konzept zum Risiko- und Krisenmanagement besteht aus fünf Phasen. Hierzu zählen die Vorplanung zur Etablierung eines Risiko- und Krisenmanagements, die Beschreibung grundsätzlicher Aspekte einer Risikoanalyse, Ausführungen zu vorbeugenden Maßnahmen, die Darstellung der Aspekte eines robusten Krisenmanagements sowie Hinweise zur Evaluierung des Risiko- und Kri-

senmanagements in einer Einrichtung. Als Einrichtung werden Unternehmen beziehungsweise Behörden verstanden, die in Anlehnung an die oben gegebene Definition zu den Kritischen Infrastrukturen gezählt werden können.

Phase 1 – Vorplanung in der Einrichtung

Eine gründliche Vorplanung schafft die Voraussetzungen für eine erfolgreiche Umsetzung des Leitfadens oder Bestandteilen davon.

Im Vorfeld der Umsetzung des Leitfadens sollten grundsätzliche Fragen geklärt werden. Hierzu zählen insbesondere die Verankerung eines Risiko- und Krisenmanagements in der Einrichtung, die Festlegung von Zuständigkeiten im Rahmen der Umsetzung, die Freistellung von Ressourcen, die Klärung rechtlicher Verpflichtungen zur Einrichtung eines Risiko- und Krisenmanagements sowie die Festlegung von strategischen Schutzziele, die im Unternehmen beziehungsweise in der Behörde erreicht werden sollen.

Phase 2 – Risikoanalyse

Eine Risikoanalyse verschafft der Einrichtung einen strukturierten Überblick über ihre einzelnen Prozesse, über die Gefahren, denen diese Prozesse ausgesetzt sein können und über die Verwundbarkeit, die den Prozessen innewohnt. Die Verknüpfung dieser Informationen führt zu einer Risikoanalyse für alle betrachteten Prozesse bezogen auf einzelne Szenarien.

Die ermittelten Risikoinformationen können miteinander verglichen werden. Hieraus entsteht ein übersichtliches Risikobild, aus dem Risikoschwerpunkte herausgelesen werden können.

Die Ergebnisse der Risikoanalyse werden mit den zuvor aufgestellten strategischen Schutzziele abgeglichen und hierdurch bewertet. Können die strategischen Schutzziele in weiten Teilen nicht erreicht werden, müssen konkrete Maßnahmen umgesetzt werden, die bestehende Risiken mindern und den Umgang mit Krisenereignissen erleichtern.

Phase 3 – Vorbeugende Maßnahmen und Strategien

Vorbeugende Maßnahmen tragen zur Minderung von Risiken für Prozesse und damit für die Dienstleistung beziehungsweise die Produktion bei. Sie heben die Krisenschwelle in der Einrichtung an und können hierdurch sowohl die Anzahl als auch die Intensität krisenhafter Ereignisse reduzieren. Vorbeugende Maßnahmen haben das Ziel, Komponenten in der Einrichtung aktiv zu schützen oder Redundanzen zu schaffen.

Zusätzlich besteht die Möglichkeit, Risiken zu vermeiden, überzuwälzen oder bewusst zu akzeptieren. Hierbei ist es wichtig zu erkennen, dass eine Risikovermeidung in den meisten Fällen Einschränkungen der Flexibilität des Unternehmens beziehungsweise der Behörde nach sich ziehen wird. Eine Risikoüberwälzung mindert physische Risiken nicht, sondern regelt lediglich einen finanziellen Ausgleich. Dieser kann im Einzelfall deutlich unterhalb des entstandenen Schadens liegen.

Phase 4 – Krisenmanagement

Kommt es trotz vorbeugender Maßnahmen zu schwerwiegenden Schäden jeglicher Art für das Unternehmen oder die Behörde, sollte ein Krisenmanagement eine Sonderorganisation zur Bewältigung dieser Situation bereitstellen.

Das Krisenmanagement beinhaltet eine besondere Aufbau- und Ablauforganisation, die sich von der Organisation im Normalbetrieb unterscheidet. Die Entscheidungskompetenz wird in der Krise gebündelt, um möglichst ohne Zeitverzögerung adäquat auf eine Situation reagieren zu können. Hierdurch können die Auswirkungen einer Krise reduziert werden und die Zeitspanne zur Wiederherstellung des Normalzustandes kann verkürzt werden.

Phase 5 – Evaluierung des Risiko- und Krisenmanagements

Die Evaluierung bezieht sich auf alle Phasen des Risiko- und Krisenmanagements, also sowohl auf die Prüfung der in der Vorplanung festgelegten Regelungen, die Prüfung der Aktualität des aufgestellten Risikoprofils, die Prüfung der umgesetzten vorbeugenden Maßnahmen auf ihre Wirksamkeit sowie die Prüfung des Krisenmanagements auf seine Effektivität. Eine solche Evaluierung sollte regelmäßig erfolgen.

Zusätzliche Evaluierungen können notwendig werden

- nach der Umsetzung von Maßnahmen,
- nach einer Erweiterung/Veränderung der Einrichtung sowie
- bei einer Änderung der Gefahrenlage.

Im Anhang des Leitfadens befinden sich ein Beispiel zur Umsetzung einer Risikoanalyse sowie Checklisten zur Überprüfung der durchgeführten Maßnahmen in der Einrichtung.

Ansprechpartner zu diesem Leitfaden:

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Abteilung II
Notfallvorsorge, Kritische Infrastrukturen
Provinzialstraße 93
53127 Bonn
<http://www.bbk.bund.de>

1

Einleitung

Infrastrukturen sind essenzieller Bestandteil unserer hoch entwickelten Gesellschaft. Wir sind alle in unserem täglichen Leben auf die Verfügbarkeit von Infrastrukturen angewiesen und verlassen uns darauf, dass sie uneingeschränkt genutzt werden können.

Seit 1997 setzt sich der Bund mit dem Schutz sogenannter Kritischer Infrastrukturen auseinander, um den Bedarf zusätzlicher Schutzmaßnahmen zu analysieren. Dabei werden Kritische Infrastrukturen als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“¹, verstanden.

Die stetige Verfügbarkeit Kritischer Infrastrukturen ist durch Naturgefahren, technisches oder menschliches Versagen sowie vorsätzliche Handlungen mit terroristischem oder kriminellem Hintergrund bedroht. Im Falle einer kriegerischen Auseinandersetzung in Deutschland würden Infrastrukturen enormen Schaden erleiden.

Die Gefahrensituation hat sich in den vergangenen Jahren stetig verändert. Es gibt Anzeichen, dass sowohl im Bereich der Naturgefahren als auch im Hinblick auf vorsätzliche Handlungen mit terroristischem oder kriminellem Hintergrund eine Zunahme von extremen Ereignissen zu verzeichnen ist. Dies stellt die Gesellschaft vor neue Herausforderungen.

Neben der Gefahrensituation verändert sich auch die Verwundbarkeit von Infrastrukturen. Die meisten Infrastruktursysteme sind heute in irgendeiner Form miteinander verknüpft. Beeinträchtigungen in einem Bereich können sich in andere Standorte, Branchen oder Sektoren fortpflanzen und sich damit weit über das ursprüngliche Schadensgebiet auswirken.

Die finanziellen und personellen Ressourcen, die den Betreibern zum Schutz ihrer Infrastruktursysteme zur Verfügung stehen, sind begrenzt. Daher ist ein effizienter und effektiver Einsatz dieser Ressourcen besonders wichtig. Voraussetzung hierfür ist die Kenntnis der Gefahren und Risiken und die Möglichkeit, Risiken vergleichen und bewerten zu können, um Risikoschwerpunkte aufzuzeigen. Darauf aufbauend können dann zielgerichtete Schutzmaßnahmen umgesetzt werden.

Der hier vorliegende Leitfaden „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden“ ist als Gemeinschaftsprodukt von Akteuren aus Unternehmen, Behörden und einer wissenschaftlichen Einrichtung entstanden. Der Leitfaden wirkt sektorübergreifend und ist als Selbstanalysewerkzeug für Unternehmen und Behörden konzipiert.

Er kombiniert theoretische Grundlagen zum Risiko- und Krisenmanagement mit praktischen Listen und einem Beispiel zur Risikoanalyse, mit dem Ziel, Unternehmen und Behörden in die Lage zu versetzen, selbstständig oder mit externer Hilfe ein effektives und effizientes Risiko- und Krisenmanagement auf- beziehungsweise auszubauen.

Das übergeordnete Ziel aus Bundessicht ist hierbei die Minderung der Auswirkungen extremer Ereignisse auf Kritische Infrastrukturen sowie die Verbesserung des Umgangs mit zu erwartenden Krisen.

¹ Definition Kritischer Infrastrukturen des Arbeitskreises KRITIS (AK KRITIS) im Bundesministerium des Innern (BMI) vom 17. November 2003.

2 Grundlagen zu Kritischen Infrastrukturen

2.1 Sektoren

Unternehmen und Behörden im Sinne der in der Einleitung genannten Definition Kritischer Infrastrukturen finden sich überwiegend in den folgenden Sektoren:

- Energie (Strom, Mineralöl, Gas)
- Versorgung (Wasser, Lebensmittel, Gesundheit, Notfallversorgung)
- Informations- und Kommunikationstechnologie
- Transport und Verkehr
- Gefahrstoffe (Chemieindustrie und Biostoffe)
- Banken und Finanzen
- Behörden, Verwaltung, Justiz
- Medien, Großforschungseinrichtungen und Kulturgüter

2.2 Rahmenbedingungen und Eigenschaften Kritischer Infrastrukturen

Beeinträchtigungen Kritischer Infrastrukturen zeigten in der jüngeren Vergangenheit zwei wiederkehrende Merkmale auf.

Merkmal 1: Es kam zu weiträumigen Einwirkungen insbesondere von Naturgefahren auf Infrastrukturen. Dies war mit regionalen, überregionalen, landes- oder europaweiten Beeinträchtigungen verbunden (Beispiel: Elbeflut im Jahr 2002 oder Orkan Kyrill im Jahr 2007).

Merkmal 2: Lokale Störungen oder Schäden führten zu Beeinträchtigungen, die vereinzelt weit über das ursprüngliche Schadensgebiet hinauswuchsen, da Vernetzungen und Verknüpfungen räumliche Grenzen und Systemgrenzen überbrückten (Beispiel: Abschaltung einer Stromleitung über die Ems im Jahr 2006, die zu Stromausfällen in Teilen von Europa führte).

Im Folgenden werden die Kernbestandteile veränderter und sich weiterhin verändernder Rahmenbedingungen und Eigenschaften analysiert, um die Basis zur Entwicklung eines Risiko- und Krisenmanagements in diesem Leitfaden zu erstellen.

2.2.1 Veränderung der Gefahrenlage

Beeinträchtigungen kritischer Prozesse von Infrastruktursystemen können weitreichende soziale und ökonomische Folgen nach sich ziehen. Anhand der folgenden Beispiele kann zwar kein eindeutiger Trend zur Verschärfung der Gefahrenlage abgeleitet werden, dennoch bestätigen diese Beispiele die Notwendigkeit eines nachhaltigen Schutzes Kritischer Infrastrukturen.

Beispiel wetterbedingte Extremereignisse

Extremereignisse können sich unmittelbar auf Infrastruktursysteme auswirken. Belastbare Aussagen zur Veränderung wetterbedingter Extremereignisse aufgrund des Klimawandels können in Deutschland derzeit noch nicht getroffen werden. Hierzu reichen die bisher gesammelten Informationen zur Klimaerwärmung und ihren Auswirkungen in Deutschland nicht aus. Einige Trends, beispielsweise die Zunahme von starken Niederschlägen, zeichnen sich jedoch in Messdaten ab. Diesem Muster folgen die Hochwasser an der Oder 1997, der Elbe im Jahr 2002 oder im Alpenraum 2005.²

Beispiel Gesundheitsgefahren (Influenzapandemie)

Im letzten Jahrhundert sind mehrere Influenzapandemien aufgetreten, darunter eine schwerwiegende im Jahr 1918 (Spanische Grippe) mit weltweit mehr als 50 Millionen Todesfällen. Heute geht man davon aus, dass die Entwicklung eines neuen, für den Menschen sehr gefährlichen Virus durch Mutationen eine Frage der Zeit ist. Eine Influenzapandemie würde sich über die internationalen Verkehrsknotenpunkte auch in Deutschland ausbreiten. Ihre Auswirkungen würden alle Lebensbereiche und damit auch sämtliche Unternehmen und Behörden bedrohen. Eine Pandemie kann dabei nicht nur eine veränderte Nachfrage nach Produkten oder Leistungen bewirken, sondern auch die Infrastrukturen der Wirtschaft und der Gesellschaft insgesamt gefährden.

² Rahmstorf u. a. 2006, Seite 70.

Eine Vielzahl von Ressourcen und Dienstleistungen könnte nicht mehr oder nur noch sehr eingeschränkt zur Verfügung stehen. Aufgrund der gegenseitigen Abhängigkeiten kann dies zu einem Dominoeffekt führen, der auch große Teile der Funktionen von Staat, Wirtschaft und Gesellschaft lähmen könnte.³ Modellberechnungen gehen für Deutschland von einer Erkrankungsrate von 15–50 Prozent aus.⁴ Neben unmittelbar erkrankten Mitarbeitern würden auch solche Mitarbeiter nicht ihre Arbeit aufnehmen können, die erkrankte Familienmitglieder pflegen oder aus Angst vor Ansteckung zu Hause bleiben, wodurch sich die Abwesenheitsquote deutlich erhöhen würde.

Beispiel internationaler Terrorismus

Der internationale Terrorismus organisiert sich in losen Netzwerkstrukturen. Die einzelnen Netzwerkbereiche unterliegen nur noch gemeinsamen Zielvorstellungen, agieren jedoch weitgehend unabhängig und ohne zentrale Befehlsstruktur. Solche losen Netzwerke sind in der Lage, unerkannt, flexibel und schnell zu agieren.⁵ Anschläge auf Infrastruktursysteme in Deutschland sind nicht auszuschließen. Im Jahr 2006 sind Anschläge auf zwei Regionalbahnen der Deutschen Bahn aus technischen Gründen fehlgeschlagen. Im Jahr 2007 konnte ein geplanter Anschlag auf mehrere US-Einrichtungen in Deutschland frühzeitig aufgedeckt und verhindert werden.

Beispiel Informationstechnologie

Fast täglich ist in den Medien von Angriffen durch Hacker oder Industrie- und Wirtschaftsspionage zu lesen. Doch neben diesen Gefahren können einfaches menschliches Versagen bei der Nutzung von Informationstechnik oder Fehlfunktionen in Hard- und Software zu erheblichen Auswirkungen und Schäden in Kritischen Infrastrukturen führen. Beispiel dafür ist der großflächige Stromausfall in den USA und Kanada im Jahr 2003, bei dem ein Fehler in der Prozessleittechnik eine wesentliche Rolle spielte. Ein weiteres Beispiel ist der Zusammenbruch des gesamten EC-Kartensystems in der Schweiz im Jahr 2000, der aus einem Fehler in einem Rechenzentrum resultierte.

2.2.2 Sozioökonomische Rahmenbedingungen

Steigende Abhängigkeit

Die Abhängigkeit der Unternehmen und Behörden von externen Dienstleistungen oder Produkten steigt. Einen hohen Stellenwert nimmt hierbei die Stromversorgung ein. Nahezu alle Dienstleistungen stützen sich unmittelbar oder mittelbar auf eine funktionierende Stromversorgung ab.

Subjektive Risikowahrnehmung

Unternehmen und Behörden investieren viel in die Sicherheit ihrer Einrichtungen und verlassen sich darauf, dass diese Investitionen effektiv wirken. Die positive Wirkung von Sicherheitsmaßnahmen lässt sich häufig jedoch nicht objektiv quantifizieren. Stattdessen werden lange Phasen ohne Ereignisse mit krisenhaften Auswirkungen für das Unternehmen oder die Behörde als Bestätigung der Effektivität der umgesetzten Maßnahmen gewertet. Dies kann dazu verleiten, dass potenzielle Gefahren und verwundbare Bereiche nicht mehr wahrgenommen werden.

Ferner werden in der Praxis häufig Risiken identifiziert, die beeinflussbar beziehungsweise kontrollierbar und deren kausale Ursache-Wirkungs-Ketten transparent erscheinen.⁶ Andere Risiken werden teilweise bewusst oder unbewusst ausgeblendet. Die möglichen Auswirkungen solcher Risiken werden bei der Umsetzung vorbeugender Maßnahmen nicht berücksichtigt.

Demografische Veränderung

Die Veränderungen der Altersstruktur der Gesellschaft sowie migrationsbedingte Veränderungen der Bevölkerungsdichte innerhalb Deutschlands schaffen neue Anforderungen an Kritische Infrastrukturen und beeinflussen damit auch sicherheitsrelevante Aspekte. Ein sinkender Wasserbedarf und die damit verbundene Reduzierung der Wasserabgabe an den Endverbraucher können beispielsweise hygienische Probleme in Wasserversorgungsanlagen hervorrufen.

Veränderung ökonomischer Rahmenbedingungen⁷

Veränderungen im Marktgeschehen, wie sie etwa durch die Liberalisierung der Märkte und die Privatisierung ehemals staatlicher Infrastrukturbetriebe stattfinden, können das Sicherheitsniveau und die Investitionen in Sicherheitsmaßnahmen beeinflussen. Die Wettbewerbssituation und der damit verbundene Preisdruck schaffen Rahmenbedingungen, in denen sicherheitsrelevante Vorkehrungen wie etwa redundante Systeme oder andere Sicherheitspuffer reduziert werden. Die Anforderungen von Regelwerken werden zwar weitgehend eingehalten. Immer genauere Berechnungsverfahren ermöglichen jedoch, Spielräume weiter auszunutzen und Sicherheitspuffer zu reduzieren. Diese Puffer können dann insbesondere in Krisensituationen fehlen.

³ Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2007.

⁴ Robert Koch Institut 2007b, Seite 4.

⁵ Vgl. Lewis 2006, Seite 1.

⁶ Dost 2006.

⁷ Vgl. International Risk Governance Council 2006, Seiten 11–17.

2.2.3 Besondere Eigenschaften Kritischer Infrastrukturen

Brancheninterne Vernetzung

Infrastrukturdienstleistungen werden über physische, virtuelle oder logische Netze in die Fläche gebracht. Diese Netze nehmen an Größe und Komplexität zu. Es bilden sich Knotenpunkte aus, die neuralgische Punkte darstellen und deren Beeinträchtigung zu regionalen, überregionalen, landesweiten oder gar weltweiten Ausfällen führen. Netze dieser Art finden sich insbesondere in der Stromversorgung, der Informations- und Kommunikationstechnologie sowie der Wasser- und Gasversorgung.

Branchenübergreifende Verknüpfungen (Interdependenz)

Infrastruktursysteme sind durch einen hohen Verknüpfungsgrad gekennzeichnet. Diese Entwicklung hat durch die explosionsartige Verbreitung der Informationstechnologie in den letzten 15 Jahren an Dynamik gewonnen. Neben einer Steigerung der Effizienz von Versorgungsprozessen führen Verknüpfungen zu Interdependenzen, deren Ausmaß häufig nur qualitativ zu erfassen ist. Viele physische, virtuelle und logische Abhängigkeiten stellen sich erst im Ereignisfall, also bei Ausfall, heraus. Der hohe Grad gegenseitiger Abhängigkeiten kann zu kaskadenartigen Ausfällen führen.⁸ Gleichzeitig reichen immer kleinere Störungen aus, um in komplexen Systemen dramatische Folgen zu verursachen (Verwundbarkeitsparadoxon).⁹

Abbildung 1 verdeutlicht die gegenseitigen Abhängigkeiten (Interdependenzen) ausgewählter Kritischer Infrastrukturen. Hierbei werden zunächst nur unmittelbare Abhängigkeiten berücksichtigt, die zwischen einzelnen Sektoren beziehungsweise Branchen bestehen.

Veränderte technologische Rahmenbedingungen

Die technologische Entwicklung insbesondere im Bereich der Informationstechnologie vollzieht sich in einem rasanten Tempo. Neuerungen können häufig nur in Teilbereichen eingeführt werden und führen zu einer Parallelexistenz von alten Bauteilen und Prozeduren neben neuen Komponenten. Durch ungenügend getestete, unausgereifte und fehlerhafte neue Hard- und Software, inkompatible Systeme, ungenügend geplante Migrationsvorhaben oder ein nicht ausreichend für die neuen Komponenten geschultes Personal entstehen Sicherheitslücken und Schwachpunkte, welche unter Umständen zu einem Versagen des Gesamtsystems führen können.

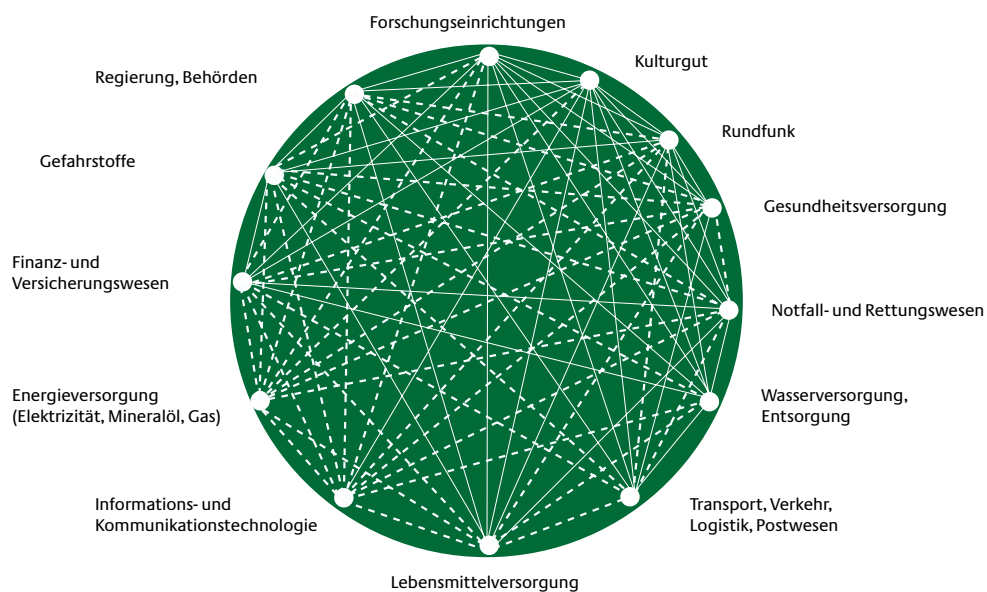
Schadenstypen

Im Bereich Kritischer Infrastrukturen gibt es viele verschiedene Schadensarten. Sie reichen von tatsächlichen physischen Schäden an Personen oder Sachschäden über ökonomische Schäden, psychische Schäden und Verunsicherung bis hin zum Vertrauensverlust der Bevölkerung in die politische Führung.

⁸ Vgl. Lewis 2006, Seite 57.

⁹ Rosenthal 1992, Seite 74 f.

Abbildung 1: Interdependenzen ausgewählter Kritischer Infrastrukturen



2.3 Rechtliche Vorgaben zum Risiko- und Krisenmanagement

Übergreifende rechtliche Vorgaben zum kontrollierten Umgang mit Risiken und Krisen existieren derzeit für Aktiengesellschaften und große Gesellschaften mit beschränkter Haftung (GmbH). Daneben gibt es Bestimmungen in der Kreditwirtschaft, die sich faktisch verpflichtend auf Einrichtungen im Finanzwesen auswirken (Beispiel: Mindestanforderungen an das Risikomanagement – MaRisk). Der Begriff der Unternehmenssicherheit umfasst in diesen Regelungen den Schutz von Personen und materiellen Dingen wie Gebäuden und Anlagen sowie die Aufrechterhaltung des Geschäftsbetriebs in jeglicher Art von Störung bis hin zur Krise – ob Börsenkrise, Naturereignis oder terroristischer Anschlag.

Mit dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurde das Aktiengesetz um die Verpflichtung ergänzt, ein Überwachungssystem im Sinne eines betrieblichen Risikomanagements einzurichten. Diese Regelung bezieht sich nur auf Aktiengesellschaften, strahlt aber in ihrer Anwendung auch auf Kommanditgesellschaften auf Aktien (KGaA) und große GmbHs, insbesondere solche mit mitbestimmten oder fakultativem Aufsichtsrat, aus.

Marktrisiken sind im Zusammenhang mit dem KonTraG eine häufig behandelte Materie. Sicherheitsrisiken¹⁰ und Naturrisiken werden hingegen oft unterschätzt, obwohl das KonTraG alle existenzgefährdenden Risiken eines Unternehmens umfasst. Die Vorstände von Aktiengesellschaften, deren Aufsichtsräte und die Abschlussprüfer sind nach § 91 Abs. 2 AktG rechtlich gebunden, „... geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkannt werden“. Allerdings gibt es keine Methode, welche vom Gesetzgeber als Maßstab angesetzt wurde. Die konkrete Ausgestaltung bleibt somit dem einzelnen Unternehmen vorbehalten. Das interne Überwachungssystem sollte jedoch so eingerichtet sein, dass gefährdende Entwicklungen rechtzeitig, also zu einem Zeitpunkt erkannt werden, an dem noch geeignete Maßnahmen zur Sicherung des Fortbestandes der Gesellschaft ergriffen werden können.

Die Unternehmensleitung hat somit eine gesetzliche Pflicht, ein funktionsfähiges Risikomanagementsystem in ihrem Unternehmen zu implementieren. Unterlässt sie es, so kann ihr unter Umständen der Bestätigungsvermerk des Abschlussprüfers verweigert werden. Der Wirtschaftsprüfer steht somit in der Pflicht zu prüfen, ob der Vorstand für ein angemessenes Risikomanagement gesorgt hat (§ 317 Abs. 4 HGB). Dazu gehören neben einer Bewertung der Gefahren auch eine Auswertung von Betriebsunterbrechungen, die Umsetzung systematischer Maßnahmen zur Vermeidung von Betriebsunterbrechungen sowie die Aufstellung und regelmäßige Pflege eines Notfallplans.¹¹ Da die Einrichtung eines Überwachungs-

systemes zu den allgemeinen Leistungspflichten eines Vorstandes gemäß § 76 Abs. 1 AktG gehört, kann der Vorstand im Schadensfall haftungsrechtlich nach § 93 Abs. 2 AktG zu Schadensersatz verpflichtet werden, wenn es zu einer haftungsbe gründenden Sorgfaltspflichtverletzung gekommen ist.

Doch nicht nur das KonTraG, auch das harmonisierte europäische Versicherungsrecht Solvency II verlangt ein Risikomanagement für Unternehmen unter Berücksichtigung aller Risiken, mit denen Versicherer konfrontiert werden können. Indem mögliche Risiken in die Versicherungsbedingungen aufgenommen werden, kann der Versicherer die Gewährung von Versicherungsschutz von Schadensvorsorgemaßnahmen und damit implizit auch von einem Risikomanagement abhängig machen. Eine Zuwiderhandlung gegen die Versicherungsbedingungen führt nach § 6 Abs. 1 VVG zu einem Deckungsschutzverlust.

Ebenso verlangt die Baseler Eigenkapitalvereinbarung (Basel II), die Bankkrisen verringern soll, explizit, im Rahmen der Kreditvergabe neben der Betrachtung von Markt- und Kreditrisiken, operationelle Risiken der Banken zu berücksichtigen. Auch wenn sich Basel II nur auf die Risiken der Kreditinstitute bezieht, ist es möglich, dass das Erfordernis einer Risikodarstellung von den Banken an die Unternehmen weitergereicht wird, das heißt ein Risikomanagement eine Voraussetzung für die Kreditvergabe darstellt. Werden alle Risiken in einem Risikomanagement hinreichend bedacht und einbezogen, so kann sich dies positiv auf die Erlangung günstiger Darlehenskonditionen auswirken, da dadurch die Kreditausfallwahrscheinlichkeit für die Bank gemindert wird.

¹⁰ Siehe hierzu Bundesministerium des Innern 2005.

¹¹ Vgl. Bockslaff 1999, Seite 109.

3 Risiko- und Krisenmanagement

zum Schutz Kritischer Infrastrukturen

Das vorgestellte Konzept zum Risiko- und Krisenmanagement bildet eine systematische Vorgehensweise ab und besteht aus fünf Phasen. Diese beschreiben den notwendigen Umfang eines prozessbezogenen Risiko- und Krisenmanagements in einem Unternehmen oder einer Behörde. Hierzu zählen zunächst eine Vorplanung zur Etablierung eines Risiko- und Krisenmanagements (Phase 1), eine Risikoanalyse (Phase 2), die Beschreibung vorbeugender Maßnahmen (Phase 3), der Aufbau eines Krisenmanagements (Phase 4) sowie die regelmäßige Evaluierung der Phasen 1 bis 4 (Phase 5). Abbildung 2 veranschaulicht dieses Konzept und bereitet den Ablauf grafisch auf.

Das hier beschriebene Risiko- und Krisenmanagement richtet sich nach einem allgemeinen „Plan-Do-Check-Act-Managementzyklus“ (PDCA). Hierdurch besteht die Möglichkeit der Integration in vorhandene Managementstrukturen, beispielsweise in das Qualitätsmanagement, das bestehende Risiko- und Krisenmanagement oder das Prozessmanagement der Einrichtung. Als Einrichtung werden Unternehmen beziehungsweise Behörden verstanden, die in Anlehnung an die in der Einleitung gegebenen Definition zu den Kritischen Infrastrukturen gezählt werden können.

Abbildung 2: Risiko- und Krisenmanagementkonzept in fünf Phasen¹²

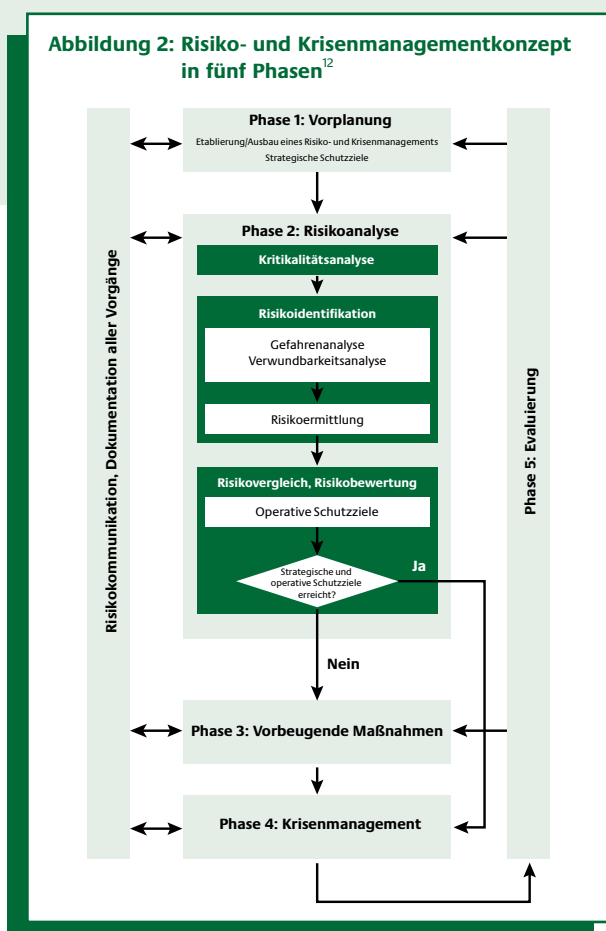
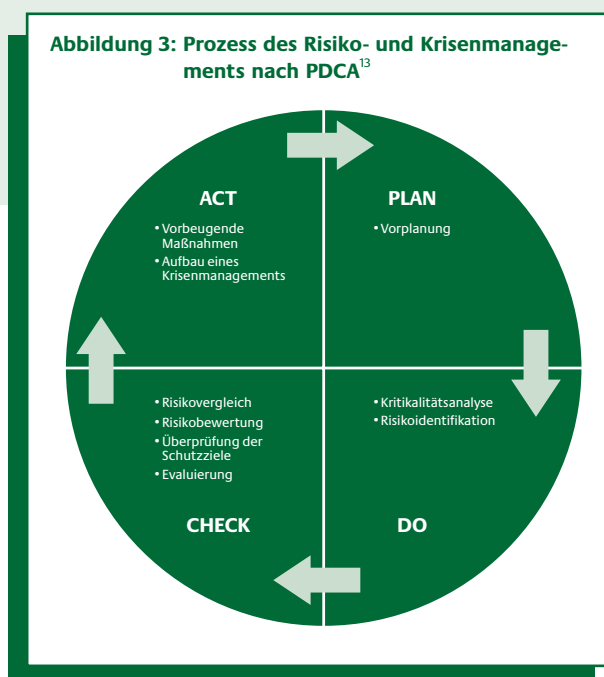


Abbildung 3: Prozess des Risiko- und Krisenmanagements nach PDCA¹³



¹² Vgl. Australian/New Zealand Standard 2004, Seite 13 sowie Trauboth 2002, Seite 23.

¹³ Vgl. Gesellschaft für Anlagen- und Reaktorsicherheit 2007, Seite 21.

3.1 Phase 1: Vorplanung in der Einrichtung

Eine gründliche Vorplanung schafft die Voraussetzungen für eine erfolgreiche Etablierung eines Risiko- und Krisenmanagements in einem Unternehmen oder einer Behörde.

Im Vorfeld der Anwendung des Leitfadens sollten grundsätzliche Fragen geklärt werden. Hierzu zählen insbesondere die Etablierung des Risiko- und Krisenmanagements durch die Leitung der Einrichtung, die Akzeptanz der Vorgehensweise, die Festlegung von Zuständigkeiten im Rahmen der Etablierung, die Schaffung von Ressourcen für die Etablierung sowie die Festlegung strategischer Schutzziele für die Einrichtung.

3.1.1 Etablierung des Risiko- und Krisenmanagements

Die Leitung initiiert den Auf- oder Ausbau eines Risiko- und Krisenmanagements und verdeutlicht die Ziele, die sie damit verfolgt. Auf den Arbeitsebenen wird das Risiko- und Krisenmanagement umgesetzt und angewendet. Die Belegschaft wird in die Etablierung eingebunden.

Der Schaffung eines Risikobewusstseins in der gesamten Einrichtung – durch eine konsequente und transparente Risikopolitik – muss besondere Aufmerksamkeit geschenkt werden, da die Qualität eines Risikomanagements mit der Akzeptanz und Motivation der Mitarbeiter steht und fällt.

3.1.2 Zuständigkeiten bei der Etablierung

Die Etablierung eines Risiko- und Krisenmanagements sollte von einem fachlichen Leiter gesteuert werden. Bei diesem liegt die inhaltliche Federführung. Im Bedarfsfall stimmt er sich mit der Leitung der Einrichtung ab. Es ist sinnvoll, den fachlichen Leiter aus dem Unternehmen beziehungsweise der Behörde auszuwählen.

Grundlegende Entscheidungen, die sich aus dem Aufbau oder der Ergänzung des Risiko- und Krisenmanagements ergeben, werden von der Einrichtungsleitung getroffen. Dies gilt insbesondere für die Bewilligung finanzieller und personeller Ressourcen.

Die Zuständigkeiten, die im Rahmen der Anwendung des Risiko- und Krisenmanagements zu regeln sind, können im Vorfeld nur unzureichend abgeschätzt werden. Diese Zuständigkeiten werden im Verlauf der Umsetzung festgelegt.

3.1.3 Ressourcen zur Etablierung

Der Bedarf zur Etablierung eines Risiko- und Krisenmanagements wird im Vorfeld abgeschätzt. Sofern es als notwendig erachtet wird, kann eine interdisziplinär besetzte Arbeitsgruppe aus dem Personalbestand der Einrichtung zusammengestellt werden, die den fachlichen Leiter unterstützt und einzelne Arbeitspakete übernimmt. Es ist von Vorteil, wenn die Mitglieder der Arbeitsgruppe einen detaillierten Einblick in die Struktur des Unternehmens beziehungsweise der Behörde haben. Die verschiedenen Linienhierarchien in der Einrichtung sollten in der Arbeitsgruppe abgebildet werden.

Sofern Expertise zum Thema Risiko- und Krisenmanagement fehlt, kann das eigene Personal geschult oder die fehlende Expertise durch externe Dienstleistungsunternehmen ergänzt werden.

Der Ressourcenbedarf, der sich aus der Anwendung des Risiko- und Krisenmanagements für die Einrichtung ergibt, wird im Verlauf des Projektes ermittelt.

3.1.4 Klärung der rechtlichen Verpflichtungen

Zur Vorplanung gehört die Klärung der rechtlichen Verpflichtungen zur Etablierung eines Risiko- und Krisenmanagements.

3.1.5 Strategische Schutzziele

Bei Etablierung eines Risiko- und Krisenmanagements sind strategische Schutzziele zu formulieren. Sie definieren prozessübergreifend, was durch das Risiko- und Krisenmanagement erreicht werden soll.

Schutzziele werden maßgeblich von ethischen, operativen, technischen, finanziellen, gesetzlichen, sozialen und umweltbezogenen Aspekten beeinflusst.¹⁴ Sie weisen folgende Merkmale auf:

- Sie beschreiben einen Sollzustand.
- Sie schaffen Lösungsräume für die Umsetzung unterschiedlicher Maßnahmen.
- Sie sind spezifisch, messbar, ausführbar, realistisch und terminiert (= „smart“).

¹⁴ Australian/New Zealand Standard 2004, Seite 15.

Beispiele hierfür sind:

- der bestmögliche Schutz des Personals und sonstiger Anwesenden (Beispiel: Kunden),
- die Aufrechterhaltung der Funktionsfähigkeit der Einrichtung auch in Extremsituationen,
- die Erfüllung gesetzlicher Auflagen,
- die Abwendung hoher wirtschaftlicher Schäden und
- die Abwendung eines potenziellen Imageschadens.

3.1.6 Risikokommunikation

Im Allgemeinen betrifft Risikokommunikation „alle Kommunikationsprozesse, die sich auf die Identifizierung, Analyse, Bewertung sowie das Management von Risiken und die dafür notwendigen Interaktionen zwischen den Beteiligten beziehen“¹⁵. Risikokommunikation ist die Plattform von Risikobewusstsein und Risikoakzeptanz in Unternehmen und Behörden. Beide Aspekte sind für ein erfolgreiches Risikomanagement unerlässlich. Im vorliegenden Kontext ist die explizite Unterscheidung von interner und externer Risikokommunikation einer Behörde/eines Unternehmens sinnvoll.

Die interne Risikokommunikation bezieht sich auf alle kommunikativen Interaktionen zu Risikothemen innerhalb der Einrichtung – von der Etablierung des Systems bis hin zur Evaluierung des Risikomanagements. Dabei sollte der Risikokommunikation hinsichtlich der Etablierung besondere Aufmerksamkeit geschenkt werden – der frühzeitige Dialog mit angehenden Verantwortlichen über Gegenstand und Zweck des Risikomanagements ist unentbehrlich. Die gelungene interne Risikokommunikation ist Grundvoraussetzung für eine erfolgreiche externe Risikokommunikation.

Externe Risikokommunikation zielt nicht auf ein bloßes Informieren und Belehren von Medien und Betroffenen, sondern auf einen adressatengerechten Dialog. Dabei muss stets bedacht werden, dass Risikothemen so zu kommunizieren sind, dass keine Missverständnisse zwischen Sender und Empfänger entstehen können. So sind beispielsweise Unterschiede in der Risikowahrnehmung zwischen Experten und Laien empirisch nachgewiesen. Um nicht akzeptablen Resultaten vorzubeugen, sollte Risikokommunikation stets zeitnah, eindeutig, adressatengerecht, konsequent und zuverlässig sein. Die bestimmenden Faktoren der Wirksamkeit jeder Risikokommunikation sind das Vertrauen in die Kommunikationsquelle und die ihr gegenüber empfundene Glaubwürdigkeit.¹⁶

3.2 Phase 2: Risikoanalyse

Eine Risikoanalyse strukturiert und objektiviert die Informationssammlung zu Gefahren und Risiken in Unternehmen und Behörden. Die Risiken werden in diesem Leitfaden auf Prozesse sowie deren Bestandteile bezogen. Sie analysiert verschiedene Prozesse und Prozessbestandteile und macht deren unterschiedliche Risiken für die Einrichtung vergleichbar. Dieser Vergleich ermöglicht die Festlegung von Dringlichkeiten und eine Priorisierung der Maßnahmen, die das Risiko maßgeblich beeinflussen können. Dadurch schafft sie die Grundlage zum effektiven und effizienten Umgang mit begrenzten finanziellen und personellen Ressourcen.

Eine Risikoanalyse im Sinne dieses Leitfadens beantwortet die folgenden Fragen:

- Welche Arten von Gefahren können auftreten?
- Mit welcher Wahrscheinlichkeit treten diese Gefahren an den Standorten der Einrichtung auf?
- Welche Schwachstellen sind vorhanden, die hinsichtlich einer Gefahrenwirkung anfällig sind?

Diese Fragen verdeutlichen, dass in die Analyse des Risikos eines Prozesses beziehungsweise Prozessbestandteils sowohl Gefahreninformationen als auch Aussagen über die Verwundbarkeit des Prozesses beziehungsweise Prozessbestandteils eingehen.

In diesem Leitfaden werden operative Prozesse betrachtet, also Kernprozesse und unterstützende Prozesse, die im weiteren Verlauf jedoch nicht weiter unterschieden werden und daher als Prozesse beziehungsweise Teilprozesse bezeichnet werden. Als Teilprozesse im Sinne dieses Leitfadens werden einzelne Abschnitte von Prozessen verstanden.

Ausgangspunkt der Risikoanalyse ist die Unterteilung des Unternehmens beziehungsweise der Behörde in Prozesse und Teilprozesse. Der Grad der Aufschlüsselung in Teilprozesse wird von der Einrichtung selbst festgelegt. Wird beispielsweise eine Leitwarte als Bestandteil eines Prozesses erkannt, kann diese als Teilprozess definiert werden. Es besteht aber auch die Möglichkeit, die Leitwarte selbst noch einmal in weitere Teilprozesse zu untergliedern. Je detaillierter die Aufschlüsselung durchgeführt wird, desto höher ist der Aufwand im Rahmen einer Risikoanalyse. Mit steigendem Detaillierungsgrad der Teilprozesse wächst aber auch die Aussagekraft einer Risikoanalyse.¹⁷

¹⁵ Jungermann u. a. 1991, Seite 5.

¹⁶ Weiterführende Hinweise zur detaillierten Planung der Risikokommunikation finden sich in Wiedemann u. a. 2000 und Gray u. a. 2000.

¹⁷ Weitere Hinweise zu den Themen Prozesse und Prozessdarstellung finden sich in Gesellschaft für Anlagen- und Reaktorsicherheit 2007.

Abbildung 4: Prozess, Teilprozesse, Risikoelemente

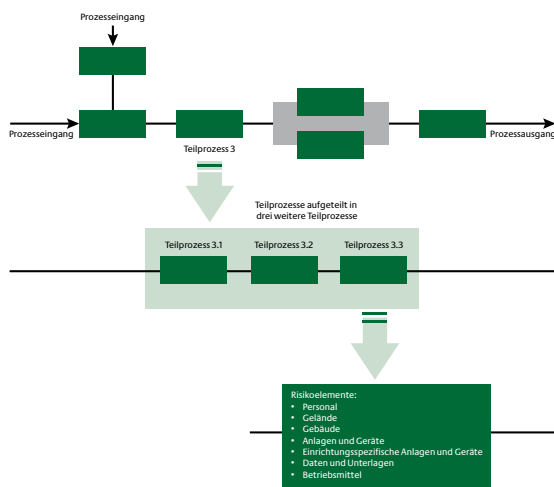


Abbildung 4 zeigt schematisch einen Prozess, dessen Teilprozesse sowie die mögliche Aufteilung eines Teilprozesses in weitere Teilprozesse und deren Bestandteile auf.

Als Bestandteile der Teilprozesse werden die Elemente verstanden, die zur Funktion eines Prozesses beitragen. Diese Elemente werden im Leitfaden als Risikoelemente bezeichnet. Sie sind physische beziehungsweise virtuelle Einzelbestandteile, die Schaden erleiden können, wodurch auch der betrachtete Teilprozess beeinträchtigt würde. In diesem Leitfaden werden die folgenden Risikoelemente berücksichtigt:

- **Menschen (Personal, sonstige Anwesende):**
Alle Anwesenden sind grundsätzlich in ausreichendem Maße vor Gefahrenwirkungen zu schützen beziehungsweise bei drohender Gefahr in Sicherheit zu bringen. Hierfür sind in allen Unternehmen und Behörden Vorkehrungen zu treffen, insbesondere um im Ereignisfall vor dem Eintreffen und nach dem Abzug von Feuerwehr, Rettungsdienst und Polizei den bestmöglichen Schutz für die anwesenden Personen gewährleisten zu können.

Als Risikoelemente im Sinne eines Funktionserhaltes von Teilprozessen sind das Personal und insbesondere das Fachpersonal zu verstehen.

- **Gelände:**
Zum Gelände gehören alle freiliegenden Verkehrs-, Lager- und Parkflächen, Grünanlagen sowie betriebsnotwendige Flächen.
- **Gebäude:**
Zu den Gebäuden zählen alle ober- und unterirdischen baulichen Strukturen wie Produktions-, Lager- und Verwaltungsgebäude sowie Parkgaragen.

■ Anlagen und Geräte:

Anlagen und Geräte von Teilprozessen können in allen Bereichen der Prozessketten in einer Einrichtung vorhanden sein, insbesondere aber in den folgenden:

- Stromversorgung
- Gasversorgung
- Fernwärme
- Wasserversorgung
- Informationstechnik (IT)
- Kommunikationstechnik (KT)
- Transport und Verkehr (inklusive Fahrzeuge und Betriebsmittelversorgung)

- **Einrichtungsspezifische Sonderanlagen und Sondergeräte:**
Hierunter werden alle Spezialanlagen und Spezialgeräte gefasst.¹⁸

WICHTIGER HINWEIS:

Die Identifizierung der relevanten einrichtungsspezifischen Risikoelemente ist eine der wichtigsten Voraussetzungen für eine erfolgreiche Risikoanalyse, da kritische Prozesse häufig unmittelbar von einrichtungsspezifischen Anlagen und Geräten abhängen.

■ Daten und Unterlagen:

Zu Daten und Unterlagen zählen alle elektronisch oder in Papierform vorgehaltenen Informationen, die zur Aufrechterhaltung von Teilprozessen in der Einrichtung notwendig sind.

■ Betriebsmittel:

Unter Betriebsmitteln werden im Rahmen dieses Leitfadens alle sonstigen Produktionsmittel verstanden, die nicht in den vorherigen Punkten genannt wurden.

3.2.1 Kritikalitätsanalyse

Durch eine Kritikalitätsanalyse können in der Einrichtung aus allen erfassten Prozessen diejenigen identifiziert werden, deren Beeinträchtigung zu weitreichenden Folgen für das Unternehmen beziehungsweise die Behörde führen würde. Diese sogenannten kritischen Prozesse müssen durch geeignete Maßnahmen ausreichend geschützt werden. Die Risikoidentifikation und vor allem die gewählten vorbeugenden Maßnahmen zur Risikominderung sollten sich zunächst auf Risikoelemente der Teilprozesse kritischer Prozesse konzentrieren.

¹⁸ Beispiele: Stueurelemente, Software, medizinisches Gerät, spezielle Haustechnik, Sicherheitsschleusen, Tanklager, Flugzeuge.

Die folgenden Kriterien können zur Ermittlung kritischer Prozesse herangezogen werden:¹⁹

- **Leben und Gesundheit:**
Welche Auswirkungen hat die Beeinträchtigung des Prozesses auf Leben und Gesundheit von Menschen?
- **Zeitraumen:**
In welchem Zeitrahmen wirkt sich eine Beeinträchtigung des Prozesses auf die gesamte Dienstleistung beziehungsweise Produktion der Einrichtung aus? Je kürzer dieser Zeitrahmen, desto kritischer ist der Prozess.
- **Volumen:**
Welches Volumen der gesamten Dienstleistung beziehungsweise der Produktion ist betroffen, wenn der betrachtete Prozess beeinträchtigt ist beziehungsweise gänzlich ausfällt?
- **Vertragliche, ordnungspolitische oder gesetzliche Relevanz:**
Welche vertraglichen, ordnungspolitischen oder gesetzlichen Folgen hat eine Beeinträchtigung des betrachteten Prozesses für die Einrichtung?
- **Wirtschaftliche Schäden:**
Wie hoch können die wirtschaftlichen Schäden eingeschätzt werden, die der Einrichtung durch die Beeinträchtigung des betrachteten Prozesses entstehen?

Es ist von der Einrichtung selbst festzulegen, welche Kriterien angewendet werden, wie viele Kriterien gleichzeitig gelten sollen und welche Klassifizierung innerhalb der Kriterien vorgenommen wird.

Ergebnis der Kritikalitätsanalyse ist die Erkennung und Erfassung aller kritischen Prozesse im Unternehmen beziehungsweise in der Behörde sowie die Darstellung der dort wirkenden Teilprozesse sowie der Risikoelemente dieser Teilprozesse.

¹⁹ The Business Continuity Institute 2005, Seite 26.

²⁰ Anhang IV gibt einen Überblick über mögliche Gefahren, ihre Eigenschaften sowie über weitere Ansprechpartner hinsichtlich der Analyse dieser Gefahren. Die Gefahrenliste im Anhang beschränkt sich auf Ereignisse aus den Bereichen Naturgefahren, technisches und/oder menschliches Versagen, vorsätzliche Handlungen und Krieg. Sie erhebt daher keinen Anspruch auf Vollständigkeit und ist gegebenenfalls durch eigene Erkenntnisse und um zusätzliche Gefahrenarten zu ergänzen. Insbesondere Gefahren mit langfristiger Ankündigung, die beispielsweise zu Finanz-, Markt- oder strategischen Risiken führen können, werden im Rahmen dieses Leitfadens nicht berücksichtigt.

3.2.2 Risikoidentifikation

Die Risiken einer Einrichtung werden durch die Gefahren, die am Standort oder an den Standorten auftreten und auf die Risikoelemente einwirken können, sowie durch die Verwundbarkeit dieser Risikoelemente bestimmt. Die Verbindung relevanter Gefahren- und Verwundbarkeitsinformationen führt zur Risikoermittlung für die betrachteten Risikoelemente und, in aggregierter Form, für die untersuchten Teilprozesse. Die Risiken für die Risikoelemente werden im Leitfaden als Teilrisiken, die für Teilprozesse aggregierten Risiken als Gesamtrisiken bezeichnet. Im Folgenden werden die Aspekte der Risikoidentifikation ausführlich beschrieben.

3.2.2.1 Gefahrenanalyse und Szenarioentwicklung

Entscheidend für eine erfolgreiche Risikoanalyse ist das Erkennen und Dokumentieren aller relevanten Gefahren. In einem ersten Schritt zur Gefahrenanalyse und Szenarioentwicklung sollte daher eine Liste derjenigen Gefahren erstellt werden, die am Standort beziehungsweise an den Standorten der Einrichtung auftreten können. Diese umfassende Liste gibt Aufschluss über generelle Eigenschaften dieser Gefahren, deren Intensität, deren Zeitdauer und deren mögliche Wirkungen.²⁰

Aus einer standortspezifischen Gefahrenliste können Szenarien entwickelt werden, die Zusatzinformationen enthalten, die in der Risikoanalyse und im Rahmen des Krisenmanagements benötigt werden. Die Szenarien sollten realistische Ereignisse, die zu Krisen führen können, abbilden. Die Anzahl der Szenarien, die in die Risikoanalyse eingeht, wird vom fachlichen Leiter für das Risiko- und Krisenmanagement festgelegt. Ziel ist eine möglichst umfassende Abdeckung des Gefahrenpotenzials.

Folgende Zusatzinformationen werden für jedes Szenario festgelegt:

- **Erwartete Exposition:**
Welche Teilprozesse und Risikoelemente können betroffen sein?

WICHTIGER HINWEIS:

Die Exposition ist Grundvoraussetzung für die Beeinträchtigung eines Prozesses, Teilprozesses beziehungsweise Risikoelementes. Dabei können lokale Einwirkungen ebenso zu Ausfällen führen wie eine weiträumige Exposition. Entscheidend ist die Betroffenheit von Teilprozessen und Risikoelementen.

- **Erwartete Intensität:**
Wie hoch ist das Zerstörungspotenzial des Szenarios bezogen auf einen Teilprozess und dessen Risikoelemente?
- **Erwartete zeitliche Ausdehnung:**
Wie lange dauert das Ereignis an?
- **Vorwarnung:**
Welche Vorwarnzeit ist für das Ereignis anzunehmen?
- **Sekundäreffekte:**
Welche Effekte entstehen aufgrund von Abhängigkeiten der Prozesse? Welche psychologische Wirkung kann das Ereignis hervorrufen? Welche Öffentlichkeitswirkung beziehungsweise Medienwirksamkeit hat das Ereignis?
- **Referenzereignisse:**
Welche Referenzereignisse können zur Erläuterung herangezogen werden?
- **Eintrittswahrscheinlichkeit:**
Welche Eintrittswahrscheinlichkeit kann für das Ereignis abgeschätzt oder ermittelt werden?

Die Eintrittswahrscheinlichkeit eines Szenarios mit zuvor festgelegter Intensität, räumlicher und zeitlicher Ausdehnung, Vorwarnung und Sekundäreffekten kann häufig nur abgeschätzt werden. So liegen beispielsweise nur für bestimmte Naturereignisse oder das Versagen technischer Bauteile lange Aufzeichnungsreihen vor, aus denen Eintrittswahrscheinlichkeiten errechnet werden können. In der praktischen Umsetzung der Szenarioentwicklung in Unternehmen und Behörden empfiehlt es sich, die Eintrittswahrscheinlichkeiten anhand einer Klasseneinteilung abzuschätzen.²¹

WICHTIGER HINWEIS – ABHÄNGIGKEITEN UND SZENARIOUMFANG:

Extreme Ereignisse bewirken in der Regel eine Vielzahl von Beeinträchtigungen. So kann sich beispielsweise ein Stromausfall auch auf die externe Wasserversorgung auswirken oder die Dienstleistung von Zulieferern erschweren.

Im Hinblick auf die Entwicklung von Szenarien sollte darauf geachtet werden, Szenarien getrennt zu betrachten, beispielsweise Szenario 1: Ausfall der externen Stromversorgung, Szenario 2: Ausfall der externen Wasserversorgung. Ansonsten entstehen wenige, sehr komplexe Szenarien, deren Auswirkungen unübersichtlich sind.

Dennoch sollten Randeffekte, die sich aus Abhängigkeiten ergeben, in die Szenarien eingebaut werden. Dies gilt insbesondere für Effekte, die zu einer Verstärkung der Auswirkungen führen.

Die ausgewählten Szenarien werden regelmäßig überprüft, überarbeitet und vervollständigt. Bei Bedarf können weitere relevante Szenarien mit aufgenommen werden, um eine auf die Einrichtung bezogene und möglichst umfassende Identifizierung von Risiken zu gewährleisten.

3.2.2.2 Verwundbarkeitsanalyse

Neben den auftretenden Gefahren entscheidet die Verwundbarkeit der Teilprozesse und Risikoelemente maßgeblich über Art und Umfang der Betroffenheit und der anfallenden Schäden. Je höher der Grad der Verwundbarkeit einzelner Teilprozesse und Risikoelemente ist, desto stärker können sich Gefahren auf die Dienstleistung oder Produktion der Einrichtung auswirken.

Die Ermittlung der Verwundbarkeit der Teilprozesse und einzelner Risikoelemente erfolgt anhand eines Kriterienkatalogs. Für jedes Risikoelement eines Teilprozesses wird auf Basis des Kriterienkatalogs eine Einschätzung der Verwundbarkeit vorgenommen. Auch diese kann anhand einer Klasseneinteilung erfolgen.²²

Aus der folgenden Kriterienliste können Einrichtungen einen für sich relevanten Kriterienkatalog zusammenstellen beziehungsweise ihren Kriterienkatalog ergänzen.

■ Abhängigkeit von Risikoelementen

Wenn ein Teilprozess für die Erbringung seiner Leistung auf ein Risikoelement angewiesen ist, macht ihn die potenzielle Nichtverfügbarkeit oder Veränderung dieses Risikoelementes verwundbar. Dieses Kriterium kann als Gewichtung gesehen werden, um die Bedeutung des Risikoelements für den Teilprozess im Rahmen der Risikoermittlung darzustellen.²³

■ Abhängigkeit von externen Infrastrukturen

Wenn ein Risikoelement für die Erbringung seiner Leistung auf eine externe Infrastruktur angewiesen ist, wird es durch die potenzielle Nichtverfügbarkeit oder Veränderung dieser Infrastruktur verwundbar.

²¹ Das Beispiel zur Risikoanalyse in Anhang VI nutzt eine fünfstufige Klassifizierung der Eintrittswahrscheinlichkeit möglicher Szenarien.

²² Das Beispiel zur Risikoanalyse in Anhang VI nutzt eine sechsstufige Skala für die Verwundbarkeit (inklusive Stufe 0 – keine Relevanz).

²³ Im Beispiel zur Risikoanalyse im Anhang wird dieses Kriterium als Gewichtungsfaktor genutzt. Er geht als Einzelfaktor in die Risikoermittlung ein. Die Abschätzungen der übrigen Verwundbarkeitskriterien werden summiert und finden daher als Sammelfaktor Eingang in die Risikoermittlung.

- **Abhängigkeit von internen Infrastrukturen**
Wenn ein Risikoelement für die Erbringung seiner Leistung auf eine interne Infrastruktur angewiesen ist, wird es durch die potenzielle Nichtverfügbarkeit dieser Infrastruktur verwundbar.

- **Robustheit**
Die physische Robustheit der Risikoelemente (insbesondere Anlagen, Geräte, Gebäude) ist ein wichtiger Faktor dafür, ob sie durch die Einwirkung eines extremen Ereignisses beschädigt werden. Hierdurch würden der oder die zugeordneten Teilprozesse beeinträchtigt werden.

- **Realisiertes Schutzniveau**
Ein Risikoelement, das nicht ausreichend gegenüber einer Gefahr geschützt ist, ist durch den potenziellen Eintritt dieser Gefahr verwundbar (Beispiel: vorhandene beziehungsweise nicht vorhandene Sicherungsmaßnahmen an Gebäuden).

- **Redundanz, Ersatz**
Der Ausfall von Risikoelementen einer Einrichtung ist besser zu bewältigen, wenn parallele Strukturen oder Ersatzstrukturen vorhanden sind, um dieselbe Leistung zu erbringen. Redundant ausgelegte Risikoelemente oder Ersatzelemente führen dazu, dass die Verwundbarkeit des betrachteten Teilprozesses reduziert wird.

- **Wiederherstellungsaufwand**
Der Wiederherstellungsaufwand beschreibt den Aufwand, der mit der Wiederherstellung eines Risikoelements nach einer Beschädigung verbunden ist. Im Hinblick auf die Verwundbarkeit eines Teilprozesses ist dabei nicht ausschließlich der finanzielle Aufwand gemeint, sondern auch der zeitliche und personelle Aufwand.

- **Anpassungsfähigkeit**
Ein Teilprozess ist verwundbar, wenn sich seine Risikoelemente verändernden Rahmenbedingungen nicht oder nur schwer anpassen können (Beispiel: Bei einem wetterbedingten Temperaturanstieg in Flüssen können dies Bauteile sein, die Kühlwasser benötigen).

- **Pufferkapazität**
Pufferkapazität heißt, dass der Teilprozess die Einwirkung eines Ereignisses in einem bestimmten Maß und über einen bestimmten Zeitraum verkraften kann, ohne beeinträchtigt zu werden.

- **Transparenz**
Transparenz bedeutet, dass die Zusammensetzung und Funktionsweise des Risikoelementes leicht nachvollziehbar ist, was beispielsweise für eine schnelle Reparatur im Krisenfall von Vorteil ist.

- **Abhängigkeit von spezifischen Umweltbedingungen**
Einrichtungen erbringen ihre Leistung unter den am jeweiligen Standort vorherrschenden Umweltbedingungen. Ist eine Einrichtung hierfür auf sehr spezifische Umweltbedingungen angewiesen, dann ist sie durch potenzielle Abweichungen in diesen Bedingungen verletzbar.

3.2.2.3 Risikoermittlung

Im Rahmen der Risikoermittlung werden berechnete Werte, Abschätzungen oder Aussagen aus der Szenarioentwicklung und der Verwundbarkeitsanalyse zu Risikowerten oder Risikoaussagen verknüpft. Die Verknüpfung von Risikowerten wird durch eine Funktion realisiert. In diesem Leitfaden werden Teilrisiken für Risikoelemente als Funktion der Eintrittswahrscheinlichkeit des betrachteten Szenarios sowie der Verwundbarkeit der Risikoelemente verstanden. Das Gesamtrisiko für einen Teilprozess ergibt sich dann aus der Aggregation der Teilrisiken der im Teilprozess enthaltenen Risikoelemente.

Grundsätzlich kann die Risikoermittlung auf drei verschiedenen Wegen erfolgen²⁴:

- **Qualitative Ermittlung von Risiken:** Diese Vorgehensweise liefert grobe Abschätzungen für Risiken und beschreibt diese in Textform, ohne dabei eine numerische Vergleichbarkeit herzustellen.
- **Semiquantitative Ermittlung von Risiken:** Im Rahmen einer semiquantitativen Risikoermittlung werden anhand einer Klasseneinteilung Werte für einzelne Risikofaktoren abgeschätzt, um eine numerische Vergleichbarkeit herzustellen.
- **Quantitative Ermittlung von Risiken:** Im Rahmen einer quantitativen Analyse werden Risikofaktoren mathematisch ermittelt, beispielsweise auf der Basis von Zeitreihenanalysen im Falle der Eintrittswahrscheinlichkeit beziehungsweise mit Hilfe von Simulationsmodellen zur Erfassung der Auswirkungen auf eine Einrichtung.

Die Entscheidung darüber, welche Methode angewendet wird, richtet sich zum einen nach dem Aufwand, der betrieben werden soll beziehungsweise kann, und zum anderen nach der Verfügbarkeit von Informationen und Daten.²⁵

²⁴ Vgl. Australian/New Zealand Standard 2004, Seiten 18–19.

²⁵ Anhang VI beschreibt an einem Beispiel die Umsetzung einer Risikoanalyse auf Basis einer semiquantitativen Ermittlung der Teilrisiken für Risikoelemente sowie der Gesamtrisiken für Teilprozesse. Eine weitere Methode zur Risikoanalyse speziell für den Bereich der Informationstechnologie findet sich unter: Bundesamt für Sicherheit in der Informationstechnik 2005.

3.2.2.4 Risikovergleich und Risikobewertung

Die so ermittelten Risikowerte beziehungsweise Risikobeschreibungen können nun miteinander verglichen werden. Dieser Vergleich ist insbesondere bei qualitativen und semiquantitativen Analysen sinnvoll, da die hierdurch ermittelten Werte und Beschreibungen keine absolute Aussagekraft haben. In Relation zueinander, also im internen Vergleich, sind die Ergebnisse aus qualitativen und semiquantitativen Analysen hingegen sehr wertvoll.

Ziel eines solchen Vergleichs ist es, diejenigen Risikoelemente und Teilprozesse in der Einrichtung zu identifizieren, die den höchsten Risiken ausgesetzt sind.

Die Risikobewertung soll aufzeigen, ob die eingangs definierten strategischen Schutzziele vor dem Hintergrund der bestehenden Risiken erreicht werden können. Bestehen zu viele hohe Teilrisiken, werden operative Schutzziele formuliert, die den Ausgangspunkt für die Umsetzung von vorbeugenden Maßnahmen bilden. Beispiele für operative Schutzziele sind

- die Reduzierung des Gesamtrisikos für Teilprozess X sowie
- die Reduzierung der höchsten Teilrisiken in allen Teilprozessen, die zu kritischen Prozessen gehören.

Maßnahmen sollten vorrangig für die Teilprozesse umgesetzt werden, die die größten Teilrisiken aufweisen.

Letztlich ist es die Aufgabe der Einrichtungsleitung und des fachlichen Leiters, über die Auswahl geeigneter operativer Schutzziele und Maßnahmen zu entscheiden.

3.3 Phase 3: Vorbeugende Maßnahmen und Strategien

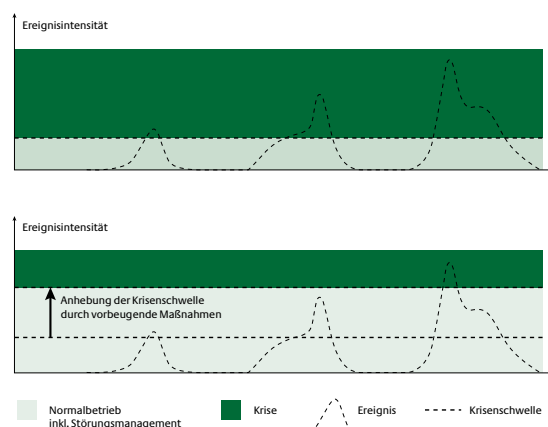
Vorbeugende Maßnahmen tragen zur Minderung von Risiken für kritische Prozesse bei. Sie helfen, operative Schutzziele zu erreichen und damit die Krisenschwelle für Ereignisse mit Krisenpotenzial in der Einrichtung anzuheben (siehe auch Abbildung 5). Hierdurch kann die Anzahl krisenhafter Ereignisse minimiert beziehungsweise die Intensität auftretender Ereignisse reduziert werden.

Vorbeugende Maßnahmen sollten einer Kosten-Nutzen-Analyse unterzogen werden. Es geht bei der Prüfung um eine Reduzierung des Gesamtrisikos. Dies geschieht durch Gegenüberstellung der potenziellen Investitionen und der direkten sowie indirekten Kosten einer Beeinträchtigung der Einrichtung im Zuge eines extremen Ereignisses. Die Verknüpfung der Ergebnisse aus einer Risikoanalyse mit denen einer Kosten-Nutzen-Analyse führt zur Auswahl derjenigen Maßnahmen, die im Rahmen des vorhandenen Budgets besonders effizient sind.²⁶

Allerdings können Maßnahmen zur Minderung von Risiken mit geringer Eintrittswahrscheinlichkeit und dramatischen Auswirkungen häufig nicht ausschließlich auf der Basis einer Risiko- und Kosten-Nutzen-Analyse gerechtfertigt werden. Neben rechtlichen Rahmenbedingungen ist es in diesen Fällen auch sinnvoll, soziale beziehungsweise ethische Überlegungen in die Entscheidung über Schutzmaßnahmen einfließen zu lassen.

Vorbeugende Strategien nutzen die Werkzeuge Risikovermeidung, Risikoüberwälzung oder Risikoakzeptanz. Sie sollten nur komplementär zu risikomindernden Maßnahmen genutzt werden, da sie wie im Falle der Risikovermeidung entweder die Flexibilität der Einrichtung stark einschränken können oder wie in den Fällen der Risikoüberwälzung und Risikoakzeptanz keinen Beitrag zur physischen Risikominderung leisten.

Abbildung 5: Ereignisintensität und Krisenschwelle



3.3.1 Risikominderung

Maßnahmen zur Risikominderung reduzieren entweder die Verwundbarkeit der Risikoelemente gegenüber der Einwirkung von Gefahren oder richten sich unmittelbar an die betriebliche Kontinuität der kritischen Prozesse durch die Schaffung von Redundanz beziehungsweise Ersatz.

²⁶ Vgl. Australian/New Zealand Standard 2004, Seiten 21–22.

Redundante Systeme oder Ersatzsysteme ermöglichen die betriebliche Kontinuität kritischer Prozesse im Rahmen des Wiederanlaufmanagements, auch wenn es zur Beeinträchtigung von Risikoelementen kommt.²⁷

3.3.2 Risikovermeidung

Risiken können vermieden werden, indem man entweder gefährdete Regionen meidet oder Maßnahmen umsetzt, die dazu führen, dass Gefährdungen nicht entstehen können.

Exponierte, also gefährdete Bereiche können im Hinblick auf Naturgefahren oder im Umfeld risikobehafteter Anlagen (Beispiel: Gefahrguttransportstrecken) häufig benannt werden. Es besteht die Möglichkeit, bei einer Neuplanung von Standorten oder Einzelgebäuden und Anlagen solche Bereiche zu meiden.

Eine vollständige Vermeidung von Risiken ist jedoch nicht möglich, da kein Standort risikofrei ist.

3.3.3 Risikoüberwälzung

Risikoüberwälzung verlagert Risiken auf andere Unternehmen beziehungsweise auf Vertragspartner, um das finanzielle Ausmaß möglicher Schäden auf die eigene Einrichtung zu reduzieren. Zu den Instrumenten der Risikoüberwälzung zählen

- die Überwälzung der Risiken auf Versicherungen und
- die Überwälzung der Risiken auf Lieferanten oder auf Kunden.

WICHTIGER HINWEIS:

Eine Risikoüberwälzung führt nicht zu einer physischen Reduzierung der Risiken für Personen oder Sachgüter. Sie verändert lediglich die finanziellen Folgen eingetretener Schäden für die Einrichtung.

3.3.4 Akzeptanz von Risiken (Restrisiken)

Die in der Einrichtung getroffenen vorbeugenden Maßnahmen und Strategien werden das Sicherheitsniveau insgesamt erhöhen. Dennoch können bestimmte Risiken nicht gänzlich ausgeschaltet werden. Die verbleibenden Restrisiken sollten dokumentiert und deren Akzeptanz durch die Einrichtung schriftlich festgehalten werden.

Aufgrund von Restrisiken kann es zu Krisen kommen, in deren Verlauf die normale Aufbau- und Ablauforganisation in der Regel überfordert ist. Hierfür wird ein Krisenmanagement benötigt, das die Einrichtung in die Lage versetzt, die Situation effektiv zu bewältigen.

3.3.5 Schadenerfahrungen der Sachversicherer

Naturgemäß haben die Sachversicherer ein besonderes Interesse am Schutz vor Sachschäden und an der Reduzierung der Auswirkungen von Schadenereignissen auf den Fortbestand von Unternehmen.

Die Erkenntnisse aus Schäden sind in zahlreichen Publikationen (Leitfäden, Richtlinien und Merkblättern) des Gesamtverbandes der Deutschen Versicherungswirtschaft zusammengetragen.²⁸ Diese können als weitere Erkenntnisquelle zur Optimierung des Schutzes einzelner Einrichtungen dienen und somit einen Beitrag zum Schutz Kritischer Infrastrukturen leisten.

3.4 Phase 4: Krisenmanagement

Eine Krise im Sinne dieses Leitfadens wird als eine Abweichung von der Normalsituation verstanden, die mit den normalen betrieblichen Strukturen allein nicht mehr bewältigt werden kann. Krisen in Einrichtungen Kritischer Infrastrukturen können zu erheblichen Beeinträchtigungen der Funktionalität von Unternehmen und Behörden und damit zu Schäden für die Bevölkerung oder zu Beeinträchtigungen des politischen, sozialen oder wirtschaftlichen Systems führen. Im Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) findet sich der Begriff der „Bestandsgefährdung“, der sehr gut als definitorische Festlegung dienen kann.²⁹ Eine Krise ist klar abzugrenzen von Ereignissen minderschweren Ausmaßes, die in diesem Leitfaden als Störungen bezeichnet werden (siehe Abbildung 5, Seite 21).

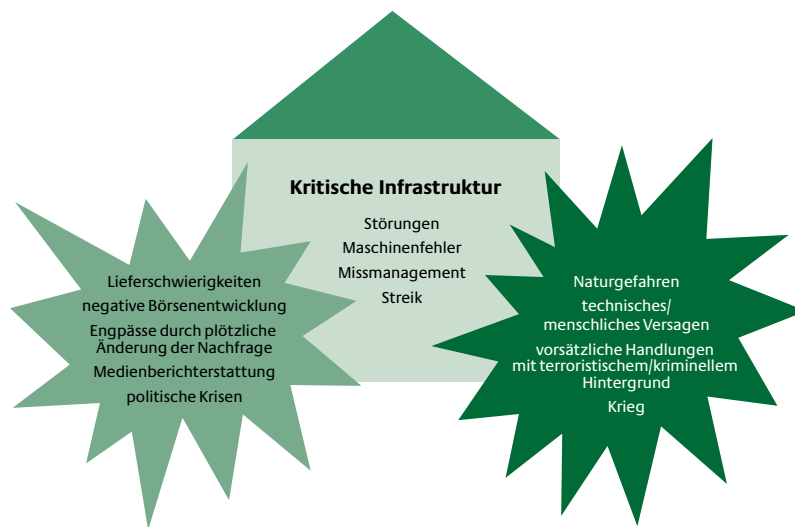
Auslöser für Krisen können im Unternehmen oder in der Behörde selbst entstehen, wie zum Beispiel Finanzkrisen als Folge von Missmanagement oder Veruntreuung (siehe Abbildung 6). Von außen induziert werden Krisen beispielsweise durch Börsenzusammenbrüche, negative Schlagzeilen oder durch Lieferschwierigkeiten. Daneben sind Naturgefahren, technisches oder menschliches Versagen sowie vorsätzliche Handlungen mit terroristischem oder kriminellem Hintergrund sowie kriegerische Auseinandersetzungen als Hauptauslöser für Krisen Kritischer Infrastrukturen anzusehen.

²⁷ In Anhang V.1 befindet sich eine umfangreiche Checkliste zur Umsetzung vorbeugender Maßnahmen.

²⁸ Siehe z. B. VdS-Richtlinien 2007.

²⁹ Vgl. Trauboth 2002, Seite 14 f.

Abbildung 6: Auslöser von inneren und äußeren Krisen



Das Krisenmanagement liefert einen signifikanten Beitrag zum Schutz von Unternehmen und Behörden und damit zum Schutz von Kritischen Infrastrukturen und der Bevölkerung. Es ist nicht vom Risikomanagement losgelöst. Die konzeptionelle, organisatorische, verfahrensmäßige und physische Vorbereitung auf Krisen basiert teilweise auf den Resultaten des Risikomanagements. Art und Umfang der Restrisiken aus dem Risikomanagement beeinflussen teilweise die Ausprägung der Krisenvorbereitung im Krisenmanagement. Da nicht alle Risiken durch risikomindernde Maßnahmen reduziert werden können und ein Restrisiko immer bestehen bleiben wird, dient das Krisenmanagement der Bewältigung von Krisen, die durch Prävention allein nicht verhindert werden können.

Ziel des Krisenmanagements in Einrichtungen Kritischer Infrastrukturen ist die Bewältigung einer Krise bei

- bestmöglicher Aufrechterhaltung der Funktionsfähigkeit beziehungsweise
- schnellstmöglichem Wiederanlauf der kritischen Prozesse.

Ein erfolgreiches Krisenmanagement ist eingebettet in weitere Managementkonzepte, wie beispielsweise in das bereits beschriebene Risikomanagement. Im Krisenmanagement werden Maßnahmen vorbereitet und aktiviert, die die Funktion der Organisation, die betriebliche oder dienstliche Kontinuität und die Rückkehr zum Normalbetrieb sicherstellen. Eine Evaluierung des Ablaufs des Krisenmanagements während eines Ereignisses und danach ermöglicht seine Weiterentwicklung und Verbesserung. Das Krisenmanagement kann also als PDCA-Teilzyklus im Risikomanagement (siehe Abbildung 3) verstanden werden. Der Prozess des Krisenmanagements ist in Abbildung 7 dargestellt.

Abbildung 7: Prozess des Krisenmanagements³⁰



³⁰ Vgl. Gesellschaft für Anlagen- und Reaktorsicherheit 2007, Seite 21.

Die wichtigsten Aufgaben eines Krisenmanagements sind:

- die konzeptionellen, organisatorischen und verfahrensmäßigen Voraussetzungen zu schaffen, um die bestmögliche Bewältigung eines Extremereignisses zu ermöglichen, sowie
- spezielle Strukturen zur Reaktion im Krisenfall zu etablieren, insbesondere die Einrichtung eines Krisenstabes.

Die wichtigsten Charakteristika eines Krisenmanagements sind:

- Es ist ein Prozess, der Planung, Umsetzung und Evaluierung eines Plans und daraus abgeleitetes Handeln umfasst, um in der Krise effektiv und effizient reagieren zu können.
- Maßnahmen erfolgen in der Regel unter Verwendung der nur eingeschränkt zur Verfügung stehenden Ressourcen und Informationen.
- Eine Unterstützung durch externe Stellen oder Ressourcen kann erforderlich sein.
- Entscheidungen werden unter Zeitdruck bei unvollständigem Informationsstand getroffen.

3.4.1 Die Organisation des Krisenmanagements

Die elementaren Bausteine des Krisenmanagements sind eine besondere, in allen Krisenfällen agierende Aufbau- und Ablauforganisation sowie szenariobezogene Teilplanungen zur Sicherstellung der betrieblichen Kontinuität. Alle hierfür erforderlichen und möglichen Vorplanungen werden in einem Krisenplan zusammengestellt.

3.4.1.1 Krisenplan

Im Krisenplan sind alle krisenrelevanten Organisationsstrukturen und planbaren Maßnahmen festgeschrieben, die von den Mitarbeitern in der Einrichtung, die mit dem Krisenmanagement und der betrieblichen beziehungsweise dienstlichen Kontinuität beauftragt sind, auszufüllen beziehungsweise durchzuführen sind. Ein guter Krisenplan ist kurz und präzise. Checklisten³¹ für den Krisenfall erleichtern die Abarbeitung der notwendigen Maßnahmen und verhindern, dass wichtige Aufgaben vergessen werden.

Der Krisenplan beinhaltet die folgenden Punkte inklusive der Festlegung von Zuständigkeiten³²:

- Zweck, Ziel und Geltungsbereich des Krisenplans
- Rechtsgrundlagen
- Entwicklung einer Aufbauorganisation für den Krisenfall
 - Krisenstab
 - Festlegung von Aufgaben, Zuständigkeiten und Kompetenzen und ihre Zuweisung zu den nominierten Funktionsträgern³³
 - konkrete Zuständigkeiten und Aktivitäten für die Krisenbewältigung
- Entwicklung einer Ablauforganisation für die Krisenbewältigung, die Rückführung in den Normalzustand und die Nachbereitung
 - Meldewege und Alarmierung
 - Eskalations- und Deeskalationsmodelle
 - Erreichbarkeit von Ansprechpartnern innerhalb und außerhalb des Unternehmens beziehungsweise der Behörde
 - ereignisspezifische Maßnahmen zum Wiederanlauf und Rückkehr zum Normalbetrieb
 - Hinweise zur Nachbereitung der Krise
- Entwicklung szenariobezogener Planbestandteile, zum Beispiel:
 - Evakuierung
 - Stromausfall
 - Pandemie
 - Ausfall IT und/oder KT

Der Krisenplan muss regelmäßig aktualisiert und seine Anwendung geübt werden.

WICHTIGER HINWEIS:

Ein Krisenplan sollte grundsätzlich erstellt werden, auch wenn im Vorfeld sehr viele vorbeugende Maßnahmen umgesetzt wurden.

³¹ Anhang V.2 enthält Checklisten zur Überprüfung von Details im Rahmen der Vorbereitung auf Krisen.

³² Ein Beispiel für den Krisenplan oder das Notfallhandbuch für den IT-Bereich findet sich unter Bundesamt für Sicherheit in der Informationstechnik 2008.

³³ Jungbluth 2005, Seite 15.

3.4.1.2 Aufbauorganisation

Krisensituationen erfordern eine Sonderorganisation. Ein Arbeitsstab für Krisensituationen (Krisenstab) hat das Ziel, schnellstmöglich und kompetent Krisen zu bewältigen. Der Aufbau der Krisenorganisation ist von der Art und den Bedürfnissen der Kritischen Infrastruktureinrichtung abhängig.

3.4.1.2.1 Krisenstab

Der Krisenstab ist das zentrale Krisenreaktionsinstrument. Er stellt eine besondere Aufbauorganisation dar, die die normale Aufbauorganisation zur Bewältigung von besonderen Lagen für die beteiligten Organisationseinheiten durchbricht und abteilungsübergreifend Kompetenzen unter einer einheitlichen Leitung bündelt. Beim Krisenstab handelt es sich um ein Entscheidungsinstrument mit koordinierenden, informierenden, beratenden und unterstützenden Zusatzfunktionen. Formal besteht der Krisenstab aus einem Leiter³⁴ und dem Krisenstabsteam. Innerhalb des Krisenstabsteams kann man unterscheiden zwischen

- dem Kernteam, bestehend aus dem Leiter und ein bis drei wichtigen Funktionsträgern,
- dem erweiterten Krisenstab, bestehend aus designierten Spezialfunktionen oder Unterstützungsgruppen,³⁵ und
- Fachberatern, die den Krisenstab beraten.

Alle nominierten und eingewiesenen Krisenstabsmitglieder und ihre Stellvertreter haben ihre spezielle Aufgabe zu kennen und müssen darauf vorbereitet sein. Bei der Besetzung der Stellvertreter sind auch Szenarien im Blick zu halten, bei denen sich große Personalausfälle auf die Mitarbeiter im Krisenstab auswirken könnten (zum Beispiel größere Epidemien oder Pandemien).³⁶ Hierfür sind mehrere Vertreter zu benennen.

Im Vorfeld einer Krise sollte speziell für den Krisenstab eine Arbeitszeitregelung (Schichtsystem) für den Krisenfall erfolgen, die auch eine Übergabezeit für das ablösende Personal berücksichtigt. Krisenzeiten sind Stresszeiten, daher sollte eine Einsatzdauer sechs bis sieben Stunden nicht überschreiten.

³⁴ Die Krisenstabsleitung kann von der Unternehmens- oder Behördenleitung wahrgenommen werden. Empfohlen wird jedoch eine Trennung,

um der Entscheidungsebene genügend Freiraum für wichtige und unabhängige Entscheidungen zu ermöglichen.

³⁵ Vgl. Trauboth 2002, Seite 45.

³⁶ Schutzmaßnahmen für das Personal und vor allem für den Krisenstab sind zum Beispiel adäquate Hygienemaßnahmen, Schutzmasken und die Einrichtung von Heimarbeitsplätzen. Weitere Informationen und Hilfestellungen zum Beispiel in Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2007, Robert Koch Institut 2005 und 2007a sowie in Anhang V.2.

In der Gefahrenabwehr und im Katastrophenschutz hat sich ein Krisenstabsmodell etabliert, das in der Feuerwehrvorschrift 100 detailliert beschrieben ist.³⁷ Dieses Modell stammt aus dem Militärbereich, beschreibt die Ausgestaltung eines Führungsstabes und richtet sich an alle Organisationen, die überwiegend operativ-taktisch tätig sind.

Parallel zu den operativ-taktischen Krisenstäben agieren im Katastrophenschutz auf Verwaltungsebene administrativ-organisatorische Verwaltungsstäbe. Sie unterstützen die operativ-taktischen Komponenten und nehmen in erster Linie Verwaltungsaufgaben wahr. Sie können bei Krisen aber auch eigenständig agieren, sofern keine operative Komponente zum Einsatz kommt.

Die Ausgestaltung des Krisenstabs in Unternehmen und Behörden, die nicht in der Gefahrenabwehr oder im Katastrophenschutz tätig sind, hängt von den Anforderungen an die Einrichtung im Krisenfall ab. In einigen Unternehmen kann eine ähnliche Einteilung des Krisenstabes, wie sie Führungs- oder Verwaltungsstäbe aufweisen, sinnvoll sein, wenn zum Beispiel ähnliche Tätigkeiten durchgeführt werden oder wenn eine enge Zusammenarbeit mit den Einsatzkräften des Katastrophenschutzes erfolgen muss. Andere Unternehmen und Behörden werden von dieser Struktur abweichen.³⁸ Wichtig ist, dass die Kommunikation zwischen dem Betreiber der Kritischen Infrastruktur und der Gefahrenabwehrbehörde beziehungsweise den Katastrophenschutzorganisationen funktioniert. Hier ist ein intensiver Austausch von Mitarbeitern im jeweils anderen Krisenstab vorteilhaft und organisatorisch im Verwaltungsstab explizit vorzusehen.

Die folgenden Stabsfunktionen beziehungsweise Aufgaben sollten in jedem Krisenstab wahrgenommen werden, unabhängig von den Aufgaben der Einrichtung³⁹:

- Regelung aller Aspekte zum Personalwesen
- Erfassung der Situation beziehungsweise der Lage und regelmäßige Aktualisierung der Informationen
- Erteilung von Aufträgen zur Behebung der Krise und Koordinierung der hierfür erforderlichen Einsätze, die durch das Personal der Einrichtung durchgeführt werden

³⁷ Feuerwehr-Dienstvorschrift 1999.

³⁸ Eine mögliche Variante für Einrichtungen mit IT-Bezug ist im BSI-Standard 100-4 beschrieben. Siehe hierzu Bundesamt für Sicherheit in der Informationstechnik 2008.

³⁹ Angepasst an Feuerwehr-Dienstvorschrift 1999.

- Presse- und Medienarbeit
- Regelung aller Aspekte zum Informations- und Kommunikationswesen
- Versorgung des im Rahmen des Krisenmanagements eingesetzten Personals

In unternehmerischen Strukturen können im Krisenstab zusätzlich folgende Funktionen abgebildet sein:

- Recht
- Finanzen/Haushalt
- Marketing
- Logistik
- Qualitätsmanagement
- Vertrieb
- Standortsicherheit
- Umweltschutz
- Anlagensicherheit
- Toxikologie
- Werksfeuerwehr
- Rettungsdienst

Für die einzelnen Funktionen können im Vorfeld von Krisen Aufgabenbeschreibungen verfasst werden, die die allgemeinen, immer wiederkehrenden Tätigkeiten in der Krisenbewältigung beschreiben.

Bei international agierenden Unternehmen beziehungsweise Gesellschaften sowie Behörden mit unmittelbarem internationalem Bezug ist eine Funktion „Ausland“ sinnvoll. Zusätzlich kann eine Krisenstabsassistentin in Erwägung gezogen werden, die vor allem bei der Erstellung des Lagebildes unterstützen kann.

Besteht ein Unternehmen oder eine Behörde aus mehreren Niederlassungen oder Zweig- beziehungsweise Außenstellen, dann ist neben den Krisenstäben vor Ort ein Konsortiums- oder Gesamtkrisenstab sinnvoll, wenn das gesamte Unternehmen oder die Behörde von der Krise betroffen ist.

3.4.1.2.2 Krisenstabsleiter

Der Krisenstabsleiter übernimmt während einer Reaktion auf ein extremes Ereignis die Leitung aller krisenbezogenen Vorgänge. Er trifft alle Entscheidungen im Rahmen der Krisenbewältigung. Daher sollte er im Unternehmen oder in der Behörde bereits eine Leitungsposition innehaben. Der Krisenstabsleiter benötigt für seine Arbeit einen vorher definierten Rechts- und Finanzrahmen.

Die Leitung eines Krisenstabes setzt eine starke Persönlichkeit und Erfahrungswerte voraus. Hierzu gehören Führungsstärke, eine hohe Belastbarkeit in Extremsituationen, eine hohe Entscheidungsfreudigkeit unter Zeitdruck, Teamfähigkeit und soziale Kompetenz. Eine schnelle Auffassungsgabe und Analysefähigkeit spiegeln die Fähigkeiten des Krisenstabslei-

ters wider. Er sollte aber auch das Vertrauen der Unternehmensleitung sowie des Krisenstabsteams haben. Vorteilhaft ist der Einsatz von Generalisten, die von Spezialisten unterstützt werden.

Es empfiehlt sich, dass sich der Krisenstabsleiter in Aus- und Weiterbildungskursen spezifische Kenntnisse zur Krisenbewältigung aneignet.

3.4.1.2.3 Krisenstabsteam

Je nach Krise wird ein bestehendes Kernteam mit ereignisspezifischen Spezialfunktionen ergänzt. Spezialfunktionen nehmen Personen wahr, die über spezifische Kompetenzen verfügen. Der Bedarf ist abhängig von der Art der Krise. Die Entscheidung über die Zusammensetzung des Krisenstabsteams trifft der Krisenstabsleiter. Die Aufgabe des Kernteams besteht in der Vorbereitung von Entscheidungen für den Krisenstabsleiter und das Veranlassen von Maßnahmen zur Ereignisbewältigung oder Schadensbegrenzung.

3.4.1.2.4 Fachberater im Krisenstab

Der Krisenstab kann durch interne und externe Fachberater ergänzt werden, die nicht formales Mitglied des Krisenstabes sind. Diese können vor allem in Entscheidungsprozesse einbezogen werden, in denen Fachinformationen benötigt werden. Hierzu gehören Kenntnisse über Betriebsabläufe, verwendete Software, Sicherheitsvorkehrungen, Finanzen, Umwelt, Produktion, das Feuerwehr- und Rettungswesen und den Katastrophenschutz auf kommunaler Ebene sowie auf Landes- und Bundesebene.

3.4.1.3 Ablauforganisation

In der Ablauforganisation sind die Aktivierung des Krisenmanagements und die Aufgaben des Krisenstabes geregelt. Dies spiegelt sich in der Ausübung von speziellen Stabsfunktionen wider, die von den entsprechend nominierten Mitarbeitern wahrgenommen werden.

Folgende Aufgaben werden im Zuge der Krisenbewältigung durchgeführt:

- Benachrichtigung, Meldung und Alarmierung
- Feststellung und Beurteilung der Lage beziehungsweise der Situation sowie der vermutlichen Lageentwicklung (hierzu gehört auch die Beschaffung von Informationen)
- Entwicklung von konkreten Bewältigungsstrategien und Veranlassung ihrer Umsetzung
- Überwachung und Kontrolle der Umsetzung
- Dokumentation der Vorgehensweise
- Kommunikation des Vorgehens, sowohl intern als auch extern
- Aktivierung von Maßnahmen zum Wiederanlauf der Prozesse
- Wiederherstellung der betrieblichen und dienstlichen Kontinuität

3.4.1.3.1 Meldewege und Alarmierung

Der schnelle und umfassende Informationsfluss ist in der Krise mitentscheidend für den Erfolg des Krisenmanagements. Kernbestandteil des Informationsflusses sind Meldungen, die mündlich oder schriftlich überbracht werden. Eine hohe Qualität der Meldungen erleichtert den Prozess der Krisenbewältigung. Diese wird erreicht, wenn Meldungen⁴⁰

- unverzüglich erfolgen,
- den Zeitpunkt und Ort der Feststellung enthalten,
- klar, sachlich und unmissverständlich sind,
- kurz gefasst, aber vollständig sind,
- Tatsachen und Vermutungen deutlich erkennbar voneinander trennen sowie
- nach ihrer Dringlichkeit geordnet sind.

Zur Weiterleitung von internen Ereignis- beziehungsweise Schadensmeldungen ist also nicht nur ein standardisierter Meldeweg festzulegen, sondern auch ein standardisiertes Meldeverfahren, das sicherstellt, dass alle notwendigen Informationen erfasst und weitergegeben werden.

Tritt ein Ereignis ein, das mit dem hausinternen Störungsmanagement allein nicht mehr bewältigt werden kann, sondern aus dem heraus eine Krise erwachsen könnte, dann ist die schnellstmögliche Benachrichtigung des Krisenstabsleiters notwendig. Erkenntnisse über Schäden im Umfeld einer Einrichtung können über eigene Mitarbeiter, Kunden, Bürger oder externe Unternehmen und Behörden übermittelt werden. In Abhängigkeit vom Ausmaß eines Ereignisses ist ein Entscheidungsträger, in der Regel der Vorgesetzte, zu informieren. Ist das Ereignis in seinem Verantwortungs- bereich nicht zu bewältigen, meldet er diesen Vorgang an den Krisenstabsleiter oder die Einrichtungsleitung. Der Krisenstabsleiter entscheidet über die Aktivierung der besonderen Aufbau- und Ablauforganisation.

Der Krisenstabsleiter beurteilt die Gefahr und stellt die Alarmierung der im Krisenmanagement aktiven Personen beziehungsweise Stellen wie des Kernteams, des erweiterten Krisenstabs, der Leitzentralen und der Unternehmens- beziehungsweise Behördenleitung sicher. Bei Bedarf werden externe Stellen über das Ereignis benachrichtigt, wie zum Beispiel Lieferanten und Kunden, Organisationen und Hilfseinrichtungen, öffentliche Einrichtungen wie Schulen und Kindergärten, Behörden und Ämter und der Öffentliche Gesundheitsdienst (unter anderem auch Ärzte und Krankenhäuser).

Der Alarmierung liegen Alarmlisten zugrunde, die Erreichbarkeiten des im Krisenmanagement aktiven Personals und relevanter externer Stellen enthalten. Die Alarmierungs- beziehungsweise Benachrichtigungslisten sind vom Unternehmen oder der Behörde im Vorfeld zu erstellen und regelmäßig zu aktualisieren.

Die Überführung des Normalbetriebs in das Krisenmanagement und die Alarmierung der Mitarbeiter kann abrupt oder eskalierend erfolgen. Die folgenden zwei Modelle sind hierbei denkbar:

■ Schwellenmodell

In diesem Fall existiert nur eine Alarmstufe vom Normalbetrieb inklusive Störungsmanagement zum Krisenmanagement. Wird diese Schwelle überschritten, ist automatisch die Situation erreicht, in der der Krisenplan aktiviert wird und ein Krisenstab die Leitung in der Krise übernimmt. Alle Mitarbeiter und relevanten Stellen, die im Krisenmanagement aktiv sind, werden alarmiert.

■ Eskalationsmodell

In diesem Fall enthält der Krisenplan eine Einteilung in mehrere Alarmstufen. Hiernach werden Personal-, Mittel- und Maßnahmeneinsatz abhängig vom Ereignis festgelegt. Dies ermöglicht die genaue Reaktion auf mögliche Ereignisse und ihre Auswirkungen, hat jedoch eine komplexere Krisenplanung zur Folge.⁴¹

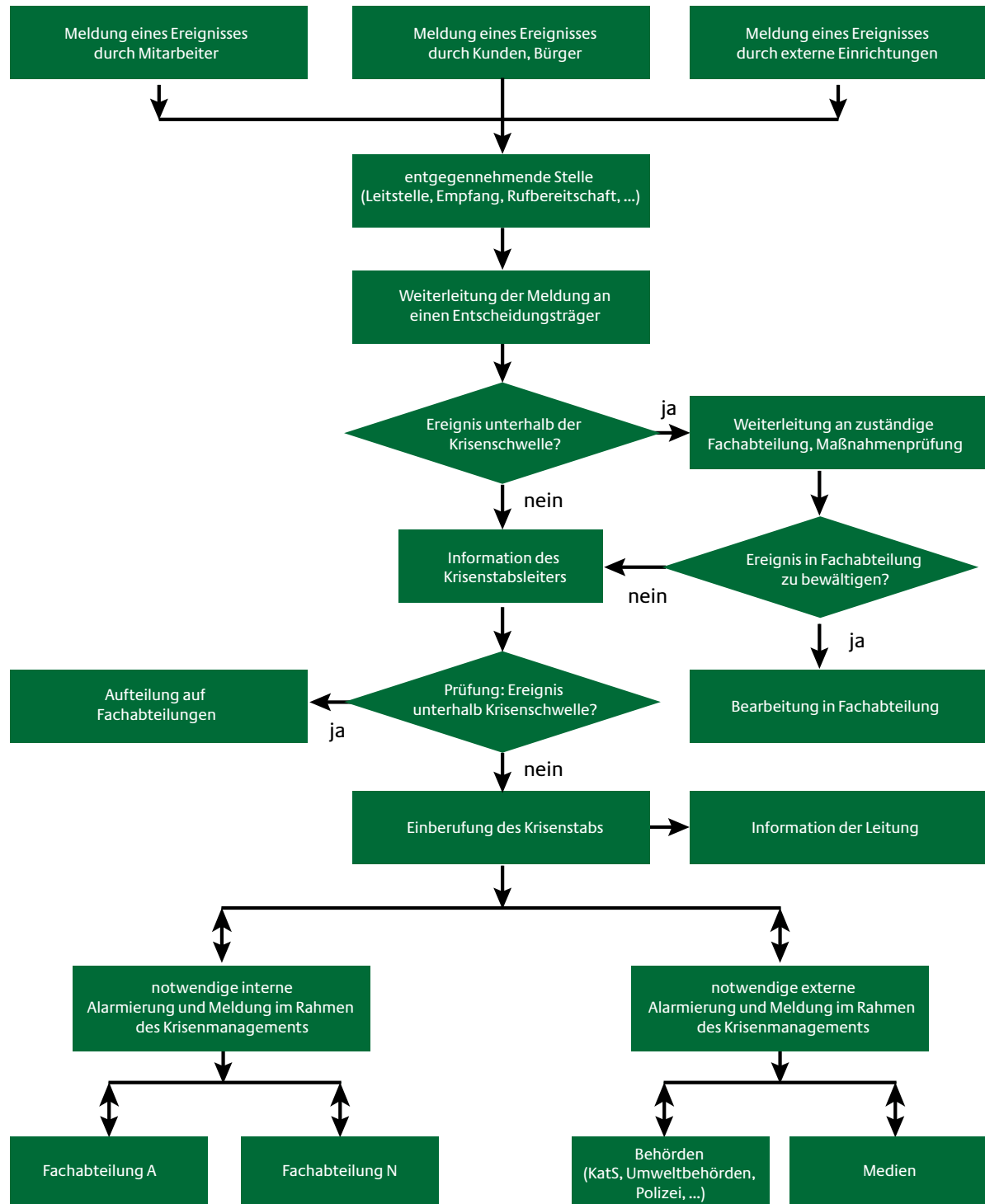
Nach der Meldung eines Ereignisses an den Krisenstabsleiter und der Alarmierung aller relevanten internen und externen Stellen setzt der Krisenstab Meldungen ab, um Aufträge in der Einrichtung zu verteilen. Das im Krisenmanagement aktive Personal übermittelt in Form von Meldungen den Sachstand an den Krisenstab. Externe Stellen informieren den Krisenstab in der Regel unmittelbar.

Abbildung 8 (Seite 28) gibt einen Überblick über Meldewege in einer Einrichtung und die Alarmierung relevanter Personen.

⁴⁰ Feuerwehr-Dienstvorschrift 1999, Seite 29.

⁴¹ Jungbluth 2005, Seite 17.

Abbildung 8: Meldewege und Alarmierung



3.4.1.3.2 Krisenkommunikation

Die Krisenkommunikation beinhaltet die Kommunikation der Krise an die Öffentlichkeit und hier insbesondere an die Medien. Diese Aufgabe wird von der Pressestelle im Rahmen der Öffentlichkeitsarbeit wahrgenommen.

In der besonders bedeutsamen Anfangsphase einer Krisenentwicklung sind die Einbeziehung und zeitnahe Benachrichtigung anderer Organisationen, der Medien, der Bevölkerung sowie die Information der eigenen Organisation von zentraler Bedeutung. Die Kriseninformationsarbeit muss unmittelbar mit der Krisenbewältigung beginnen. Pressemitteilungen müssen innerhalb kürzester Zeit herausgegeben werden können. Aber auch eine Geheimhaltung von Informationen ist eine Form der Krisenkommunikation. Die Identifizierung geheim zu haltender Informationen ist daher besonders wichtig.

Für Krisen, die die Bevölkerung betreffen, sollten Hotlines und benutzerfreundliche Internetseiten vorbereitet sein. Besonders ausgebildetes Personal, inklusive Verstärkungspersonal, muss unmittelbar in einer Krise einberufen werden können, um die erhöhten Anforderungen der Bevölkerungskommunikation bewältigen zu können. In dieser Phase ist es ferner zwingend erforderlich, die interne Kommunikation zu intensivieren.

Die ersten Meldungen über ein Ereignis oder eine Krise werden oft durch die Medien vermittelt. Bereits im Vorfeld einer Krise ist daher mindestens ein Pressesprecher zu benennen, der jegliche Kommunikation mit den Medien übernimmt. Kontakte zu Journalisten bestehen deshalb schon in der frühesten Phase der Lage- beziehungsweise Situationsentwicklung. Die Wahrnehmung der Krise und das Image des Krisenmanagements sind im beachtlichen Umfang von der Medienberichterstattung abhängig. Eine zielführende und effiziente mediale Krisenkommunikation erfordert demzufolge unter anderem

- ein etabliertes Netzwerk mit lokalen, regionalen beziehungsweise nationalen Medien,
- Handlungsempfehlungen für die ersten Kontakte mit Medien bei Eintritt einer Krise,
- vorbereitete Hintergrundunterlagen und Muster für Pressemitteilungen, Sprechzettel etc.,
- Erfahrungen mit Pressekonferenzen und spezielles Medientraining sowie
- gegebenenfalls externe Unterstützung durch Krisenkommunikationsspezialisten.

Es ist wichtig, dass bei Krisen, die die Öffentlichkeit betreffen, verantwortliche Entscheidungsträger (Unternehmensleiter, Behördenleiter, Pressesprecher oder Informationsverantwortliche der Einrichtung) frühzeitig/rechtzeitig und lageangepasst in den Medien auftreten. Die Aussagen müssen balanciert formuliert werden sowie eindeutige und wahre Informationen in einer verständlichen Sprache vermitteln. Grundregeln einer externen Krisenkommunikation sind:

- Jede Krise ist auch eine Informationskrise.
- Krisenmanagement ist auch Informationsmanagement.
- Die ersten Stunden einer Krise sind von entscheidender Bedeutung: Während dieser Phase wird durch vermittelte Informationen ein Eindruck erweckt, der leicht einen bleibenden Charakter hat.
- Die Qualität der Krisenkommunikation bestimmt den öffentlichen Eindruck, ob die Verantwortlichen der Krise gewachsen sind oder nicht.
- Die Information muss die Bedürfnisse der Öffentlichkeit befriedigen.
- Informationsverantwortliche sollen den Krisenstab über Informationsbedürfnisse der Öffentlichkeit und der Medien sowie über die festgestellten Wirkungen unterrichten.

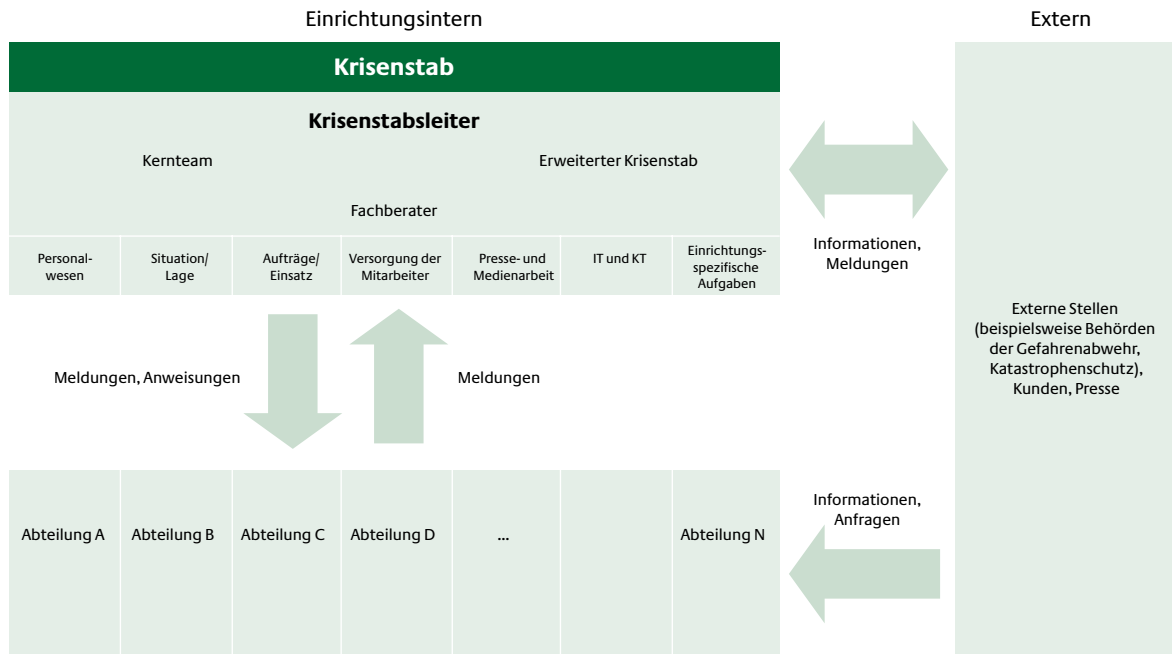
WICHTIGER HINWEIS

Es ist darauf zu achten, dass nur autorisiertes Personal Informationen nach außen gibt.

Bei längeren, schweren Ereignissen ist es ratsam, dass ein Vertreter aus der Unternehmens- beziehungsweise Behördenleitung die Kommunikation nach außen übernimmt. Hierfür wird er vom Krisenstab stetig mit aktuellen Informationen versorgt und intensiv beraten. Der Krisenstabsleiter übernimmt in diesem Fall die Koordination der internen Krisenbewältigung und trifft nach wie vor alle Entscheidungen.

Die folgende Abbildung (Abbildung 9, Seite 30) fasst die Struktur von Aufbau- und Ablauforganisation schematisch zusammen.

Abbildung 9: Aufbau- und Ablauforganisation



3.4.1.4 Krisenstabsraum

Der Krisenstabsraum ist der Raum, der speziell dem Krisenstab vor, während und nach einer Krise zur Verfügung steht. Er wird auch als Lagezentrum oder Krisenbesprechungsbe- reich bezeichnet.

Der Krisenstabsraum dient als Sammelpunkt für die Mit- glieder des Krisenstabes. Bei der Planung und Einrichtung dieses Raumes sind die Aspekte Standort, Ausweichstandort und Ausstattung zu berücksichtigen.

Der Standort sollte im Vorfeld festgelegt und gut erreichbar sein sowie Schutz vor Gefahrenwirkungen bieten. Für den Fall des Funktionsausfalls am ersten Standort ist ein Alterna- tivstandort vorzusehen, über dessen Existenz und Lage gege- benenfalls nur die Unternehmens- beziehungsweise Behör- denleitung, der Krisenstab und sein Leiter informiert sind. Zur Ausstattung des Krisenstabsraumes gehören eine re- dundante Kommunikations- und Informationsinfrastruktur sowie effektive technische Mittel zur Informationsbeschaf- fung, Verarbeitung und Darstellung. Eine Notstromversor- gung für alle technischen Geräte und die Beleuchtung sollte zur Verfügung stehen.⁴²

⁴² Eine detaillierte Zusammenstellung der räumlichen und tech- nischen Ausstattung des Krisenstabsraumes sowie sonstiger Ausstattungsmerkmale findet sich in Anhang V.6.

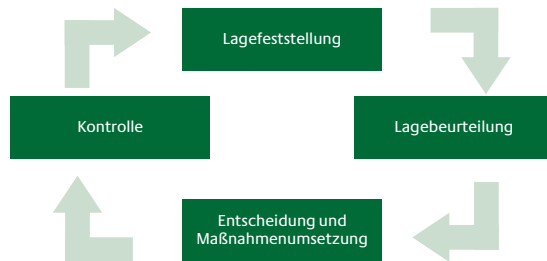
Sicherheitsaspekte im Krisenstabsraum wie Nichteinsehbar- keit und Abhörsicherheit sollten gegebenenfalls gewährleis- tet sein. Der Raum und seine Ausstattung sind in regelmä- ßigen Abständen auf ihre Funktionsfähigkeit zu überprüfen.

Die Art und Größe der personellen, räumlichen und tech- nischen Ausstattung des Krisenstabes und des dazugehörigen Raumes für die Krisensituation ist abhängig von den beste- henden Risiken, der Art und dem Umfang der Aufgaben und Prozesse, der Größe und der Spartenvielfalt der Einrichtung, von örtlichen Besonderheiten und davon, ob es sich um den Hauptsitz des Unternehmens oder der Behörde handelt oder um Niederlassungen oder Zweigbetriebe.

3.4.2 Krisenbewältigung

Nach Aktivierung des Krisenstabes beginnen Tätigkeiten zur Krisenbewältigung. Treffpunkt ist der Krisenstabsraum, Handlungsgrundlage der Krisenplan. Eine wesentliche Vor- aussetzung für die Krisenbewältigung sind die Informations- und Kommunikationsverbindungen. Sie sollten (wieder) funktionieren. Alle Handlungen und Entscheidungen im Rahmen der Krisenbewältigung werden vom Beginn der Krisenstabsarbeit an dokumentiert.

Abbildung 10: Kreislauf zur Bewältigung von Extremereignissen⁴³



Die Bewältigung eines Extremereignisses vollzieht sich in einem Kreislauf, der aus den Elementen Lagefeststellung, Lagebeurteilung, Entscheidung und Maßnahmenumsetzung sowie Kontrolle besteht. Dieser Kreislauf wird nach jedem neuen Teilereignis sowie jeder Maßnahme, die die Krisensituation signifikant verändert, erneut durchlaufen bis zur Rückkehr zur Normalsituation.

3.4.2.1 Lagefeststellung Informationssammlung

Der Krisenstab sammelt Informationen zum Ereignis. Das aus der Informationssammlung geschaffene Lagebild bildet die Voraussetzung für eine sinnvolle Beurteilung der Krise sowie der Entscheidung zur Umsetzung von Aktivitäten zur Schadensminimierung. Es gibt Aufschluss über

- Art, Umfang und Abläufe der Ereignisse,
- die Auswirkungen und mögliche Entwicklungen der Lage,
- die Möglichkeiten der Reaktion sowie
- die bisher ergriffenen Maßnahmen.⁴⁴

Erfasst werden alle bisherigen Meldungen und persönlichen Erkundungen. Benötigt werden auch Informationen über die Gefahren- und Schadenslage sowie über eigene personelle und technische Kapazitäten.

Die Zusammenstellung von Plan- und Kartenmaterial im Vorfeld einer Krise erleichtert die Informationssammlung während der Bewältigungsphase. Zu den Materialien zur Informationssammlung gehören

- Lagepläne und Karten (Gelände, Gebäude),
- Gebäudepläne (Feuerlöscher, Ausgänge, Notausgänge, Fluchtwege, Schutzräume, Krisenstabsraum) sowie
- Anlagenpläne und Netzpläne (Hauptschalter für Stromversorgung, Haupthähne für Gas und Wasser sowie Rohrleitungen).

Die Pläne und das Kartenmaterial sind regelmäßig zu aktualisieren.

Mittel der Informationssammlung und Informationsverarbeitung

Grundlage der Informationssammlung sind Meldungen der Mitarbeiter der Einrichtung, von Kunden und Bürgern, externen privaten und öffentlichen Akteuren (zum Beispiel Kunden, Polizei, Katastrophenschutz) sowie Meldungen aus den Medien.

Die notwendigen Ausstattungsmittel zur Informationssammlung gehören zum Teil zu den Ausstattungsmerkmalen des Krisenstabsraumes.⁴⁵ Hierzu zählen beispielsweise Telefonapparate, Internet, Radio und TV-Geräte. Diese Mittel werden um oben genannte Karten sowie Nachschlagewerke ergänzt.

Insbesondere eine grafische Aufbereitung erleichtert das intuitive Erfassen der Informationen für alle Beteiligten. Wird in der Einrichtung ein geografisches Informationssystem⁴⁶ verwendet, können bereits im Vorfeld wichtige Rauminformationen elektronisch vorgehalten und dargestellt werden.

Darstellung eines Lagebildes

Im Krisenstab wird ein aktuelles Situations- beziehungsweise Lagebild erstellt. Das Lagebild bestimmt sich aus den Faktoren Ort, Zeit, gegebenenfalls Wetter, Schadensereignis/Gefahrenlage, eingeleitete Maßnahmen und den weiteren Reaktionsmöglichkeiten.⁴⁷ Es fasst alle bisherigen Meldungen und erhaltenen Informationen zusammen und generiert dar-

⁴³ Nach Feuerwehr-Dienstvorschrift 1999, Seite 25.

⁴⁴ Jungbluth 2005, Seite 38.

⁴⁵ Siehe Anhang V.6.

⁴⁶ Geografische Informationssysteme sind datenbankgestützte Softwareprodukte, mit Hilfe deren raumbezogene Daten erfasst und analysiert werden können.

⁴⁷ Feuerwehr-Dienstvorschrift 1999, Seite 26.

aus eine komprimierte Übersicht zum momentanen Status. Zu wichtigen Unterlagen für die Lagedarstellung zählen:

- Lagekarten
- Gebäudepläne
- Berichte über das Ereignis
- Ton- und Bildaufzeichnungen⁴⁸

Die folgende Abbildung fasst die wichtigsten Punkte zur Lagefeststellung zusammen.

Abbildung 11: Überblick zur Lagebildfeststellung⁴⁹

Schadensereignis • Schadensart • Schadensursache Schadensobjekt • Art • Größe • Material • Konstruktion • Umgebung Schadensumfang • Menschen • Funktionalität • Tiere, Umwelt • Sachwerte • Produktionsprozesse • Zustand der Funktionsfähigkeit des Unternehmens oder der Behörde • Mittelbare Schäden	Krisenbewältigung • Krisenstabsabteilung • Krisenstab Personal mit Funktion im Krisenfall • Stärke • Verfügbarkeit • Zusatzausbildung (Beispiel: Erste Hilfe) • Leistungsvermögen Mittel • IT • Fahrzeuge • Geräte
--	---

3.4.2.2 Lagebeurteilung, Entscheidung und Maßnahmenumsetzung

Das Lagebild wird systematisch beurteilt. Hieraus ergibt sich die Entscheidung über weitere Maßnahmen. Nach Beurteilung der Lage entscheidet der Krisenstabsleiter über das weitere Vorgehen.

Unter Mittel zur Lagebeurteilung fallen⁵⁰:

- das Lagebild selbst
- gesetzliche Grundlagen
- Richtlinien
- Merkblätter

Die Lage wird regelmäßig und bei Bedarf in Lagebesprechungen erörtert. Der Leiter des Krisenstabes muss bei allen denkbaren Krisen klare Entscheidungen zur Umsetzung von Maßnahmen treffen.⁵¹

3.4.2.3 Kontrolle

Im Rahmen der Kontrolle wird überprüft, ob die Anweisungen des Krisenstabes das Personal (zum Beispiel Niederlassungen oder Einsatzkräfte) auch erreicht hat und diese verstanden und korrekt umgesetzt wurden. Weiteres Ziel einer Kontrolle ist die Beobachtung der Auswirkungen von Entscheidungen.

Nach der Umsetzung einer Maßnahme ergibt sich ein neues Lagebild, das wiederum erfasst und dargestellt wird. Das neue Lagebild dient als Grundlage, die Auswirkungen der zu diesem Zeitpunkt getroffenen Maßnahmen zu kontrollieren und die weiteren Schritte zu planen.

3.4.2.4 Sicherstellung der betrieblichen und dienstlichen Kontinuität

Ein wesentliches Element der Krisenbewältigung in Kritischen Infrastruktureinrichtungen ist die Aktivierung von Notmaßnahmen, redundanten Systemen und Ersatzsystemen, die während des Risikomanagementprozesses als präventive Maßnahmen zur betrieblichen und dienstlichen Kontinuität identifiziert und installiert wurden.⁵²

3.4.2.5 Rückkehr zum Normalbetrieb

Analog zur Aktivierung des Krisenmanagements erfolgen die Aufhebung des aktiven Krisenmanagements und die Rückkehr zum Normalbetrieb durch den Krisenstabsleiter. Auch hierfür sind ein Schwellenmodell oder ein Deeskalationsmodell denkbar.⁵³ Im Falle des Schwellenmodells erfolgt die Überführung in den Normalbetrieb ohne Zeitverzögerung. Im Rahmen des Deeskalationsmodells erfolgt die Überführung stufenweise. Es ist anzunehmen, dass dieses Modell in den meisten Krisenfällen zum Tragen kommt, insbesondere nach Krisen mit Auswirkungen auf verschiedene Bereiche der Einrichtung.

3.4.2.6 Dokumentation der Krisenbewältigung

Alle eingehenden und ausgehenden Meldungen (beispielsweise über Telefon, Fax, E-Mail) sowie alle Entscheidungen und Maßnahmen und Aktivitäten sollten schriftlich dokumentiert werden. Hierbei können standardisierte Formblätter helfen, die jeweils mit Datum und dem Namen des Bearbeiters versehen sind. Weitere Hilfsmittel zur Dokumentation sind:

⁴⁸ Angepasst nach Feuerwehr-Dienstvorschrift 1999, Seite 41.

⁴⁹ Nach Feuerwehr-Dienstvorschrift 1999, Seite 27.

⁵⁰ Nach Feuerwehr-Dienstvorschrift 1999, Seite 45.

⁵¹ Anhang V.3 enthält für ausgewählte Krisensituationen Checklisten zur Umsetzung erster Maßnahmen.

⁵² Vgl. Kapitel 3.3.1.

⁵³ Vgl. Kapitel 3.4.1.3.1.

- Vordrucke
- Ein- und Ausgangsnachweise
- Ereignistagebücher
- Meldeprotokolle
- elektronische Medien

Die Dokumentation während einer Krise dient der Evaluierung sowie der Klärung von Finanzierungs-, Versicherungs- und Rechtsangelegenheiten. Daher sollte sie gerichtsfest erfolgen.

3.4.3 Nachbereitung

Nach der Rückkehr zum Normalbetrieb erfolgt anhand der Dokumentation eine Nachbereitung der Krisenbewältigung. Diese kann in Form eines Berichtes erfolgen, der zeitnah und vertraulich von dem Leiter des Krisenstabes erstellt und an die Unternehmens- beziehungsweise Behördenleitung übermittelt wird. Dieser Bericht dient der Unternehmens- beziehungsweise Behördenleitung als Grundlage zur Beurteilung eventueller Rechtsfolgen für/gegen das Unternehmen beziehungsweise die Behörde oder eingesetztes Personal. Weiteres wichtiges Ziel der Nachbereitung ist die Prüfung der Funktionsfähigkeit und Praktikabilität des Krisenplans, um Lücken im Krisenmanagement aufzudecken und diese mit Hilfe ergänzender Planung zu schließen.⁵⁴

3.4.4 Übungen

Extreme Ereignisse sind in der Regel sehr selten. Daher sollten Strukturen und Abläufe in einer Krise in regelmäßigen Abständen geübt werden, damit sie im Ereignisfall reibungslos funktionieren. Ziele solcher Übungen sind⁵⁵:

- die Funktionsfähigkeit und die Praktikabilität des Krisenplans zu überprüfen,
- die Krisenkoordination und -kommunikation zu trainieren und
- krisenspezifische Abläufe zu testen.

Zur Realisierung von Übungen stehen verschiedene Übungsarten und -methoden zur Verfügung, die sich in Abstraktionsgrad und Übungsaufwand unterscheiden. Hierzu zählen:

- **Stabsübungen** (Beteiligte: Mitglieder des Krisenstabes – theoretische Bewältigung eines Schadensszenarios)

- **Stabsrahmenübungen** (Beteiligte: zusätzlich zum Stab werden weitere Bereiche einbezogen – theoretische Bewältigung eines Schadensszenarios)
- **Vollübungen** (Beteiligte: alle Leitungsebenen und Stellen – tatsächliche Abarbeitung eines Übungsszenarios)
- **Übungen für Teilfunktionen** (beispielsweise Evakuierungsübungen, Kommunikationstraining)
- **Alarmierungsübungen** (Feststellung der Erreichbarkeit und der Zeiten bis zur Einsatzbereitschaft)

Kriterien zur Auswahl einer bestimmten Übungsmethode sind:

- das vorgegebene Ziel
- die gewünschten Wiederholungsintervalle
- der eingeplante Übungsaufwand

Nahe an der Wirklichkeit sind Vollübungen, die alle Führungsebenen und Mitarbeiter mit einbeziehen. Diese sind aber sehr aufwändig in der Vorbereitung und Durchführung.

Stabsübungen und Stabsrahmenübungen beinhalten dagegen die theoretische Bewältigung von Schadensszenarios. Im Rahmen von Stabsübungen werden die Kernbereiche der Krisenmanagementstruktur geübt, beispielsweise der Krisenstab und die Funktionalität des Krisenplans. Stabsrahmenübungen beziehen weitere Stellen inklusive zusätzlicher Entscheidungs- und Berichtswege mit in die Übung ein.

Bei Stabsübungen und Stabsrahmenübungen werden alle Teilereignisse mit Hilfe eines Übungsdrehbuches, mit dem die Übungsleitung die Übungen überwacht und steuert, eingespielt. Das Übungsdrehbuch ist den übenden Akteuren in der Regel nicht bekannt. Es antizipiert mögliche Reaktionen der Akteure. Unvorhergesehene Reaktionen können von der Übungsleitung kurzfristig in die Übung integriert werden.

Der Nachteil von Stabs- und Stabsrahmenübungen liegt in der theoretischen Bewältigung des Schadensszenarios begründet. Dennoch ermöglicht eine Stabs- oder Stabsrahmenübung die Beübung der strategischen Kernbereiche des Krisenmanagements, ohne den Aufwand einer Vollübung unter Beteiligung aller Mitarbeiter betreiben zu müssen.

Mit Übungen für Teilfunktionen können ausgewählte Ziele verfolgt werden, die einen geringeren Planungsaufwand als Vollübungen benötigen.

⁵⁴ Anhang V.4 beinhaltet eine Liste erster konkreter Schritte im Rahmen der Nachbereitung und analysiert, welche Verbesserungsmöglichkeiten zur Vorbereitung auf eine potenzielle neue Krise bestehen. Weitere Informationen sind beispielsweise unter Bundesamt für Sicherheit in der Informationstechnik 2006 zu finden.

⁵⁵ Gustin 2004, Seite 226.

Alarmierungsübungen dienen zum Test der Alarmierungspläne und des Schwellen- beziehungsweise Eskalationsmodells.

Zu den Übungsvorbereitungen gehören folgende Entscheidungen über Planungsgrundlagen⁵⁶, die für alle Arten von Übungen gelten:

- Welche Übungsart wird gewählt?
- Welche Ziele verfolgt die Übung?
- Wer soll an der Übung teilnehmen?
- Wer soll die Übungssteuerung übernehmen?
- Wann und wo soll die Übung stattfinden?
- Welche technischen Hilfsmittel sind für die Durchführung der Übung erforderlich?
- Welche Aspekte sollte das Drehbuch der Übung beinhalten?
- Wie wird die Übung dokumentiert und evaluiert?

Am Ende der Übung werden die Reaktionen der Teilnehmer und insbesondere der reibungslose Ablauf des Krisenplans anhand einer Dokumentation überprüft. Hierdurch können Schwachstellen identifiziert und der Krisenplan aktualisiert werden.⁵⁷

3.5 Phase 5: Evaluierung des Risiko- und Krisenmanagements

Die Evaluierung bezieht sich auf alle Phasen, also sowohl auf die Prüfung der in der Vorplanung festgelegten Punkte, die Prüfung der Aktualität bestehender Risiken, die Prüfung der umgesetzten vorbeugenden Maßnahmen auf ihre Wirksamkeit sowie die Prüfung des Krisenmanagements. Sie sollte regelmäßig erfolgen, vorzugsweise jährlich.

Zusätzliche Evaluierungen sind notwendig:

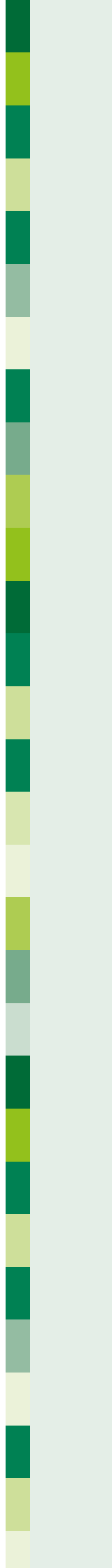
- nach der Umsetzung von Maßnahmen,
- nach einer Erweiterung der/Veränderung in der Einrichtung sowie
- bei einer Änderung der Gefährdungslage.

Ein Risiko- und Krisenmanagement muss gelebt werden. Ein dauerhafter Mehrwert aus einem Risiko- und Krisenmanagement kann sich für die Einrichtung nur einstellen, wenn alle Phasen regelmäßig durchlaufen werden und so die Grundlage für eine stetige Optimierung des Sicherheitsniveaus im Unternehmen beziehungsweise in der Behörde gelegt wird.

⁵⁶ Gustin 2004, Seite 262.

⁵⁷ Anhang V.5 beinhaltet eine Checkliste zu Krisenübungen.

Anhang



I. Literaturverzeichnis

American Water Works Association (2001) (Hrsg.): Emergency Planning for Water Utilities, Manual of Water Supply Practices M19. Denver.

Australian/New Zealand Standard (2004) (Hrsg.): Risk Management AS/NZS 4360:2004. Standards Australia/Standards New Zealand. Sydney/Wellington.

Bockslaff, K. (1999): Die eventuelle Verpflichtung zur Errichtung eines sicherungstechnischen Risikomanagements. In: NVersZ. Nr. 3, S. 104–110.

Bockslaff, K. (2004): Sicherheit – ein Beitrag zur Wertschöpfung im Unternehmen. In: WIK – Zeitschrift für die Sicherheit der Wirtschaft. Nr. 5, S. 27–32.

British Standard (2006) (Hrsg.): DPC BS 25999-1 Code of practice for business continuity management. London (Entwurf).

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2005): Leitfaden für die Errichtung und den Betrieb einer Notstromversorgung in Behörden und anderen wichtigen öffentlichen Einrichtungen. http://www.bbk.bund.de/cln_007/nn_398726/DE/05_Publikationen/05_Fachpublikationen/03_Leitfaeden/Leitfaeden__node.html__nnn=true (15. Oktober 2007).

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2007): Betriebliche Pandemieplanung – Kurzinformation der Bund-Länder-Arbeitsgruppe „Influenzapandemieplanung in Unternehmen“. http://www.bbk.bund.de/cln_027/nn_402322/SharedDocs/Publikationen/Publikation_20KatMed/Betr-Pandemiepla,templateId=raw,property=publicationFile.pdf/Betr-Pandemiepla.pdf (15. Oktober 2007).

Bundesamt für Sicherheit in der Informationstechnik (2005): BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“. http://www.bsi.bund.de/literat/bsi_standard/standard_1003.pdf (4. Oktober 2007).

Bundesamt für Sicherheit in der Informationstechnik (2006): COMCHECK und ALEX. Beschreibungen, Checkliste und Hilfen für Kommunikationsüberprüfungen und Alarmierungsübungen. <http://www.bsi.bund.de/fachthem/kritis/com-check.pdf> (16. Oktober 2007).

Bundesamt für Sicherheit in der Informationstechnik (2007): G 1 Gefährdungskatalog Höhere Gewalt. <http://www.bsi.bund.de/gshb/deutsch/g/g01.htm> (10. Oktober 2007).

Bundesamt für Sicherheit in der Informationstechnik (2008): BSI-Standard 100-4 „Notfallmanagement“. (Veröffentlichung im Internet voraussichtlich Januar 2008.)

Bundesministerium des Innern (2005): Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Empfehlungen für Unternehmen. http://www.bbk.bund.de/cln_007/nn_398726/DE/05_Publikationen/05_Fachpublikationen/03_Leitfaeden/Leitfaeden__node.html__nnn=true (15. Oktober 2007).

Department of Health and Human Services and the Centers for Disease Control and Prevention (2007): Business Pandemic Influenza Planning Checklist. <http://www.pandemicflu.gov/plan/workplaceplanning/businesschecklist.html> (15. Oktober 2007). [Übersetzung des Verbandes deutscher Betriebs- und Werksärzte, Berufsverband deutscher Arbeitsmediziner VDBW e. V.: http://www.vdbw.de/de/grippe_pandemie/Checkliste_fuer_Firmen_im_Rahmen_der_Influenza.pdf (15. Oktober 2007).]

Department of Homeland Security (2006): Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructures. <http://www.pandemicflu.gov/plan/pdf/cikrpandemicinfluenzaguide.pdf> (15. Oktober 2007).

Dost, S. (2006): Risk Management – Features of Corporate Risks and the Likelihood of Identification. Innovation and Technical Progress: Benefit without Risk? In: Book of Abstracts of the 15th Annual Conference of the Society for Risk Analysis (Ljubljana, September 11–13, 2006), S. 21.

Egli, T. (1999): Richtlinie Objektschutz gegen Naturgefahren. St. Gallen.

Federal Emergency Management Agency (2003) (Hrsg.): Risk Management Series Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings – FEMA 426. <http://www.fema.gov/plan/prevent/rms/rmsp426> (15. Oktober 2007).

Feuerwehr-Dienstvorschrift 100 (1999): Führung und Leitung im Einsatz – Führungssystem. <http://www.idf.nrw.de/download/normen/fwdv100.pdf> (15. Oktober 2007).

Gesellschaft für Anlagen- und Reaktorsicherheit (2007) (Hrsg.): Managementsysteme in Kernkraftwerken, GRS – 229. Köln.

Gray, P. C. R. u. a. (2000): Risk communication in print and on the web. A critical guide to manuals and internet resources on risk communication and issues management. <http://www.fz-juelich.de/inb/inb-mut/rc/inhalt.html> (4. Oktober 2007).

Gustin J. F. (2004): Disaster & Recovery Planning: A Guide for Facility Managers. Lilburn.

International Risk Governance Council (2006) (Hrsg.): White paper on managing and reducing social vulnerabilities from coupled critical infrastructures. <http://www.irgc.org/irgc/IMG/pdf/IRGC%20WP%20No%203%20Critical%20Infrastructures.pdf> (15. Oktober 2007).

Jungbluth, F. (2005) (Hrsg. Euroforum Verlag): Recht & Haftung für technische Manager, Grundlagen, Aufbau und Methoden eines effektiven Notfallmanagements. Düsseldorf.

Jungermann, H. u. a. (1991): Risikokontroversen – Konzepte, Konflikte, Kommunikation. Berlin.

Lewis, T. G. (2006): Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation. Hoboken.

National Fire Protection Association – NFPA 1600 (2004) (Hrsg.): Standard on Disaster/Emergency Management and Business Continuity. Quincy.

Rahmstorf, S. u. a. (2006): Der Klimawandel. München.

Robert Koch Institut (2005): Beispiel von Maßnahmenplanungen im Influenza-Pandemiefall. http://www.rki.de/cln_049/nn_200120/DE/Content/InfAZ/I/Influenza/Pandemieplanung_Konzern-28102005,templateId=raw,property=publicationFile.pdf/Pandemieplanung_Konzern-28102005.pdf (22. Oktober 2007).

Robert Koch Institut (2007a): Nationaler Pandemieplan, Teil II. http://www.rki.de/cln_048/nn_200132/DE/Content/InfAZ/I/Influenza/influenzapandemieplan__II,templateId=raw,property=publicationFile.pdf/influenzapandemieplan__II.pdf (6. Oktober 2007).

Robert Koch Institut (2007b): Anhang zum Influenzapandemieplan. http://www.rki.de/cln_048/nn_200132/DE/Content/InfAZ/I/Influenza/Influenzapandemieplan__Anhang,templateId=raw,property=publicationFile.pdf/Influenzapandemieplan__Anhang.pdf (6. Oktober 2007).

Rosenthal, U. (1992): Crisis management: On the thin line between success and failure. In: Asian Review of Public Administration. Vol. IV No.2, S. 73–78.

Rössing, R. von (2005): Betriebliches Kontinuitätsmanagement. Bonn.

The Business Continuity Institute (2005): Business Continuity Management, Good Practice Richtlinien. http://www.thebci.org/BCIGPG2005_de.pdf (15. Oktober 2007).

Trauboth, J. H. (2002): Krisenmanagement bei Unternehmensbedrohungen. Präventions- und Bewältigungsstrategien. Stuttgart, München, Hannover, Berlin, Weimar, Dresden.

Umweltbundesamt Bundesrepublik Deutschland (2001a): Checklisten für die Untersuchung und Beurteilung des Zustandes von Anlagen mit wassergefährdenden Stoffen und Zubereitungen; Nr. 10 Betriebliche Alarm- und Gefahrenabwehrplanung. http://www.umweltbundesamt.de/anlagen/jeg/downloads/deutsch/check10_bagap_rev00.pdf (15. Oktober 2007).

Umweltbundesamt Bundesrepublik Deutschland (2001b): Checklisten für die Untersuchung und Beurteilung des Zustandes von Anlagen mit wassergefährdenden Stoffen und Zubereitungen; Nr. 11 Hochwassergefährdete Anlagen. http://www.umweltbundesamt.de/anlagen/jeg/downloads/deutsch/check11_hochwasser_rev00.pdf (15. Oktober 2007).

VdS-Richtlinien (2007): Gesamtprogramm. <http://www.vds.de/Gesamtverzeichnis.487.0.html> (9. November 2007).

Verwaltungs-Berufsgenossenschaft VBG (2007) (Hrsg.): Zwischenfall, Notfall, Katastrophe – Leitfaden für die Sicherheits- und Notfallorganisation. Hamburg.

Wiedemann, P. M. u. a. (2000): Risikokommunikation für Unternehmen. Düsseldorf.

Zentrum für Alpine Umweltforschung (2000) (Hrsg.): Leitfaden für erdbebensicheres Bauen. Sion.

II. Abkürzungen

ABC	Atomar, biologisch, chemisch
AktG	Aktiengesetz
ARE	Abhängigkeit von Risikoelement
BA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
DIN	Deutsches Institut für Normung
EW	Eintrittswahrscheinlichkeit
HGB	Handelsgesetzbuch
IT	Informationstechnik
KGaA	Kommanditgesellschaft auf Aktien
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KT	Kommunikationstechnik
THW	Bundesanstalt Technisches Hilfswerk
TUIS	Transport-Unfall-Informationen- und Hilfeleistungssystem
V1 (bis 5)	Verwundbarkeitskriterium 1 (bis 5)
VVG	Gesetz über den Versicherungsvertrag

III. Begriffe

WICHTIGER HINWEIS:

Im Rahmen der Erstellung des Leitfadens ist deutlich geworden, dass es für die Themenfelder Risiko- und Krisenmanagement derzeit keine allgemeingültigen Definitionen gibt. Die hier aufgeführten Definitionen geben daher die Bedeutung der Begriffe wieder, wie sie im Leitfaden verwendet werden. Diese Verwendung der Begriffe im Leitfaden kann sich durchaus von der Verwendung in anderen Publikationen unterscheiden.

Begriff	Definition
Ablauforganisation	Die Ablauforganisation beschreibt und regelt die Arbeitsprozesse einer Organisationseinheit unter Berücksichtigung von Raum, Zeit, Personen und Sachmitteln.
Alarmierung	Information der Mitarbeiter, Einsatzkräfte und der Bevölkerung über eine akute Gefahr
Alarmstufe	Einstufung einer Lage bzw. einer Situation im Hinblick auf die zu ergreifenden Maßnahmen
Aufbauorganisation	Die Aufbauorganisation beschäftigt sich mit der Strukturierung einer Unternehmung in statische, vornehmlich hierarchische Einheiten.
Betriebliches Kontinuitätsmanagement	Management der Maßnahmen zur Aufrechterhaltung der Geschäftstätigkeiten im Krisenfall, beispielsweise die Aktivierung einer redundanten Leitwarte (Betriebliches Kontinuitätsmanagement = Business Continuity Management) ⁵⁸
Bevölkerungsschutz	Bevölkerungsschutz ist der Schutz sowie die Begrenzung und Bewältigung vor und von Auswirkungen von Kriegen, bewaffneten Konflikten, Naturkatastrophen und besonders schweren Unglücksfällen durch zivile Maßnahmen. Bund, Länder, Kommunen und Hilfeleistungsorganisationen arbeiten zum Schutz der Bevölkerung zusammen.
Einrichtung	Als Einrichtungen im Sinne dieses Leitfadens werden alle Unternehmen, Behörden und sonstigen Institutionen bezeichnet, die eine Kritische Infrastruktur betreiben.
Einzelverwundbarkeit	Bezieht sich in diesem Leitfaden auf ein Risikoelement und ein Verwundbarkeitskriterium
Epidemie	Zeitliche und örtliche Häufung einer Krankheit innerhalb einer Population

⁵⁸ Von Rössing 2005, Seite 426.

Begriff	Definition
Eskalationsmodell	Mechanismus der Einschätzung der Lage und Weiterleitung an das Management ⁵⁹
Evaluierung	Bewertung von Tätigkeiten
Exposition	Ausgesetztsein eines Objektes gegenüber einer Gefahr
Extremereignis	Extremereignisse sind seltene Ereignisse, die stark vom Durchschnitt abweichen und zu Krisen führen können.
Gefahr	Ursache einer möglichen Beeinträchtigung ⁶⁰
Gefährdung	Durch eine Gefahr ausgelöste negative Auswirkung auf Personen, Sachen, Sachverhalte, Umwelt oder Tiere
Katastrophe	Schadensereignis, das stark über die Ausmaße normaler Schadensereignisse hinausgeht und dabei Leben, Gesundheit, Sachgüter oder wichtige Infrastrukturen erheblich gefährdet oder zerstört
Krise	Eine vom Normalzustand abweichende Situation, die trotz vorbeugender Maßnahmen im Unternehmen bzw. der Behörde eintritt und mit der normalen Aufbau- und Ablauforganisation nicht bewältigt werden kann
Krisenkommunikation	Alle kommunikativen Aktivitäten, die im Zusammenhang mit einer Krisensituation durchgeführt werden zur Verhinderung oder Begrenzung von Vertrauensverlust, Imageeinbußen und Schadensbegrenzung. Krisenkommunikation impliziert die klare Zuordnung von Zuständigkeiten und Verantwortlichkeiten sowie eine eindeutige Kommunikationslinie für ein inhaltlich und argumentativ einheitliches Auftreten.
Krisenmanagement	Alle Tätigkeiten zur Vorbereitung auf Krisen, zur Krisenbewältigung und zur Nachbereitung von Krisen
Krisenplan	Masterplan für das Krisenmanagement, der alle Maßnahmen abdeckt, die im Zuge einer Krise zu ergreifen sind
Krisenstab	Struktur, die die Voraussetzungen zur Koordination aller krisenbezogenen Tätigkeiten schafft
Krisenstabsraum	Raum, der speziell dem Krisenstab während und nach einer Krise sowie im Vorfeld zur Durchführung von Übungen zur Verfügung steht
Kritische Infrastrukturen	Kritische Infrastrukturen sind Organisationen und Einrichtungen mit besonderer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. ⁶¹
Kritische Punkte	Siehe neuralgische Punkte

⁵⁹ Vgl. von Rössing 2005, Seite 428.

⁶⁰ Australian/New Zealand Standard 2004, Seite 3.

⁶¹ Definition Kritischer Infrastrukturen des AK KRITIS im Bundesministerium des Innern (BMI) vom 17. November 2003.

Begriff	Definition
Lage (oder Situation)	Art und Umfang der Beeinträchtigungen bzw. Schäden sowie ihre voraussichtliche Entwicklung
Lagebeurteilung	Bewertung von Beeinträchtigungen bzw. Schäden hinsichtlich der Auswirkungen und möglicher Maßnahmen
Lagefeststellung	Sammlung, Ordnung, Speicherung und Darstellung von Informationen über eine Lage
Maßnahmen, vorbereitende	Handlungsoptionen, die im Vorfeld von Krisen entwickelt, jedoch erst im Krisenfall angewendet werden.
Maßnahmen, vorbeugende	Handlungsschritte und Mittel, die im Vorfeld von Krisen entwickelt und umgesetzt bzw. eingesetzt werden und die Risiken für ein Unternehmen bzw. eine Behörde mindern. Hierzu zählen risikomindernde Maßnahmen, die Risikoelemente physisch schützen oder die Funktionsfähigkeit von Prozessen durch redundante Systeme oder Ersatzsysteme unterstützen. Beide Aspekte tragen zur betrieblichen Kontinuität bei.
Meldung	Berichte mit kurzen und präzisen Angaben über Vorgänge, Wahrnehmungen und Gegebenheiten zur Unterrichtung über eine Lage
Neuralgische Punkte	Prozessbereiche oder einzelne Risikoelemente, deren Beeinträchtigung zu weitreichenden Ausfällen oder Schäden führen
Pandemie	Länderübergreifender oder sogar weltweiter Ausbruch einer Krankheit
Plan-Do-Check-Act-Zyklus oder PDCA-Zyklus	Eine Vorgehensweise im Management von Prozessen zur stetigen Verbesserung der Qualität dieser Prozesse. Plan steht hierbei für eine umfassende Gesamtplanung von Prozessen, Do für die Umsetzung einer Planung, Check für die Überprüfung der Wirksamkeit von Prozessen und Act für die Verbesserung von Prozessen. Dieser Zyklus findet im hier beschriebenen Risiko- und Krisenmanagement auf unterschiedlichen Ebenen Anwendung.
Restrisiken	Risiken, die nach der Umsetzung von vorbeugenden Maßnahmen bestehen bleiben ⁶²
Risiko	Risiko wird als Funktion der Gefährdung und Verwundbarkeit von Risikoelementen und Teilprozessen betrachtet. Der Aspekt der Eintrittswahrscheinlichkeit eines Ereignisses ist Bestandteil der Gefährdungsanalyse.
Risikoanalyse	Systematisches Verfahren zur Ermittlung von Risikowerten Im Rahmen dieses Leitfadens gehören hierzu: ⁶³ • eine Analyse der Gefahren und der Exposition • eine Analyse der Verwundbarkeit aller relevanten Teilprozesse und Risikoelemente • ein Vergleich von Teilrisiken bezüglich einzelner Risikoelemente sowie ein Vergleich szenariobezogener Gesamtrisiken von Teilprozessen

⁶² Angepasst nach Australian/New Zealand Standard 2004, Seite 3.

⁶³ Australian/New Zealand Standard 2004, Seite 4.

Begriff	Definition
Risikobewertung	Verfahren, mit dem das Risiko für einen Teilprozess oder ein Risikoelement, das von einem Ereignis ausgeht, in ein Verhältnis zu zuvor entwickelten Zielen gesetzt wird. Es wird hierdurch ermittelt, ob das Risiko akzeptabel ist und eventuelle Restrisiken vertretbar sind.
Risikoelement	Einzelbestandteil kritischer Teilprozesse. Im Rahmen dieses Leitfadens zählen hierzu: • Menschen (Personal, sonstige Anwesende) • Gelände • Gebäude • Anlagen und Geräte • einrichtungsspezifische Sonderanlagen und Sondergeräte • Daten und Unterlagen • Betriebsmittel
Risikokommunikation	Verfahren für Unternehmen bzw. Behörden im Rahmen des Risikomanagements zum Erhalt und zur Herausgabe von Informationen über ein Risiko. Risikokommunikation betrifft dabei alle Kommunikationsprozesse, die sich auf die Identifizierung, Analyse, Bewertung sowie das Management von Risiken und die dafür notwendigen Interaktionen zwischen den Beteiligten beziehen. ⁶⁴
Risikomanagement	Prozess bzw. Verfahren zum planvollen Umgang mit Risiken
Risikominderung	Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit oder der Auswirkungen von Ereignissen auf die Einrichtung ⁶⁵
Risikoüberwälzung	Strategie, die bestehende Risiken auf andere Unternehmen, Behörden oder Versicherungen verlagert
Risikovermeidung	Strategische Entscheidungen, die dazu führen, dass Gefahren beseitigt werden oder die Eintrittswahrscheinlichkeit gegen null geht und somit Risiken nicht entstehen
Stabsrahmenübung	Stabsübung unter Mitwirkung zusätzlicher Einrichtungsebenen (Beispiel: Fachabteilungen)
Stabsübung	Übung mit ausschließlicher Beteiligung der Mitglieder des Krisenstabes und der Leitung der Einrichtung
Störung	Abweichung vom Normalzustand oder Normalablauf. Ursachen können eigen- oder fremdverursacht sein. Eine Störung wird von der normalen Aufbau- und Ablauforganisation bewältigt.
Störungsmanagement	Konzeptionelle, organisatorische, verfahrensmäßige und physische Voraussetzungen in der betrieblichen Aufbau- und Ablauforganisation, die eine bestmögliche Bewältigung der Störung ermöglichen

⁶⁴ Jungermann et al. 1991, Seite 5.

⁶⁵ Australian/New Zealand Standard 2004, Seite 5.

Begriff	Definition
Strategische Schutzziele	Beschreibungen von anzustrebenden Sollzuständen, die zu einer Evaluierung umgesetzter Maßnahmen herangezogen werden können
Szenario	Zusammenstellung von Annahmen über die mögliche Abfolge von Ereignissen bezüglich des jeweiligen Untersuchungsgegenstands, um kausale Zusammenhänge und Entscheidungspunkte herauszuarbeiten
Teilrisiko	Risiko, das sich auf ein Risikoelement bezieht
Teilverwundbarkeit	Verwundbarkeit, die sich auf ein Risikoelement bezieht
Verwundbarkeit	Anfälligkeit eines Objekts oder Systems gegenüber Gefahren
Verwundbarkeitskriterium	Bedingungen zur Einschätzung der Verwundbarkeit
Wahrscheinlichkeit	Maß für die Möglichkeit des Eintreffens eines Ereignisses zwischen null und eins
Wiederanlauf	Phase nach Abschluss der Krisenreaktion bis zur Einleitung des Notbetriebs ⁶⁶
Wiederherstellung	Vollständige Wiederherstellung des Normalzustands, der vor Eintreten der Krise vorlag ⁶⁷

⁶⁶ Rössing 2005, Seite 439.

⁶⁷ Rössing 2005, Seite 439.

IV. Gefahrenliste –

Anhaltspunkte zu Art, Exposition, Intensität, Wirkungen und möglichen Ansprechpartnern

WICHTIGER HINWEIS:

Diese Beispielliste gibt Hinweise auf mögliche Gefahren, die im Umfeld der Einrichtung auftreten können. Es wird kein Anspruch auf Vollständigkeit erhoben, weswegen die Liste im Bedarfsfall an die Gegebenheiten der untersuchten Standorte angepasst werden sollte.

Art der Gefahr	Exposition	Mögliche Intensität	Mögliche Wirkung	Zuständigkeiten, mögliche Informationsquellen
Hochwasser	insbesondere flussnahe und tief liegende Bereiche, Unter- und Erdgeschosse	weiträumige Überschwemmungen, Wasserstand bis mehrere Meter über Normalwasserstand, hohe Fließgeschwindigkeiten in Mittelgebirgen	Ausspülungen, Einstau (Feuchtigkeitsschäden)	Umweltbehörden, Hochwasserzentralen, Versicherungen
Sturm/Tornado	deutschlandweit möglich	in Böen sehr hohe Geschwindigkeiten	Druck- und Sogwirkung auf Bauwerke und sonstige Gegenstände, Zerstörung	Umweltbehörden, Deutscher Wetterdienst
Erdbeben	Standorte in Erdbebengebieten (Rheingraben, Kölner Bucht, Vogtland, Schwäbische Alb)	enorme horizontale und vertikale Kräfte, hoher Energieeintrag	Zerstörung von Rohrleitungen, Tanks, Transformatoren, Verbindungen von Anlagen und Bauwerken, Trümmerbildung	Bundesanstalt für Geowissenschaften und Rohstoffe
Großbrand/ Flächenbrand	weiträumig bewaldete Gebiete	extreme Hitzeentwicklung	Bedrohung des Personals, Zerstörung von Anlagen aufgrund der Hitzeentwicklung; betroffen sind Anlagen der Stromversorgung und IT	Umweltbehörden, Deutscher Wetterdienst, Feuerwehren, Ordnungsbehörden

Art der Gefahr	Exposition	Mögliche Intensität	Mögliche Wirkung	Zuständigkeiten, mögliche Informationsquellen
Dürre	insbesondere trockene, niederschlagsarme Regionen	langfristiges Ausbleiben von Niederschlägen, sehr geringe Niederschlagsmengen	Absinken des Grundwasserspiegels, Kühlwassermangel, Trinkwassermangel, Stromausfälle, Transportprobleme auf Wasserstraßen	Betreiber, Umweltbehörden, Deutscher Wetterdienst
Hitzewelle	deutschlandweit möglich	hohe Tages- und Nachttemperaturen	gesundheitliche Beeinträchtigung des Personals und der Kunden	Gesundheitsämter, Deutscher Wetterdienst
Größere Epidemie/Pandemie	weltweit/deutschlandweit/regional möglich	hoher Infektionsgrad, schneller Ausbreitungsgrad, Virulenz des Virus	Erkrankung des Personals und der Kunden, Verunsicherung von Mitarbeitern (psychologische Effekte wie Panik), Ausfall von Mitarbeitern mit erkrankten Angehörigen (Pflege)	Gesundheitsämter, Robert Koch Institut, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Ausfall der externen Stromversorgung	deutschlandweit möglich, mehrtägig, großflächig	–	Beeinträchtigung von Anlagen und Geräten	Versorger, Feuerwehr, Hilfsorganisationen
Ausfall der externen Wasserversorgung	deutschlandweit möglich	–	Beeinträchtigung von Personal, Anlagen und Geräten	Versorger, Feuerwehr, Hilfsorganisationen
Ausfall von ausgelagerten Spezialdienstleistungen	deutschlandweit möglich	–	Beeinträchtigung von Personal und Betriebsmitteln	Ordnungsbehörden, Verkehrsbehörden je nach Verkehrsträger
Gefahrgutunfall in der Einrichtung oder im näheren Umfeld der Einrichtung	im Umfeld von Gefahrgutstrecken (Schiene und Straße), im Umfeld von Anlagen, in denen Gefahrgut verwendet wird	hohe Konzentration des freigesetzten Agens, hohe toxische Wirkung des freigesetzten Agens	Beeinträchtigung des Personals, der Kunden, der Gebäude (Kontamination)	Umweltbehörden, Feuerwehren, TUIS ⁶⁸ , Gesundheitsämter

⁶⁸ Das Transport-Unfall-Informations- und Hilfeleistungssystem TUIS leistet seit 1982 bei Transport- und Lagerunfällen mit chemischen Produkten in ganz Deutschland Hilfe. An TUIS sind rund 130 Chemieunternehmen mit ihren Werkfeuerwehren und Spezialisten wie Chemikern, Toxikologen oder Fachleuten aus der Produktion

beteiligt. Die TUIS-Mitgliedsunternehmen sind rund um die Uhr und jeden Tag im Jahr telefonisch für öffentliche Dienststellen wie Feuerwehr, Polizei und andere Katastrophenschutz Helfer sowie die Deutsche Bahn AG erreichbar und helfen im Rahmen eines dreistufigen Systems.

Art der Gefahr	Exposition	Mögliche Intensität	Mögliche Wirkung	Zuständigkeiten, mögliche Informationsquellen
Anschlag mit konventioneller Spreng- und Brandvorrichtung	deutschlandweit möglich	lokal extrem hohe Zerstörungskraft	Beeinträchtigung des Personals, der Kunden, der Gebäude und Anlagen; Trümmerbildung	Polizei, Feuerwehr
Anschlag mit unkonventioneller Spreng- und Brandvorrichtung bzw. Freisetzung von ABC-Agenzien in der Einrichtung oder im näheren Umfeld	deutschlandweit möglich	hohe Konzentration des freigesetzten Agens, hohe toxische Wirkung des freigesetzten Agens	Beeinträchtigung des Personals, der Kunden, der Gebäude und Anlagen (Kontamination)	Polizei, Feuerwehr
Versagen der Informationstechnik	deutschlandweit möglich	hohes Schädigungspotenzial, schnelle Verbreitung	Beeinträchtigung von Anlagen und Geräten	Bundesamt für Sicherheit in der Informationstechnik/ Gefährdungskataloge ⁶⁹
menschliches Versagen im Zusammenhang mit IT-Systemen	deutschlandweit möglich	hohes Schädigungspotenzial, schnelle Verbreitung	Beeinträchtigung von Anlagen und Geräten	Bundesamt für Sicherheit in der Informationstechnik/ Gefährdungskataloge ⁶⁹
vorsätzliche Handlungen mit Hilfe oder auf IT	deutschlandweit möglich	hohes Schädigungspotenzial, schnelle Verbreitung	Beeinträchtigung von Anlagen und Geräten	Bundesamt für Sicherheit in der Informationstechnik/ Gefährdungskataloge ⁶⁹
Entführung	deutschlandweit möglich	–	Beeinträchtigung von Personal	Polizei
Erpressung	deutschlandweit möglich	–	Beeinträchtigung von Personal oder Produkten	Polizei
Diebstahl kritischer Anlagen, Geräte und/oder sonstiger Betriebsmittel	deutschlandweit möglich	–	mögliche Beeinträchtigung von Daten, Unterlagen, Anlagen und Geräten	Polizei

⁶⁹ Bundesamt für Sicherheit in der Informationstechnik 2007.

V. Checklisten

WICHTIGER HINWEIS:

Die hier aufgeführten Checklisten sollten an die individuellen Eigenschaften der Einrichtung angepasst werden. Die Anwendung dieser Checklisten ersetzt nicht den umfassenden Aufbau eines Risiko- und Krisenmanagements. Es wird kein Anspruch auf Vollständigkeit erhoben.

Die nachfolgenden Checklisten wurden mit Hilfe folgender Literatur erstellt:

- American Water Works Association 2001
- British Standard 2006
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2005
- Bundesministerium des Innern 2005
- Egli 1999
- Federal Emergency Management Agency 2003
- Gustin 2004
- Jungbluth 2005
- National Fire Protection Association 2004
- Umweltbundesamt 2005a
- Umweltbundesamt 2005b
- Zentrum für Alpine Umweltforschung 2000

Weiterführende Hinweise finden sich unter:

- Verwaltungs-Berufsgenossenschaft VBG 2007
- VdS-Richtlinien: Gesamtprogramm 2007

Weiterführende Hinweise insbesondere zum Thema Pandemieplanung finden sich unter:

- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2007
- Department of Health and Human Services and the Centers for Disease Control and Prevention
- Department of Homeland Security 2006

V.1 Vorbeugende Maßnahmen

V.1.1 Risiko- und Krisenmanagement – Allgemein

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Existiert ein Risiko-management?	Planung, Umsetzung, Aufrechterhaltung und ständige Verbesserung	☐	☐	☐	
2. Sind die Arbeitsabläufe im Rahmen des Risiko-managements geregelt?		☐	☐	☐	
3. Wurden strategische Schutzziele definiert?		☐	☐	☐	
4. Sind die kritischen Prozesse inventarisiert, klassifiziert und Richtlinien für den Umgang aufgestellt?	Inventarisierung, Kritikalitätsanalyse, Priorisierung kritischer Prozesse	☐	☐	☐	
5. Existiert ein Krisen-management (Management von Vorfällen)?	Meldewege, Meldeverfahren, Management von Vorfällen und Verbesserungen	☐	☐	☐	
6. Sind eine betriebliche Kontinuitätsplanung und ein betriebliches Kontinuitätsmanagement etabliert?	Planung von redundanten Systemen und Ersatzsystemen sowie Management dieser im Ereignisfall	☐	☐	☐	
7. Wird die Einhaltung von rechtlichen bzw. gesetzlichen Verpflichtungen überprüft?	Einhaltung von gesetzlichen Verpflichtungen, Richtlinien und Normen, Audit von Systemen	☐	☐	☐	
8. Werden Sicherheitsaspekte in der Personalentwicklung berücksichtigt?	Aufgaben und Verantwortlichkeiten, Überprüfung, Schulung und Sensibilisierung	☐	☐	☐	

V.1.2 Gelände, Gebäude, Anlagen – Hochwasser

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Gebäude					
1.1 Kann eine Überflutung geplanter oder bestehender Anlagen ausgeschlossen werden?		☐	☐	☐	
a) bedingt durch Hochwasser		☐	☐	☐	
b) bedingt durch Rückstau aus dem Kanalnetz		☐	☐	☐	
c) bedingt durch Grundwasseranstieg		☐	☐	☐	
d) bedingt durch zurückgehaltenes Löschwasser		☐	☐	☐	
1.2 Sind Maßnahmen zum Schutz der Einrichtung vor Hochwasser getroffen worden?		☐	☐	☐	
1.3 Wird bei der Neuplanung von Bauwerken, sofern möglich, auf eine erhöhte Anordnung geachtet?	Dies bezieht sich auf die Gebäude sowie alle Eintrittsöffnungen.	☐	☐	☐	
1.4 Ist die Gebäudehülle hochwassersicher?		☐	☐	☐	
1.5 Sind Öffnungen in der Gebäudehülle der Bauwerke hochwassersicher?	Hierzu zählen temporäre bzw. mobile sowie permanente Maßnahmen.	☐	☐	☐	
1.6 Sind Einrichtung und Nutzung der Innenräume an eine mögliche Hochwassergefahr angepasst?	Zum Beispiel durch die Nutzung wasserunempfindlicher Baumaterialien	☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1.7 Ist im Falle der Hebung des Grundwassers durch Hochwasser die Standsicherheit in Gefahr?	Zum Beispiel bei Unterschoßen (Aufschwimmeffekt)	☐	☐	☐	
1.8 Drohen Veränderungen des Baugrundes durch Auswaschungen?		☐	☐	☐	

2. Anlagen

2.1 Sind Behälter und Rohrleitungen ausreichend gegen Auftrieb gesichert bzw. verankert?	Hierzu zählen Verankerungen, die Bemessung der Öl- und Dieseltanks unter Berücksichtigung des hydrostatischen Drucks, die Bemessung der Zu- und Abflussleitungen, die Tankentlüftung sowie die Zuflussleitung zum Brenner.	☐	☐	☐	
2.2 Sind Behälter und Rohrleitungen ausreichend gegen mechanische Beschädigung durch Treibgut gesichert bzw. verankert?	Hierzu zählen Verankerungen, die Bemessung der Öl- und Dieseltanks unter Berücksichtigung des hydrostatischen Drucks, die Bemessung der Zu- und Abflussleitungen, die Tankentlüftung sowie die Zuflussleitung zum Brenner.	☐	☐	☐	
2.3 Wurde ein Rückstauschutz in der Kanalisation installiert?		☐	☐	☐	

V.1.3 Gelände, Gebäude, Anlagen – Erdbeben

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Gebäude					
1.1 Bieten die Gebäude/ Bauwerke Erdbeben- lasten hinreichenden Widerstand?	Hierzu zählen die Beach- tung der Normenwerke (DIN 4149, Eurocode 8) sowie die freiwillige Anwendung darüber hinausgehender Empfehlungen.	☐	☐	☐	
1.2 Sind Anlagen im Bau- werk hinreichend ver- ankert?	Hierzu zählen Tanks, Trans- formatoren etc.	☐	☐	☐	
1.3 Können strukturschwä- chende Veränderungen an tragenden Bauteilen ausgeschlossen werden?	Hierzu zählen große Bohr- löcher sowie nachträglich angebrachte Aussparungen.	☐	☐	☐	
2. Unterirdische Anlagen					
2.1 Werden Rohrleitungen in Erdbebengebieten im Hinblick auf die potenzielle Belastung verlegt?	Hierzu zählen eine Beach- tung der Bodenbeschaf- fenheit, eine Verlegung im rechten Winkel zu bekannten Verwerfungen mit flexiblen Verbindungen und Sicherheitsventilen sowie eine Verlegung re- dundanter Rohrleitungen.	☐	☐	☐	

V.1.4 Gelände, Gebäude – Stürme

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Dächer					
1.1 Sind Dächer hinrei- chend in den Bauwer- ken verankert?		☐	☐	☐	

V.1.5 Gelände, Gebäude – Vorsätzliche Handlungen mit kriminellem und/oder terroristischem Hintergrund

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Zugang					
1.1 Werden Zugangs-kontrollen zum Gelände der Einrichtung durchgeführt?		☐	☐	☐	
1.2 Sind Zonen erschweren Zugangs auf dem Gelände der Einrichtung eingerichtet?	Eine wesentliche Komponente der Prävention terroristischer Anschläge oder Sabotage ist die Erzeugung von Distanz zwischen den Bauwerken und einem möglichen Angriff mittels Sprengladung in einem Fahrzeug. Barrieren und Hindernisse zur Distanzerzeugung wie Höhengsprünge, Poller, Zäune oder Betonelemente können ein Heranfahren an kritische Bereiche be- oder verhindern.	☐	☐	☐	
1.3 Sind in den Bauwerken Zonen erschweren Zugangs eingerichtet?	Es sollte geprüft werden, ob im Eingangsbereich und beim Zugang zu kritischen Bereichen Vereinzelungsanlagen installiert werden können, eventuell in Kombination mit Kartenlesegeräten, um den Zutritt zu kontrollieren und für Nichtbetriebsangehörige zu erschweren.	☐	☐	☐	
1.4 Werden in den Bauwerken Zugangskontrollen durchgeführt?	Zum Beispiel durch den Pförtner	☐	☐	☐	
1.5 Sind kritische Bereiche verschlossen und nur für autorisiertes Personal zugänglich?		☐	☐	☐	
2. Konstruktion					
2.1 Sind die Fassaden inklusive der Fenster und Türen gehärtet?	Türen und Fenster sollten Verbundsicherheitsglas enthalten.	☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
2.2 Wurden geschützte Räume für Mitarbeiter und sonstige anwesenden Personen eingerichtet?	Im Falle eines Terroranschlages, eines Unfalls mit Gefahrgut oder einer Industriehavarie kann es sinnvoll sein, geschützte Bereiche im Objekt zu integrieren, die Mitarbeitern und Gästen eine Zufluchtsmöglichkeit bieten. Hierfür eignen sich statische Tragkerne wie Treppenhäuser oder Bereiche der Untergeschosse, die mit rauchdichten Türen und Kommunikationsanlagen ausgestattet sind. Die Möglichkeit zur Einrichtung solcher geschützten Bereiche sollte anhand der bestehenden Planung geprüft werden.	☐	☐	☐	
2.3 Sind Lüftungseingänge so angebracht, dass sie von außen schwer zugänglich sind?	Hiermit ist die Anbringung in ausreichender Höhe oder an unzugänglichen Stellen gemeint.	☐	☐	☐	
3. Elektronische Überwachung					
3.1 Werden kritische Bereiche videoüberwacht?		☐	☐	☐	
3.2 Findet eine Auswertung der Videoüberwachung statt?		☐	☐	☐	
3.3 Sind Alarmanlagen in Kernbereichen installiert?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
4. Ansprechpartner					
4.1 Sind spezialisierte Ansprechpartner bekannt, die im Falle eines Anschlags mit chemischen, biologischen oder radiologischen Agenzien kontaktiert werden können?	Im Falle eines Unfalls oder eines terroristischen Anschlags können Unternehmen und Behörden mit Agenzien konfrontiert werden, deren Einschätzung Spezialwissen voraussetzt. Zusätzlich zu den Gesundheitsbehörden sollten mögliche Kooperationspartner im Vorfeld identifiziert und kontaktiert werden.	☐	☐	☐	

V.1.6 Anlagen und Geräte – Stromversorgung

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Stromversorgung					
1.1 Liegen mehrere Strom-einspeisungen vor und befinden sich diese in möglichst unabhängigen Netzbereichen?		☐	☐	☐	
2. Notstromversorgung					
2.1 Sind die kritischen Bereiche, die im Krisenfall mit Notstrom versorgt werden müssen, identifiziert?	Zu den kritischen Bereichen zählen Steuerzentralen, Rechenzentren, Klimaanlage in Rechenzentren.	☐	☐	☐	
2.2 Ist sichergestellt, dass ausschließlich die für den Notbetrieb vorgesehenen Verbraucher der kritischen Bereiche an die Notstromversorgung angeschlossen sind?		☐	☐	☐	
2.3 Wurde festgelegt, für welchen Zeitraum die kritischen Bereiche mit Notstrom versorgt werden sollen?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
2.4 Wurde der Gesamtenergiebedarf zur Aufrechterhaltung der kritischen Bereiche ermittelt?		☐	☐	☐	
2.5 Entspricht die Auslegung der Notstromaggregate den aktuellen Kapazitäts- und Qualitätsanforderungen?	Kapazitäts- und Qualitätsanforderungen ändern sich mit der Entwicklung neuer, moderner Anlagen.	☐	☐	☐	
2.6 Liegt eine ausreichende Menge Kraftstoff für die festgelegte Betriebsdauer der Notstromversorgung vor?		☐	☐	☐	
2.7 Werden alle Notstromaggregate regelmäßig gewartet?		☐	☐	☐	
2.8 Werden alle Notstromaggregate regelmäßig unter Vollast getestet?		☐	☐	☐	
2.9 Ist die störungsfreie Inbetriebnahme der Notstromaggregate im Krisenfall gewährleistet?	Starthilfen wie Stromversorgung oder Batterien können im Krisenfall ausfallen. Betriebsmittel müssen häufig vorgewärmt werden.	☐	☐	☐	
2.10 Läuft im Krisenfall die Information über die Notwendigkeit zum Nachtanken des Notstromaggregates auf?	Wie und wo?	☐	☐	☐	
2.11 Sind sensible technische Komponenten mit einer unterbrechungsfreien Stromversorgung abgesichert?	Hierzu zählt eine Batteriepufferung, die den Betrieb von IT-Anlagen über einige Minuten gewährleisten kann.	☐	☐	☐	
2.12 Haben Sie Übereinkünfte oder Verträge mit den Lieferanten abgeschlossen, die Ihnen die Betriebsmittel für Notstromaggregate liefern?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
3. Stromunabhängige Sicherheits- und Warnsysteme					
3.1 Wurde eine von der öffentlichen Stromversorgung unabhängige Notbeleuchtung installiert?	Eine Notbeleuchtung ist von der öffentlichen Stromversorgung unabhängig, wenn sie beispielsweise von einer Batterie betrieben wird.	☐	☐	☐	
3.2 Wurde ein stromunabhängiges Alarm- und Warnsystem installiert?	Ein Alarm- und Warnsystem ist von der öffentlichen Stromversorgung unabhängig, wenn es beispielsweise von einer Batterie betrieben wird.	☐	☐	☐	

V.1.7 Anlagen und Geräte – Informationstechnologie

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Allgemein					
1.1 Ist ein funktionierendes IT-Management vorhanden (Beschaffung, Entwicklung und Wartung von Informationssystemen)?	Sicherheitsanforderung an Systeme, korrekte Verarbeitung in Anwendungen, kryptografische Maßnahmen, Sicherheit von Systemdateien und bei Prozessen, Schwachstellenmanagement	☐	☐	☐	
2. Zugriffssicherung					
2.1 Ist die mit öffentlichen Datennetzwerken verknüpfte IT ausreichend vor Zugriff von außen gesichert?		☐	☐	☐	
3. Datenerhaltung					
3.1 Existiert ein Datensicherungskonzept?		☐	☐	☐	
3.2 Werden kritische Daten an verschiedenen Orten vorgehalten?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
4. Prozesssteuerung					
4.1 Existiert eine redundante, örtlich getrennte Prozesssteuerung?		☐	☐	☐	
4.2 Sind Prozesssteuerung und Sicherheitssysteme (Alarmanlage, Videoüberwachung etc.) voneinander getrennt (separate Netze)?	Sofern im Rahmen der Prozesssteuerung eine Verbindung zum Internet vorliegt und Prozesssteuerung und Sicherheitssysteme verknüpft sind, können beide Systeme von außen manipuliert werden.	☐	☐	☐	

V.1.8 Anlagen und Geräte – Kommunikationstechnologie

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Festnetz					
1.1 Ist die Telefonanlage über eine unterbrechungsfreie Stromversorgung gesichert?		☐	☐	☐	
1.2 Ist die Telefonanlage ebenfalls über ein Notstromaggregat gesichert?		☐	☐	☐	
1.3 Wurde eine Vorrangschaltung beantragt?		☐	☐	☐	
2. Mobilfunk					
2.1 Stehen Mitarbeitern im Krisenfall Mobilfunktelefone zur Verfügung?		☐	☐	☐	
3. Funk					
3.1 Steht im Unternehmen ein Funksprechsystem für den Krisenfall zur Verfügung?		☐	☐	☐	

V.2 Revision des Krisenmanagements

V.2.1 Allgemeine Organisation

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Verantwortlichkeiten und Aufgaben					
1.1 Ist die personelle Besetzung der notwendigen Positionen für das Krisenmanagement in der Einrichtung festgelegt?		☐	☐	☐	
1.2 Sind alle relevanten Aufgaben im Krisenmanagement festgelegt und Personen und deren Vertretern zugewiesen?		☐	☐	☐	
1.3 Werden Mitarbeiter hinsichtlich ihrer Eignung für die im Krisenfall zugeteilte Rolle aus- und weitergebildet?		☐	☐	☐	
2. Alarmierung					
2.1 Sind interne und externe Alarmierungs- und Informationsvorgänge klar festgelegt?		☐	☐	☐	
2.2 Existieren konkrete Handlungsanweisungen für Personen, die in einer Gefahrensituation für die Weitergabe von Meldungen zuständig sind?		☐	☐	☐	
2.3 Werden konkrete Handlungen und Entscheidungen in der Krise dokumentiert?		☐	☐	☐	
2.4 Werden interne und externe Alarmierungs- und Informationsvorgänge geübt?	Hierzu zählen interne Übungen sowie die Einbindung in Übungen des örtlichen Katastrophenschutzes.	☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
3. Alarmierung					
3.1 Ist entsprechend den möglichen Auswirkungen von Extremereignissen die Alarmierung festgelegt?	Vereinfachte Festlegung z. B. nach folgenden Kriterien: 1) Auswirkungen bleiben auf einen Teilbereich der Einrichtung beschränkt. 2) Auswirkungen manifestieren sich in der gesamten Einrichtung, bleiben jedoch auf die Einrichtung selbst begrenzt. 3) Auswirkungen betreffen die gesamte Einrichtung sowie die Umgebung/ Region. 4) Auswirkungen betreffen die Einrichtung, die nähere Umgebung sowie überregionale Bereiche.	☐	☐	☐	
4. Warnung					
4.1 Ist die Warnung der von einem Extremereignis in der Einrichtung betroffenen Bevölkerung geregelt?	Anwohner, Kunden etc.	☐	☐	☐	
5. Stäbe					
5.1 Tritt im Krisenfall ein Krisenstab in der Einrichtung zusammen?		☐	☐	☐	
5.2 Ist die Einrichtung im Krisenfall in den Krisenstäben des Katastrophenschutzes (Einsatzleitung, Verwaltungsstab) mit Verbindungspersonal vertreten?	Entscheidungen im Krisenfall, die die Einrichtung betreffen, können besser beeinflusst werden, wenn Verbindungspersonal in diesen Stäben vertreten ist. Ansprechpartner sind die örtlichen Feuerwehren bzw. Kreis-, Stadt- oder Gemeindeverwaltungen.	☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
5.3 Sind in der Einrichtung Räumlichkeiten vorgesehen, die im Krisenfall für den Krisenstab zur Verfügung stehen und die die notwendige technische Ausstattung sowie eine Notstromversorgung aufweisen?		☐	☐	☐	
5.4 Liegen Konzepte zur Weiterführung der Krisenstabsfunktion bei Ausfall der Kommunikationssysteme vor?	Beispielsweise durch die Einrichtung von Personenmeldern mit oder ohne Kraftfahrzeug oder Kraftrad	☐	☐	☐	
5.5 Liegen Konzepte zur Weiterführung der Krisenstabsfunktion bei Ausfall der Datenverarbeitungssysteme vor?	Beispielsweise durch die Vorhaltung von Plänen und Informationen in Papierform	☐	☐	☐	
5.6 Liegen Konzepte zur Weiterführung der Krisenstabsarbeit bei Ausfall des Krisenstabsraums vor?		☐	☐	☐	

6. Notwendige Informationen und Unterlagen

6.1 Liegen Etagenpläne der Gebäude sowie Lagepläne von Ver- und Entsorgungsleitungen sowie der Zufahrtswege möglichst in digitaler und Papierform vor?	Zu den Ver- und Entsorgungsleitungen zählen Strom, Gas, Wasser.	☐	☐	☐	
6.2 Beinhalten die Etagenpläne alle für den Krisenfall notwendigen Informationen und kennzeichnen diese?	Hierzu zählen Fluchtwege, Notausgänge, Treppenhäuser, Feuerlöscher, Verbandskästen, sichere Rückzugsräume, Vorratsräume, Räume mit notwendigen Ausrüstungsgegenständen, Notstromaggregate, Sammelplätze, Rohrleitungen, Ventile, Schieber etc.	☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
6.3 Sind alle wichtigen Unterlagen griffbereit?	Beispiel: Verträge	☐	☐	☐	
6.4 Liegen Pläne und Unterlagen, die im Krisenfall auch im Freien genutzt werden müssen, nässegeschützt vor?		☐	☐	☐	
6.5 Liegen Formblätter zur Dokumentation von Meldeeingängen und -ausgängen vor?		☐	☐	☐	
6.6 Liegen Formblätter zur Erstellung von Informationen für die Bevölkerung vor?		☐	☐	☐	

7. Erreichbarkeiten

7.1 Liegen aktuelle, zentral gepflegte Personal- und Erreichbarkeitslisten vor?	Die Listen enthalten Namen, Adressen, Telefonnummern dienstlich und privat sowie eine Beschreibung der Positionen in der Einrichtung.	☐	☐	☐	
7.2 Liegen aktuelle Informationslisten über wichtige externe Unternehmen und Behörden vor?	Die Listen enthalten Informationen zur Organisation, die Adresse, den Namen eines Ansprechpartners, die Telefonnummern, eine Beschreibung der Dienstleistungen sowie Informationen zu vertraglichen Vereinbarungen und Hinweise auf Versorgungsprioritäten. Hierzu zählen u. a. Krankenhäuser, Kindergärten, Schulen und Lieferanten für Betriebsstoffe.	☐	☐	☐	
7.3 Werden alle Listen regelmäßig auf Aktualität untersucht?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
8. Eventuelle Abstimmung mit den zuständigen Behörden					
8.1 Sind die einzelnen zu informierenden Behörden im Krisenplan erfasst?	Beispiele: Polizei, Gesundheitsamt, Umweltamt, Feuerwehr, Katastrophenschutz	☐	☐	☐	
8.2 Sind die einzelnen Funktionsträger in der Einrichtung diesen Behörden bekannt?		☐	☐	☐	
8.3 Werden die zuständigen Behörden über die Krisenpläne informiert?		☐	☐	☐	
8.4 Besteht Kontakt zu Behörden der polizeilichen Gefahrenabwehr?	Diese Behörden (Polizei des Bundes und der Länder, Landeskriminalämter, Bundeskriminalamt) beraten zu Fragestellungen im Rahmen von Ereignissen mit kriminellem oder terroristischem Hintergrund bzw. Sabotage.	☐	☐	☐	

V.2.2 Personal – Allgemein

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Liegen Konzepte und Maßnahmen vor, die den Schutz der Mitarbeiter auch in Extremsituationen gewährleisten?	Hierzu zählen die Ausbildung ausgewählter Mitarbeiter zu Evakuierungshelfern, Erst- und Pandemiehelfern, Evakuierungspläne, hochwasser- und trümmerfreie Fluchtwege, Sammelplätze, Rückzugsräume, Schutzräume, Schutzausrüstungen, Erste-Hilfe-Ausrüstungen sowie eine Lebensmittelbevorratung.	☐	☐	☐	
2. Verfügt die Einrichtung in ausreichendem Maße über Personal mit Ortskenntnissen?		☐	☐	☐	

3. Haben Mitarbeiter bereichsübergreifend Erfahrung gesammelt (Rotationsprinzip)?	Bereichsübergreifende Tätigkeiten im Rotationsprinzip versetzen Mitarbeiter in die Lage, beim Ausfall des zuständigen Personals Funktionen auch außerhalb ihres eigentlichen Verantwortungsbereichs zu übernehmen.	☐ ☐ ☐
4. Kann im Krisenfall auf Ersatzpersonal zurückgegriffen werden?	Beispielsweise bei Pandemien kann unter Umständen auf Personal aus benachbarten Unternehmen und Behörden, Personal in Ruhestand oder Personal in Ausbildung zurückgegriffen werden.	☐ ☐ ☐
5. Existieren Alarmkonzepte für Ein-Personen-Arbeitsplätze?	Hierzu zählen Alarmknöpfe sowie eine automatisierte Alarmierung bei Funktionsstörungen, Fehlverhalten und fehlender Korrektur in Leitstellen/Leitwarten.	☐ ☐ ☐
6. Werden die Mitarbeiter der Einrichtung über das Krisenmanagement informiert?		☐ ☐ ☐

V.2.3 Krisenmanagement – Pandemieplanung (insbesondere Influenzapandemie)

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Allgemein					
1.1 Ist dafür gesorgt, dass bei grundlegendem Personalmangel eine kontrollierte Stilllegung der Prozesse in der Einrichtung erfolgen kann?		☐	☐	☐	
1.2 Sind für den Fall einer Epidemie bzw. Pandemie Ausweicharbeitsplätze festgelegt?	Beispiel: Telearbeit	☐	☐	☐	
1.3 Sind Vereinbarungen mit externen Dienstleistungseinrichtungen zur Übernahme von Aufgaben getroffen worden?		☐	☐	☐	
1.4 Besteht im Rahmen der Vorplanung eine Kooperation mit den lokalen Gesundheitsbehörden?		☐	☐	☐	
1.5 Werden antivirale Arzneimittel bevorratet?		☐	☐	☐	
1.6 Werden von der Einrichtung Impfungen angeboten bzw. wird über Impfmöglichkeiten informiert?		☐	☐	☐	
1.7 Ist dafür gesorgt, dass die Klimaanlage im akuten Fall teilweise ausgeschaltet wird?	Hierbei ist zu beachten, dass bestimmte Räume und Anlagen eine kontinuierliche Klimatisierung brauchen, beispielsweise Serverräume. Die Klimatisierung solcher Räume und Anlagen ist separat zu regeln.	☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
2. Personal					
2.1 Werden Mitarbeiter hinsichtlich des The- mas sensibilisiert?		☐	☐	☐	
2.2 Werden Mitarbeiter hinsichtlich des Ver- haltens im Ereignisfall geschult?	Beispiele: ☐ Kontakt von Händen und Gesicht vermeiden ☐ Händeschütteln vermei- den ☐ Hände regelmäßig waschen ☐ Persönliche Schutzaus- rüstung anlegen (Mund- und Nasenschutz, Brille)	☐	☐	☐	
2.3 Ist kritisches Personal identifiziert worden?		☐	☐	☐	
2.4 Ist mit kritischem Per- sonal im Ereignisfall eine Isolierung bespro- chen worden?		☐	☐	☐	
2.5 Wird zusätzliches Personal für spezielle Abläufe in der Einrich- tung weitergebildet?		☐	☐	☐	

V.3 Krisenbewältigung

V.3.1 Allgemeine Verfahren in der Krise

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Generelle Verfahren					
1.1 Ist eine Lagefest- stellung erfolgt?		☐	☐	☐	
1.2 Kann die Funktions- fähigkeit der Einrich- tung wiederhergestellt werden?		☐	☐	☐	
1.3 Werden Schutzvorkeh- rungen für Personal, Gäste und Kunden getroffen?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1.4 Werden Schutzvorkehrungen für Gebäude, Anlagen und Geräte, Daten und Unterlagen getroffen?		☐	☐	☐	

2. Administrative Verfahren

2.1 Werden Personal, Gäste und Kunden bei Eintritt eines extremen Ereignisses gewarnt?		☐	☐	☐	
2.2 Werden alle Mitarbeiter, die im Rahmen der Krisenbewältigung tätig sind, identifiziert?		☐	☐	☐	
2.3 Werden alle Mitarbeiter identifiziert, die in Gefahrenzonen tätig sind?		☐	☐	☐	
2.4 Wird Hilfe für verletzte, feststehende oder verirrte Mitarbeiter bereitgestellt?		☐	☐	☐	
2.5 Werden für das Personal Informationen über das Ereignis bereitgestellt?		☐	☐	☐	
2.6 Werden für die Familien der Mitarbeiter Informationen über das Ereignis bereitgestellt?		☐	☐	☐	
2.7 Werden alle Verletzungen und die diesbezüglich eingeleiteten Maßnahmen dokumentiert?		☐	☐	☐	
2.8 Werden alle Teilereignisse dokumentiert?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
2.9 Werden alle Anlagen und Geräte, sofern möglich, aus den Schadenszonen verlagert?		☐	☐	☐	
2.10 Werden Zugangskontrollen zum Schadensgebiet durchgeführt?		☐	☐	☐	
2.11 Werden Protokolle über alle Telefonate erstellt?		☐	☐	☐	
2.12 Werden Pressemitteilungen herausgegeben?		☐	☐	☐	
2.13 Werden nach Ablauf der Krisensituation die Rücknahme der Alarmierung und die Wiedereinsetzung der betrieblichen Aufbauorganisation veranlasst?		☐	☐	☐	
3. Logistik					
3.1 Werden alle notwendigen Ausrüstungsgegenstände bereitgestellt?		☐	☐	☐	
3.2 Werden Lebensmittel und Bedarfsmaterial bereitgestellt?		☐	☐	☐	
3.3 Ist der Krisenstabsraum funktionsbereit?		☐	☐	☐	
3.4 Werden alle notwendigen Pläne bereitgestellt?	Gebäudepläne, Energieversorgung, Wasserversorgung, Entsorgung etc.	☐	☐	☐	
3.5 Werden alle redundanten Einrichtungen und Ausrüstungsgegenstände bereitgestellt?	Alternativer Krisenstabsraum, Funkgeräte etc.	☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
3.6 Wird eine Reparatur beschädigter Anlagen und Geräte vorgenommen bzw. in die Wege geleitet?		☐	☐	☐	
3.7 Wird medizinische Unterstützung für zu erwartende Verletzungen bereitgestellt?		☐	☐	☐	
3.8 Ist die Notstromversorgung angelaufen?		☐	☐	☐	

V.3.2 Spezielle Verfahren in der Krise

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Retten, bergen, löschen					
1.1 Werden alle notwendigen Schritte zum Retten von Personen und Bergen von Gegenständen eingeleitet?	Information externer Stellen	☐	☐	☐	
1.2 Werden alle notwendigen Schritte zum Löschen von Bränden eingeleitet?	Eigene Maßnahmen, Information externer Stellen	☐	☐	☐	
2. Medizinische Erstversorgung					
2.1 Werden alle notwendigen Schritte zur medizinischen Erstversorgung eingeleitet?	Eigene Maßnahmen, Information externer Stellen	☐	☐	☐	
2.2 Werden alle notwendigen externen Stellen zur medizinischen Erstversorgung alarmiert?	Rettungsdienst, Feuerwehr etc.	☐	☐	☐	
3. Absperrung und Zugangskontrollen					
3.1 Werden alle notwendigen Absperrmaßnahmen eingeleitet?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
3.2 Werden Zugangskontrollen in die Krisenzonen durchgeführt?		☐	☐	☐	

4. Sichere Unterkünfte

4.1 Werden sichere Unterkünfte für alle Mitglieder des Krisenstabes zur Verfügung gestellt?	Zum Aufenthalt tagsüber und zur Übernachtung im Bedarfsfall	☐	☐	☐	
4.2 Werden sichere Unterkünfte für Personal, Kunden und Gäste bereitgestellt?	Zum Aufenthalt tagsüber und zur Übernachtung im Bedarfsfall	☐	☐	☐	

5. Evakuierung von Gebäuden

5.1 Werden alle Anwesenden von den Evakuierungshelfern zum festgelegten Sammelplatz geleitet?		☐	☐	☐	
5.2 Wird die Vollständigkeit aller Anwesenden auf dem Sammelplatz kontrolliert?		☐	☐	☐	
5.3 Wird die Beendigung der Evakuierung gemeldet?		☐	☐	☐	
5.4 Werden zum Weitertransport aller Anwesenden Transportmöglichkeiten bereitgestellt?		☐	☐	☐	

6. Reaktion bei Bombendrohung

6.1 Ist die Polizei eingeschaltet?		☐	☐	☐	
6.2 Werden Hinweise auf verdächtige Aktivitäten aufgenommen und weitergeleitet?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
6.3 Werden Hinweise auf verdächtige Gegenstände aufgenommen und weitergeleitet?	Zum Beispiel durch Verwendung eines Formblattes	☐	☐	☐	

7. Koordination der Zusammenarbeit mit externen Unternehmen und Behörden

7.1 Ist das Verfahren zur Zusammenarbeit mit externen Unternehmen und Behörden aktiviert?	Beispiele: Feuerwehr, Polizei	☐	☐	☐	
7.2 Wird der Zugang von Mitarbeitern externer Einrichtungen kontrolliert?		☐	☐	☐	
7.3 Sind die notwendigen Kommunikationswege aktiviert?		☐	☐	☐	

8. Kontrollierte Außerbetrieb- und Wiederinbetriebnahme von Anlagen

8.1 Wird die Einrichtung in Rücksprache mit dem Krisenstabsleiter ganz oder in Teilen außer Betrieb gesetzt?		☐	☐	☐	
8.2 Werden alle zeitlichen Fristen berücksichtigt?	Mögliche Vorlaufzeiten	☐	☐	☐	
8.3 Werden die Auswirkungen einer partiellen oder vollständigen Außerbetriebnahme von Anlagen erfasst und berücksichtigt?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
9. Umgang mit kritischen Daten und Unterlagen					
9.1 Werden wichtige Datenträger und Unterlagen immer in wasserdichten und feuerfesten Behältern verpackt?		☐	☐	☐	
9.2 Werden wichtige Datenträger, Unterlagen und Behälter gekennzeichnet?		☐	☐	☐	
9.3 Werden wichtige Datenträger und Unterlagen aus dem Schadensgebiet ausgelagert?		☐	☐	☐	
10. Medien					
10.1 Sind alle geschulten Mediensprecher einberufen?		☐	☐	☐	
10.2 Liegen alle vorformulierten Texte griffbereit vor?		☐	☐	☐	
10.3 Liegt Hintergrundmaterial zur Einrichtung bereit?		☐	☐	☐	
10.4 Wird das festgelegte Verfahren zur Freigabe von Informationen nach außen berücksichtigt?		☐	☐	☐	
10.5 Liegen alle Listen mit Ansprechpartnern der Einrichtung für Medienvertreter vor?		☐	☐	☐	
10.6 Liegt ein Fragenkatalog zur Überprüfung der Medienvertreter bereit?	Authentizität, Überprüfung Ausweis	☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
10.7 Werden allen Medienvertretern gleiche Voraussetzungen eingeräumt?		☐	☐	☐	
10.8 Medien					
a. Werden Pressemitteilungen abgesetzt?		☐	☐	☐	
b. Werden Pressekonferenzen abgehalten?		☐	☐	☐	
c. Werden Anzeigen zur Information geschaltet?		☐	☐	☐	
d. Werden Informationen über Rundfunk und Fernsehen verteilt?		☐	☐	☐	

11. Finanzielle Unterstützung in einer Krise

11.1 Werden benötigte Mittel zur Bewältigung der Krise bereitgestellt?		☐	☐	☐	
--	--	-----------------------	-----------------------	-----------------------	--

12. Dokumentation/Beweissicherung

12.1 Werden alle Entscheidungen dokumentiert?	Formblätter, Protokolle	☐	☐	☐	
12.2 Werden alle Personenschäden dokumentiert?	Berichte, Fotos, Videomaterial	☐	☐	☐	
12.3 Werden alle Sachschäden dokumentiert?	Berichte, Fotos, Videomaterial	☐	☐	☐	

V.4 Nachbereitung

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Werden Handlungsprioritäten festgelegt?		☐	☐	☐	
2. Ist der Grad der Restgefährdung ermittelt?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
3. Wird eine Befragung der Mitarbeiter zum Krisenmanagement durchgeführt?		☐	☐	☐	
4. Werden Schadensinformationen ausgewertet?	Berichte, Fotos, Videomaterial	☐	☐	☐	
5. Sind alle Rechnungen beglichen?		☐	☐	☐	
6. Werden externe Akteure über den Sachstand informiert?	Versicherungen, Behörden	☐	☐	☐	
7. Ist eine Kontaktaufnahme mit den betroffenen Kunden erfolgt?		☐	☐	☐	
8. Werden alle notwendigen Aufräumarbeiten initiiert?	Lüften, Trümmer wegräumen, Trocknung etc.	☐	☐	☐	
9. Wird eine Inventarisierung aller beschädigten Gebäude, Anlagen und Geräte vorgenommen?		☐	☐	☐	
10. Wird eine Abschätzung des monetären Schadens vorgenommen?		☐	☐	☐	
11. Werden die Ergebnisse aus der Nachbereitung zur Anpassung des Krisenmanagements genutzt?		☐	☐	☐	

V.5 Übungen

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Stabsrahmenübungen					
1.1 Wird die Übernahme von krisenbezogenen Aufgaben und Verantwortungen geübt?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1.2 Werden Alarmierungs-, Meldewege und Wege der Warnung geübt?		☐	☐	☐	
1.3 Werden interne und externe Kommunikationswege getestet?		☐	☐	☐	
1.4 Werden Kommunikationsmittel getestet?		☐	☐	☐	
1.5 Werden Erreichbarkeitslisten getestet?	Beispiel: Telefonlisten	☐	☐	☐	

2. Teil-, Vollübungen

2.1 Werden Evakuierungen vorgenommen?		☐	☐	☐	
2.2 Wird die Vollständigkeit der Mitarbeiter nach einer Evakuierung überprüft?		☐	☐	☐	
2.3 Werden alle Ausstattungs- und Ausrüstungsgegenstände getestet?	Beispiel: Persönliche Schutzausrüstung	☐	☐	☐	
2.4 Wird ein kontrolliertes Herunterfahren von Anlagen und Bereichen geübt?		☐	☐	☐	
2.5 Wird die Aktivierung alternativer Standorte bzw. alternativer Ausstattung getestet?		☐	☐	☐	
2.6 Wird die Aktivierung redundanter Systeme als „Notbetrieb“ getestet?		☐	☐	☐	
2.7 Wird die Rückkehr zum Normalbetrieb geübt?		☐	☐	☐	

V.6 Auswahl und Ausstattung eines Krisenstabsraumes

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1. Räumliche Infrastruktur					
1.1 Liegt der Krisenstabsraum möglichst in einem gesicherten Betriebsbereich bzw. an einem Ausweichstandort?		☐	☐	☐	
1.2 Ist der Krisenstabsraum zentral erreichbar?		☐	☐	☐	
1.3 Besteht eine direkte Erreichbarkeit für Mitglieder/Funktionen des Krisenstabes?		☐	☐	☐	
1.4 Gibt es ausreichende Parkflächen in unmittelbarer Nähe?		☐	☐	☐	
1.5 Existiert ein ausreichend dimensionierter und vom Arbeitsraum abgesetzter Besprechungsraum (ohne Telefone) für Lagebesprechungen?		☐	☐	☐	
1.6 Gibt es zusätzlich kleine Besprechungsräume für Arbeitsgruppen/Detailabstimmungen?		☐	☐	☐	
1.7 Wurde an einen ausreichend dimensionierten Arbeitsraum für die Unterbringung des Krisenstabes und der unterstützenden Funktionen gedacht?		☐	☐	☐	
1.8 Wurde an die Anbringung eines Sichtschutzes an den Fensterfronten sowie an die Abhörsicherheit des Krisenstabsraumes gedacht?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
1.9 Befinden sich in der Nähe des Krisenstabs- raumes Rückzugs- räume/-flächen für Ruhepausen und zur Verpflegungsaufnah- me, evtl. mit Schlaf- möglichkeiten?		☐	☐	☐	
1.10 Besteht die Möglich- keit der Abdunkelung bei Präsentationen?		☐	☐	☐	

2. Technische Infrastruktur

2.1 Stehen PC-Arbeitsplät- ze mit Internetzugang, E-Mail-Funktionen und externe Speichermedi- en zum Transport von Daten bereit?	CD-ROM, externe Festplat- ten, USB-Sticks	☐	☐	☐	
2.2 Stehen Laptops, Note- books und PDAs bereit?		☐	☐	☐	
2.3 Existiert ein E-Mail- Sammelpostfach mit geregelter Verteilung?		☐	☐	☐	
2.4 Gibt es Mobiltelefone mit Ladekabeln sowie stromunabhängige analoge Telefone?		☐	☐	☐	
2.5 Besteht eventuell eine Direktleitung zu wich- tigen Unternehmen und Behörden?		☐	☐	☐	
2.6 Gibt es eine ausrei- chende Anzahl von Faxgeräten bzw. Fax- servern auf PCs?		☐	☐	☐	
2.7 Stehen Scanner zur Verfügung?	Zum Einscannen von Doku- menten, Bildmaterial etc.	☐	☐	☐	
2.8 Besteht ein Zugriff auf die betriebseigene Videoüberwachung?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
2.9 Besteht ein Zugriff auf die betriebseigenen Informationssysteme?		☐	☐	☐	
2.10 Besteht ein Zugriff auf den Betriebsfunk und die Betriebsfunktechnik?		☐	☐	☐	
2.11 Wird an Visualisierungstechnik gedacht?	Beispiele: Leinwand, Beamer, Flipchart, Whiteboard	☐	☐	☐	
2.12 Steht eine ausreichende Anzahl von TV-, Radio- und Videogeräten zur Verfügung?	Zum Verfolgen, Auswerten und Aufzeichnen von Kamerabildern und Berichterstattungen	☐	☐	☐	
2.13 Ist gewährleistet, dass Aufzeichnungen in abspielbaren Datenformaten vorliegen?		☐	☐	☐	
2.14 Steht ein Kopiergerät zur Verfügung?					
2.15 Stehen Fotoapparate zur Verfügung?		☐	☐	☐	
2.16 Ist an eine unterbrechungsfreie Stromversorgung bzw. Netzersatzanlage gedacht?		☐	☐	☐	
3. Sonstiges					
3.1 Sind Formblätter, Protokollblätter und Vorlagen vorbereitet?		☐	☐	☐	
3.2 Liegen Formblätter für Lagebesprechungen vor?		☐	☐	☐	
3.3 Liegen Telefonlisten und Erreichbarkeitslisten sowie Listen über Ressourcen vor?	Personal, Geräte, Bevorratung, Dienstleistungen im Krisenfall, Verträge in digitaler sowie in Papierform	☐	☐	☐	
3.4 Liegen Teilnehmerlisten für Lagebesprechungen vor?		☐	☐	☐	

Fragen	Erläuterungen	Ja	Nein	Entfällt	Eigener Kommentar
3.5 Gibt es einen Sitzplan für den Krisenstab?		☐	☐	☐	
3.6 Liegt aktuelles Plan- und Bildmaterial der Einrichtung vor?		☐	☐	☐	
3.7 Ist an Namensschilder mit Funktionsbezeichnungen für Mitglieder und Funktionen des Krisenstabes gedacht?	Ggf. Tischschilder mit Bereichsbezeichnung bei wechselnder Besetzung	☐	☐	☐	
3.8 Gibt es genügend Büromaterial?	Papier, Stifte etc.	☐	☐	☐	
3.9 Existiert ein Pressezentrum mit entsprechender Ausstattung wie Fernsehen oder Radio?	Für größere Unternehmen und Behörden	☐	☐	☐	
3.10 Ist an die Einrichtung einer Zugangskontrolle für das Betreten des Krisenstabsraums gedacht?		☐	☐	☐	
3.11 Werden Personalausweise, Dienstaussweise und Betriebsausweise kontrolliert?		☐	☐	☐	
3.12 Liegen Visitenkarten vor?	Beispielsweise für Medienvertreter	☐	☐	☐	
3.13 Ist die Verpflegung für den Ereignisfall sichergestellt?		☐	☐	☐	
3.14 Gibt es Schutzausrüstungen für alle Mitarbeiter?	Schutzbrillen, Helme, Sicherheitsschuhe, Schutzmasken sowie Körperschutzanzüge	☐	☐	☐	

VI. Beispiel Risikoanalyse

Am folgenden Beispiel wird die praktische Umsetzung einer Risikoanalyse anhand einer fiktiven Einrichtung aufgezeigt. Es wird der Teilprozess Leitwarte beispielhaft herausgegriffen und untersucht. Eine Unterteilung der Leitwarte in weitere Teilprozesse erfolgt hier nicht.

Als Plattform zur Bearbeitung der Risikoanalyse für die Leitwarte wird eine Risikotabelle in einem Tabellenkalkulationsprogramm genutzt.

VI.1 Kritikalitätsanalyse

Zur Ermittlung der Kritikalität der Leitwarte werden zwei der vier Kriterien aus Kapitel 3.2.1 herangezogen und anhand der folgenden Klassifizierung abgeschätzt. Diese Einteilungen sind als Vorschläge zu verstehen und können auf die Gegebenheiten in der Einrichtung angepasst werden. Die jeweils fett umrandete Klasse wurde für den Teilprozess „Leitwarte“ ausgewählt.

a) Zeitrahmen:

In welchem Zeitrahmen wirkt sich eine Beeinträchtigung des Teilprozesses auf die gesamte Dienstleistung bzw. Produktion der Einrichtung aus?

Klassen	Zeitspanne bis zur Beeinträchtigung der Dienstleistung bzw. Produktion	Verbale Klassen
1	sehr kurze Zeitspanne (z. B. Sekunden bzw. Minuten)	Teilprozess ist sehr kritisch
2	kurze Zeitspanne (z. B. Stunden)	Teilprozess ist kritisch
3	mittlere Zeitspanne (z. B. Tage)	Teilprozess ist wichtig, aber nicht kritisch
4	lange Zeitspanne (z. B. Wochen)	Teilprozess ist nicht sehr kritisch
5	sehr lange Zeitspanne (z. B. Monate, Jahre)	Teilprozess ist nahezu unkritisch

Tabelle 1: Klasseneinteilung zum Kritikalitätskriterium „Zeitrahmen“

b) Volumen:

Welches Volumen der gesamten Dienstleistung bzw. der Produktion ist betroffen, wenn der betrachtete kritische Teilprozess beeinträchtigt ist bzw. gänzlich ausfällt?

Klassen	Volumen der Beeinträchtigung der Dienstleistung bzw. Produktion	Verbale Klassen
1	sehr großes Volumen (z. B. 80 bis 100% der gesamten Dienstleistung bzw. Produktion)	Teilprozess ist sehr kritisch
2	großes Volumen (z. B. 50 bis 80% der gesamten Dienstleistung bzw. Produktion)	Teilprozess ist kritisch
3	mittleres Volumen (z. B. 30 bis 50% der gesamten Dienstleistung bzw. Produktion)	Teilprozess ist wichtig, aber nicht kritisch
4	geringes Volumen (z. B. 10 bis 30% der gesamten Dienstleistung bzw. Produktion)	Teilprozess ist nicht sehr kritisch
5	sehr geringes Volumen (z. B. 0 bis 10% der gesamten Dienstleistung bzw. Produktion)	Teilprozess ist nahezu unkritisch

Tabelle 2: Klasseneinteilung zum Kritikalitätskriterium „Volumen“

Die Zeitspanne bis zur Beeinträchtigung der gesamten Dienstleistung der fiktiven Einrichtung ist sehr kurz und kann der Klasse 1 zugeordnet werden. Im Hinblick auf das Kriterium „Zeitraum“ ist der Teilprozess also als sehr kritisch einzustufen.

Das Volumen der ausfallenden Dienstleistung in der Einrichtung kann bei Beeinträchtigung der Leitwarte als sehr hoch angenommen werden und wird der Klasse 2 zugeordnet. Im Hinblick auf das Kriterium „Volumen“ ist der Teilprozess also als kritisch einzustufen.

Insgesamt wird der Teilprozess „Leitwarte“ als sehr kritisch eingestuft und im Rahmen der Risikoanalyse weiter untersucht.

VI.2 Gefahrenanalyse und Szenarioentwicklung

Als mögliche Gefahr für die fiktive Einrichtung wird beispielhaft ein Stromausfall herausgegriffen. Hieraus kann folgendes Szenario entwickelt werden.

Szenario: Stromausfall

Intensität	5 Millionen Menschen sind europaweit ohne Strom. Alle stromabhängigen Anlagen ohne Netzersatzanlage fallen aus. Die Notstromaggregate des Katastrophenschutzes reichen bei Weitem nicht aus, den Bedarf an externer Notstromversorgung zu decken.
Räumliche Ausdehnung	Regionale Ausfälle in vielen regionalen Teilnetzen; die eigene Leitwarte ist vom Stromausfall betroffen.
Zeitliche Ausdehnung	4 Tage
Warnung	Keine Vorwarnung
Referenzereignisse	Stromausfall im Münsterland im November 2005 mit regionalen Ausfällen von bis zu 5 Tagen für bis zu 250.000 Personen

Tabelle 3: Szenario Ausfall der externen Stromversorgung

Die Eintrittswahrscheinlichkeit dieses Szenarios ist quantitativ nahezu nicht zu erfassen. Daher ist es notwendig, sie abzuschätzen. Die jüngere Vergangenheit hat gezeigt, dass kurzfristige Stromausfälle durchaus auftreten. Vor dem Hintergrund einer

Zunahme von extremen Naturereignissen und einer wachsenden Bedrohung durch terroristische Anschläge wird die Eintrittswahrscheinlichkeit für dieses Szenario als „mittel“ eingestuft. Dieser Klassifizierung entspricht der Punktwert 3.

Frage: Wie groß schätzen Sie die Eintrittswahrscheinlichkeit ein, dass ein entsprechendes Szenario mit dem beschriebenen Ausmaß auftritt?

Klassen	Verbale Klassen	Punktwert
1	sehr gering	1
2	gering	2
3	mittel	3
4	hoch	4
5	sehr hoch	5

Tabelle 4: Klasseneinteilung Eintrittswahrscheinlichkeit

VI.3 Verwundbarkeitsanalyse

Aus den in Kapitel 3.2.2.2 beschriebenen Verwundbarkeitskriterien werden die folgenden Kriterien für die Leitwerte ausgewählt:

- Abhängigkeit von Risikoelementen
- Abhängigkeit von externen Infrastrukturen – Stromversorgung
- Abhängigkeit von externen Infrastrukturen – Verkehr, Transport und Logistik
- Robustheit/realisiertes Schutzniveau
- Redundanz, Ersatz
- Wiederherstellungsaufwand

Es wird angenommen, dass diese Kriterien für die fiktive Einrichtung eine besondere Relevanz haben. Im Rahmen der Vereinfachung des Beispiels ist diese Auswahl nicht begründet. Sie zeigt jedoch an, dass nicht alle Verwundbarkeitskriterien für alle Einrichtungen angewendet werden müssen. Das Kriterium „Abhängigkeit von Risikoelementen“ fungiert als Gewichtungsfaktor, die übrigen Werte der Verwundbarkeit gehen als Summe in die Risikoermittlung ein.

Die Abschätzung der Werte für die Verwundbarkeit der Risikoelemente erfolgt wie bei der Abschätzung der Eintrittswahrscheinlichkeit des Szenarios über eine verbale Klasseneinteilung und die Zuweisung von Punktwerten zu diesen Klassen.

Die Verwundbarkeit unterscheidet sich von Szenario zu Szenario, weswegen nicht für jedes Feld ein Eintrag existieren muss. Daher wurde die Klasse 0 eingeführt, die ein Ausblenden der betrachteten Kombination ermöglicht. Die übrigen Klassen entsprechen der Systematik, die auch für die Bewertung der Eintrittswahrscheinlichkeit herangezogen wurde.

Klassen	Verbale Klassen	Beschreibung	Punktwert
0	keine Relevanz	Das Szenario hat keinerlei Bedeutung für das Risikoelement.	0
1	sehr gering	Verwundbarkeit des Teilprozesses aufgrund der Wirkung des Szenarios auf das Risikoelement	1
2	gering	Verwundbarkeit des Teilprozesses aufgrund der Wirkung des Szenarios auf das Risikoelement	2
3	mittel	Verwundbarkeit des Teilprozesses aufgrund der Wirkung des Szenarios auf das Risikoelement	3
4	hoch	Verwundbarkeit des Teilprozesses aufgrund der Wirkung des Szenarios auf das Risikoelement	4
5	sehr hoch	Verwundbarkeit des Teilprozesses aufgrund der Wirkung des Szenarios auf das Risikoelement	5

Tabelle 5: Klasseneinteilung Verwundbarkeit

In der Risikotabelle wird nun für jedes Risikoelement und jedes Verwundbarkeitskriterium eine Verwundbarkeit abgeschätzt. Die Punktwerte hierfür, V1 bis V5⁷⁰, werden in die dafür vorgesehenen Zellen eingetragen.

Der Vorgang wird für alle Risikoelemente wiederholt. Am Ende des Arbeitsschrittes steht eine Risikotabelle, die für den ausgewählten Teilprozess Teilverwundbarkeiten und Teilrisiken sowie eine Gesamtverwundbarkeit und ein Gesamtrisiko aufzeigt.

VI.4 Risikoermittlung

Die Verknüpfung, also die Berechnung der Werte, erfolgt anhand der Risikotabelle folgendermaßen:

Punktwerte, die in die Tabelle eingetragen werden:

EW: Eintrittswahrscheinlichkeit

ARE: Abhängigkeit von Risikoelementen

V1: Abhängigkeit von externen Infrastrukturen – Stromversorgung

V2: Abhängigkeit von externen Infrastrukturen – Verkehr, Transport und Logistik
V3: Robustheit/realisiertes Schutzniveau
V4: Redundanz, Ersatz
V5: Wiederherstellungsaufwand

Werte mit Bezug zu Risikoelementen, die in der Tabelle berechnet werden:

Teilverwundbarkeit = $ARE * (V1 + V2 + V3 + V4 + V5)$

Teilrisiko = $EW * ARE * (V1 + V2 + V3 + V4 + V5)$

Werte mit Prozessbezug, die in der Tabelle berechnet werden:

Gesamtverwundbarkeit = Summe aller Teilverwundbarkeiten

Gesamtrisiko = Summe aller Teilrisiken

⁷⁰ Siehe hierzu Tabellen 6 und 7.

Teilprozess	Leitwarte	Kriterien zur Verwundbarkeit der Leitwarte						Berechnung	
		Abhängigkeit von Risiko- elementen	Abhängigkeit von externen Infrastruktu- ren – Strom- versorgung	Abhängigkeit von externen Infrastrukturen – Verkehr, Trans- port, Logistik	Robustheit/ realisiertes Schutzniveau	Redundanz, Ersatz	Wiederher- stellungsaufwand	Teilver- wund- barkeit	Teilrisiko
Personal									
	EW:	3							
	Leitfrage	Wie hoch ist die Abhän- gigkeit der Leitwarte von Spezial- personal ein- zuschätzen?	Wie schätzen Sie die Ver- wundbarkeit der Leitwarte aufgrund der Abhängigkeit des Person- als von der externen Strom- versorgung ein?	Wie schätzen Sie die Ver- wundbarkeit der Leitwarte aufgrund der Abhängigkeit des Personals von Verkehr, Transport und Logistik ein?	Wie schätzen Sie die Ver- wundbarkeit der Leitwarte aufgrund fehlenden Schutzes des Personals ein?	Wie schätzen Sie die Ver- wundbarkeit der Leitwarte durch fehlendes Ersatzpersonal im Falle eines Strom- ausfalls ein?	Wie hoch ist die Verwund- barkeit des Teilprozesses im Hinblick auf den Zeit- aufwand zur Wieder- einsetzung des Personal ein- zuschätzen?		
Personal	Kommen- tar	Die Leitwarte ist vom Per- sonal sehr abhängig.	Das Personal ist nur bedingt vom Strom abhängig. Fehlende Not- beleuchtung beispielsweise kann zur Beein- trächtigung der Tätigkeit führen.	Die externe Stromver- sorgung betrifft möglicherweise den Bereich Verkehr und Transport. Das Personal kann möglicherweise die Arbeitsstelle nicht erreichen.	Bei fehlender Notbeleuch- tung kann es zu Unfällen und Verletzungen kommen.	Der Stromausfall wird voraus- sichtlich nur geringfügig oder in mittlerem Umfang dazu beitragen, dass Ersatzpersonal fehlt (Beeinträch- tigung ÖPNV, Bahnverkehr).	Nach dem Stromausfall wird das Perso- nal nicht mehr beeinträchtigt sein.		
	Punktwert	5	1	3	1	2	1	40	120

Tabelle 6: Ausschnitt der Risikotabelle für die Leitwarte

Die folgende Tabelle zeigt ein Beispielergebnis für alle Risikoelemente der Leitwarte. In dieser Tabelle wurden alle Leitfragen und Kommentare aus Gründen der Übersichtlichkeit gelöscht.

Alle einrichtungsspezifischen Anlagen und Geräte werden im Beispiel unter „Anlagen und Geräte“ zusammengefasst.

Teilprozess	Leitwarte	Kriterien zur Verwundbarkeit der Leitwarte						Berechnung	
Szenario:	Ausfall der externen Stromversorgung	Abhängigkeit von Risikoelementen	Abhängigkeit von externen Infrastrukturen – Stromversorgung	Abhängigkeit von externen Infrastrukturen – Verkehr, Transport, Logistik	Robustheit/realisiertes Schutzniveau	Redundanz, Ersatz	Wiederherstellungsaufwand	Teilverwundbarkeit	Teilrisiko
EW:	3								
Personal	Punktwert	5	1	3	1	2	1	40	120
Gelände, Gebäude	Punktwert	5	0	0	0	3	0	15	45
Anlagen, Geräte	Punktwert	5	5	0	3	1	2	55	165
Daten, Software	Punktwert	5	5	1	4	5	3	90	270
Unterlagen	Punktwert	2	0	0	0	0	0	0	0
Betriebsstoffe	Punktwert	5	2	2	0	4	0	40	120
Gesamtverwundbarkeit, Gesamtrisiko (Teilprozess, Szenario):								240	720

Tabelle 7: Risikotabelle für die Leitwarte ohne Leitfragen und Kommentare

VI.5 Risikovergleich

Durch die Analyse aller kritischen Prozesse sowie deren Teilprozesse in der Einrichtung und der verschiedenen für die Einrichtung relevanten Szenarien entsteht eine Sammlung von Risikotabellen, die nun nebeneinander gelegt werden können. Die Ergebnisse werden auf gleicher standardisierter, methodischer und inhaltlicher Basis generiert. Es kann dadurch ein umfassender Vergleich folgender Aspekte vorgenommen werden:

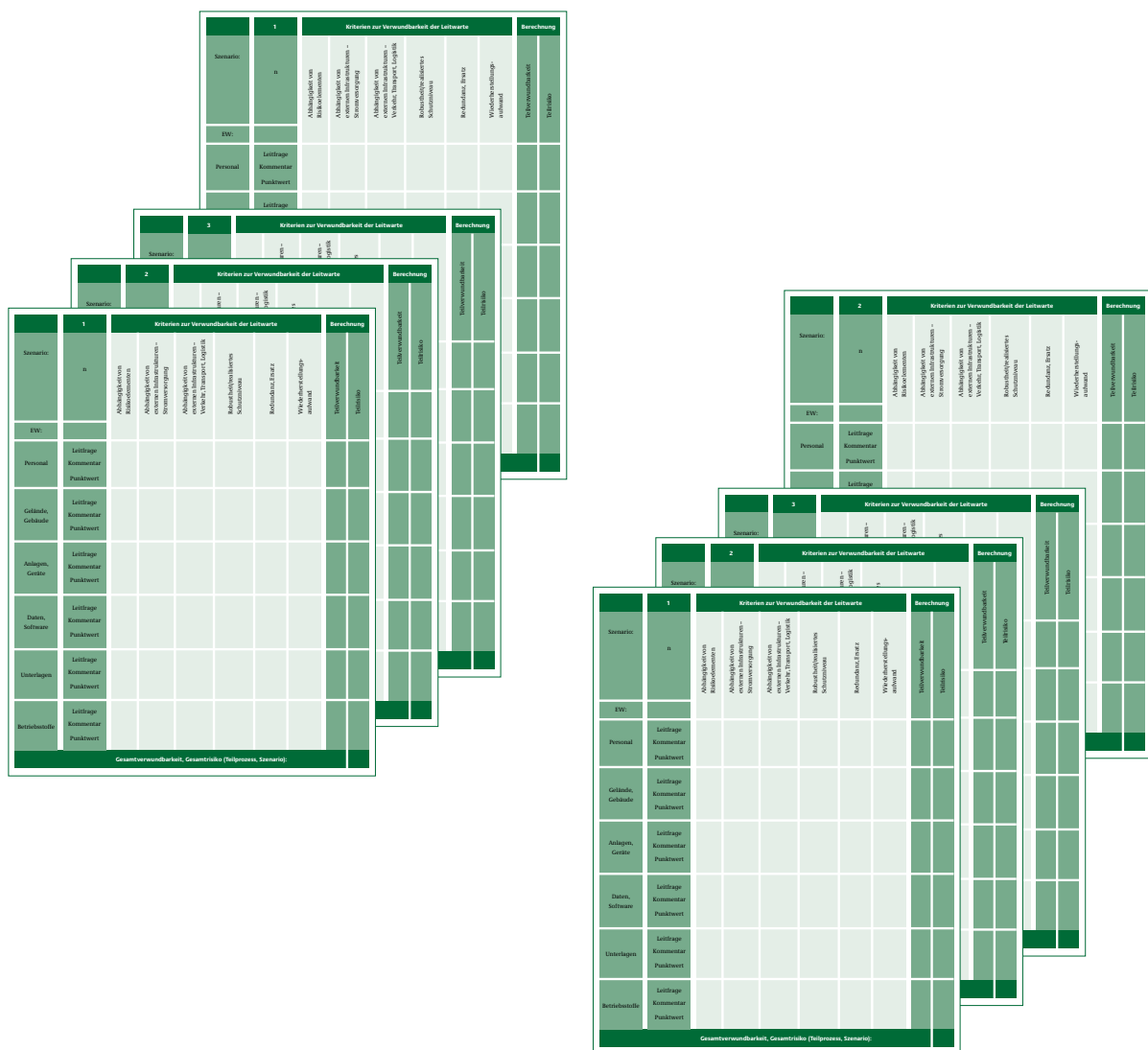
- ein Vergleich von Teilverwundbarkeiten und Teilrisiken der Risikoelemente innerhalb eines Teilprozesses
- ein Vergleich von Teilverwundbarkeiten und Teilrisiken gleicher Risikoelemente unterschiedlicher Teilprozesse

- ein Vergleich von Teilverwundbarkeiten und Teilrisiken unterschiedlicher Teilprozesse
- ein Vergleich der Gesamtverwundbarkeiten und Gesamtrisiken unterschiedlicher Teilprozesse

Das Beispiel kann nur einen auf die Leitwerte bezogenen Vergleich von Teilverwundbarkeiten und Teilrisiken liefern. Dehnt man die Vorgehensweise auf andere Teilprozesse aus, entsteht ein weitreichender Vergleich innerhalb der gesamten Einrichtung.

Die folgende Abbildung zeigt schematisch den Vergleich zweier Teilprozesse und verschiedener Szenarien.

Abbildung 12: Zwei Teilprozesse, mehrere Szenarien



Die Ergebnisse aus den Berechnungen der Teilverwundbarkeiten und Teilrisiken lassen sich in verbale Klassen einteilen. Die hier gewählten Klasseneinteilungen zählen einen Wert dann zur nächsthöheren Klasse, wenn der Maximalwert der betrachteten Klasse um einen Punkt überschritten ist.

Für das Risikoelement „Daten, Software“ ergibt sich folgendes Ergebnis. Die Teilverwundbarkeit ist mit 90 als sehr hoch, das Teilrisiko mit 270 als hoch einzustufen.⁷¹

Teilverwundbarkeit	
Punktwert	Verbale Klassen
0	keine Teilverwundbarkeit
1 bis 5	sehr geringe Teilverwundbarkeit
6 bis 20	geringe Teilverwundbarkeit
21 bis 45	mittlere Teilverwundbarkeit
46 bis 80	hohe Teilverwundbarkeit
81 bis 125	sehr hohe Teilverwundbarkeit

Tabelle 8: Klasseneinteilung der Ergebnisse aus der Berechnung der Teilverwundbarkeiten

Teilrisiken		
Klassen	Punktwert	Verbale Klassen
0	0	kein Teilrisiko
1	1 bis 5	sehr geringes Teilrisiko
2	6 bis 40	geringes Teilrisiko
3	41 bis 135	mittleres Teilrisiko
4	136 bis 320	hohes Teilrisiko
5	321 bis 625	sehr hohes Teilrisiko

Tabelle 9: Klasseneinteilung der Ergebnisse aus der Berechnung der Teilrisiken

Auch die Gesamtverwundbarkeit und das Gesamtrisiko des Teilprozesses „Leitwarte“ lassen sich auf diese Weise einstufen. Die Gesamtverwundbarkeit und das Gesamtrisiko können mit Werten von 240 beziehungsweise 720 als mittel eingestuft werden.

Gesamtverwundbarkeit	
Punktwert	Verbale Klassen
0	keine Gesamtverwundbarkeit
1 bis 35	sehr geringe Gesamtverwundbarkeit
36 bis 140	geringe Gesamtverwundbarkeit
141 bis 315	mittlere Gesamtverwundbarkeit
316 bis 560	hohe Gesamtverwundbarkeit
561 bis 875	sehr hohe Gesamtverwundbarkeit

Tabelle 10: Klasseneinteilung der Ergebnisse aus der Berechnung der Gesamtverwundbarkeiten

Gesamtrisiken		
Klassen	Punktwert	Verbale Klassen
0	0	kein Gesamtrisiko
1	1 bis 35	sehr geringes Gesamtrisiko
2	36 bis 280	geringes Gesamtrisiko
3	281 bis 945	mittleres Gesamtrisiko
4	946 bis 2240	hohes Gesamtrisiko
5	2241 bis 4375	sehr hohes Gesamtrisiko

Tabelle 11: Klasseneinteilung der Ergebnisse aus der Berechnung der Gesamtrisiken

⁷¹Vgl. Kap. VI. 4. Risikoermittlung Tabelle 7.

Die Leitwerte zeigt eine mittlere Gesamtverwundbarkeit sowie ein mittleres Gesamtrisiko auf. Für das Risikoelement „Daten und Software“ besteht hingegen eine sehr hohe Teilverwundbarkeit und ein hohes Teilrisiko. Das zweithöchste Teilrisiko zeigt sich bei den Anlagen und Geräten. Auch dieses Teilrisiko kann als hoch eingeschätzt werden. Wären im Realfall Maßnahmen zur weiterführenden Sicherung eingeplant, sollten diese im Bereich der beiden genannten Risikoelemente umgesetzt werden.

WICHTIGER HINWEIS:

Im Risikovergleich sollte der Schwerpunkt auf dem Vergleich von Teilrisiken liegen. Hohe Teilrisiken machen einen Teilprozess besonders anfällig und sind daher zu reduzieren.

Eine hohe Gesamtverwundbarkeit oder ein hohes Gesamtrisiko eines Teilprozesses können darauf hinweisen, dass mehrere hohe Teilrisiken vorliegen. In einem solchen Fall ist der Aufwand der Risikoreduzierung besonders hoch. Gesamtrisiken, die sich ausschließlich aus mittleren Teilrisiken zusammensetzen, sind dagegen weniger relevant.

Alternativ zum Vergleich ausgedruckter Risikotabellen können alle berechneten Werte wie Teilverwundbarkeiten und Teilrisiken auch in ein neues Tabellenblatt übertragen werden.

So können alle Ergebnisse auf einem Blatt zusammengefasst werden. Dies ermöglicht auch eine einfache grafische Auswertung mit Hilfe der Diagrammfunktion des Tabellenkalkulationsprogramms.

Herausgeber:

Bundesministerium des Innern
Referat KM 4
Alt-Moabit 101 D
10559 Berlin
www.bmi.bund.de

Redaktion:

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
Abteilung II Notfallvorsorge, Kritische Infrastrukturen

Gesamtgestaltung:

MEDIA CONSULTA Deutschland GmbH,
Anita Drbohlav (Kreation),
Petra Grampe, Helmut Spörl (Redaktion),
Patrick Pabst (Produktion)

Bildnachweis:

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
Bundesanstalt Technisches Hilfswerk

Druck:

Koelblin Fortuna, Baden-Baden

1. Auflage (Dezember 2007)

5.000 Exemplare

Die Broschüre kann kostenlos bestellt werden.

Publikationsversand der Bundesregierung

Postfach 48 10 09

18132 Rostock

Telefon: 0 18 05-77 80 90

(Festpreis 14 Ct/Min, abweichende Preise a. d. Mobilfunknetzen möglich; Stand Sept. 2007)

Telefax: 0 18 05-77 80 94

(Festpreis 14 Ct/Min, abweichende Preise a. d. Mobilfunknetzen möglich; Stand Sept. 2007)

E-Mail: publikationen@bundesregierung.de

Artikelnummer: BMI07326

Ihre zum Versand der Publikationen angegebenen personen-
bezogenen Daten werden nach erfolgter Lieferung gelöscht.