Bundesministerium
des Innern

Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement

Leitfaden für Unternehmen und Behörden

Vorwort

Liebe Leserinnen und Leser,

Kritische Infrastrukturen sind die Lebensadern unserer Gesellschaft. Wir alle sind darauf angewiesen, dass der Strom aus der Steckdose kommt, unser Trinkwasser aus dem Hahn fließt, die IT und das Verkehrsnetz funktionieren.

Kritische Infrastrukturen sind mannigfaltigen Gefahren ausgesetzt: extremen Wetter- und Witterungsbedingungen, menschlichem Fehlverhalten oder technischem Versagen.

Fallen Kritische Infrastrukturen ganz oder teilweise aus, kann dies zu erheblichen Belastungen für Staat, Wirtschaft und große Teile der Bevölkerung führen. Deshalb ist die Gewährleistung des Schutzes der Infrastrukturen eine Kernaufgabe staatlicher und unternehmerischer Sicherheitsvorsorge und fester Bestandteil der Sicherheitspolitik unseres Landes.

Da heute etwa 80 Prozent der Kritischen Infrastrukturen ausschließlich von privaten oder privatisierten Unternehmen betrieben werden, liegt mir als Bundesminister des Innern die partnerschaftliche Zusammenarbeit von Staat und Wirtschaft besonders am Herzen.

Am 17. Juni 2009 hat die Bundesregierung daher die „Nationale Strategie zum Schutz Kritischer Infrastrukturen“, die KRITIS-Strategie, beschlossen. Alle Akteure der KRITIS-Strategie – vor allem Bund, Länder, Kommunen und die Privatwirtschaft – sind dazu aufgerufen, im Dreiklang von Prävention, Reaktion und Nachhaltigkeit das Schutzniveau für Kritische Infrastrukturen in unserem Land zu erhöhen.

Ein Ergebnis der in der Strategie beschriebenen Kooperation ist der Leitfaden „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement“ für Unternehmen und Behörden, welcher unter der Verantwortung meines Hauses entwickelt wurde. Das Bundesministerium des Innern (BMI), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden dabei durch Experten der unternehmerischen Praxis unterstützt.

Der Leitfaden bietet das Handwerkszeug, um ein Risiko- und Krisenmanagement in Einrichtungen aufzubauen oder bestehende Systeme zu ergänzen. Seit seiner erstmaligen Veröffentlichung im Jahr 2008 wurden nahezu 7.500 deutsche sowie einige Hundert englische und zahlreiche französische Exemplare verteilt. Zusätzlich steht die digitale Version der Broschüre auf den Internetseiten des BMI, des BBK, des BSI und des Bevölkerungsschutzportals zum Download zur Verfügung.

Aufgrund der hohen Nachfrage und zahlreicher Verbesserungsvorschläge, die aus den Erfahrungen bei der Anwendung des Leitfadens im privaten und im öffentlichen Sektor resultieren, haben wir den Leitfaden mit inhaltlichen Aktualisierungen neu aufgelegt.

Um die Ausfallsicherheit Kritischer Infrastrukturen ist es hierzulande gut bestellt. Dennoch müssen Sicherheitsmaßnahmen ständig überprüft und an neue Risiken angepasst werden. Mithilfe dieses Leitfadens können Lücken strukturiert erfasst und geschlossen werden. Damit leisten wir einen wichtigen Beitrag zu einem noch besseren Schutz der Kritischen Infrastrukturen in Deutschland.

Allen Mitgestaltern dieses Leitfadens danke ich ganz herzlich für ihre wertvollen Anregungen und ihre engagierte Mitarbeit.

Dr. Hans-Peter Friedrich, MdB
Bundesminister des Innern

Danksagung

Für ihre Mitarbeit während des gesamten Prozesses der Entstehung des Anfang 2008 erstmals erschienenen Leitfadens dankt das Bundesministerium des Innern folgenden Partnern:

- 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 gesetzlichen Unfallversicherung VBG, Herrn Bernd Marquardt und Herrn Hans-Jürgen Penz
- 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.

Dank gilt ferner folgenden Partnern, die sich mit Rat und Anregungen in die Erstellung eingebracht haben: EnBW Regional AG, Gesamtverband der Deutschen Versicherungswirtschaft e. V. sowie Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V.

Es verbleibt die angenehme Pflicht, denjenigen Dank zu sagen, die uns bei der Entstehung dieser überarbeiteten Auflage maßgeblich unterstützt haben. Dafür dankt das Bundesministerium des Innern den größtenteils oben genannten Partnern sowie:

- dem Polizeipräsidium Köln, ZA 331-Qualitätsmangement, Herrn Friedhelm Fischer und Frau Andrea Grote
- den Mitgliedern der Projektgruppe Notfallplanung der Stadt Wuppertal

sowie ihren Mitarbeiterinnen und Mitarbeitern.

Sie alle haben sich große Verdienste um diesen Leitfaden erworben.

Berlin im Mai 2011

Inhalt

Zusammenfassung

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

Phase 1 – Vorplanung in der Einrichtung

Eine gründliche Vorplanung schafft die Voraussetzungen für eine erfolgreiche Umsetzung des Leitfadens. 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 Bereitstellung von Ressourcen, die Klärung rechtlicher Verpflichtungen zur Einrichtung eines Risiko- und Krisenmanagements sowie die Festlegung von strategischen Schutzzielen, die in einer Einrichtung 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 Schutzzielen abgeglichen und hierdurch bewertet. Können die strategischen Schutzziele in weiten Teilen nicht erreicht werden, sind konkrete Maßnahmen umzusetzen, die bestehende Risiken mindern und den Umgang mit Krisenereignissen erleichtern.

Phase 3 – Vorbeugende Maßnahmen und Strategien

Vorbeugende Maßnahmen tragen zur Minderung von Risiken von Prozessen und damit zur Sicherung einer Dienstleistung beziehungsweise einer 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 auch Einschränkungen der Flexibilität einer Einrichtung nach sich ziehen kann. 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 in einer Einrichtung, sollte ein Krisenmanagement als Sonderorganisation zur Bewältigung dieser Situation bereitstehen.

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 und die Zeitspanne zur Wiederherstellung des Normalzustandes verkürzt werden.

Phase 5 – Evaluierung des Risiko- und Krisenmanagements

Die Evaluierung bezieht sich auf alle Phasen des Risiko- und Krisenmanagements, also auf die Prüfung der in der Vorplanung festgelegten Regelungen, die Prüfung der Aktualität des aufgestellten Risikobildes, die Prüfung der umgesetzten vorbeugenden Maßnahmen auf ihre Wirksamkeit sowie die Prüfung des Krisenmanagements auf seine Effektivität. Es ist sinnvoll, eine solche Evaluierung regelmäßig durchzuführen.

Zusätzliche Evaluierungen können notwendig werden, und zwar

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

Ansprechpartner zu diesem Leitfaden:

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Abteilung II Notfallvorsorge,
Kritische Infrastrukturen,
Internationale Angelegenheiten
Provinzialstraße 93
53127 Bonn
www.bbk.bund.de

1 Einleitung

Infrastrukturen sind essentieller Bestandteil unserer hoch entwickelten Gesellschaft. Moderne Gesellschaften sind auf die uneingeschränkte Verfügbarkeit von Infrastrukturen angewiesen. Ein Ausfall der Energie- oder Wasserversorgung, eine Beeinträchtigung von Informations- und Kommunikationstechnologie, wie beispielsweise dem Internet, eine gravierende Störung im Gesundheitswesen oder der Lebensmittelversorgung, der Zusammenbruch von Finanzdienstleistungen oder der Wegfall wichtiger staatlicher Dienstleistungen kann weitreichende Folgen für die Bevölkerung in Deutschland und darüber hinaus haben.

Der Bund setzt sich seit 1997 branchenübergreifend mit dem Schutz sogenannter Kritischer Infrastrukturen auseinander, um solche Ereignisse zu vermeiden beziehungsweise deren Folgen zu minimieren. Im Juni 2009 wurde durch das Bundeskabinett die „Nationale Strategie zum Schutz Kritischer Infrastrukturen“ verabschiedet, die die Eckpunkte zum Schutz Kritischer Infrastrukturen festschreibt. In der nationalen Strategie 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“ definiert.[1]

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 in andere Standorte, Branchen oder Sektoren hineinwirken und sich damit weit über das ursprüngliche Schadensgebiet auswirken.

Die finanziellen und personellen Ressourcen, die den Einrichtungen 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, die auf die Infrastrukturen einwirken können. Risiken müssen verglichen und bewertet werden können, um Risikoschwerpunkte zu erkennen. 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 Einrichtungen konzipiert, die Kritische Infrastrukturen betreiben.

Er kombiniert theoretische Grundlagen zum Risiko- und Krisenmanagement mit praktischen Listen und einem Beispiel zur Risikoanalyse. Ziel ist es, Einrichtungen beim Auf- beziehungsweise Ausbau eines effektiven und effizienten Risiko- und Krisenmanagements zu unterstützen.

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

[1] Bundesministerium des Innern 2009, Seite 3.

2 Grundlagen zu Kritischen Infrastrukturen

2.1 Sektoren

Unternehmen und Behörden im Sinne der in der Einleitung genannten Definition finden sich überwiegend in den folgenden Sektoren:[2]

- Energie (Strom, Mineralöl, Gas)
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Staat und Verwaltung
- Medien und Kultur

2.2 Rahmenbedingungen und Eigenschaften Kritischer Infrastrukturen

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

Schadensbild 1: Es kam zu weiträumigen Einwirkungen auf Kritische Infrastrukturen, die insbesondere von Naturgefahren ausgelöst wurden. Dies war mit regionalen, überregionalen, landes- oder europaweiten Beeinträchtigungen verbunden (Beispiele: Elbeflut 2002, Orkan Kyrill 2007 oder Orkan Xynthia 2010, Ausbruch des Vulkans Eyjafjallajökull, Island, und insbesondere die daraus entstandenen Aschewolken 2010).

Schadensbild 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 (Beispiele: Abschaltung einer Stromleitung über die Ems im Jahr 2006, die zu Stromausfällen in vielen 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
Wetterbedingte Extremereignisse können sich unmittelbar auf Infrastruktursysteme auswirken. Belastbare Aussagen zur Veränderung solcher Ereignisse 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 2002, im Alpenraum 2005[3] oder an der Neiße 2010.

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 Mutation nur eine Frage der Zeit ist. Eine Influenzapandemie würde sich über die internationalen Verkehrsknotenpunkte auch in Deutschland ausbreiten. Ihre Auswirkungen können alle Lebensbereiche bedrohen. Viele Dienstleistungs- und Produktionsprozesse könnten nicht mehr oder nur noch sehr eingeschränkt aufrechterhalten werden. Aufgrund der gegenseitigen Abhängigkeiten in den Infrastruktursystemen würde dies zu einem Dominoeffekt führen, der große Teile der Funktionen von Staat, Wirtschaft und Gesellschaft lähmen

[2] Einteilung gemäß KRITIS des Bundes.

[3] Rahmstorf u. a. 2006, Seite 70.

würde.[4] Modellberechnungen gehen für Deutschland von einer Erkrankungsrate von 15 bis 50 Prozent aus.[5] Neben unmittelbar erkrankten Beschäftigten würden auch solche Beschäftigte nicht ihre Arbeit aufnehmen können, die erkrankte Familienmitglieder pflegen oder aus Angst vor Ansteckung zu Hause bleiben. Die Abwesenheitsquote würde also deutlich über der Erkrankungsrate liegen. Die weltweit aufgetretene Pandemie H1N1 in den Jahren 2009 und 2010 hat zwar im Vergleich zur Spanischen Grippe von 1918 geringere Auswirkungen gehabt, aber dennoch die bestehenden Risiken einer Pandemie deutlich vor Augen geführt.

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.[6] Anschläge auf Infrastruktursysteme in Deutschland sind nicht auszuschließen. Im Jahr 2006 sind Anschläge auf zwei Regionalzüge der Deutschen Bahn 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. Im Jahr 2010 waren durch den Trojaner Stuxnet weltweit Prozesssteuerungssysteme mehrerer Einrichtungen betroffen.

2.2.2 Sozioökonomische Rahmenbedingungen

Steigende Abhängigkeit
Die Abhängigkeit vieler Einrichtungen von externen Dienstleistungen oder Produkten steigt. Einen hohen Stellenwert nimmt hierbei die Stromversorgung ein. Nahezu alle Dienstleistungs- und Produktionsprozesse stützen sich unmittelbar oder mittelbar auf eine funktionierende Stromversorgung.

Subjektive Risikowahrnehmung
Einrichtungen investieren viel in ihre Sicherheit und verlassen sich darauf, dass die umgesetzten Maßnahmen wirken. Eine konkrete positive Wirkung von Sicherheitsmaßnahmen lässt sich vielfach nicht objektiv erfassen. Stattdessen werden lange krisenfreie Phasen 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.[7] 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 Alterstruktur der Gesellschaft sowie Veränderungen der Bevölkerungsdichte in Deutschland 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 Rahmenbedingungen[8]
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.

4 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2007.

5 Robert Koch Institut 2007b, Seite 4.

6 Vgl. Lewis 2006, Seite 1.

7 Dost 2006.

8 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 zur Verfügung gestellt. 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 Gasversorgung.

Branchenübergreifende Verknüpfungen (Interdependenz)

Infrastruktursysteme sind zunehmend voneinander abhängig. Viele physische, virtuelle und logische Abhängigkeiten stellen sich erst bei Ausfall heraus. Der hohe Grad gegenseitiger Abhängigkeiten kann zu kaskadenartigen Ausfällen führen.[9] Gleichzeitig reichen immer kleinere Störungen aus, um in komplexen Systemen dramatische Folgen zu verursachen (Verwundbarkeitsparadoxon).[10]

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.

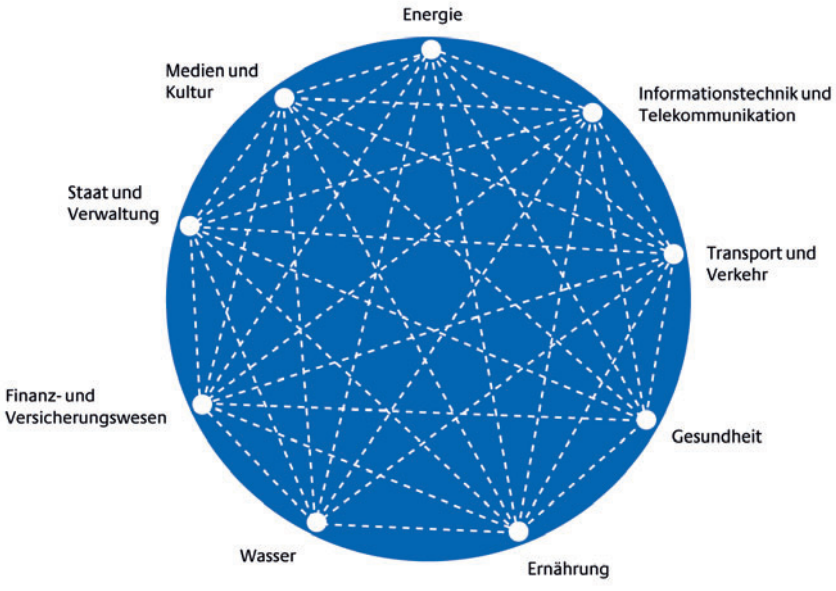
Schadenstypen

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 zu Vertrauensverlust der Nutzer in eine Dienstleistung oder ein Produkt.

[9] Vgl. Lewis 2006, Seite 57.

[10] Rosenthal 1992, Seite 74f.

Abbildung 1: Interdependenzen 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 Geschäftsbetriebes in jeglicher Art, von der Störung bis hin zur Krise – ob Börsenkrise, Naturereignis oder terroristischer Anschlag.

Die Vorstände von Aktiengesellschaften, ihre Aufsichtsräte und 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. Es ist jedoch sinnvoll, das interne Überwachungssystem so einzurichten, 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 die 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 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] Im Schadensfall kann der Vorstand haftungsrechtlich nach § 93 Abs. 2 AktG zu Schadensersatz verpflichtet werden, wenn es zu einer haftungsbegründeten Sorgfaltspflichtverletzung gekommen ist.

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 des Versicherungsschutzes 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.

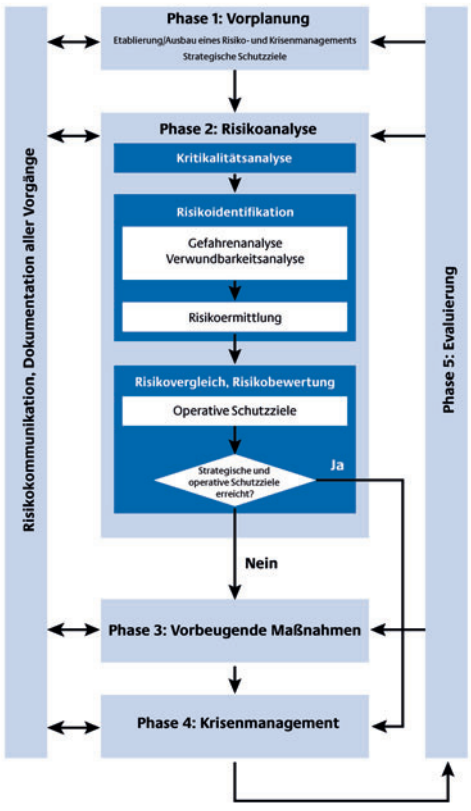
Ebenso verlangt die Baseler Eigenkapitalvereinbarung (Basel II), die Bankkrisen verringern soll, explizit im Rahmen der Kreditvergabe, neben der Betrachtung von Markt- und Kreditrisiken operationelle Risiken der Banken zu berücksichtigen. Auch wenn sich Basel II nur auf die Risiken der Kreditinstitute bezieht, ist es möglich, dass das Erfordernis einer Risikodarstellung von den Banken, zum Beispiel als Voraussetzung für eine Kreditvergabe, an die Unternehmen weitergereicht wird. 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.

[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 einer Einrichtung. Hierzu zählen zunächst eine Vorplanung zur Etablierung eines Risiko- und Krisenmanagements (Phase 1), eine Risikoanalyse (Phase 2), die Beschreibung vorbeugender Maßnahmen (Phase 3), der Auf- oder Ausbau eines Krisenmanagements (Phase 4) sowie die regelmäßige Evaluierung der Phasen 1 bis 4 (Phase 5). Der Auf- oder Ausbau eines Krisenmanagements folgt in diesem Leitfaden auf die Durchführung vorbeugender Maßnahmen und schließt somit an die Etablierung des Risikomanagements an. Das Krisenmanagement hat Verknüpfungen zum Risikomanagement, kann jedoch auch als eigenständiger Vorgang betrachtet werden. Abbildung 2 veranschaulicht dieses Konzept und bereitet den Ablauf grafisch auf.

Abbildung 2: Risiko- und Krisenmanagement-konzept in fünf Phasen[12]



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 des Auf- oder Ausbaus eines Risiko- und Krisenmanagements sollten grundsätzliche Festlegungen getroffen 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 Bereitstellung von Ressourcen für die Etablierung sowie die Festlegung strategischer Schutzziele für die Einrichtung.

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 sollte besondere Aufmerksamkeit geschenkt werden, da die Qualität eines Risikomanagements mit der Akzeptanz und Motivation der Mitarbeiter steht und fällt.

Zuständigkeiten bei der Etablierung

Die Etablierung eines Risiko- und Krisenmanagements wird von einem fachlichen Leiter gesteuert, der möglichst aus der Einrichtung stammt. Bei diesem liegt die inhaltliche Federführung. Im Bedarfsfall stimmt er sich mit der Leitung der Einrichtung ab.

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 daher im Verlauf der Umsetzung festgelegt.

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

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 können in der Arbeitsgruppe abgebildet werden.

Sofern eine 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.

Klärung der rechtlichen Verpflichtungen

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

Strategische Schutzziele

Es ist sinnvoll, im Rahmen der Etablierung eines Risiko- und Krisenmanagements strategische Schutzziele zu formulieren. Sie definieren prozessübergreifend, was durch das Risiko- und Krisenmanagement erreicht werden soll.

Strategische Schutzziele werden maßgeblich von ethischen, operativen, technischen, finanziellen, gesetzlichen, sozialen und umweltbezogenen Aspekten beeinflusst.[13] Sie weisen folgende Merkmale auf:

- Sie beschreiben einen Sollzustand.
- Sie schaffen Lösungsräume für die Umsetzung unterschiedlicher Maßnahmen.

Beispiele für strategische Schutzziele sind:

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

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“.[14] Risikokommunikation ist die Plattform von Risikobewusstsein und Risikoakzeptanz in Einrichtungen. Beide Aspekte sind für ein erfolgreiches Risikomanagement unerlässlich. Für eine erfolgreiche Risikokommunikation ist von vornherein festzulegen, welches Ziel erreicht werden soll und welche Risikothemen diesbezüglich zu kommunizieren sind. Im vorliegenden Kontext ist die explizite Unterscheidung von interner und externer Risikokommunikation einer Einrichtung sinnvoll.

Die interne Risikokommunikation bezieht sich auf alle kommunikativen Interaktionen zu Risikothemen innerhalb der Einrichtung – von der Etablierung bis hin zur Evaluierung des Risikomanagements. Der Risikokommunikation ist hinsichtlich der Etablierung besondere Aufmerksamkeit zu schenken – 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. Es ist wichtig darauf zu achten, alle betroffenen Parteien am Risikokommunikationsprozess zu beteiligen und auch kritische Positionen zuzulassen, um Sachlichkeit und Vertrauen zu schaffen. Außerdem ist es sinnvoll, sowohl für die interne als auch für die externe Risikokommunikation eine Struktur festzulegen, die die einzelnen Schritte des Risikokommunikationsprozesses festlegt. Abschließend werden sowohl der interne als auch der externe Risikokommunikationsprozess evaluiert. Für diese Evaluierung können die Anforderungen von Qualitätsmanagementsystemen (zum Beispiel EN ISO 9000) zugrunde gelegt werden.[15]

Externe Risikokommunikation zielt nicht auf ein bloßes Informieren von Medien und Betroffenen ab, sondern auf einen adressatengerechten Dialog. Dabei ist stets zu bedenken, Risikothemen so zu kommunizieren, dass keine Missverständnisse

[13] Australian/New Zealand Standard 2004, Seite 15.

[14] Jungermann u. a. 1991, Seite 5.

[15] Hertel 2003, Seite 590.

zwischen Sender und Empfänger entstehen können. So sind beispielsweise Unterschiede in der Risikowahrnehmung zwischen Experten und Laien empirisch nachgewiesen. Um ungewollten 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 für bestehende und potenzielle Risiken in Einrichtungen. Die Risiken werden in diesem Leitfaden auf Prozesse sowie ihre Bestandteile bezogen.

Besonders für Unternehmen ist es ratsam, auch die etablierten branchenspezifischen Risiken mit in die Risikoanalyse einzubeziehen. Die Risikoanalyse betrachtet die Gründe und Ursachen von Risiken, untersucht die Konsequenzen und bestimmt den Rahmen, in dem diese Konsequenzen auftreten können.[17] Durch den Vergleich der Risiken der Prozesse in einer Einrichtung und die damit verbundene Erfassung von Risikospitzen schafft sie die Grundlage zum effektiven und effizienten Umgang mit begrenzten finanziellen und personellen Ressourcen.

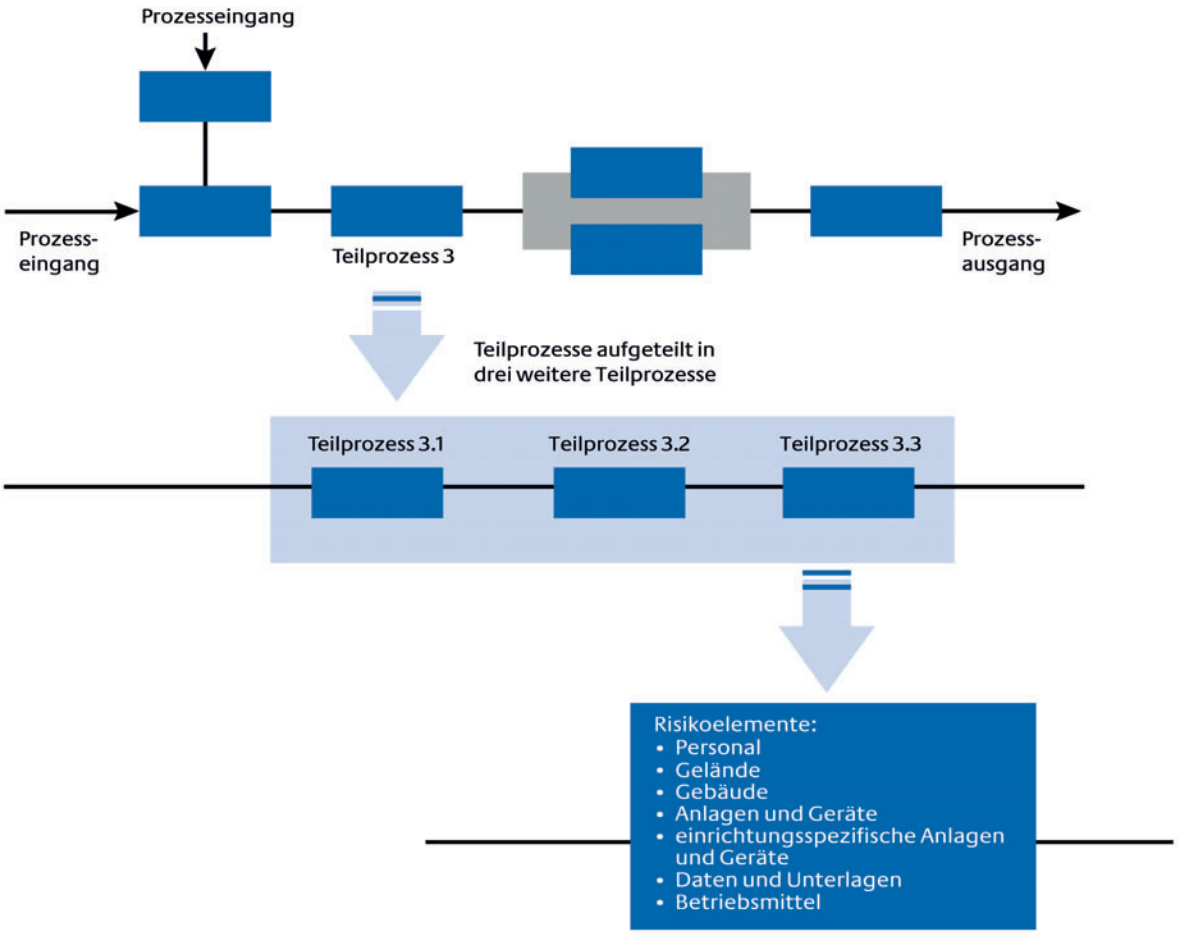
Eine Risikoanalyse im Sinne dieses Leitfadens beantwortet die folgenden Fragen:

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

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

[17] International Organization for Standardization 31000, Seite 18.

Abbildung 3: Prozess, Teilprozesse, Risikoelemente



- Mit welchem Schaden ist bei Eintritt unterschiedlicher Gefahren zu rechnen?
- Welche Auswirkungen für die Funktionsfähigkeit der Einrichtung hat ein Ausfall von Prozessen aufgrund der Gefahreneinwirkung?

Diese Fragen verdeutlichen, dass in die Analyse des Risikos für einen Prozess beziehungsweise Prozessbestandteil sowohl Gefahreninformationen als auch Aussagen über die Verwundbarkeit und Kritikalität dieses 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. Sie werden daher als Prozesse beziehungsweise Teilprozesse bezeichnet. Als Teilprozesse im Sinne dieses Leitfadens werden einzelne Abschnitte von Prozessen verstanden.

Ausgangspunkt der Risikoanalyse ist die Unterteilung der Einrichtung in Prozesse und Teilprozesse. Der Grad der Aufschlüsselung in Teilprozesse wird von der Einrichtung selbst festgelegt. Wird beispielsweise eine Steuerzentrale als Bestandteil eines Prozesses erkannt, kann diese als Teilprozess definiert werden. Es besteht aber auch die Möglichkeit, die Steuerzentrale 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 wächst aber auch die Aussagekraft einer Risikoanalyse.[18]

Abbildung 3 zeigt schematisch einen Prozess, seine 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 dieses Teilprozesses 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 Personen sind grundsätzlich in ausreichendem Maße vor Gefahreneinwirkungen zu schützen beziehungsweise bei drohender Gefahr in Sicherheit zu bringen.

  Hierfür sind in allen Einrichtungen 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 frei liegenden Verkehrs-, Lager- und Parkflächen, Grünanlagen sowie betriebsnotwendigen 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.[19]

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.

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

[19] Beispiele: Steuerelemente, Software, medizinisches Gerät, spezielle Haustechnik, Sicherheitsschleusen, Tanklager, Flugzeuge.

- **Betriebsmittel**
  Unter Betriebsmittel werden im Rahmen dieses Leitfadens alle sonstigen Produktions- oder Hilfsmittel verstanden, die nicht in den vorherigen Punkten genannt wurden.

- **Umwelt**
  Zur Umwelt zählen alle Umweltfaktoren, die zur Aufrechterhaltung von Teilprozessen in der Einrichtung notwendig sind.

Der Schutz und die Sicherheit der Risikoelemente ist eine wesentliche Aufgabe des Risikomanagements. Eine Einrichtung trägt die Verantwortung dafür, dass ihre Mitarbeiter, Kunden und andere Anwesende umfassend vor möglichen Gefahren geschützt sind und ein Höchstmaß an Sicherheit garantiert wird.

3.2.1 Kritikalitätsanalyse

Durch eine Kritikalitätsanalyse können in der Einrichtung aus allen erfassten Prozessen diejenigen identifiziert werden, deren Beeinträchtigung zu weitreichenden Folgen für die Einrichtung führen würde und die entscheidend für die Gewährleistung der Funktionsfähigkeit der Einrichtung sind. Ein Ausfall kritischer Prozesse hat somit gravierende Auswirkungen auf die Einrichtung und möglicherweise auch auf die Versorgung und den Schutz der Bevölkerung. 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.

Die folgenden Kriterien können zur Ermittlung kritischer Prozesse herangezogen werden:[20]

- **Leben und Gesundheit**
  Hat die Beeinträchtigung des Prozesses Auswirkungen auf Leben und Gesundheit von Menschen?

- **Volumen**
  Ist ein erheblicher Umfang der gesamten Dienstleistung beziehungsweise der Produktion betroffen, wenn der betrachtete Prozess beeinträchtigt ist beziehungsweise gänzlich ausfällt? (Zum Beispiel: betroffenes Volumen ≥ 30 Prozent der gesamten Dienstleistung oder Produktion)

- **Auswirkungszeitpunkt**
  Wie schnell wirkt sich die Beeinträchtigung des Prozesses auf die gesamte Dienstleistung beziehungsweise Produktion der Einrichtung aus? (Zum Beispiel: Auswirkungszeitpunkt der Beeinträchtigung liegt innerhalb eines Zeitraums von 24 Stunden.)

- **Vertragliche, ordnungspolitische oder gesetzliche Relevanz**
  Hat die Beeinträchtigung des betrachteten Prozesses vertragliche, ordnungspolitische oder gesetzliche Folgen für die Einrichtung?

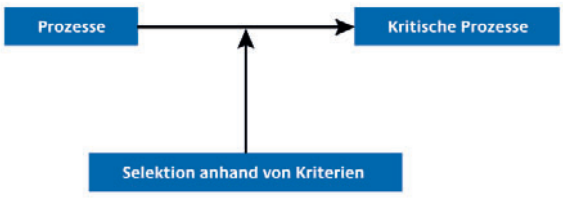
- **Wirtschaftliche Schäden**
  Sind die geschätzten wirtschaftlichen Schäden, die der Einrichtung durch die Beeinträchtigung des betrachteten Prozesses entstehen, erheblich? (Zum Beispiel: wirtschaftlicher Schaden ≥ 5 Prozent des jährlichen Umsatzes/Budgets der Einrichtung)

- **Umwelt**
  Hat die Beeinträchtigung des Prozesses negative Konsequenzen für die Umwelt?

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. Die Fragen zu den einzelnen Kritikalitätskriterien werden nacheinander beantwortet. Sobald eine Frage positiv beantwortet wird, ist der Prozess als kritisch einzustufen und wird somit im Rahmen der Risikoanalyse untersucht. Die Schwellenwerte für die jeweiligen Kritikalitätskriterien können von jeder Einrichtung selbst festgelegt werden.

WICHTIGER HINWEIS:
Die Kritikalität von Prozessen bezieht sich auf die Bedeutsamkeit der Prozesse für die Funktionsfähigkeit einer Einrichtung. Sie ist ein Maß für die Auswirkungen, die ein Ausfall eines Prozesses zur Folge haben kann.

Abbildung 4: Ablaufschema Kritikalitätsanalyse[21]



Ergebnis der Kritikalitätsanalyse ist das Erkennen und Erfassen aller kritischen Prozesse in der Einrichtung (siehe Abbildung 4) sowie die Darstellung der dort wirkenden Teilprozesse und der Risikoelemente.

[20] The Business Continuity Institute 2005, Seite 26.

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

3.2.2 Risikoidentifikation

Die Risiken für eine Einrichtung werden durch die Gefahren, die am Standort oder an den Standorten auftreten und auf die Risikoelemente einwirken können, sowie durch die Verwundbarkeit der Risikoelemente gegenüber diesen Gefahren bestimmt. Die Verbindung relevanter Gefahren- und Verwundbarkeitsinformationen führt zur Risikoermittlung für die betrachteten Risikoelemente. Werden die Risiken der Risikoelemente zusammengeführt, ergibt sich das Risiko für einen Teilprozess. Die Risiken für die Risikoelemente werden im Leitfaden als Teilrisiken, die für Teilprozesse aggregierten Risiken als Gesamtrisiken der Teilprozesse bezeichnet. Im Folgenden werden die Aspekte der Risikoidentifikation ausführlich beschrieben.

WICHTIGER HINWEIS:
Ein Ereignis kann auch bei nicht vorhandenen Auswirkungen auf das Leben und die Gesundheit von Menschen und geringen wirtschaftlichen Schäden zu einem bedeutenden Imageverlust einer Einrichtung führen. Dieser Imageverlust wirkt sich zunächst nur indirekt auf die Einrichtung aus, kann aber insbesondere für Unternehmen längerfristig erheblich höhere wirtschaftliche Schäden/Einbußen zur Folge haben, als durch das Ereignis selbst entstanden sind. Gegenüber Behörden kann es zu einem starken Vertrauensverlust kommen.

Gefahrenanalyse und Szenarioentwicklung

Entscheidend für eine erfolgreiche Risikoanalyse ist das Erkennen und Dokumentieren aller relevanten Gefahren. In einem ersten Schritt zur Gefahrenanalyse und Szenarioentwicklung wird daher eine Liste derjenigen Gefahren erstellt, die am Standort beziehungsweise an den Standorten der Einrichtung auftreten können. Diese umfassende Liste gibt Aufschluss über generelle Eigenschaften der Gefahren, ihre mögliche Intensität, Dauer, räumliche Ausprägung, Vorwarnzeit und Wirkungen.[22] Referenzereignisse können ebenfalls aufgeführt werden.

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

Folgende Informationen werden für jedes Szenario festgelegt:

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

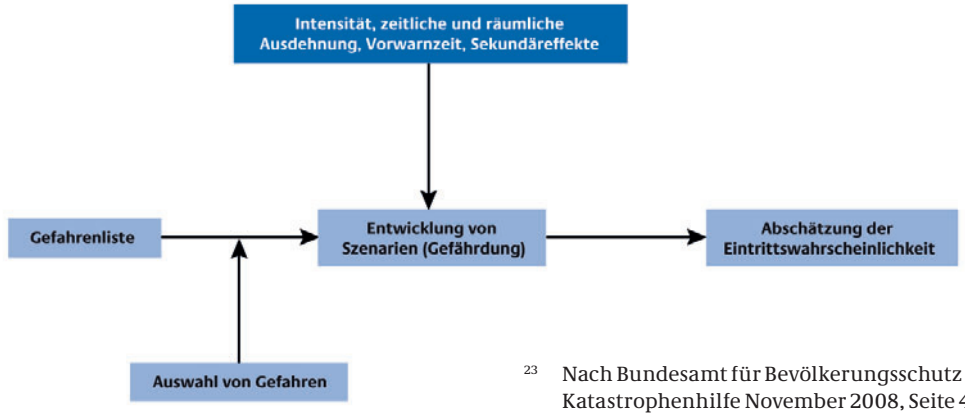
WICHTIGER HINWEIS:
Die Exposition ist Grundvoraussetzung für die Beeinträchtigung eines Prozesses, Teilprozesses oder Risikoelementes. Dabei können lokale Einwirkungen ebenso zu Ausfällen führen wie eine weiträumige Exposition. Entscheidend ist die Betroffenheit von Teilprozessen und Risikoelementen.

- **Erwartete Intensität**
  Wie hoch ist das Störungspotenzial des Szenarios bezogen auf einen Prozess, Teilprozess und dessen Risikoelemente?

- **Erwartete zeitliche Ausdehnung**
  Wie lange dauert das Ereignis an?

[22] 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.

Abbildung 5: Ablaufschema Gefahrenanalyse[23]



[23] Nach Bundesamt für Bevölkerungsschutz und Katastrophenhilfe November 2008, Seite 42.

- **Erwartete räumliche Ausdehnung**
  Welche Fläche ist von dem Ereignis betroffen?

- **Vorwarnung**
  Welche Vorwarnzeit ist für das Ereignis anzunehmen?

- **Sekundäreffekte**
  Welche Effekte entstehen aufgrund von Abhängigkeiten der Prozesse, Teilprozesse und Risikoelemente? Welche psychologische Wirkung kann das Ereignis hervorrufen? Welche Öffentlichkeitswirkung beziehungsweise Medienwirksamkeit kann das Ereignis haben?

- **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 (siehe Abbildung 5). 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 Einrichtungen empfiehlt es sich daher, die Eintrittswahrscheinlichkeiten anhand einer Klasseneinteilung abzuschätzen.

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. Zum Beispiel:
Szenario 1: Ausfall der externen Stromversorgung
Szenario 2: Ausfall der externen Wasserversorgung
Ansonsten entstehen wenige, sehr komplexe Szenarien, deren Auswirkungen unübersichtlich sind.

Effekte, die direkt mit dem Szenario zusammenhängen, diesem immanent sind und zu einer Verstärkung der Auswirkungen führen, sind nach Möglichkeit mit dem Szenario zu betrachten (zum Beispiel Grundwasseranstieg bei Hochwasser).

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

Verwundbarkeitsanalyse

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

Die Verwundbarkeit setzt sich aus den Faktoren Funktionsanfälligkeit und Ersetzbarkeit zusammen.

Diese Faktoren ergeben sich aus einzelnen Verwundbarkeitskriterien. Für eine detaillierte Betrachtung der Verwundbarkeit können Einrichtungen optional aus der folgenden Kriterienliste einen für sich relevanten Kriterienkatalog zusammenstellen beziehungsweise ihren bereits bestehenden Kriterienkatalog ergänzen.

Kriterien der Funktionsanfälligkeit:

- **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 Risikoelementes für den Teilprozess im Rahmen der Risikoermittlung darzustellen.

- **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. (Beispiel: Abhängigkeit von der externen Stromversorgung)

- **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. (Beispiel: Abhängigkeit eines Krankenhausbetriebes von der in der Einrichtung befindlichen Wäscherei)

- **Robustheit**
  Die physische Robustheit der Risikoelemente (insbesondere Anlagen, Geräte, Gebäude) ist ein

wichtiger Indikator dafür, ob diese durch die Einwirkung eines extremen Ereignisses beschädigt werden. Hierdurch würden die zugeordneten Teilprozesse beeinträchtigt werden. Entscheidend für die Robustheit sind beispielsweise das verwendete Material oder die Zusammensetzung der Risikoelemente. (Beispiel: Robustheit wasserdichter Geräte gegenüber Wassereinwirkungen)

- **Realisiertes Schutzniveau**
  Die getroffenen vorbeugenden Maßnahmen bestimmen das realisierte 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)

- **Anpassungsfähigkeit**
  Ein Teilprozess ist verwundbar, wenn sich seine Risikoelemente verändernden Rahmenbedingungen nicht oder nur schwer anpassen können.

- **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.

- **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 verwundbar. (Beispiel: Bei einem wetterbedingten Temperaturanstieg in Flüssen können dies Anlagenteile sein, die Kühlwasser benötigen.)

Kriterien der Ersetzbarkeit:

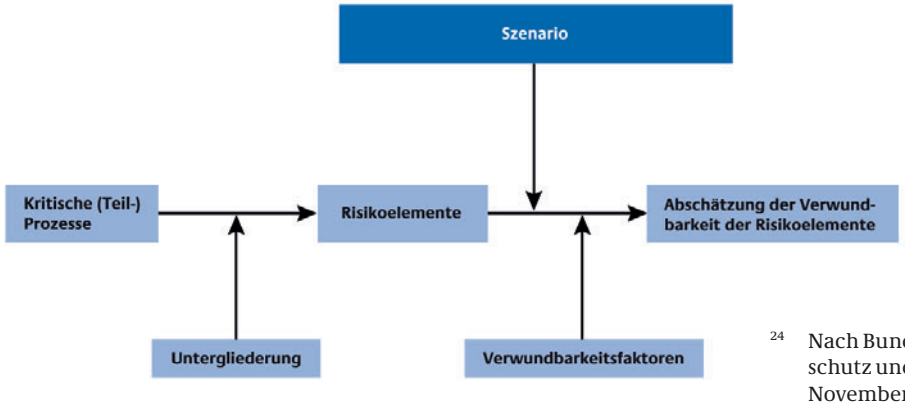
- **Redundanz, Ersatz**
  Der Ausfall von Risikoelementen einer Einrichtung ist besser zu bewältigen, wenn parallele Strukturen oder Ersatzstrukturen vorhanden sind, um dieselbe Leistung zu erbringen. Es ist nach Möglichkeit sowohl eine technische als auch eine organisatorische Ersetzbarkeit beziehungsweise Redundanz zu gewährleisten. 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 Risikoelementes nach einer Beschädigung verbunden ist. Im Hinblick auf die Verwundbarkeit eines Teilprozesses ist dabei nicht ausschließlich der finanzielle Aufwand gemeint, sondern auch der zeitliche oder personelle Aufwand.

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

Die Verwundbarkeitsfaktoren Funktionsanfälligkeit und Ersetzbarkeit dienen als Indikatoren zur Bestimmung der Verwundbarkeit von Teilprozessen/Risikoelementen einer Einrichtung und sind somit für die Verwundbarkeit von Einrichtungen entscheidend. Abbildung 6 zeigt den grundsätzlichen Ablauf einer Verwundbarkeitsanalyse für die Risikoelemente. Aus der Summe der Verwundbarkeit der einzelnen Risikoelemente eines Teilprozesses ergibt sich die gesamte Verwundbarkeit dieses Teilprozesses.

Abbildung 6: Ablaufschema Verwundbarkeitsanalyse[24]



[24] Nach Bundesamt für Bevölkerungsschutz und Katastrophenhilfe November 2008, Seite 42.

Risikoermittlung

Im Rahmen der Risikoermittlung werden berechnete Werte, Abschätzungen oder Aussagen aus der Szenarioentwicklung und der Verwundbarkeitsanalyse zu Risikowerten oder Risikoaussagen verknüpft. 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 erfolgen:[25]

- **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 mithilfe 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.[26]

Risikovergleich und -bewertung

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, für die die höchsten Risiken bestehen.

Die Risikobewertung zeigt auf, 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. Beispielhaft können solche operative Schutzziele folgendermaßen lauten:

- Reduzierung des Gesamtrisikos für Teilprozess X

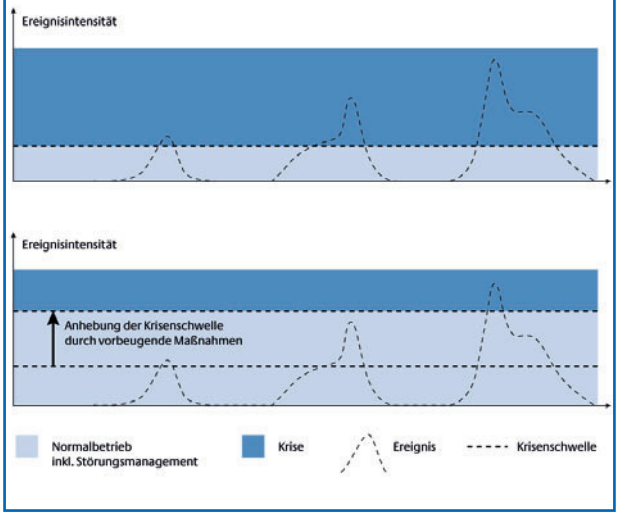
- Reduzierung der höchsten Teilrisiken in allen Teilprozessen, die zu kritischen Prozessen gehören

Maßnahmen sind vorrangig für die Teilprozesse umzusetzen, die die größten Risiken aufweisen. Letztlich ist es die Aufgabe der Entscheidungsträger in der Einrichtung, 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 dabei, operative Schutzziele zu erreichen und damit die Krisenschwelle für Ereignisse mit Krisenpotenzial in der Einrichtung anzuheben (siehe Abbildung 7). Hierdurch kann die Anzahl krisenhafter Ereignisse minimiert beziehungsweise die Intensität auftretender Ereignisse reduziert werden.

Abbildung 7: Ereignisintensität und Krisenschwelle



[25] Vgl. Australian/New Zealand Standard 2004, Seiten 18–19.

[26] Anhang VI verweist auf ein Beispiel, das auf der Internetseite des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe zur Verfügung gestellt wird. Eine weitere Methode zur Risikoanalyse speziell für den Bereich der Informationstechnologie findet sich unter Bundesamt für Sicherheit in der Informationstechnik 2005.

Es ist sinnvoll, vorbeugende Maßnahmen einer Kosten-Nutzen-Analyse zu unterziehen. 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.[27]

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 sowie ökologische Überlegungen in die Entscheidung über Schutzmaßnahmen einfließen zu lassen. Das heißt, die Entscheidung über Schutzmaßnahmen sollte mit den grundlegenden Wertvorstellungen einer Gesellschaft vereinbar sein, der gesellschaftlichen Verantwortung der Einrichtung gerecht werden und Schäden an der Umwelt vermeiden. Außerdem erscheint es sinnvoll, die Schutzmaßnahmen an der Unternehmensphilosophie und der Kultur der Einrichtung auszurichten. Damit wird die Glaubwürdigkeit der Einrichtung unterstrichen.

Vorbeugende Strategien nutzen die Werkzeuge Risikovermeidung, Risikoüberwälzung oder Risikoakzeptanz. Sie werden in der Regel nur komplementär zu risikomindernden Maßnahmen genutzt.

Risikovermeidende Maßnahmen können die Handlungsfreiheit der Einrichtung gegebenenfalls einschränken, beispielsweise bei Entscheidungen gegen risikobehaftete Standorte. Dennoch sind solche Entscheidungen natürlich sinnvoll, da Risiken hierdurch frühzeitig vermieden werden.

Risikoüberwälzende Maßnahmen und die Akzeptanz von Risiken leisten dahingegen keinen Beitrag zur Risikominderung.

3.3.1 Risikominderung

Maßnahmen zur Risikominderung reduzieren entweder die Funktionsanfälligkeit der Risikoelemente gegenüber der Einwirkung von Gefahren (zum Beispiel durch bauliche Schutzmaßnahmen) oder richten sich unmittelbar an die betriebliche Kontinuität der kritischen Prozesse durch die Schaffung von Redundanz beziehungsweise Ersatz. Redundante Systeme oder Ersatzsysteme ermöglichen die betriebliche Kontinuität kritischer Prozesse im Rahmen des Wiederanlaufmanagements, auch wenn es zur Beeinträchtigung von Risikoelementen kommt.[28]

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, Einzelgebäuden oder 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
- 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. Es ist sinnvoll, die verbleibenden Restrisiken zu dokumentieren und deren Akzeptanz durch die Einrichtung schriftlich festzuhalten.

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.

[27] Vgl. Australian/New Zealand Standard 2004, Seite 21f.

[28] In Anhang V befindet sich eine umfangreiche Checkliste zur Umsetzung vorbeugender Maßnahmen.

3.3.5 Schadenerfahrungen der Sachversicherer

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

Die Erkenntnisse aus Schäden sind in zahlreichen Publikationen des Gesamtverbandes der Deutschen Versicherungswirtschaft zusammengetragen.[29] Diese können als weitere Erkenntnisquelle zur Optimierung des Schutzes einzelner Organisationen und 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 ihrer Funktionalität 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.[30] Eine Krise ist klar abzugrenzen von Ereignissen minderschweren Ausmaßes, die in diesem Leitfaden als Störungen bezeichnet werden.

Auslöser für Krisen können in Einrichtungen selbst entstehen, wie zum Beispiel Finanzkrisen als Folge von Missmanagement oder Veruntreuung (siehe Abbildung 8). 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.

Das Krisenmanagement liefert einen signifikanten Beitrag zum Schutz von Einrichtungen und damit zum Schutz von Kritischen Infrastrukturen und der Bevölkerung. Wechselwirkungen bestehen zum Risikomanagement, da nicht alle Risiken durch risikomindernde Maßnahmen reduziert werden können und immer ein Restrisiko bestehen bleibt. Das Krisenmanagement bietet deshalb eine Struktur zur Bewältigung von Krisen, die trotz Prävention 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.

[29] Siehe zum Beispiel VdS-Richtlinien 2007.

[30] Vgl. Trauboth 2002, Seite 14f.

Abbildung 8: Auslöser von inneren und äußeren Krisen

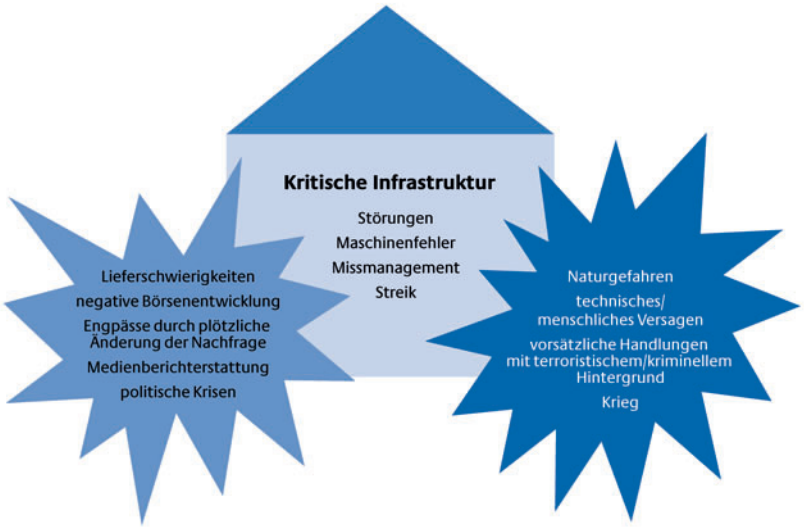
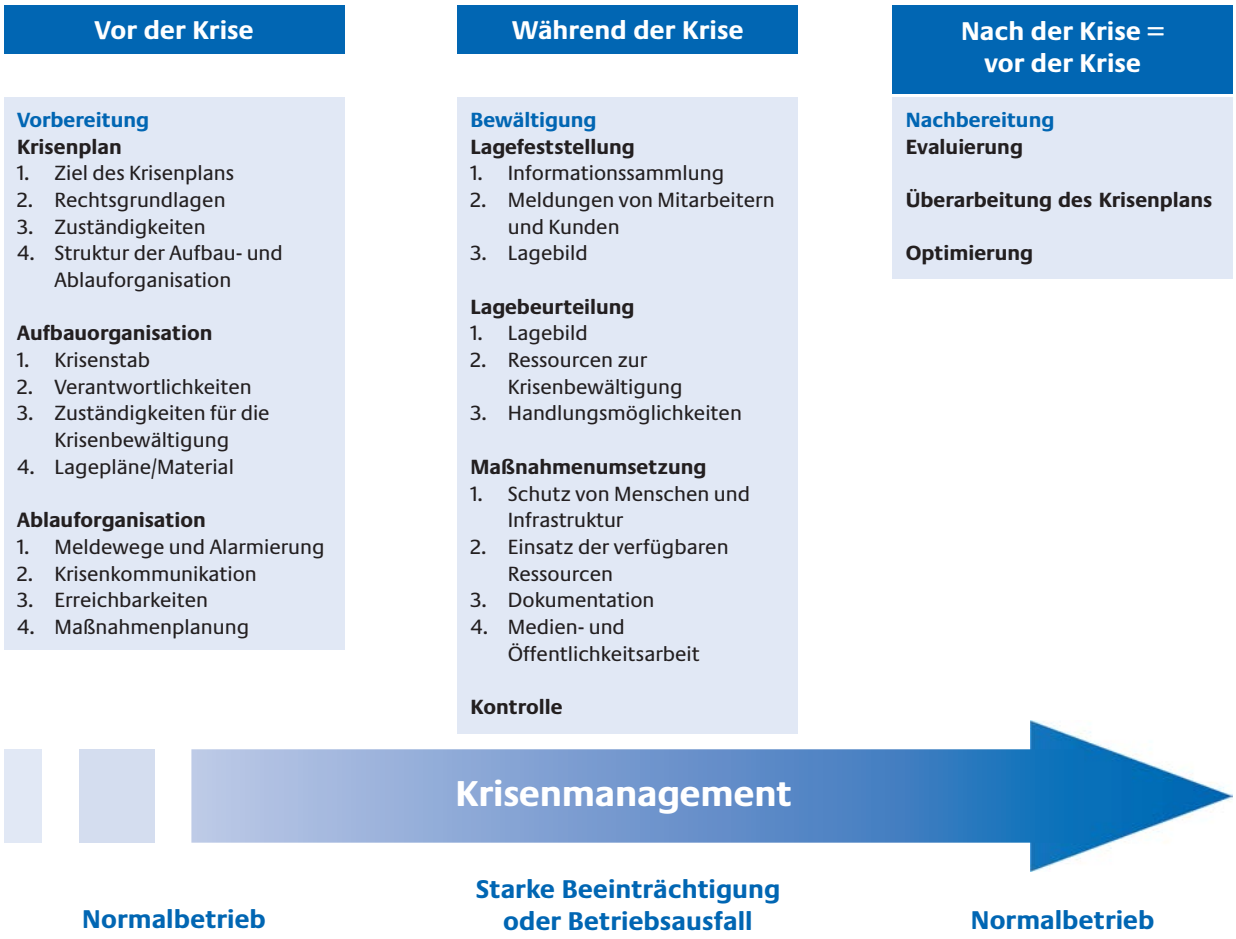


Abbildung 9: Bestandteile des Krisenmanagements[31]



Ein erfolgreiches Krisenmanagement ist eingebettet in weitere Managementkonzepte, beispielsweise in das bereits beschriebene Risikomanagement. Im Krisenmanagement werden Maßnahmen vorbereitet und aktiviert, die die Funktion der Einrichtung, 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.

Die wichtigsten Aufgaben eines Krisenmanagements sind:

- die konzeptionellen, organisatorischen und verfahrensmäßigen Voraussetzungen zu schaffen, um die bestmögliche Bewältigung eines Extremereignisses zu ermöglichen
- 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 Stäbe, Stellen oder Ressourcen kann erforderlich sein.
- Entscheidungen müssen unter Zeitdruck bei unvollständigem Informationsstand getroffen werden.

Das Krisenmanagement ist durch die Vorbereitung, die Krisenbewältigung und die Nachbereitung strukturiert (siehe Abbildung 9).

Das Krisenmanagement muss genauso wie das Risikomanagement von der Einrichtungsleitung gewollt und unterstützt werden.

[31] Angelehnt an Bundesamt für Bevölkerungsschutz und Katastrophenschutz November 2008, Seite 64.

3.4.1 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.

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 und durchzuführen sind. Ein guter Krisenplan ist kurz und präzise. Checklisten[32] 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 Zuständigkeiten:[33]

- Zweck, Ziel und Geltungsbereich
- Rechtsgrundlagen
- Entwicklung einer Aufbauorganisation für den Krisenfall
  - Krisenstab
  - Festlegung von Aufgaben, Zuständigkeiten und Kompetenzen sowie deren Zuweisung zu den nominierten Funktionsinhabern[34]
  - 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
  - Evakuierung
  - Stromausfall
  - Personalausfall
  - 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.

Aufbauorganisation

Krisensituationen erfordern eine Sonderorganisation in Form eines Arbeitsstabes für Krisensituationen (Krisenstab). Dieser hat das Ziel, schnellstmöglich und kompetent Krisen zu bewältigen. Der Aufbau der Krisenorganisation ist von der Art und den Bedürfnissen der Kritische-Infrastruktur-Einrichtung abhängig.

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 Leiter[35] 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,[36] und
- Fachberatern, die den Krisenstab beraten.

Krisenstabsleiter

Der Krisenstabsleiter übernimmt während einer Reaktion auf ein extremes Ereignis die Leitung aller krisenbezogenen Vorgänge. Er trifft alle Entscheidungen im Rahmen der Krisenbewältigung.

[32] Anhang V enthält Checklisten zur Überprüfung von Detailaspekten im Rahmen der Vorbereitung auf Krisen.

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

[34] Jungbluth 2005, Seite 15.

[35] 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.

[36] Vgl. Trauboth 2002, Seite 45.

Daher sollte er in der Einrichtung 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 Führungserfahrung voraus. Hierzu gehören neben der generellen Führungsstärke insbesondere:

- eine schnelle Auffassungsgabe und Analysefähigkeit
- eine hohe Belastbarkeit in Extremsituationen
- eine hohe Entscheidungsfreudigkeit unter Zeitdruck
- Teamfähigkeit
- soziale Kompetenz

Der Krisenstabsleiter muss das Vertrauen der Einrichtungsleitung 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.

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 im Veranlassen von Maßnahmen zur Ereignisbewältigung oder Schadenbegrenzung.

Fachberater im Krisenstab

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

Regelungen im Detail

Alle nominierten und eingewiesenen Krisenstabsmitglieder und ihre Stellvertreter haben ihre spezielle Aufgabe zu kennen und sollten darauf vorbereitet sein.

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. In der öffentlichen Gefahrenabwehr werden Stäbe gebildet, die entweder operativ (operativ-taktische Komponente, zum Beispiel technische Einsatzleitung Feuerwehr) oder administrativ (administrativ-organisatorische Komponente, zum Beispiel Verwaltungsstab) agieren. Je nach Lage werden beide Stäbe gleichzeitig oder lediglich ein Stab allein tätig. Die Struktur dieser Stäbe richtet sich nach Landesrecht und wird sowohl in Dienstanweisungen für den Bevölkerungsschutz als auch in der Feuerwehr-Dienstvorschrift 100 detailliert beschrieben.[37] In der Regel sind ab der Ebene der Mittelbehörden nur administrative Stäbe tätig.[38]

Die Ausgestaltung des Krisenstabes in Einrichtungen, 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 Einrichtungen werden von dieser Struktur abweichen.[39] Wichtig ist, dass die Kommunikation zwischen dem Betreiber der Kritischen Infrastruktur und der Gefahrenabwehrbehörde beziehungsweise den Katastrophenschutzorganisationen funktioniert.

Die folgenden Stabsfunktionen beziehungsweise Aufgaben sollten in jedem Krisenstab wahrgenommen werden, unabhängig von den Aufgaben der Einrichtung:[40]

- 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 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bevölkerungsschutz in Deutschland 2009.

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

40 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
- Marketing
- Logistik
- Qualitätsmanagement
- Vertrieb
- Finanzen
- Standortsicherheit
- Umweltschutz
- Anlagensicherheit
- Toxikologie
- Werksfeuerwehr
- Rettungsdienst
- Arbeitnehmervertretung

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 Einrichtungen ist eine Funktion „Ausland“ sinnvoll. Zusätzlich kann eine Krisenstabsassistenz in Erwägung gezogen werden, die vor allem bei der Erstellung des Lagebildes unterstützen kann.

Besteht eine Einrichtung aus mehreren Niederlassungen oder Zweig- beziehungsweise Außenstellen, sollte eine aufeinander aufbauende Krisenstruktur für alle Einrichtungsebenen aufgebaut werden. Über Eskalationsstufen können dann Aktivierung und Zuständigkeiten der einzelnen Krisenstäbe geregelt werden.

Ablauforganisation

In der Ablauforganisation sind die Aktivierung des Krisenmanagements sowie die Aufgaben und die Arbeitsweise des Krisenstabes geregelt. Dies spiegelt sich in der Ausübung von speziellen Stabsfunktionen wieder, 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

Meldewege und Alarmierung

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

- 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.[41]

Zur Weiterleitung von internen Ereignis- beziehungsweise Schadensmeldungen ist also nicht nur ein standardisierter Meldeweg festzulegen, sondern auch ein standardisiertes Meldeverfahren,

[41] Feuerwehr-Dienstvorschrift 1999, Seite 29.

das sicherstellt, dass alle erforderlichen Informationen erfasst und weitergegeben werden.

Tritt ein Ereignis ein, das mit dem hausinternen Störungsmanagement allein nicht mehr bewältigt werden, sondern aus dem heraus eine Krise erwachsen kann, 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 Verantwortungsbereich 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 Krisenstabes, der Leitzentralen und der Einrichtungsleitung 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 die Erreichbarkeiten des im Krisenmanagement aktiven Personals und relevanter externer Stellen enthalten. Die Alarmierungs- beziehungsweise Benachrichtigungslisten sind von der Einrichtung im Vorfeld zu erstellen und regelmäßig zu aktualisieren.

Die Überführung des Normalbetriebes 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.[42]

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 10 gibt einen Überblick über Meldewege in einer Einrichtung und die Alarmierung relevanter Personen.

Krisenkommunikation

Die Krisenkommunikation beinhaltet die Kommunikation im Krisenfall innerhalb einer Einrichtung sowie gegenüber der Öffentlichkeit und hier insbesondere gegenüber den Medien. Diese Aufgabe wird von der Pressestelle im Rahmen der Öffentlichkeitsarbeit wahrgenommen.

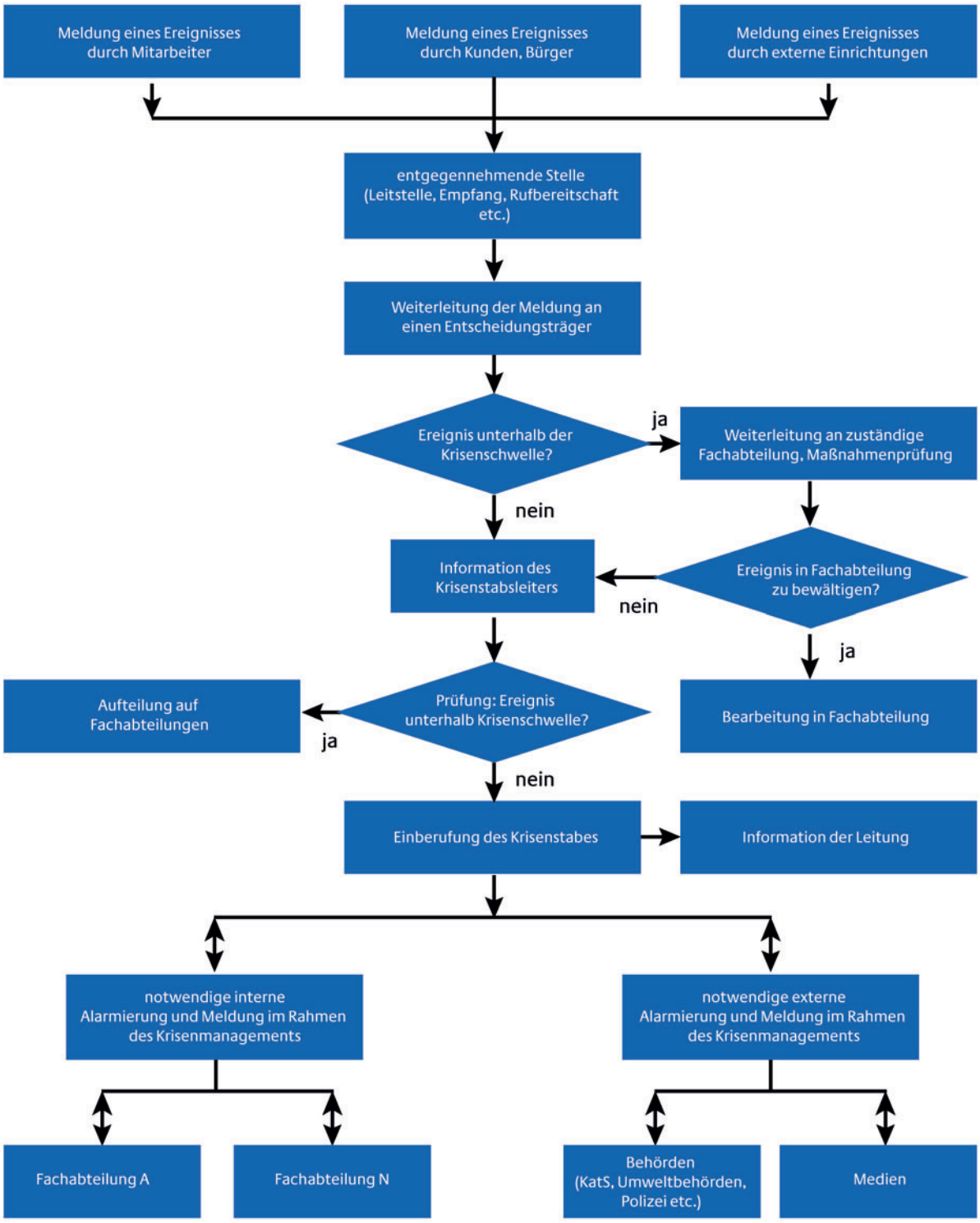
In der besonders bedeutsamen Anfangsphase einer Krisenentwicklung sind die Einbeziehung und zeitnahe Benachrichtigung anderer Organisationen, der Medien, der Bevölkerung sowie die Information der eigenen Organisation von zentraler Bedeutung. Die Kriseninformationsarbeit muss unmittelbar mit der Krisenbewältigung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

Für Krisen, die die Bevölkerung betreffen, können Hotlines und benutzerfreundliche Internetseiten (Dark-Sites) vorbereitet und im Ereignisfall aktiviert werden. Besonders ausgebildetes Personal, inklusive Verstärkungspersonal, sollte 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

[42] Jungbluth 2005, Seite 17.

Abbildung 10: Meldewege und Alarmierung



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,
- Einrichtung sogenannter Dark-Sites zur Bereitstellung von Informationen über das Internet,
- vorbereitete Hintergrundunterlagen und Muster für Pressemitteilungen, Sprechzettel etc.,

- Erfahrungen mit Pressekonferenzen und spezielles Medientraining,
- One-Voice-Policy[43], die einheitliche Sprachregelungen, klare Zuständigkeiten für den Umgang mit Medien und strukturierte innere Abstimmungen enthält, 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 Lage-angepasst in den Medien auftreten. Die Aussagen müssen balanciert formuliert werden, nur eindeutige und wahre Informationen sollen, in einer verständlichen Sprache, kommuniziert werden.

Grundregeln externer Krisenkommunikation sind:

- Jede Krise ist auch eine Informationskrise.
- Krisenmanagement ist auch Informationsmanagement.
- Die ersten Stunden einer Krise sind von entscheidender Bedeutung: Während dieser Phase vermittelte Informationen hinterlassen einen bleibenden Eindruck, ob die Verantwortlichen der Krise gewachsen sind oder nicht.
- Der Informationsfluss sollte kontinuierlich, widerspruchsfrei und präzise erfolgen sowie den Informationsbedürfnissen der Öffentlichkeit entsprechen.
- 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 Einrichtungsleitung die Kommunikation nach außen übernimmt. Hierfür wird er vom Krisenstab stetig mit aktuellen Informationen versorgt und intensiv beraten.

Abbildung 11 fasst die Struktur von Aufbau- und Ablauforganisation schematisch zusammen.

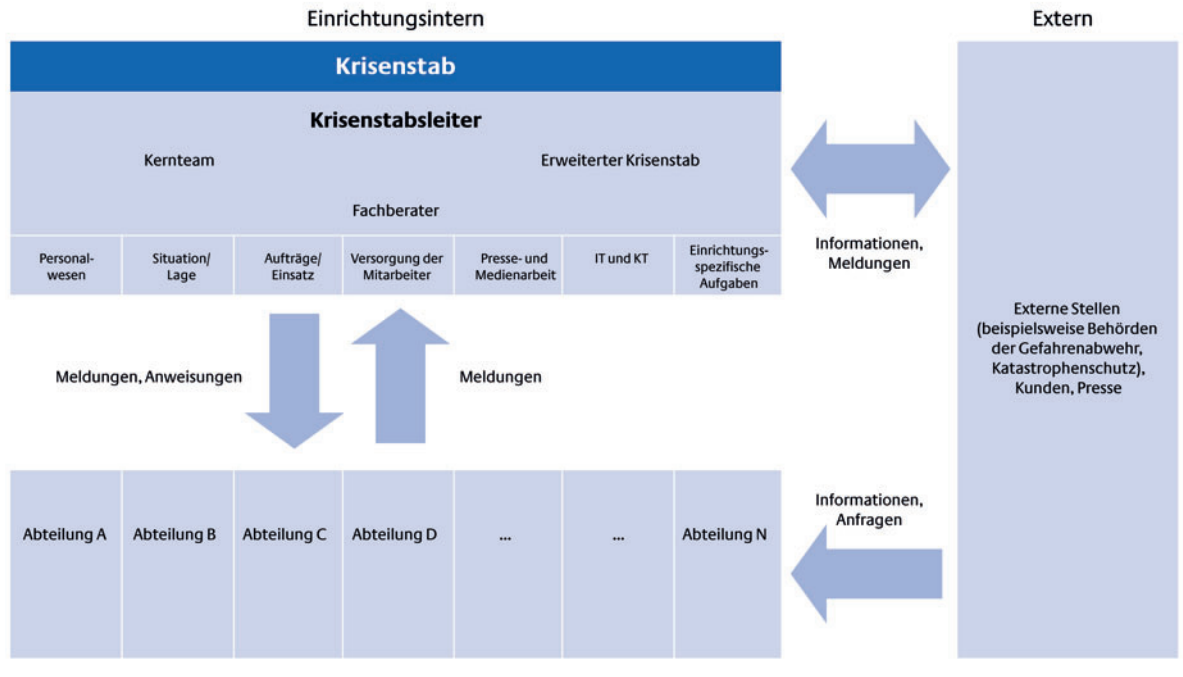
Krisenstabsraum

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

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

[43] Innenministerium Baden-Württemberg und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2010, Seite E7.

Abbildung 11: Aufbau- und Ablauforganisation



Der Standort sollte im Vorfeld festgelegt und gut erreichbar sein sowie Schutz vor Gefahreneinwirkungen bieten. Für den Fall des Funktionsausfalles am ersten Standort ist ein Alternativstandort vorzusehen, über dessen Existenz und Lage gegebenenfalls nur die Einrichtungsleitung, der Krisenstab und sein Leiter informiert sind.

Zur Ausstattung des Krisenstabraumes gehören eine redundante Kommunikations- und Informationsinfrastruktur sowie effektive technische Mittel zur Informationsbeschaffung, -verarbeitung und -darstellung. Eine Notstromversorgung für alle technischen Geräte und die Beleuchtung sollte zur Verfügung stehen.

Sicherheitsaspekte im Krisenstabsraum wie Nichteinsehbarkeit und Abhörsicherheit sind gegebenenfalls zu berücksichtigen. Der Raum und seine Ausstattung sollten in regelmäßigen Abständen auf ihre Funktionsfähigkeit überprüft werden.

Die Art und Größe der personellen, räumlichen und technischen Ausstattung des Krisenstabes und des dazugehörigen Raumes für die Krisensituation ist abhängig von den bestehenden 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 der Einrichtung 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 Voraussetzung für die Krisenbewältigung sind die Informations- und Kommunikationsverbindungen. Sie sollten (wieder) funktionieren. Alle Handlungen und Entscheidungen im Rahmen der Krisenbewältigung werden von Beginn der Krisenstabsarbeit an dokumentiert.

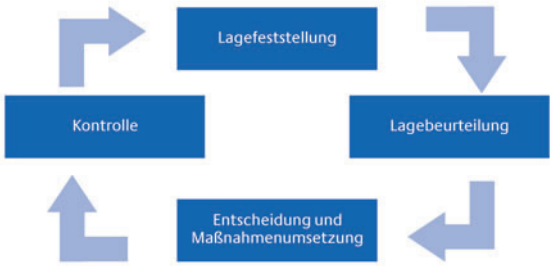
Die Bewältigung eines Extremereignisses vollzieht sich in einem Kreislauf (siehe Abbildung 12), der aus den Elementen Lagefeststellung, Lagebeurteilung, Entscheidung und Maßnahmenumsetzung sowie Kontrolle besteht. Dieser Kreislauf wird nach jedem neuen Teilereignis sowie jeder Maßnahme, die die Krisensituation signifikant verändert, erneut durchlaufen, bis zur Rückkehr zur Normalsituation.

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

Abbildung 12: Kreislauf zur Bewältigung von Extremereignissen[44]



- Art, Umfang und Abläufe der Ereignisse,
- die Auswirkungen und mögliche Entwicklung der Lage,
- die Möglichkeiten der Reaktion sowie
- die bereits ergriffenen Maßnahmen.[45]

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, externer privater und öffentlicher Akteure (zum Beispiel Kunden, Polizei, Katastrophenschutz) sowie Meldungen aus den Medien.

Die notwendigen Ausstattungsmittel zur Informationssammlung gehören zum Teil zu den

[44] Feuerwehr-Dienstvorschrift 1999, Seite 25.

[45] Jungbluth 2005, Seite 38.

Ausstattungsmerkmalen des Krisenstabsraumes. Hierzu zählen beispielsweise Telefon, Internet, Radio und TV-Geräte. Diese Mittel werden um die oben genannten Karten sowie Nachschlagewerke ergänzt.

Insbesondere eine grafische Aufbereitung erleichtert das intuitive Erfassen der Informationen für alle Beteiligten. Wird in der Einrichtung ein Geografisches Informationssystem[46] verwendet, können bereits im Vorfeld wichtige Rauminformationen elektronisch vorgehalten und dargestellt werden.

Darstellung eines Lagebildes

Im Krisenstab wird kontinuierlich ein aktuelles Situations- beziehungsweise Lagebild geführt. 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 daraus eine komprimierte Übersicht zum momentanen Status. Zu den wichtigen Unterlagen für die Lagedarstellung zählen:

- Lagekarten
- Gebäudepläne
- Berichte über das Ereignis
- Ton- und Bildaufzeichnungen[48]

Die folgende Abbildung fasst die wichtigsten Punkte zur Lagebilddarstellung zusammen.

Abbildung 13: Überblick zur Lagebildfeststellung[49]

Schadensereignis	Schadensabwehr
Schaden • Schadensart • Schadensursache **Schadensobjekt** • Art • Größe • Material • Konstruktion • Umgebung **Schadensumfang** • Menschen • Funktionalität • Tiere, Umwelt • Sachwerte • Produktionsprozesse • Zustand der Funktionsfähigkeit der Einrichtung • Mittelbare Schäden	**Krisenbewältigung** • Krisenorganisation • Mittel zur Informationsgewinnung, -verarbeitung und -übertragung **Eingesetztes Personal** • Stärke • Verfügbarkeit • Gliederung • Ausbildung • Leistungsvermögen • Reserven **Mittel** • Fahrzeuge • Geräte und Materialien • Reserven **Ort** **Zeit** **Wetter**

Lagebeurteilung, Entscheidung und Maßnahmenumsetzung

Die Lage wird systematisch und regelmäßig, insbesondere unter Berücksichtigung der eigenen Ziele und unter Abwägung aller Optionen, beurteilt. Hierfür können Lagebesprechungen ein geeignetes Mittel sein. Aus der Lagebeurteilung ergeben sich die Entscheidungen über weitere Maßnahmen.

Unter Mittel zur Lagebeurteilung fallen:[50]

- das Lagebild selbst
- gesetzliche Grundlagen
- Richtlinien
- Merkblätter

Nach Beurteilung der Lage entscheidet der Krisenstabsleiter über das weitere Vorgehen. Dieser muss klare Entscheidungen zur Umsetzung von Maßnahmen treffen.[51]

Kontrolle

Im Rahmen der Kontrolle wird überprüft, ob die Anweisungen des Krisenstabes das Personal (zum Beispiel Niederlassungen oder Einsatzkräfte) auch erreicht haben und ob 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.

Sicherstellung der betrieblichen und dienstlichen Kontinuität

Ein wesentliches Element der Krisenbewältigung in Kritische-Infrastruktur-Einrichtungen 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.

Rückkehr zum Normalbetrieb

Analog zur Aktivierung des Krisenmanagements erfolgen die Beendigung des aktiven Krisenmanagements und die Rückkehr zum Normalbetrieb durch den Krisenstabsleiter. Auch hierfür sind ein Schwellenmodell oder ein Deeskalationsmodell

46 Geografische Informationssysteme sind datenbankgestützte Softwareprodukte, mithilfe derer raumbezogene Daten erfasst und analysiert werden können.

47 Feuerwehr-Dienstvorschrift 1999, Seite 26.

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 enthält für ausgewählte Krisensituationen Checklisten zur Umsetzung erster Maßnahmen.

denkbar. 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.

Dokumentation der Krisenbewältigung

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

- Vordrucke
- Ein- und Ausgangsnachweise
- Ereignis-Tagebücher
- Lagekarten
- Meldeprotokolle
- elektronische Medien

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

3.4.3 Nachbereitung

Nach der Rückkehr zum Normalbetrieb wird anhand der Dokumentation eine Nachbereitung der Krisenbewältigung vorgenommen. Diese kann in Form eines Berichtes erfolgen, der zeitnah und vertraulich von dem Leiter des Krisenstabes erstellt und an die Leitung der Einrichtung übermittelt wird. Dieser Bericht dient der Unternehmensbeziehungsweise Behördenleitung als Grundlage zur Beurteilung eventueller Rechtsfolgen für/gegen die Einrichtung oder eingesetztes Personal. Weiteres wichtiges Ziel der Nachbereitung ist die Prüfung der Funktionsfähigkeit und Praktikabilität des Krisenplans, um Lücken im Krisenmanagement aufzudecken und diese mithilfe ergänzender Maßnahmen zu schließen.[52]

[52] Anhang V 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.

3.4.4 Übungen

Die Strukturen und Verfahren des Krisenmanagements, insbesondere für Ereignisse mit geringer Eintrittswahrscheinlichkeit, aber hohem Schadensausmaß, sollten in regelmäßigen Abständen geübt werden. Damit können die Planungen an aktuelle Entwicklungen und Erkenntnisse angepasst werden und funktionieren im Ereignisfall reibungslos. Ziele solcher Übungen sind:[53]

- Überprüfung der Funktionsfähigkeit und der Praktikabilität des Krisenplans
- Training der Krisenkoordination und -kommunikation
- Test der krisenspezifischen Abläufe
- Schaffung von Vorgaben zur Entwicklung benötigter Strukturen und Verfahren

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

- **Planbesprechung/Planübung**
  Einzige diskussionsorientierte Übung; sie ist sowohl für die taktische als auch für die strategische Ebene tauglich und kann als Allzweckmittel zur Übung beliebiger Inhalte verwendet werden. Es handelt sich um eine Besprechung des Ablaufs einer Krisenreaktion auf der Basis festgelegter Szenarien mit Fachleuten und Führungskräften am „Grünen Tisch“ als gemeinsame konstruktive Diskussion mit Moderation und Gesprächsleitfaden, gegebenenfalls auch mit Fachvortrag zum beübten Thema.
- **Stabsübungen**
  Beteiligte: Mitglieder des Krisenstabes – theoretische Bewältigung eines Schadensszenarios
- **Stabsrahmenübungen**
  Beteiligte: zusätzlich zum Stab oder zu mehreren Stäben werden weitere benachbarte oder nachgeordnete Bereiche einbezogen – Bewältigung eines Schadensszenarios ohne den realen Einsatz operativ-taktischer Ressourcen
- **Strategische Krisenmanagementübungen**
  Beteiligte: verschiedene Krisenstäbe beziehungsweise politisch-administrative Führungsstäbe auf verschiedenen Verwaltungsebenen unter Einbindung des privaten Sektors und sonstiger Non-Profit-Organisationen und Ein-

[53] Gustin 2004, Seite 226.

richtungen, sogenannter gesamtgesellschaftlicher Ansatz; Ziel ist es, übergreifende Krisenstabsstrukturen und -verfahren zu entwickeln und Krisenkommunikation und Krisenkoordination zu erproben.

- **Vollübungen**
  Beteiligte: alle Leitungsebenen und Stellen – realer Einsatz operativ-taktischer Ressourcen zur 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 und
- der eingeplante/mögliche Übungsaufwand.

Vollübungen, die alle Führungsebenen und Mitarbeiter mit einbeziehen können, sind wegen des intensiven Einsatzes von Personal und Einsatztechnik sowie benötigtem Verbrauchsmaterial in der Vorbereitung und Durchführung sehr aufwändig.

Stabsübungen und Stabsrahmenübungen bedürfen dagegen nur der Mitarbeit in übenden Stäben und Strukturen zur Bewältigung von Schadensszenarien. Die Darstellung nicht übender Bereiche und Sektoren bindet jedoch zusätzliches Personal auf der Steuerungsseite der Übung. Stabsrahmenübungen beziehen zusätzlich Entscheidungs- und Berichtswege zwischen den übenden Organisationsstrukturen in die Übung ein.

Bei Stabsübungen und Stabsrahmenübungen werden alle Teilereignisse mithilfe eines Übungsdrehbuches, mit dem die Übungsleitung die Übungen überwacht und steuert, eingespielt. Das Übungsdrehbuch ist den übenden Akteuren bei Alarmierungs- oder Vollübungen in der Regel nicht bekannt. Es antizipiert mögliche Reaktionen der Akteure. Unvorhergesehene Reaktionen können von der Übungsleitung kurzfristig in die Übung integriert werden. Bei Stabsübungen oder Stabsrahmenübungen mit komplexen Übungsinhalten ist es angeraten, Fachpersonal aus den übenden Organisationsstrukturen in die Planungsgruppe einzubeziehen und einen offenen Vorbereitungsprozess zu führen. Die Übenden erhalten dabei jedoch kein Detailwissen.

Der Nachteil von Stabsübungen und Stabsrahmenübungen liegt in der ausschließlichen Beteiligung im Bereich der betroffenen Stäbe. Die Einflüsse operativ-taktischer Maßnahmen und Entscheidungen werden nur theoretisch eingebracht oder rückgekoppelt. Dennoch ermöglicht eine Stabsübung oder Stabsrahmenübung die Beübung der strategischen Kernbereiche des Krisenmanagements, ohne den Aufwand einer Vollübung unter Beteiligung aller Mitarbeiter betreiben zu müssen, sofern diese realitätsnah durch das Drehbuch und die Steuerungsorganisation eingebracht werden.

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

Alarmierungsübungen dienen zum Test von Alarmierungsplänen und des Schwellen- beziehungsweise Eskalationsmodells.

Zu den Übungsvorbereitungen gehören folgende Entscheidungen über Planungsgrundlagen[54], 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 Beobachtungen der Schiedsrichter/des Steuerungspersonals, insbesondere zur Umsetzung des Krisenplans, anhand einer Abschlussbesprechung und einer darauf folgenden Evaluierung (zum Beispiel mit Fragebögen oder Berichten) dokumentiert und ausgewertet. Hierdurch können Schwachstellen identifiziert und der Krisenplan weiterentwickelt werden.[55]

[54] Gustin 2004, Seite 262.

[55] Anhang V beinhaltet eine Checkliste zu Krisenübungen.

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 einem Krisenereignis,
- nach einer Erweiterung/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 und realistisch bewertet werden und so die Grundlage für eine stetige Optimierung des Sicherheitsniveaus in einer Einrichtung gelegt wird.

Anhang

I. Literaturverzeichnis

Ackermann, S./Rudy, M. (2008): „Blackout im Münsterland" – Krisenkommunikation bei Stromausfällen im RWE-Netz. In: Krisenmanagement in der Praxis. Von erfolgreichen Krisenmanagern lernen. Hrsg.: Roselieb, F./Dreher, M. Berlin, S. 15–27.

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 (Version 6.1, 23. Juni 2006).

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 Bevölkerungsschutz und Katastrophenhilfe (November 2008): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens. http://www.bbk.bund.de/cln_027/nn_1258620/SharedDocs/Publikationen/Praxis__Bevoelkerungsschutz/Langfassung__Leitfaden__Krankenh__Risiko-Kritis.html__nnn=true (26. Juni 2010).

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2009): Bevölkerungsschutz in Deutschland: Informationen für Betreiber Kritischer Infrastrukturen. http://www.bbk.bund.de/cln_007/nn_1258620/SharedDocs/Publikationen/Broschueren__Flyer/Faltblatt__bevoelkerungsschutz-management.html__nnn=true.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe & Regierungspräsidium Stuttgart, Landesgesundheitsamt (2007): Handbuch Betriebliche Pandemieplanung. http://www.gesundheitsamt-bw.de/servlet/PB/show/1238642/HandbuchBePPv2.2B_090716.pdf (5. August 2010).

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2010): Abschätzung der Verwundbarkeit gegenüber Hochwasserereignissen auf kommunaler Ebene.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2011): Leitfaden für strategische Krisenmanagement-Übungen.

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/comcheck.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". https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf

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).

Bundesministerium des Inneren (Juli 2008): Krisenkommunikation. Leitfaden für Unternehmen und Behörden. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/DE/2008/Krisenkommunikation.pdf?__blob=publicationFile (30. August 2010).

Bundesministerium des Innern (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). http://www.bmi.bund.de/cae/servlet/contentblob/598730/publicationFile/34416/kritis.pdf (16. November 2010).

Bundesministerium für Verkehr, Bau und Stadtentwicklung (2008): Hochwasserschutzfibel. Bauliche Schutz- und Vorsorgemaßnahmen in hochwassergefährdeten Gebieten. http://www.bmvbs.de/Anlage/original_1060054/Hochwasserschutzfibel-Stand-2008.pdf (21. Juli 2010).

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.

Hertel, R. F. (2003): Behördliche Risikokommunikation. Diskursives Verfahren. In: Bundesgesundheitsblatt – Gesundheitsforschung – Gesundheitsschutz. 7/2003.

Innenministerium Baden-Württemberg und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) (2010): Krisenhandbuch Stromausfall. Langfassung. Krisenmanagement bei einer großflächigen Unterbrechung der Stromversorgung am Beispiel Baden-Württemberg.

International Organization for Standardization (2009): Risk management – Principles and guidelines. ISO/FDIS 31000.

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

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

CBRN	Chemisch, biologisch, radiologisch, nuklear
AktG	Aktiengesetz
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
DIN	Deutsches Institut für Normung
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-Informations- und Hilfeleistungssystem
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 beziehungsweise einer Situation im Hinblick auf die zu ergreifenden Maßnahmen
Aufbauorganisation	Organisationsform zur Wahrnehmung von Aufgaben sowie Festlegung der Zuständigkeiten und Kommunikationswege
Betriebliches Kontinuitätsmanagement	Management der Maßnahmen zur Aufrechterhaltung der Geschäftstätigkeiten, insbesondere im Krisenfall; beispielsweise die Aktivierung einer redundanten Steuerzentrale (Betriebliches Kontinuitätsmanagement = Business Continuity Management)[56]
Bevölkerungsschutz	Der Bevölkerungsschutz beschreibt als Oberbegriff alle Aufgaben und Maßnahmen der Kommunen und der Länder im Katastrophenschutz sowie des Bundes im Zivilschutz. Anmerkung: Der Bevölkerungsschutz umfasst somit alle nicht polizeilichen und nicht militärischen Maßnahmen zum Schutz der Bevölkerung und ihrer Lebensgrundlagen vor Katastrophen und anderen schweren Notlagen sowie vor den Auswirkungen von Kriegen und bewaffneten Konflikten. Der Bevölkerungsschutz umfasst auch Maßnahmen zur Vermeidung, Begrenzung und Bewältigung der genannten Ereignisse.
Einrichtung	Als Einrichtungen im Sinne dieses Leitfadens werden alle Unternehmen, Behörden und sonstigen Institutionen bezeichnet, die eine Kritische Infrastruktur betreiben.
Epidemie	Zeitlich und räumlich begrenztes massenhaftes Auftreten einer Krankheit innerhalb einer Population

[56] Rössing 2005, Seite 426.

Begriff	Definition
Ereignis	Räumliches und zeitliches Zusammentreffen von Prozess/Risikoelement und Gefahr
Eskalationsmodell	Mechanismus der Einschätzung der Lage, Festlegung von Alarmstufen und Weiterleitung von Meldungen an das Management[57]
Evaluierung	Bewertung von Tätigkeiten
Exposition	a) Allgemein: Ausgesetztsein eines Prozesses/Risikoelementes gegenüber seinen Umgebungseinflüssen b) Im Bereich Risikoanalyse: Ausgesetztsein eines Prozesses/Risikoelementes gegenüber einer Gefahr
Extremereignis	Extremereignisse sind seltene Ereignisse, die stark vom Durchschnitt abweichen und zu Krisen führen können.
Gefahr	Zustand, Umstand oder Vorgang, durch dessen Einwirkung ein Schaden an einem Risikoelement und eine Beeinträchtigung eines Prozesses entstehen kann
Gefahrenanalyse	Systematisches Verfahren zur Untersuchung und Bestimmung von Zuständen, Umständen oder Vorgängen, aus denen ein Schaden an einem Risikoelement und eine Beeinträchtigung eines Prozesses entstehen kann
Gefahrenpotenzial	Gesamtheit der möglichen Ausprägungen einer Gefahr
Gefahrenlage	Faktoren wie örtliche, zeitliche und klimatisch bedingte Verhältnisse, die auf einen bestimmten Raum zu einer bestimmten Zeit einwirken und aus denen sich ein Zustand, Umstand oder Vorgang ergeben kann, durch dessen Einwirkung ein Schaden an einem Risikoelement und eine Beeinträchtigung eines Prozesses entstehen kann
Gefährdung	Möglichkeit, dass an einem konkreten Ort aus einer Gefahr ein Ereignis mit einer bestimmten Intensität erwächst, das Schaden an einem Risikoelement /Prozess/ Schutzgut verursachen kann
Katastrophe	a) Schadensereignis, das stark über die Ausmaße normaler Schadensereignisse hinausgeht und dabei Leben, Gesundheit, Sachgüter oder wichtige Infrastrukturen erheblich gefährdet oder zerstört b) Eine Katastrophe ist ein Geschehen, bei dem Leben oder Gesundheit einer Vielzahl von Menschen oder die natürlichen Lebensgrundlagen oder bedeutende Sachwerte in so ungewöhnlichem Ausmaß gefährdet oder geschädigt werden, dass die Gefahr nur abgewehrt oder die Störung nur unterbunden und beseitigt werden kann, wenn die im Katastrophenschutz mitwirkenden Behörden, Organisationen und Einrichtungen unter einheitlicher Führung und Leitung durch die Katastrophenschutzbehörde zur Gefahrenabwehr tätig werden.
Katastrophenschutz	Der Katastrophenschutz (KatS) ist eine landesrechtliche Organisationsform der kommunalen und staatlichen Verwaltungen in den Ländern zur Gefahrenabwehr bei Katastrophen, bei der alle an der Gefahrenabwehr beteiligten Behörden, Organisationen und Einrichtungen unter einheitlicher Führung durch die örtlich zuständige Katastrophenschutzbehörde zusammenarbeiten.
Krieg	Organisierter, mit Waffen gewaltsam ausgetragener Konflikt zwischen völkerrechtlich anerkannten Subjekten

[57] Vgl. Rössing 2005, Seite 428.

Begriff	Definition
Krise	Vom Normalzustand abweichende Situation mit dem Potenzial für oder mit bereits eingetretenen Schäden in einer Einrichtung, die mit der normalen Ablauf- und Aufbauorganisation eines Unternehmens, einer Behörde oder eines Staates nicht mehr bewältigt werden kann
Krisenkommunikation	Austausch von Informationen und Meinungen während einer Krise zur Verhinderung oder Begrenzung von Schäden in einer Einrichtung
Krisenmanagement	Alle Maßnahmen zur Vermeidung von, Vorbereitung auf, Erkennung und Bewältigung sowie Nachbereitung von Krisen
Krisenplan	Masterplan für das Krisenmanagement, der alle Maßnahmen abdeckt, die im Zuge einer Krise zu ergreifen sind
Krisenstab	Struktur/Institution, die die Voraussetzungen zur Koordination aller krisenbezogenen Tätigkeiten schafft und die Krisenbewältigung leitet
Krisenstabsraum	Raum, der speziell dem Krisenstab während und nach einer Krise sowie im Vorfeld zur Koordination der Krisenbewältigung und Durchführung von Übungen zur Verfügung steht
Kritikalität	Maß für die Bedeutsamkeit eines Prozesses in Bezug auf die Konsequenzen, die eine Beeinträchtigung oder ein Ausfall des Prozesses für die Funktionsfähigkeit einer Einrichtung hat
Kritische Infrastrukturen	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
Kritische Punkte	Siehe neuralgische Punkte
Lage (oder Situation)	Beschreibung der bestehenden Situation, einschließlich a) allgemeine Lage b) Schadenslage c) Möglichkeiten der Schadensabwehr d) eigene Lage
Lagebeurteilung	Bewertung von Beeinträchtigungen beziehungsweise Schäden hinsichtlich der Auswirkungen und möglicher Maßnahmen
Lagebild	Aufbereitung von Informationen zu einem Schadensereignis in textlicher und/oder visualisierter Form
Lagefeststellung	Sammlung, Ordnung, Speicherung und Darstellung von Informationen über eine Lage
Maßnahmen, vorbereitende	Handlungsoptionen, die im Vorfeld von Krisen für eine bessere Krisenbewältigung entwickelt, jedoch erst im Krisenfall angewendet werden
Maßnahmen, vorbeugende	Handlungsschritte und Mittel, die im Vorfeld von Krisen entwickelt und umgesetzt beziehungsweise eingesetzt werden und die Risiken für eine Einrichtung 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.

Begriff	Definition
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
Öffentlichkeitsarbeit	Management von Kommunikationsprozessen für Organisationen mit deren Bezugsgruppen
Operatives Schutzziel	Konkrete Beschreibung eines anzustrebenden Sollzustandes, der der Erreichung eines strategischen Schutzziels dient
Pandemie	Im Gegensatz zur Epidemie länder- oder/und kontinentübergreifendes massenhaftes Auftreten einer Erkrankung
Prävention	Maßnahmen zur Vermeidung von Schadensereignissen und Beeinträchtigungen
Prozess	Vorgang/Funktion in einer Einrichtung zur Bereitstellung einer Dienstleistung oder eines Produktes
Restrisiken	Risiken, die nach der Umsetzung von vorbeugenden Maßnahmen bestehen bleiben[58]
Rettungsdienst	Öffentliche Aufgabe der Gesundheitsvorsorge und der Gefahrenabwehr, die sich in Notfallrettung und Krankentransport gliedert
Risiko	Maß für die Wahrscheinlichkeit des Eintritts eines bestimmten Schadens an einem Schutzgut unter Berücksichtigung des potenziellen Schadensausmaßes
Risikoanalyse	a) Systematisches Verfahren zur Bestimmung des Risikos b) Systematisches Verfahren zur Ermittlung von Risikowerten. Im Rahmen dieses Leitfadens gehören hierzu: [59] • eine Analyse der Gefahren und der Exposition • eine Analyse der Verwundbarkeit aller relevanten Teilprozesse und Risikoelemente • eine Analyse der Kritikalität aller relevanten Prozesse • ein Vergleich von Teilrisiken bezüglich einzelner Risikoelemente sowie ein Vergleich szenariobezogener Gesamtrisiken von Teilprozessen und Prozessen
Risikobewertung	Verfahren, mit dem 1) festgestellt wird, in welchem Ausmaß das zuvor definierte Schutzziel im Falle eines bestimmten Ereignisses erreicht wird 2) entschieden wird, welches verbleibende Risiko akzeptabel ist 3) entschieden wird, ob Maßnahmen zur Minimierung ergriffen werden können/müssen
Risikoelement	Einzelbestandteil kritischer Teilprozesse im Rahmen des Risikomanagements; im Kontext dieses Leitfadens zählen hierzu: • Menschen (Personal, sonstige Anwesende) • Gelände • Gebäude • Anlagen und Geräte • einrichtungsspezifische Sonderanlagen und Sondergeräte • Daten und Unterlagen • Betriebsmittel • Umwelt

[58] Australian/New Zealand Standard 2004, Seite 3.

[59] Australian/New Zealand Standard 2004, Seite 4.

Begriff	Definition
Risikoidentifikation	Prozess der Entdeckung, Erkennung und Beschreibung von Risiken[60]
Risikokommunikation	a) Austausch von Informationen und Meinungen über Risiken zur Risikovermeidung, -minimierung und -akzeptanz b) Verfahren für eine Einrichtung 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[61]
Risikomanagement	Kontinuierlich ablaufendes, systematisches Verfahren zum zielgerichteten Umgang mit Risiken, das die Analyse und Bewertung von Risiken sowie die Planung und Umsetzung von Maßnahmen, insbesondere zur Risikovermeidung/-minimierung und -akzeptanz, beinhaltet
Risikominderung	Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit oder der Auswirkungen von Ereignissen auf eine Einrichtung[62]
Risikopolitik	Strategie einer Einrichtung, die den systematischen Umgang und die Vorgehensweise mit Risiken sowie den Rahmen und die Ziele für das Risikomanagement festlegt
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
Risikowahrnehmung	Prozess der subjektiven Aufnahme, Verarbeitung und Bewertung von risikobezogenen Informationen, die aus der eigenen Erfahrung, der direkten Beobachtung, der Rezeption von vermittelten Botschaften (etwa durch Medien) sowie der direkten Kommunikation mit Individuen stammen
Schaden	Negativ bewertete Auswirkung eines Ereignisses auf ein Risikoelement
Schadensereignis	Zusammentreffen von Gefahr und Risikoelement mit negativem Ausgang
Schadensgebiet	Raum, in dem sich der Schaden realisiert und auswirkt
Sektor	Bereich Kritischer Infrastrukturen
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 fremd verursacht 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

60 International Organization for Standardization 31000, Seite 4.

61 Jungermann et al. 1991, Seite 5.

62 Australian/New Zealand Standard 2004, Seite 5.

Begriff	Definition
Strategisches Schutzziel	Beschreibung von anzustrebenden Sollzuständen, die zu einer Evaluierung umgesetzter Maßnahmen herangezogen werden kann
Szenario; Szenarioentwicklung	Annahme von möglichen Ereignissen oder Abfolgen von Ereignissen und deren Einwirkungen auf Risikoelemente/Prozesse
Teilrisiko	Risiko, das sich auf ein Risikoelement bezieht
Teilverwundbarkeit	Verwundbarkeit, die sich auf ein Risikoelement bezieht
Verwundbarkeit	Maß für die anzunehmende Schadensanfälligkeit eines Risikoelementes/Prozesses in Bezug auf ein bestimmtes Ereignis
Verwundbarkeitskriterium	Bedingungen zur Einschätzung der Verwundbarkeit
Wiederanlauf	Phase nach Abschluss der Krisenreaktion bis zur Einleitung des Notbetriebes[63]
Wiederherstellung	Vollständige Wiederherstellung des Normalzustandes, der vor Eintreten der Krise vorlag[64]

63 Rössing 2005, Seite 439.

64 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 einer 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	hohe Geschwindigkeiten bis 250 km/h (Bsp.: Sturm Lothar)	Druck- und Sogwirkung auf Bauwerke und sonstige Gegenstände; Zerstörung	Umweltbehörden, Deutscher Wetterdienst
Erdbeben	Standorte in Erdbebengebieten (Bsp.: Rheingraben, Kölner Bucht, Vogtland, Schwäbische Alb)	enorme horizontale und vertikale Kräfte; hoher Energieeintrag	Zerstörung von Rohrleitungen, Tanks, Transformatoren, Verbindungen von Anlagen, Gebäuden und Bauwerken; Trümmerbildung	Bundesanstalt für Geowissenschaften und Rohstoffe
Erdsenkung	Bergbaugebiete, umfangreiche Tiefbau- und Karstgebiete	langsame Bodensenkung bis schlagartige Einstürze	Einstürze der Erdoberfläche: in Bergbaugebieten großflächig möglich, in Karstgebieten in Deutschland eher kleinere Einsturztrichter	Bundesanstalt für Geowissenschaften und Rohstoffe

Art der Gefahr	Exposition	Mögliche Intensität	Mögliche Wirkung	Zuständigkeiten, mögliche Informationsquellen
Großbrand/ Flächenbrand	weiträumig bewaldete Gebiete	extreme Hitzeentwicklung, starke Rauchentwicklung	Bedrohung des Personals, Zerstörung von Anlagen aufgrund der Hitzeentwicklung; betroffen sind z. B. Anlagen der Stromversorgung und IT	Umweltbehörden, Deutscher Wetterdienst, Feuerwehr, Ordnungsbehörden
Dürre	insbesondere trockene, niederschlagsarme Regionen	langfristiges Ausbleiben von Niederschlägen, sehr geringe Niederschlagsmengen	Absinken des Grundwasserspiegels; Kühlwassermangel, Trinkwassermangel; Stromausfälle, Transportprobleme auf Wasserstraßen, Ernteausfälle	Betreiber, Umweltbehörden, Deutscher Wetterdienst
Hitzewelle	deutschlandweit möglich	hohe Tages- und Nachttemperaturen	gesundheitliche Beeinträchtigung des Personals und der Kunden	Gesundheitsämter, Deutscher Wetterdienst
Kältewelle	deutschlandweit möglich	geringe Tages- und Nachttemperaturen, Glatteis, Zufrieren der Binnengewässer, starker Frost	Zerstörung von Rohrleitungen, Tanks, Transformatoren, Verbindungen von Anlagen und Bauwerken aufgrund von Eis- und Frostbildung, Kühlwassermangel, Ernteausfälle, Transportprobleme auf den Wasserstraßen, Stromausfälle	Umweltbehörden, Deutscher Wetterdienst
gravitative Massenbewegung	kleinräumig, Standorte an Hängen, in Gebirgen	sturzartige Bewegungen, Hunderte Millionen Kubikmeter Material, Sturz in (Stau-) Seen und Flüsse, Verursachung von Aufstauung und Sturzfluten bei Dammbruch	Zerstörung von Anlagen, Versorgungsinfrastrukturen, Gebäuden im Wirkbereich der gravitativen Massenbewegung sowie Unterhalt eines möglichen Dammbruchs bei Aufstauungen von Flüssen	Umweltbehörden, Landesämter für Geologie
Sturmflut	deutsche Küstengebiete	weiträumige Überschwemmungen, Wasserstand bis mehrere Meter über Normalwasserstand	Zerstörung von Anlagen, Gebäude, Beeinträchtigung der Stromversorgung, Ausspülungen	Küstenschutzbehörden, Umweltbehörden, Deutscher Wetterdienst

Art der Gefahr	Exposition	Mögliche Intensität	Mögliche Wirkung	Zuständigkeiten, mögliche Informationsquellen
Starkregen	deutschlandweit möglich	intensive Regenfälle und Blitzeinschläge	Beschädigung von Gebäuden und Anlagen, Aus- und Unterspülungen	Umweltbehörden, Deutscher Wetterdienst
Sturzflut	in Hanglagen	lokal, starker Abfluss von Oberflächenwasser nach Starkregen	Beschädigung von Gebäuden und Anlagen, Aus- und Unterspülungen	Umweltbehörden, Deutscher Wetterdienst
Schneefall/Schneeverwehungen/ Hagel	deutschlandweit möglich	intensive Schneefälle, meterhohe Schneeverwehungen, große Hagelkörner	Beeinträchtigung von Personal, Kunden und Lieferanten, Beschädigung von Gebäuden und Anlagen	Umweltbehörden, Deutscher Wetterdienst
größere Epidemie/ Pandemie	weltweit/ deutschlandweit/ regional möglich	hoher Infektionsgrad, schneller Ausbreitungsgrad, hohe Ausfallzahlen	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, Energieversorger, Bundesnetzagentur
Ausfall der externen Wasserversorgung	deutschlandweit möglich	–	Beeinträchtigung von Personal, Anlagen und Geräten	Versorger, Feuerwehr, Hilfsorganisationen
Ausfall von ausgelagerten Spezialdienstleistungen	deutschlandweit möglich	–	Beeinträchtigung der Dienstleistung/ Produktion	Zulieferer
massive Beeinträchtigung der externen Verkehrs- und Transportwege	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, Feuerwehr, TUIS[65], Gesundheitsämter

[65] 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 Katastrophenschutzhelfer 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, örtliche Gesundheitsbehörden
Anschlag mit unkonventioneller Spreng- und Brandvorrichtung bzw. Freisetzung von CBRN-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, örtliche Gesundheitsbehörden
Versagen der Informationstechnik	deutschlandweit möglich	hohes Schädigungspotenzial, schnelle Verbreitung	Beeinträchtigung von Anlagen und Geräten	Bundesamt für Sicherheit in der Informationstechnik/Gefährdungskataloge[66]
menschliches Versagen im Zusammenhang mit IT-Systemen	deutschlandweit möglich	hohes Schädigungspotenzial, schnelle Verbreitung	Beeinträchtigung von Anlagen und Geräten	Bundesamt für Sicherheit in der Informationstechnik/Gefährungskataloge
vorsätzliche Handlungen mithilfe oder auf Basis von IT	deutschlandweit möglich	hohes Schädigungspotenzial, schnelle Verbreitung	Beeinträchtigung von Anlagen und Geräten	Bundesamt für Sicherheit in der Informationstechnik/Gefährdungskataloge
Entführung	deutschlandweit möglich	–	Beeinträchtigung von Personal	Polizei, Landeskriminalamt, ggf. Auswärtiges Amt
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

66 Bundesamt für Sicherheit in der Informationstechnik 2007.

V. Checklisten

Im folgenden Teil des Anhangs finden sich Checklisten zum Risiko- und Krisenmanagement. Die Checklisten können zur Ermittlung des Status quo in einer Einrichtung genutzt werden und ermöglichen einen Überblick, in welchen Bereichen das Risiko- und Krisenmanagement verbessert werden sollte.

Die Checkliste „V.1 Risiko- und Krisenmanagement – allgemein“ kann als Schnelltest für die zu betrachtende Einrichtung herangezogen werden. Es werden die grundlegenden Voraussetzungen für ein funktionsfähiges Risiko- und Krisenmanagement abgefragt. Ist eine dieser Voraussetzungen nicht erfüllt, sollte das vorhandene Risiko- und Krisenmanagementsystem umfassend überprüft und gegebenenfalls angepasst werden.

WICHTIGER HINWEIS:
Die hier aufgeführten Checklisten erheben keinen Anspruch auf Vollständigkeit. Die Anwendung ersetzt NICHT den umfassenden Auf- beziehungsweise Ausbau eines Risiko- und Krisenmanagements. Die Checklisten sollten an die individuellen Eigenschaften der Einrichtung angepasst werden.

Die nachfolgenden Checklisten wurden mithilfe 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
- Innenministerium Baden-Württemberg und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2010
- Jungbluth 2005
- National Fire Protection Association 2004
- Umweltbundesamt 2005a
- Umweltbundesamt 2005b
- Zentrum für Alpine Umweltforschung 2000

Weiterführende Hinweise finden sich unter:

- VdS-Richtlinien 2007
- Verwaltungs-Berufsgenossenschaft VBG 2007

Weiterführende Hinweise 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 2007
- Department of Homeland Security 2006

Weiterführende Hinweise zum Thema IT-Sicherheit finden sich unter:

- Bundesministerium des Innern Dezember 2008

V.1 Risiko- und Krisenmanagement – allgemein (Schnelltest)

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
1. Risiko- und Krisenmanagement						
1.1 Ist die Notwendigkeit zur Einrichtung eines Risiko- und Krisenmanagements erkannt?		☐	☐	☐	☐	☐
1.2 Werden die verwendeten Begriffe einheitlich definiert?	Für das Risiko- und Krisenmanagement sind wichtige Begriffe einrichtungsintern klar zu definieren und zu dokumentieren.	☐	☐	☐	☐	☐
2. Risikomanagement						
2.1 Existiert ein Risikomanagement?	Planung, Umsetzung, Aufrechterhaltung und ständige Verbesserung	☐	☐	☐	☐	☐
2.2 Wurden die rechtlichen Verpflichtungen geklärt?	Erfüllung von ggf. internationalen Verträgen oder hoheitlichen Aufgaben	☐	☐	☐	☐	☐
2.3 Wurden strategische Schutzziele definiert?		☐	☐	☐	☐	☐
2.4 Sind die Arbeitsabläufe im Rahmen des Risikomanagements geregelt?		☐	☐	☐	☐	☐
2.5 Sind die kritischen Prozesse inventarisiert und klassifiziert sowie Richtlinien für den Umgang aufgestellt?	Inventarisierung, Kritikalitätsanalyse, Priorisierung kritischer Prozesse; Identifizierung von Dienstleistungen, Materialien und Betriebsstoffen, die für die kritischen Prozesse essentiell sind	☐	☐	☐	☐	☐
2.6 Wurden die einrichtungsspezifischen Risikoelemente identifiziert?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
2.7 Wurden die Risiken für die Einrichtung identifiziert und analysiert?	Gefahrenanalyse, Verwundbarkeitsanalyse und Einbezug der Kritikalitätsanalyse	☐	☐	☐	☐	☐
2.8 Wurden die Risiken verglichen und bewertet?		☐	☐	☐	☐	☐
2.9 Besteht eine betriebliche Kontinuitätsplanung?	Planung von redundanten Systemen und Ersatzsystemen auf Basis der Identifizierung kritischer Kernprozesse und -funktionen	☐	☐	☐	☐	☐
2.10 Gibt es ein Konzept zur Reduzierung der identifizierten Risiken?		☐	☐	☐	☐	☐
2.11 Wird die Risikoanalyse regelmäßig bzw. nach veränderten Randbedingungen überarbeitet?	Änderung der Gefahrensituation, Einführung neuer Prozesse, Organisationsänderungen etc.	☐	☐	☐	☐	☐
3. Krisenmanagement						
3.1 Existiert ein Krisenmanagement (Management von Vorfällen)?	Meldewege, Meldeverfahren, Management von Vorfällen und Verbesserungen	☐	☐	☐	☐	☐
3.2 Wird die Einhaltung von rechtlichen bzw. gesetzlichen Verpflichtungen überprüft?	Einhaltung von gesetzlichen Verpflichtungen, Richtlinien und Normen, Audit von Systemen	☐	☐	☐	☐	☐
3.3 Ist die Aufbau- und Ablauforganisation festgelegt?	Krisenstab, Krisenstabsraum, Krisenplan, Funktionen	☐	☐	☐	☐	☐
3.4 Existiert ein Krisenkommunikationsplan?	Festlegung der Kommunikationsstrategie, Zielgruppe identifizieren, Verfügbarkeit der Infrastruktur für die Krisenkommunikation	☐	☐	☐	☐	☐
3.5 Sind die Krisenkommunikationswege festgelegt?	Bestimmung der internen und externen Informationswege, einheitliche Sprachregelung, Auswahl eines Pressesprechers	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
3.6 Ist ein betriebliches Kontinuitätsmanagement etabliert?	Management von redundanten Systemen und Ersatzsystemen im Ereignisfall	☐	☐	☐	☐	☐
3.7 Wird das Krisenmanagement regelmäßig geübt?		☐	☐	☐	☐	☐

V.2 Personal

V.2.1 Personal – allgemein

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
1 Liegen Konzepte und Maßnahmen vor, die den Schutz der Mitarbeiter auch in Extremsituationen gewährleisten?	Hierzu zählen unter anderem die Ausbildung ausgewählter Mitarbeiter zu Evakuierungshelfern, Erst- und Pandemiehelfern, Evakuierungspläne, hochwasser- und trümmerfreie Fluchtwege, Sammelplätze, Rückzugsräume, Schutzräume, Schutzausrüstungen, Erste-Hilfe-Ausrüstungen, Information der Mitarbeiter sowie eine Lebensmittelbevorratung.	☐	☐	☐	☐	☐
2 Werden Sicherheitsaspekte in der Personalentwicklung berücksichtigt?	Aufgaben und Verantwortlichkeiten, Überprüfung, Schulung und Sensibilisierung	☐	☐	☐	☐	☐
3 Ist das Schlüsselpersonal für kritische Kernprozesse identifiziert?		☐	☐	☐	☐	☐
4 Verfügt die Einrichtung in ausreichendem Maße über Personal mit Ortskenntnissen?		☐	☐	☐	☐	☐
5 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.	☐	☐	☐	☐	☐

	Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
6	Kann im Krisenfall auf Ersatzpersonal zurückgegriffen werden?	Beispielsweise kann bei Pandemien unter Umständen auf Personal aus benachbarten Einrichtungen, Personal in Ruhestand oder Personal in Ausbildung zurückgegriffen werden.	☐	☐	☐	☐	☐
7	Ist eine umfassende Versorgung des Personals im Krisenfall gewährleistet?	Versorgung mit Lebensmitteln, Wasser, Medikamenten, aktuellen Informationen	☐	☐	☐	☐	☐
8	Existieren Alarmkonzepte für Ein-Personen-Arbeitsplätze?	Hierzu zählen Alarmknöpfe sowie eine automatisierte Alarmierung bei Funktionsstörungen, Fehlverhalten und fehlender Korrektur in Leitstellen/Steuerzentralen.	☐	☐	☐	☐	☐
9	Werden Schulungen mit den Mitarbeitern hinsichtlich des Verhaltens bei Eintritt eines Szenarios durchgeführt?	Kenntnisse der Fluchtwege, Umgang mit Feuerlöschern, Kenntnis von Erste-Hilfe-Maßnahmen, kontrolliertes Verlassen der Gebäude etc.	☐	☐	☐	☐	☐
10	Sind Ausweicharbeitsplätze identifiziert und festgelegt?	Erfassung alternativer Arbeitsplätze, der Tätigkeiten und Personen sowie der dafür notwendigen Ausstattung	☐	☐	☐	☐	☐
11	Werden die Mitarbeiter der Einrichtung über das Krisenmanagement informiert?	Information der Mitarbeiter über die Struktur, Zuständigkeiten, Meldewege und Kommunikation des Krisenmanagements	☐	☐	☐	☐	☐

V.2.2 Personal – Pandemieplanung (insbesondere Influenzapandemie)

	Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
1	Ist dafür gesorgt, dass bei grundlegendem Personalmangel eine kontrollierte Stilllegung der Prozesse in der Einrichtung erfolgen kann?		☐	☐	☐	☐	☐

	Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
2	Sind für den Fall einer Epidemie bzw. Pandemie Ausweicharbeitsplätze festgelegt?	Zum Beispiel: Telearbeit	☐	☐	☐	☐	☐
3	Sind Vereinbarungen mit externen Dienstleistungseinrichtungen zur Übernahme von Aufgaben getroffen worden?		☐	☐	☐	☐	☐
4	Besteht im Rahmen der Vorplanung eine Kooperation mit den lokalen Gesundheitsbehörden?		☐	☐	☐	☐	☐
5	Werden antivirale Arzneimittel bevorratet?		☐	☐	☐	☐	☐
6	Werden von der Einrichtung Impfungen angeboten bzw. wird über Impfmöglichkeiten informiert?		☐	☐	☐	☐	☐
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.	☐	☐	☐	☐	☐
8	Werden Mitarbeiter hinsichtlich des Verhaltens im Ereignisfall geschult?	Beispiele: - Kontakt mit Händen und Gesicht vermeiden - Händeschütteln vermeiden - Hände regelmäßig waschen - persönliche Schutzausrüstung anlegen (Mund- und Nasenschutz, Brille) - Sensibilisierung	☐	☐	☐	☐	☐
9	Ist Personal mit einem erhöhten Infektionsrisiko identifiziert worden?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
10 Ist mit diesem Personal eine Isolierung im Ereignisfall besprochen worden?		☐	☐	☐	☐	☐
11 Wird zusätzliches Personal für spezielle Abläufe in der Einrichtung weitergebildet?	Ausbildung eines Influenzamanagers	☐	☐	☐	☐	☐

V.3 Vorbeugende Maßnahmen

V.3.1 Gebäude, Anlagen – Hochwasser

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
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?	erhöhte Anordnung von Gebäudeöffnungen und Bauwerken sowie bauliche Schutzmaßnahmen (temporär und permanent)	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
1.3 Sind Einrichtung und Nutzung der Innenräume an eine mögliche Hochwassergefahr angepasst?	Nutzung von wasserresistenten Baumaterialien, Verlagerung essentieller Versorgungseinrichtungen und -anlagen in höhere Stockwerke (zum Beispiel Heizkessel, IT, Stromverteiler)	☐	☐	☐	☐	☐
1.4 Ist im Falle des Anstieges des Grundwassers durch Hochwasser die Standsicherheit in Gefahr?	Zum Beispiel bei Untergeschossen (Auftriebsgefahr, Unterspülung und Aufschwimmeffekt)	☐	☐	☐	☐	☐
1.5 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?		☐	☐	☐	☐	☐
2.4 Lagern gesundheits-, wasser- und umweltgefährdende Stoffe in von Überschwemmung gefährdeten Bereichen?	Festlegung von alternativen Lagerungsstandorten, entsprechende Kennzeichnung	☐	☐	☐	☐	☐

V.3.2 Gebäude, Anlagen – Erdbeben

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
1. Gebäude						
1.1 Bieten die Gebäude/Bauwerke Erdbebenlasten hinreichenden Widerstand?	Hierzu zählen die Beachtung der Normenwerke (DIN 4149, Eurocode 8) sowie die freiwillige Anwendung darüber hinausgehender Empfehlungen.	☐	☐	☐	☐	☐
1.2 Sind Anlagen im Bauwerk hinreichend verankert?	Hierzu zählen Tanks, Transformatoren etc.	☐	☐	☐	☐	☐
1.3 Können strukturschwächende Veränderungen an tragenden Bauteilen ausgeschlossen werden?	Hierzu zählen große Bohrlöcher sowie nachträglich angebrachte Aussparungen.	☐	☐	☐	☐	☐
2. Unterirdische Anlagen						
2.1 Werden Rohrleitungen in Erdbebengebieten im Hinblick auf die potenzielle Belastung verlegt?	Hierzu zählen eine Beachtung der Bodenbeschaffenheit, eine Verlegung im rechten Winkel zu bekannten Verwerfungen mit flexiblen Verbindungen und Sicherheitsventilen sowie eine Verlegung redundanter Rohrleitungen.	☐	☐	☐	☐	☐

V.3.3 Gelände, Gebäude – Stürme

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
1. Gebäude						
1.1 Sind Dächer hinreichend in den Bauwerken verankert?	Standhalten der Dächer bis einschließlich Sturmstärke 12	☐	☐	☐	☐	☐
1.2 Sind die Gebäude und Anlagen in unmittelbarer Nähe frei von sturmanfälligen Bäumen oder nicht fest verankerten Gegenständen?		☐	☐	☐	☐	☐
1.3 Wurde die Exposition der Einrichtung bzw. die Angriffsfläche von Gebäudeteilen beurteilt?	Für potenzielle Sturmschäden sind insbesondere die topografische Lage und die Bauform der Gebäude von Bedeutung.	☐	☐	☐	☐	☐
2. Gelände						
2.1 Sind alle Sammeleinrichtungen für Regenwasser frei?	Laub und andere Gegenstände können Regenrinnen, Gullideckel etc. verstopfen und vermeidbare Überschwemmungen hervorrufen.	☐	☐	☐	☐	☐
2.2 Sind Zuwege/ Zufahrten so gesichert, dass sie nicht durch Gegenstände oder umfallende Bäume versperrt werden können?	Aus Gründen der Verkehrssicherheit und der Erreichbarkeit Kritischer Infrastrukturen jederzeit zu gewährleisten	☐	☐	☐	☐	☐

V.3.4 Gelände, Gebäude – vorsätzliche Handlungen mit kriminellem und/oder terroristischem Hintergrund

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
1. Zugang						
1.1 Werden Zugangskontrollen zum Gelände und den Bauwerken der Einrichtung durchgeführt?	Zum Beispiel durch den Pförtner oder ein elektronisches Sicherheitssystem	☐	☐	☐	☐	☐
1.2 Sind Zonen erschwerten 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 Höhensprünge, Poller, Zäune oder Betonelemente können ein Heranfahren an kritische Bereiche be- oder verhindern.	☐	☐	☐	☐	☐
1.3 Sind in den Bauwerken Zonen erschwerten 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 nicht Betriebsangehörige zu erschweren.	☐	☐	☐	☐	☐
1.4 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	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
2.2 Wurden geschützte Räume für Mitarbeiter und sonstige anwesende Personen eingerichtet?	Im Falle eines Terroranschlages, eines Unfalls mit Gefahrgut oder einer Industriehavarie ist es sinnvoll, 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 geschützter 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?	Dies schließt die Auswertung des Videomaterials mit ein.	☐	☐	☐	☐	☐
3.2 Sind Alarmanlagen in Kernbereichen installiert?		☐	☐	☐	☐	☐
4. Ansprechpartner						
4.1 Sind spezialisierte Ansprechpartner bekannt, die im Falle eines Anschlages mit chemischen, biologischen oder radiologischen Agenzien kontaktiert werden können?	Im Falle eines Unfalls oder eines terroristischen Anschlages können Einrichtungen mit Agenzien konfrontiert werden, deren Einschätzung Spezialwissen voraussetzt. Zusätzlich zu den Gesundheitsbehörden sollten mögliche Kooperationspartner hier im Vorfeld identifiziert und kontaktiert werden.	☐	☐	☐	☐	☐

V.3.5 Gebäude, Anlagen – Brände

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
1. Gebäude						
1.1 Sind in dem Gebäude Brandschutzmaß-nahmen vorhanden?	Installation von z. B. Brandschutztüren, Rauchmeldern, Feuer-löschern, Rauch- und Wärmeabzug	☐	☐	☐	☐	☐
1.2 Sind die Fluchtwege klar und einheitlich gekennzeichnet?	Es sollte stets ein zweiter Fluchtweg zugänglich sein (z. B. über das Treppenhaus).	☐	☐	☐	☐	☐
1.3 Sind kritische Bereiche zusätz-lich vor Bränden geschützt?	Zu kritischen Bereichen zählen Öltanks, Gefahrengutlager, Gasleitungen etc.	☐	☐	☐	☐	☐
1.4 Ist eine Werks- bzw. Betriebsfeuerwehr vorhanden?	Dies gilt vor allem für größere Einrichtungen, die mit leicht brenn-baren Gefahrenstoffen arbeiten.	☐	☐	☐	☐	☐
1.5 Ist ein Brand-schutzbeauftragter benannt?		☐	☐	☐	☐	☐
2. Konstruktion						
2.1 Sind die Fassaden inklusive der Fenster und Türen feuer-resistent?		☐	☐	☐	☐	☐
2.2 Halten tragende Konstruktionsele-mente auch hohen Temperaturen stand?		☐	☐	☐	☐	☐

V.3.6 Gebäude, Anlagen, Geräte – Stromausfall

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
1. Gebäude						
1.1 Kann ein Kurzschluss im Gebäude ausgeschlossen werden?		☐	☐	☐	☐	☐
1.2 Sind die Beleuchtung und das Belüftungssystem an die Notstromversorgung angeschlossen?		☐	☐	☐	☐	☐
1.3 Sind in den Gebäuden ausreichend Taschenlampen und Mobiltelefone vorhanden?		☐	☐	☐	☐	☐
2. Anlagen und Geräte						
2.1 Ist der Gesamtenergiebedarf zur Aufrechterhaltung der geschäftskritischen Prozesse/Fachaufgaben ermittelt worden?	• Informationstechnologie • Telekommunikation • Haustechnik	☐	☐	☐	☐	☐
2.2 Können kritische Anlagen und Geräte notfalls mit mobilen Notstromaggregaten betrieben werden?		☐	☐	☐	☐	☐
2.3 Besteht ein automatisiertes Datensicherungssystem für die Anlagen und Geräte?	Ein Datensicherungssystem verhindert den Verlust von wichtigen Informationen beim kurzfristigen Ausfall der Anlagen und Geräte.	☐	☐	☐	☐	☐
2.4 Kann eine notwendige Kühlung kritischer Bereiche auch bei längerem Stromausfall gewährleistet werden?		☐	☐	☐	☐	☐
2.5 Können Anlagen und Geräte kontrolliert heruntergefahren werden?	Sicherheitsshutdown, Vermeidung von Anlagenschäden, Verschmutzungen und Gefahrstofffreisetzung	☐	☐	☐	☐	☐

V.3.7 Anlagen, Geräte – Informationstechnologie

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
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. Verfügbarkeit						
2.1 Sind sämtliche für die kritischen Prozesse notwendigen internen IT-Systeme im Krisenfall verfügbar?		☐	☐	☐	☐	☐
2.2 Sind kritische externe Verbindungen bekannt und in einer Krise verfügbar?		☐	☐	☐	☐	☐
3. Zugriffssicherung						
3.1 Ist die mit öffentlichen Datennetzwerken verknüpfte IT ausreichend vor Zugriff von außen gesichert?	Firewall, Virenscanner, Identifizierung der Nutzer etc.	☐	☐	☐	☐	☐
4. Datenerhaltung						
4.1 Existiert ein Datensicherungskonzept?		☐	☐	☐	☐	☐
4.2 Besteht ein automatisiertes Datensicherungssystem für die Anlagen und Geräte?	Ein Datensicherungssystem verhindert den Verlust von wichtigen Informationen beim kurzfristigen Ausfall der Anlagen und Geräte.	☐	☐	☐	☐	☐
4.3 Werden kritische Daten an verschiedenen Orten vorgehalten?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
5. Prozesssteuerung						
5.1 Existiert eine redundante und örtlich getrennte Prozesssteuerung?		☐	☐	☐	☐	☐
5.2 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.3.8 Anlagen, Geräte – Kommunikationstechnologie

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
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?		☐	☐	☐	☐	☐
2.2 Sind im Mobilfunk Bevorrechtigungen/ Vorrangschaltungen vereinbart worden?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
3. Funk						
3.1 Steht in der Einrichtung ein Funksprechsystem für den Krisenfall zur Verfügung?		☐	☐	☐	☐	☐

V.4 Krisenmanagement

V.4.1 Allgemeine Organisation

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
1. Krisenplan						
1.1 Ist die krisenrelevante Organisationsstruktur festgelegt?	Ziel und Geltung des Krisenplans, Aufbauorganisation, Ablauforganisation, planbare Maßnahmen	☐	☐	☐	☐	☐
2. Aufbauorganisation						
2.1 Ist die personelle Besetzung der notwendigen Positionen für das Krisenmanagement in der Einrichtung festgelegt?		☐	☐	☐	☐	☐
2.2 Sind alle relevanten Aufgaben im Krisenmanagement festgelegt und Personen und deren Vertretern zugewiesen?		☐	☐	☐	☐	☐
2.3 Werden Mitarbeiter hinsichtlich ihrer Eignung für die im Krisenfall zugeteilte Rolle aus- und weitergebildet?		☐	☐	☐	☐	☐
2.4 Besteht eine Festlegung von Eskalationsstufen und Alarmierungskriterien?		☐	☐	☐	☐	

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
2.5 Krisenstab						
2.5.1 Tritt im Krisenfall ein Krisenstab in der Einrichtung zusammen?		☐	☐	☐	☐	☐
2.5.2 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. Kontaktieren Sie die örtlichen Katastrophenschutzbehörden. Ansprechpartner sind die örtlichen Feuerwehren bzw. Kreis-, Stadt- oder Gemeindeverwaltungen.	☐	☐	☐	☐	☐
2.5.3 Liegen Konzepte zur Weiterführung der Krisenstabsfunktion bei Ausfall der Kommunikationssysteme vor?	Beispielsweise durch die Einrichtung von Personenmeldern mit oder ohne Kraftfahrzeug oder Kraftrad.	☐	☐	☐	☐	☐
2.5.4 Liegen Konzepte zur Weiterführung der Krisenstabsfunktion bei Ausfall der Datenverarbeitungssysteme vor?	Beispielsweise durch die Vorhaltung von Plänen und Informationen in Papierform	☐	☐	☐	☐	☐
2.5.5 Liegen Konzepte zur Weiterführung der Krisenstabsarbeit bei Ausfall des Krisenstabsraumes vor?		☐	☐	☐	☐	☐
3. Ablauforganisation						
3.1 Ist die Aktivierung des Krisenmanagements festgelegt?	Ausübung von speziellen Stabsfunktionen	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
3.2 Alarmierung						
3.2.1 Sind interne und externe Alarmierungs- und Informationsvorgänge klar festgelegt?		☐	☐	☐	☐	☐
3.2.2 Existieren konkrete Handlungsanweisungen für Personen, die in einer Gefahrensituation für die Weitergabe von Meldungen zuständig sind?		☐	☐	☐	☐	☐
3.2.3 Werden konkrete Handlungen und Entscheidungen in der Krise dokumentiert?		☐	☐	☐	☐	☐
3.2.4 Werden interne und externe Alarmierungs- und Informationsvorgänge beübt?	Hierzu zählen interne Übungen sowie die Einbindung in Übungen des örtlichen Katastrophenschutzes.	☐	☐	☐	☐	☐
3.2.5 Ist entsprechend den möglichen Auswirkungen von Extremereignissen die Alarmierung festgelegt?	Vereinfachte Festlegung zum Beispiel 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.	☐	☐	☐	☐	☐
3.2.6 Ist die Warnung der von einem Extremereignis in der Einrichtung betroffenen Bevölkerung geregelt?	Anwohner, Kunden etc.	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
3.3 Notwendige Informationen und Unterlagen						
3.3.1 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 und Wasser.	☐	☐	☐	☐	☐
3.3.2 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.	☐	☐	☐	☐	☐
3.3.3 Sind alle wichtigen Unterlagen griffbereit?		☐	☐	☐	☐	☐
3.3.4 Liegen Pläne und Unterlagen, die im Krisenfall auch im Freien genutzt werden müssen, nässegeschützt vor?		☐	☐	☐	☐	☐
3.3.5 Liegen Formblätter zur Dokumentation von Meldeeingängen und -ausgängen vor?		☐	☐	☐	☐	☐
3.3.6 Liegen Formblätter zur Erstellung von Informationen für die Bevölkerung vor?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
3.4 Erreichbarkeiten						
3.4.1 Liegen aktuelle, zentral gepflegte Personal- und Erreichbarkeits-listen vor?	Die Listen enthalten Namen, Adressen, Tele-fonnummern (dienstlich und privat) sowie eine Beschreibung der Positi-onen in der Einrichtung.	☐	☐	☐	☐	☐
3.4.2 Liegen aktuelle Informationslisten über wichtige externe Einrich-tungen vor?	Die Listen enthalten regelmäßig aktuali-sierte Informationen zur Organisation, die Adresse, den Namen eines Ansprechpartners, die Telefonnummern, eine Beschreibung der Dienstleistungen sowie Informationen zu vertraglichen Vereinba-rungen und Hinweise auf Versorgungsprioritäten. Hierzu zählen u. a. Kran-kenhäuser, Kindergärten, Schulen und Lieferanten für Betriebsstoffe.	☐	☐	☐	☐	☐
3.4.3 Sind die im Krisen-fall zu informie-renden Behörden im Krisenplan erfasst?	Beispiele: Polizei, Gesundheitsamt, Umweltamt, Feuerwehr und Katastrophenschutz	☐	☐	☐	☐	☐
3.4.4 Werden alle Listen regelmäßig auf Aktualität unter-sucht?		☐	☐	☐	☐	☐
4 Krisenstabsraum						
4.1 Liegt der Krisen-stabsraum möglichst in einem gesicherten Betriebsbereich bzw. an einem Ausweich-standort?		☐	☐	☐	☐	☐
4.2 Ist der Krisen-stabsraum zentral erreichbar?	Anschluss an den ÖPNV, Nähe zur Autobahn und Verfügbarkeit von ausrei-chenden Parkflächen	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
4.3 Existiert ein ausreichend dimensionierter und vom Arbeitsraum abgesetzter Besprechungsraum (ohne Telefone) für Lagebesprechungen?	Verfügbarkeit von kleinen Besprechungsräumen für Arbeitsgruppen/ Detailabstimmungen	☐	☐	☐	☐	☐
4.4 Ist der Krisenstabsraum durch eine Zugangskontrolle geschützt?	Elektronisches Sicherheitssystem etc.	☐	☐	☐	☐	☐
4.5 Wird der Krisenstabsraum durch einen Sichtschutz an den Fensterfronten und durch Maßnahmen zur Abhörsicherheit geschützt?		☐	☐	☐	☐	☐
4.6 Befinden sich in der Nähe des Krisenstabsraumes Rückzugsräume/ -flächen für Ruhepausen und zur Verpflegungsaufnahme, evtl. mit Schlafmöglichkeiten?		☐	☐	☐	☐	☐
4.7 Technische Infrastruktur						
4.7.1 Ist eine unterbrechungsfreie Stromversorgung bzw. Netzersatzanlage verfügbar?		☐	☐	☐	☐	☐
4.7.2 Stehen PC-Arbeitsplätze mit Internetzugang und E-Mail-Funktion sowie externe Speichermedien zum Transport von Daten bereit?	CD-ROM, externe Festplatten, USB-Sticks	☐	☐	☐	☐	☐
4.7.3 Stehen Laptops, Notebooks und PDAs bereit?		☐	☐	☐	☐	☐
4.7.4 Existiert ein E-Mail-Sammelpostfach mit geregelter Verteilung?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
4.7.5 Gibt es Mobiltelefone mit Ladekabeln sowie stromunabhängige analoge Telefone?		☐	☐	☐	☐	☐
4.7.6 Besteht eventuell eine Direktleitung zu wichtigen Einrichtungen?		☐	☐	☐	☐	☐
4.7.7 Sind die für das Krisenmanagement notwendigen Kommunikationsmittel und Informationswege vorhanden und zugänglich?	Verfügbarkeit von TV-, Radio- und Videogeräten, Scannern, Faxgeräten und Faxservern auf PCs, Fotoapparaten, Kopiergeräten und Visualisierungstechnik (Beamer etc.)	☐	☐	☐	☐	☐
4.7.8 Besteht ein Zugriff auf die betriebseigenen Informationssysteme, Betriebsfunk und Videoüberwachung?		☐	☐	☐	☐	☐
5 Sonstiges						
5.1 Sind Formblätter, Protokollblätter und Vorlagen vorbereitet?		☐	☐	☐	☐	☐
5.2 Liegen Telefonlisten und Erreichbarkeitslisten sowie Listen über Ressourcen vor?	Personal, Geräte, Bevorratung, Dienstleistungen im Krisenfall, Verträge in digitaler sowie in Papierform	☐	☐	☐	☐	☐
5.3 Liegt aktuelles Plan- und Bildmaterial der Einrichtung vor?		☐	☐	☐	☐	☐
5.4 Existiert ein Pressezentrum mit entsprechender Ausstattung wie Fernsehen oder Radio?	Für größere Einrichtungen	☐	☐	☐	☐	☐
5.5 Werden Personalausweise, Dienstausweise und Betriebsausweise kontrolliert?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
5.6 Ist die Verpflegung der Mitarbeiter und Hilfskräfte für den Ereignisfall sicher-gestellt?		☐	☐	☐	☐	☐
5.7 Gibt es Schutzaus-rüstungen für alle Mitarbeiter?	Schutzbrillen, Helme, Sicherheitsschuhe, Schutzmasken sowie Kör-perschutzanzüge	☐	☐	☐	☐	☐

V.4.2 Krisenbewältigung

V.4.2.1 Verfahren in der Krise

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
1 Generelle Verfahren						
1.1 Ist eine Lagefest-stellung erfolgt?	Erfassung des Lagebildes, des Ereignisablaufes und von Gegenmaßnahmen	☐	☐	☐	☐	☐
1.2 Kann die Funktions-fähigkeit betroffener Bereiche in der Einrichtung wieder hergestellt werden?		☐	☐	☐	☐	☐
1.3 Werden Schutz-vorkehrungen für Personal, Gäste und Kunden getroffen?		☐	☐	☐	☐	☐
1.4 Werden Schutz-vorkehrungen für Gebäude, Anlagen und Geräte, Daten und Unterlagen getroffen?		☐	☐	☐	☐	☐
2 Administrative Verfahren						
2.1 Werden alle Mit-arbeiter, die im Rahmen der Krisen-bewältigung tätig sind, identifiziert?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
2.2 Werden alle Mitarbeiter identifiziert, die in Gefahrenzonen tätig sind?		☐	☐	☐	☐	☐
2.3 Wird Hilfe für verletzte, festsitzende oder verirrte Mitarbeiter bereitgestellt?		☐	☐	☐	☐	☐
2.4 Werden für das Personal Informationen über das Ereignis bereitgestellt?		☐	☐	☐	☐	☐
2.5 Werden für die Familien der Mitarbeiter Informationen über das Ereignis bereitgestellt?		☐	☐	☐	☐	☐
2.6 Werden alle Verletzungen und die diesbezüglich eingeleiteten Maßnahmen dokumentiert?		☐	☐	☐	☐	☐
2.7 Werden alle Teilereignisse dokumentiert?		☐	☐	☐	☐	☐
2.8 Werden alle Anlagen und Geräte, sofern möglich, aus den Schadenszonen verlagert?		☐	☐	☐	☐	☐
2.9 Werden Zugangskontrollen zum Schadensgebiet durchgeführt?		☐	☐	☐	☐	☐
2.10 Werden Protokolle über alle Telefonate erstellt?		☐	☐	☐	☐	☐
2.11 Werden alle Entscheidungen dokumentiert?	Formblätter, Protokolle	☐	☐	☐	☐	☐
2.12 Werden alle Personenschäden dokumentiert?	Berichte, Fotos, Videomaterial	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
2.13 Werden alle Sachschäden dokumentiert?	Berichte, Fotos, Videomaterial	☐	☐	☐	☐	☐
2.14 Werden benötigte Mittel zur Bewältigung der Krise bereitgestellt?		☐	☐	☐	☐	☐
2.15 Werden nach Ablauf der Krisensituation die Rücknahme der Alarmierung und die Wiedereinsetzung der betrieblichen Aufbauorganisation veranlasst?		☐	☐	☐	☐	☐
3 Medien						
3.1 Sind alle geschulten Mediensprecher einberufen?		☐	☐	☐	☐	☐
3.2 Liegen alle vorformulierten Texte griffbereit vor?		☐	☐	☐	☐	☐
3.3 Liegt Hintergrundmaterial zur Einrichtung bereit?		☐	☐	☐	☐	☐
3.4 Wird das festgelegte Verfahren zur Freigabe von Informationen nach außen berücksichtigt?		☐	☐	☐	☐	☐
3.5 Liegen alle Listen mit Ansprechpartnern der Einrichtung für Medienvertreter vor?		☐	☐	☐	☐	☐
3.6 Liegt ein Fragenkatalog zur Überprüfung der Medienvertreter bereit?	Authentizität, Überprüfung des Ausweises	☐	☐	☐	☐	☐
3.7 Werden die Medien umfassend durch die Mediensprecher informiert?	Information durch Pressemitteilungen, Pressekonferenzen, Anzeigen, Botschaften in Hörfunk und Fernsehen	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
4 Logistik						
4.1 Werden alle notwendigen Mittel zur Krisenbewältigung bereitgestellt?	Ausrüstungsgegenstände, Lebensmittel, Bedarfsmaterial, funktionierender Krisenstabsraum, medizinisches Hilfsmaterial	☐	☐	☐	☐	☐
4.2 Sind der Krisenstabsraum und die daran angeschlossenen Räume funktionsbereit und zugangsbeschränkt?	Der Krisenstabsraum sowie Aufenthaltsräume für Krisenstabsmitglieder sollten nur für diese zugänglich sein.	☐	☐	☐	☐	☐
4.3 Werden alle notwendigen Pläne bereitgestellt?	Gebäudepläne, Energieversorgung, Wasserversorgung, Entsorgung etc.	☐	☐	☐	☐	☐
4.4 Werden alle redundanten Einrichtungs- und Ausrüstungsgegenstände bereitgestellt?	Alternativer Krisenstabsraum, Funkgeräte etc.	☐	☐	☐	☐	☐
4.5 Ist die Notstromversorgung angelaufen?		☐	☐	☐	☐	☐

V.4.2.2 Entscheidung und Maßnahmenumsetzung

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
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	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
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?		☐	☐	☐	☐	☐
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 Sind die Evakuierungsmaßnahmen angelaufen?	Festlegung eines Sammelplatzes, Prüfung der Vollzähligkeit aller Anwesenden auf dem Sammelplatz, Meldung der Beendigung der Evakuierung, Möglichkeiten zum Weitertransport aller Anwesenden	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
6 Reaktion bei Bombendrohung						
6.1 Ist die Polizei eingeschaltet?		☐	☐	☐	☐	☐
6.2 Werden Hinweise auf verdächtige Aktivitäten aufgenommen und weitergeleitet?		☐	☐	☐	☐	☐
6.3 Werden Hinweise auf verdächtige Gegenstände aufgenommen und weitergeleitet?	Zum Beispiel durch Verwendung eines Formblattes	☐	☐	☐	☐	☐
6.4 Werden Alarmstufen eingeschaltet und Zugangsmöglichkeiten für gefährdete und kritische Bereiche eingeschränkt?		☐	☐	☐	☐	☐
7 Koordination der Zusammenarbeit mit externen Einrichtungen						
7.1 Ist das Verfahren zur Zusammenarbeit mit externen Einrichtungen aktiviert?	Beispiel: Feuerwehr, Polizei	☐	☐	☐	☐	☐
7.2 Wird der Zugang von Mitarbeitern externer Einrichtungen kontrolliert?	Zugangskontrolle und Personenkontrolle	☐	☐	☐	☐	☐
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?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
8.2 Werden alle zeitlichen Fristen berücksichtigt?	Mögliche Vorlaufzeiten	☐	☐	☐	☐	☐
8.3 Werden die Auswirkungen einer partiellen oder vollständigen Außerbetriebnahme von Anlagen erfasst und berücksichtigt?		☐	☐	☐	☐	☐
9 Umgang mit kritischen Daten und Unterlagen						
9.1 Werden wichtige Datenträger und Unterlagen vor Gefahren geschützt?	Lagerung in wasserdichten und feuerfesten Behältern, Schutz vor gewaltsamem und unbefugtem Zugang	☐	☐	☐	☐	☐
9.2 Werden wichtige Datenträger, Unterlagen und Behälter gekennzeichnet?		☐	☐	☐	☐	☐
9.3 Werden wichtige Datenträger und Unterlagen aus dem Schadensgebiet ausgelagert?		☐	☐	☐	☐	☐

V.5 Nachbereitung

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
1 Werden Handlungsprioritäten festgelegt?		☐	☐	☐	☐	☐
2 Ist die Einrichtung zum Normalbetrieb zurückgekehrt?	Information der Mitarbeiter, kontrollierte Wiederinbetriebnahme der gesamten Produktion/ Dienstleistung	☐	☐	☐	☐	☐
3 Ist der Grad der Restgefährdung ermittelt?		☐	☐	☐	☐	☐
4 Werden Schadensinformationen ausgewertet?	Berichte, Fotos, Videomaterial	☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
5 Werden externe Akteure über den Sachstand informiert?	Versicherungen, Behörden	☐	☐	☐	☐	☐
6 Ist eine Kontaktaufnahme mit den betroffenen Kunden erfolgt?		☐	☐	☐	☐	☐
7 Werden alle notwendigen Aufräumarbeiten initiiert?	Lüften, Trümmer wegräumen, Trocknung etc.	☐	☐	☐	☐	☐
8 Wird eine Inventarisierung aller beschädigten Gebäude, Anlagen und Geräte vorgenommen?		☐	☐	☐	☐	☐
9 Wird eine Abschätzung des monetären Schadens vorgenommen?		☐	☐	☐	☐	☐
10 Wird eine Befragung der Mitarbeiter zum Krisenmanagement durchgeführt?		☐	☐	☐	☐	☐
11 Werden die Ergebnisse aus der Nachbereitung zur Anpassung des Krisenmanagements genutzt?		☐	☐	☐	☐	☐

V.6 Übungen

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwend-bar
1 Stabsrahmenübungen						
1.1 Wird die Übernahme krisenbezogener Aufgaben und Verantwortung geübt?		☐	☐	☐	☐	☐
1.2 Werden Alarmierungs- und Meldewege sowie Wege der Warnung geübt?		☐	☐	☐	☐	☐

Fragen	Erläuterungen	Vollständig/ ja	In großen Teilen	In einigen Teilen	Kaum oder gar nicht/ nein	Nicht anwendbar
1.3 Werden interne und externe Kommunikationswege getestet?		☐	☐	☐	☐	☐
1.4 Werden Kommunikationsmittel getestet?	Werden alle beteiligten und betroffenen Personen frühzeitig und umfassend gewarnt sowie informiert?	☐	☐	☐	☐	☐
1.5 Werden Erreichbarkeitslisten getestet?	Beispiel: Telefonlisten	☐	☐	☐	☐	☐
2 Teil-, Vollübungen						
2.1 Werden Evakuierungen vorgenommen?		☐	☐	☐	☐	☐
2.2 Wird die Vollzähligkeit 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?		☐	☐	☐	☐	☐

VI. Vorgehensweise bei der beispielhaften Risikoanalyse

Das detaillierte Vorgehen und die Erklärung der einzelnen Analyseschritte einer Risikoanalyse, wie in diesem Leitfaden beschrieben, werden als Powerpointpräsentation auf der Homepage des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe zur Verfügung gestellt. Im Rahmen der beispielhaften Risikoanalyse wird dabei der Teilprozess „Steuerzentrale“ untersucht und das Risiko bei einem Szenario „Stromausfall“ nach der hier dargestellten Vorgehensweise analysiert.

Das Beispiel findet sich unter der folgenden Adresse: www.bbk.bund.de
Suchbegriff: RMKM2011

Vorgehensweise bei der beispielhaften Risikoanalyse

Abbildung 14: Abfolge einer Risikoanalyse

VII. Umsetzungshilfe

VII.1 Einleitung

Die Umsetzungshilfe soll bei der Etablierung eines Risiko- und Krisenmanagements im Sinne des Leitfadens unterstützen und wichtige Hinweise für die Umsetzung liefern. Die Umsetzungshilfe enthält Erfahrungen, die Einrichtungen aus dem Bereich Kritischer Infrastrukturen bei der Anwendung des Leitfadens gesammelt haben und liefert Ratschläge bezüglich der Aspekte, die bei der Umsetzung der einzelnen Phasen des Risiko- und Krisenmanagements zu beachten sind.

VII.2 Risiko- und Krisenmanagement

Bei der Umsetzung des Leitfadens wird zunächst festgelegt, welche Ziele im Rahmen eines Risiko- und Krisenmanagements erreicht werden sollen. Anhand dieser Ziele werden die einzelnen Schritte zur Etablierung eines Risiko- und Krisenmanagements umgesetzt.

Ein Risikomanagement ist ein Führungsinstrument, das sich an den bereits umgesetzten Schutz- und Sicherheitsmaßnahmen orientieren kann. Es ermöglicht eine effektive Risikosteuerung. Die positiven Steuerungsimpulse eines Risikomanagements eignen sich insbesondere dazu, die Akzeptanz der Leitungsebene einer Einrichtung zu erlangen. Ein etabliertes Risikomanagement ermöglicht darüber hinaus insbesondere für Unternehmen die Erfüllung von Rating-Standards durch Nachweis von Führungsqualität und Risikotragfähigkeit. Außerdem wird durch ein umfassendes Risiko- und Krisenmanagement eine hohe Akzeptanz seitens der Mitarbeiter durch Transparenz der Bewertungs- und Entscheidungsprozesse geschaffen. Der Risikomanagementprozess kann vor allem durch Anwendung spezifischer EDV-Unterstützung kosten- und zeiteffektiv gestaltet werden.

VII.2.1 Vorplanung des Risiko- und Krisenmanagements

In der Vorplanung zum Risiko- und Krisenmanagement ist zunächst in Kooperation mit der Einrichtungsleitung festzulegen, mit welcher Detailtiefe, über welchen Zeitraum und mit welchem Aufwand das Risiko- und Krisenmanagement etabliert und die einzelnen Schritte des Risikomanagements durchgeführt werden sollen.

Um einen direkten Einstieg in das Risiko- und Krisenmanagement zu ermöglichen, bietet sich eine Auftaktveranstaltung an, bei der sich die relevanten Akteure kennenlernen, die Erfordernisse und Chancen eines Risiko- und Krisenmanagements für die Einrichtung thematisiert und das systematische Vorgehen festgelegt werden.

Grundsätzlich ist es vorteilhaft, die einzelnen Phasen des Risikomanagements so detailliert wie möglich umzusetzen. Mit der Detailtiefe steigt allerdings auch der damit verbundene Aufwand. Somit ist eine genaue Zielsetzung und präzise Analyse der verfügbaren Ressourcen unabdingbar, um ein der Einrichtung angepasstes Risiko- und Krisenmanagement zu etablieren.

Eine effiziente Umsetzung des Leitfadens zum Risiko- und Krisenmanagement ist vor allem gewährleistet, wenn eine eigene Projektgruppe mit Spezialisten aus den jeweiligen Teilbereichen der Einrichtung eingerichtet wird, die sich ausschließlich mit der Umsetzung des Leitfadens beschäftigt und in Absprache mit der Leitungsebene von anderen Aufgaben freigestellt ist. Gegebenenfalls kann jeweils für das Risiko- und für das Krisenmanagement eine eigene Projektgruppe eingerichtet werden. In diesem Zusammenhang sollte überlegt werden, wie die Projektgruppe in die allgemeine Organisationsstruktur eingefügt werden kann.
Es ist ratsam, die weiteren Akteure zu identifizieren, die mit in die Projektarbeit integriert werden sollen. In der Vorplanung werden die organisatorischen und strukturellen Voraussetzungen für das Risiko- und Krisenmanagement (Zuständigkeiten, Ressourcen, Kompetenzen, rechtliche Verpflichtungen, Risikokommunikation) geschaffen.

In der Vorplanung wird für das Risikomanagement genauso wie für das Krisenmanagement eine Kommunikationsstrategie ausgearbeitet. Dafür sind zunächst die Verantwortlichen und Beteiligten am Risiko- und Krisenmanagement zu identifizieren beziehungsweise auszuwählen.

Sowohl bei der internen als auch bei der externen Risikokommunikation ist auf eine einfache und verständliche Wortwahl zu achten. Die Führungsebene einer Einrichtung hat in der Regel nicht die Möglichkeiten und freien Kapazitäten, sich intensiv mit den einzelnen Schritten des Risiko- und Krisenmanagements zu befassen. Somit ist es beispielsweise die Aufgabe des Verantwortlichen für die Etablierung des Risikomanagements, die Ergebnisse der Risikoanalyse und weiterer Vorgänge des Risikomanagements kompakt und adressatengerecht aufzubereiten sowie zu kommunizieren.

Es ist wichtig, sich auf die wesentlichen Risiken für und von einer Einrichtung zu konzentrieren, da ansonsten die Gefahr besteht, den Überblick zu verlieren und letztendlich keine brauchbaren Ergeb-

nisse zu erhalten. In diesem Zusammenhang sollte auch in der Vorplanung bereits eine regelmäßige Erhebung der „wesentlichen" Risiken vereinbart werden, damit das Risikomanagement stets den sich wandelnden Gegebenheiten angepasst wird.

Die Projektgruppe, die mit der Umsetzung des Risiko- und Krisenmanagements beauftragt ist, sollte unbedingt regelmäßige Gesprächstermine festsetzen, an denen sich alle Teilnehmer beteiligen. Durch die Anwesenheit aller Projektmitglieder werden die Kontinuität in der Umsetzung gewährleistet und sich wiederholende Diskussionen vermieden.

Gegebenenfalls sollte geklärt werden, ob vorab ein Austausch mit anderen Unternehmen oder Behörden möglich ist (am besten aus der gleichen Branche), die bereits ein Risiko- und Krisenmanagement etabliert haben.

VII.2.1.2 Strategische Schutzziele

Die strategischen Schutzziele werden klar formuliert und von der gesamten Einrichtung getragen. Der Zweck des Risikomanagements ist es, die strategischen Schutzziele und somit eine umfassende Grundlage für vorbeugende Maßnahmen und den Schutz der Einrichtung sowie seiner Mitarbeiter und Kunden zu erreichen.

VII.2.1.3 Information der Führungskräfte

Die Führungskräfte und die Leitungsebene einer Einrichtung sind regelmäßig über den Vorgang des Risiko- und Krisenmanagements zu informieren, sodass eine Übereinstimmung mit der Leitung einer Einrichtung herrscht. Die Akzeptanz der Leitungsebene kann dadurch gewonnen werden, dass die positiven Steuerungsimpulse des Risikomanagements aufgezeigt werden. Ein Risiko- und Krisenmanagementsystem kann nur dann effizient umgesetzt werden, wenn die Etablierung auch von der Leitungsebene unterstützt wird. Somit hängt die Qualität des Risiko- und Krisenmanagements stets mit dem Umsetzungswillen auf der Leitungsebene einer Einrichtung zusammen.

VII.2.2 Risikoanalyse

Für eine umfassende Risikoanalyse sind zunächst die relevanten einrichtungsspezifischen Risikoelemente zu identifizieren. Die Identifizierung ist eine der wichtigsten Voraussetzungen für eine erfolgreiche Risikoanalyse, da kritische Prozesse häufig unmittelbar von spezifischen Anlagen und Geräten abhängen. Es werden Informationen über Gefahren und Risiken für das Unternehmen oder die Behörde gesammelt. Dabei sollte zuerst überlegt werden, welche Gefahren an dem Standort des Unternehmens oder der Behörde auftreten können und von welchen Stellen man Informationen und Daten zu diesen Gefahren bekommt.[67]

Insbesondere bei der Identifizierung der Risiken wird häufig der Fehler gemacht, dass sich zu sehr auf Erfahrungswerte der Vergangenheit verlassen wird. Es ist somit unerlässlich, eine regelmäßige Aktualisierung der Risikoanalyse durchzuführen, um sich wandelnde Risiken rechtzeitig zu erkennen und in der Maßnahmenplanung zu berücksichtigen. Dabei ist insbesondere die Frühwarnfunktion der Risikoanalyse zu beachten.

Im Rahmen der Risikoanalyse ist vor allem die Schaffung des Risikobewusstseins bei den Mitarbeitern essentiell. Häufig verfügen die Mitarbeiter nur über ein geringes Risikobewusstsein und sollten somit für die vorhandenen Risiken sensibilisiert werden. Diese Sensibilisierung kann vor allem erreicht werden, indem die Folgen von Referenzereignissen aufgezeigt werden und eine transparente Szenarioentwicklung durchgeführt wird. Die Leitung einer Einrichtung hat die Aufgabe, den Mitarbeitern deutlich zu machen, aus welchen Gründen welche Risiken bestehen und warum dagegen entsprechende Maßnahmen eingeleitet werden.

VII.2.2.1 Identifizierung der wesentlichen Prozesse

Die Identifizierung der wesentlichen Prozesse dient einer Vorauswahl der kritischen Prozesse einer Einrichtung. Durch diesen Vorgang kann ein erheblicher Aufwand gespart werden, da nicht alle Prozesse einer Einrichtung einer Risikoanalyse unterzogen werden müssen.

Im Rahmen der Identifizierung der wesentlichen Prozesse einer Einrichtung ist es essentiell, dass einzelne Aufgaben der Einrichtung detailliert bekannt sind. Die Aufgaben einer Einrichtung können durch eine Organisationsuntersuchung erfasst werden. Bei der Ermittlung der wesentlichen Aufgaben sollten pro Abteilung jedoch nicht mehr als zehn Aufgaben aufgenommen werden, damit eine Übersichtlichkeit und mögliche Bewertung der Prozesse gegeben ist. In diesem Kontext gilt es festzuhalten, welche die Kernfunktionen der Einrichtung sind. Nur diese Kernfunktionen sind unbedingt aufrechtzuerhalten und vor bestehenden Gefahren umfassend zu schützen. Um die wesentlichen Prozesse zu identifizieren, werden zunächst die Ansprechpartner der einzelnen Abteilungen für die Bestandsaufnahme kontaktiert. Diese Ansprechpartner tragen die wesentlichen Prozesse in ihren Abteilungen zusammen und

[67] Siehe Anhang IV Gefahrenliste – Anhaltspunkte zu Art, Exposition, Intensität, Wirkungen und möglichen Ansprechpartnern.

vermitteln ihre Ergebnisse der Projektgruppe des Risikomanagements.

WICHTIGER HINWEIS:
Sowohl bei der Identifizierung der wesentlichen Prozesse als auch beim Schritt der Ermittlung kritischer Prozesse ist gegenüber den eigenen Mitarbeitern deutlich zu kommunizieren, dass die Ergebnisse dieser Analyseschritte in keiner Hinsicht Auskunft über die Entbehrlichkeit von Aufgaben im Regelbetrieb oder der Rationalisierung von Stellen dient und damit folglich keine versteckten Ziele verfolgt werden.

VII.2.2.2 Ermittlung kritischer Prozesse

Zur Ermittlung der kritischen Prozesse empfiehlt es sich, dass die Arbeitsgruppe Risikoanalyse in Zusammenarbeit mit den einzelnen Sachgebieten die Kritikalität der wesentlichen Aufgaben/Prozesse anhand von Kritikalitätskriterien analysiert.

Die entscheidenden Kritikalitätskriterien bei der Kritikalitätsanalyse sind der Mensch und die Gesundheit. Sobald in irgendeinem Maße der Mensch und/oder die Gesundheit beeinträchtigt werden, ist ein Prozess unabhängig von den anderen Kriterien stets als besonders kritisch einzustufen. Jede Einrichtung kann für sich die passenden Kritikalitätskriterien auswählen. Es empfiehlt sich aber, wie bereits im Leitfaden erläutert, auf jeden Fall die Kritikalitätskriterien Mensch und Gesundheit, Volumen und Auswirkungszeitpunkt im Rahmen der Kritikalitätsanalyse zu prüfen. Es ist besonders wichtig, bei der Bewertung der Kritikalität sowie der Verwundbarkeit der einzelnen Prozesse und Teilprozesse, die Begründung für die Bewertung schriftlich festzuhalten, damit bei der späteren Maßnahmenplanung noch nachvollzogen werden kann, aus welchen Gründen die jeweiligen Prozesse und Teilprozesse als kritisch und verwundbar bewertet wurden. Der Sinn und Zweck der Kritikalitätsanalyse ist gegenüber den Mitarbeitern wie bei der Identifizierung der wesentlichen Prozesse eindeutig zu formulieren und offenzulegen. Der Fokus und die Sensibilisierung sind auf den möglichen Krisenfall auszurichten.

VII.2.2.3 Identifizierung der Gefahren und Szenarioentwicklung

Bei der Identifizierung der Gefahren kann insbesondere auf Informationen von externen Einrichtungen zurückgegriffen werden. Die Gefahren können in die Kategorien Naturgefahren, technische Gefahren und terroristische/kriminelle Gefahren unterteilt werden. Für Informationen über die jeweiligen Gefahren können die zuständigen Einrichtungen kontaktiert werden (zum Beispiel Hochwassergefahr in Köln: Hochwasserzentrale Köln). Es ist insbesondere auf Wechselwirkungen von häufig zeitgleich auftretenden Gefahren (zum Beispiel Hochwasser und Stromausfall) und den direkten Folgewirkungen der Gefahr für die Eintrittswahrscheinlichkeit weiterer Gefahren zu achten (zum Beispiel Grundwasseranstieg durch Starkregen/Hochwasser). Die Wechselwirkungen sind zu entschlüsseln und nach Möglichkeit einzeln zu untersuchen. Gegebenenfalls können mehrere Gefahren, die zwar unterschiedliche Entstehungsbedingungen aufweisen, aber ähnliche Auswirkungen für die Einrichtung haben, auch zusammengefasst werden. Im Anschluss an die Identifizierung der Gefahren wird mithilfe der gesammelten Informationen ein Szenario für jede Gefahr entwickelt, das Informationen zur Intensität, Dauer, räumlichen Ausprägung, Vorwarnung und Eintrittswahrscheinlichkeit enthält. Bei der Szenarioentwicklung für die identifizierten Gefahren ist eine Beschränkung auf maximal fünf wesentliche Gefahren empfehlenswert, um die Bewertung der daraus resultierenden Risiken überschaubar zu halten. Außerdem ist es ratsam, die Auswirkungen der Szenarien nur für die wesentlichen beziehungsweise kritischen Prozesse einer Einrichtung zu analysieren und daraufhin die Verwundbarkeiten und resultierenden Risiken zu berechnen.

VII.2.2.4 Verwundbarkeitsanalyse

Bei der Verwundbarkeitsanalyse ist eine Analyse auf der Ebene der Risikoelemente der kritischen Prozesse sinnvoll. Es ist darauf zu achten, dass die Verwundbarkeit der einzelnen Organisationseinheiten einer Einrichtung nach den gleichen Kriterien bewertet wird, damit eine Vergleichbarkeit der jeweiligen Teilverwundbarkeiten gewährleistet ist. Auf der Grundlage der eingangs festgelegten Detailtiefe der Risikoanalyse wird nun das entsprechende Verfahren zur Analyse der Verwundbarkeit ausgesucht. Für eine umfassende Betrachtung der Verwundbarkeit empfiehlt sich das Vorgehen der Verwundbarkeitsermittlung.

Auch bei der Verwundbarkeitsanalyse ist wie bei der Kritikalitätsanalyse die Kommunikation und Moderation mit den Gruppen/Beschäftigten essentiell. Nach Möglichkeit sollten die Beschäftigten der Projektgruppe Risikomanagement speziell für die kommunikativen Anforderungen geschult werden.

VII.2.2.5 Risikoermittlung und -vergleich

Bei der Risikoermittlung werden die Eintrittswahrscheinlichkeiten der verschiedenen Szenarien mit den Verwundbarkeitswerten der Teilprozesse und Risikoelemente einer Einrichtung verknüpft, sodass verschiedene Risikowerte entstehen. Diese Risikowerte können verglichen und bewertet werden. Aus diesem Risikovergleich kann eine Priorisierung der vorbeugenden Maßnahmen und

Strategien für die einzelnen Risikoelemente der Prozesse und Teilprozesse abgeleitet werden.

VII.2.3 Vorbeugende Maßnahmen und Strategien

Die vorbeugenden Maßnahmen sollen Risiken reduzieren. Es ist hilfreich die Prozesse nach Prioritäten zu ordnen, nach denen die vorbeugenden Maßnahmen umgesetzt werden. Zunächst sind vor allem die kritischen Prozesse zu schützen.

Wenn mehrere Prozesse intuitiv ähnlich kritisch sind, kann sich die Abfolge der Maßnahmenumsetzung an den Risikowerten dieser Prozesse orientieren. Durch diese Vorgehensweise entsteht folgende Hierarchie der Schutzmaßnahmen für die Prozesse einer Einrichtung:

- 1. kritische und risikobehaftete Prozesse
- 2. kritische Prozesse
- 3. risikobehaftete Prozesse
- 4. unkritische und wenig risikobehaftete Prozesse

Die Auswahl der vorbeugenden Maßnahmen richtet sich in erster Linie nach einer Kosten-Nutzen-Analyse. In diese Kosten-Nutzen-Analyse sollten nach Möglichkeit auch die Erkenntnisse von möglichen Auswirkungen bei Ausbleiben der jeweiligen Schutzinvestitionen für die Einrichtung einfließen. Aufgrund dieser Informationen ist es die Aufgabe der Leitung einer Einrichtung, zu entscheiden, welche vorbeugenden Maßnahmen umgesetzt werden.

Die Maßnahmenplanung kann auf der Ebene der Kritikalität, der Verwundbarkeit und für bestimmte Gefahren auf der Ebene der Eintrittswahrscheinlichkeit eines Szenarios (zum Beispiel Reduzierung der Eintrittswahrscheinlichkeit technischen Versagens durch regelmäßige Wartung der Anlagen) greifen.

Im Anschluss an die Maßnahmenplanung empfiehlt sich eine Neubewertung des Risikos, um zu prüfen, welche Maßnahmen eine besonders große Effektivität aufweisen. Die ermittelte Effektivität bietet den Personen mit Entscheidungskompetenz in Kombination mit der Kostenanalyse der möglichen Maßnahmen eine solide Entscheidungsgrundlage. Um der Leitungsebene eine möglichst gute Übersicht zu geben, empfiehlt es sich, die möglichen Schutzmaßnahmen und Strategien inklusive der jeweiligen Kosten-Nutzen-Analyse in einer Liste zusammenzufassen.

VII.2.4 Dokumentation des Risiko- und Krisenmanagementsystems

Die Vorgehensweise der einzelnen Schritte und Phasen des Risiko- und Krisenmanagements sind detailliert zu dokumentieren. Eine Dokumentation hilft im Nachhinein nachzuvollziehen, aus welchen Gründen welche Schritte eingeleitet wurden, und dient darüber hinaus der Transparenz gegenüber Mitarbeitern und Kunden. Es empfiehlt sich auch, die analysierten Risiken genau zu dokumentieren, um mögliche Veränderungen bei den Risiken frühzeitig zu erkennen. Außerdem erleichtert eine Dokumentation eine stetige Verbesserung des Risiko- und Krisenmanagementsystems, da Schwachstellen schnell identifiziert und untersucht werden können. Aus diesen Gründen ist es darüber hinaus ratsam, auch die eingeleiteten vorbeugenden Maßnahmen zu dokumentieren.

VII.2.5 Krisenplanung

Für die Krisenplanung sind insbesondere die Prozesse festzuhalten, die für die Aufrechterhaltung beziehungsweise zügige Wiederherstellung der Kernfunktionen einer Einrichtung im Krisenfall unverzichtbar sind. Für die Krisenbewältigung sollten im Vorhinein Überlegungen zur grundlegenden Versorgung des Personals mit Lebensmitteln, zur Bereitstellung von Finanzmitteln sowie zu den Mitarbeitern, die diese zur Verfügung stellen und deren ordnungsgemäße Verwendung gewährleisten können (zum Beispiel Buchhalter), angestellt werden. Sollte die Einrichtung aufgrund eines Ereignisses nicht mehr betretbar sein und konnte kein Ausweichsitz bereitgestellt werden, kann ein im Vorfeld entwickeltes Konzept für die Auslagerung von Arbeitsplätzen (zum Beispiel Heimarbeitsplätze) hilfreich sein. Die Mitarbeiter und Abteilungen, die keine im Schadenfall kritischen Aufgaben ausführen, können für den Krisenfall andere Aufgaben zugewiesen bekommen und für die flexible Erfüllung von Aufgaben im Krisenfall geschult werden. Folglich sollte auch die Anzahl der verfügbaren Mitarbeiter bekannt sein. Auf dieser Grundlage wird ein Plan ausgearbeitet, der den flexiblen Einsatz der frei verfügbaren Mitarbeiter regelt. Die Inhalte und Ziele des Krisenplans sollten klar formuliert sein, damit jedem Mitarbeiter der Zweck des Krisenmanagements bewusst wird und die Zuständigkeiten im Krisenfall klar verteilt sind, sodass Missverständnisse und Kompetenzstreitigkeiten vermieden werden.

Des Weiteren sollte klar geregelt werden, welche Kompetenzen der Krisenstab hat und für wann der Krisenstab einberufen wird. Außerdem empfiehlt es sich, dass das Kernteam des Krisenstabes langfristig aus denselben Personen besteht, sodass bei einer Krise lediglich die externen Experten für die jeweiligen Gefahren ausgetauscht werden müssen.

Dies ermöglicht eine breite Vertrauensbasis innerhalb des Krisenstabes und erleichtert den Ablauf der Krisenkoordination und -bewältigung.

Für die Erstellung des Krisenplans und die Umsetzung des Krisenmanagements ist für Unternehmen eine aktions- oder prozessorientierte Herangehensweise empfehlenswert, da diese mit den etablierten Managementmethoden sehr stark korrespondiert.

VII.2.5.1 Krisenorganisation

Die Bildung des Krisenstabes erfordert eine gründliche Planung. Es ist wichtig, die internen Abläufe eines Krisenstabes genau zu analysieren sowie klare Ziele und Aufgaben des Krisenstabes zu formulieren, um den Krisenstab dementsprechend zu strukturieren und die Mitglieder des Kernteams auszuwählen. Die Aufgaben des Krisenstabes sollten deutlich priorisiert und den einzelnen Bereichen/ Mitgliedern des Krisenstabs zugewiesen werden.

Der Krisenstab sollte sich in seiner Arbeit auf die kritischen Geschäftsprozesse fokussieren und die verfügbaren Ressourcen zielgenau einsetzen. Dafür ist es wichtig, dass alle verfügbaren Informationen über das Krisenereignis, seine Entwicklung und eingeleitete Gegenmaßnahmen frühzeitig an den Krisenstab weitergeleitet werden.

Vor allem von dem Krisenstabsleiter und dem Kernteam ist ein interdisziplinäres und vernetztes Denken sowie Entscheiden gefordert. Es werden für das Krisenmanagement somit insbesondere Generalisten mit einem ganzheitlichen Überblick benötigt, die durch spezialisierte Fachkräfte in den jeweiligen Situationen und bei den Aufgaben beraten werden.

Ein wichtiger Bestandteil des Krisenmanagements ist es, die sehr seltenen Krisensituationen intensiv und regelmäßig zu üben. Eine Krise ist eine Sondersituation, in der nicht auf Anhieb alles nach Plan verläuft. Deswegen ist es essentiell, dass der Umgang mit solchen Sondersituationen regelmäßig geübt wird. Dadurch kann auch in einer realen Krise routiniert, souverän und bedacht gehandelt sowie ein Vertrauen der Mitarbeiter in den Krisenstab und eine Vertrauensbasis innerhalb des Krisenstabes geschaffen werden.

VII.2.5.2 Krisenkommunikation

Eine Krisenkommunikationsstrategie ermöglicht es, in einer Krise angemessen zu reagieren und grobe Fehler in der Kommunikation mit den eigenen Mitarbeitern und den Medien zu vermeiden.
Es ist wichtig, sowohl die eigenen Beschäftigten als auch die Medien und Kunden frühzeitig zu informieren. Innerhalb der ersten zwei Stunden nach Ausbruch des Krisenereignisses sollte eine Medienkonferenz einberufen werden.

Dennoch sind Informationen an die Beschäftigten und an die Medien erst weiterzugeben, wenn sich der Krisenstab ein Lagebild von der Krise verschafft hat. Gerade die Medien sollten lediglich mit gesicherten Fakten informiert werden. Es dürfen keine Vermutungen an die Öffentlichkeit gelangen, da dadurch leicht Gerüchte entstehen und der Eindruck vermittelt wird, dass die betroffene Einrichtung nicht in der Lage ist, sich ein genaues Lagebild zu verschaffen und sichere Informationen über die Krise zu erlangen. Verunsicherungen in der Bevölkerung werden dadurch abgebaut, dass man sie mit gesicherten Fakten informiert.

Beim Umgang mit den Medien ist es wichtig, alle Medien und Pressevertreter gleich zu behandeln und den Informationsfluss nach außen durchgängig aufrechtzuerhalten. Es ist sinnvoll, alle zwei Stunden die neuesten Meldungen an die Medien weiterzugeben. Das schafft Transparenz und hält die Medien von eigenen Recherchen mit Spekulationen ab.

Es ist ratsam, die folgenden Handlungsanweisungen bei der Krisenkommunikation unbedingt einzuhalten:[68]

- 1. unverzügliche, transparente, sachgerechte und wahrheitsgetreue Berichterstattung
- 2. Information der Medien und Öffentlichkeit über Ursachen und Auswirkungen der Krise
- 3. aktiv informieren und Informationsstrom nicht abbrechen lassen
- 4. einheitliche Sprachregelung („mit einer Stimme sprechen“)
- 5. Informationsbedürfnis der Öffentlichkeit berücksichtigen und darauf eingehen
- 6. ehrliche Darstellung und klare Problemanalyse
- 7. Krisenvorsorge, Kontakte zu Journalisten und Medien aufbauen und pflegen

VII.3 Evaluierung des Risiko- und Krisenmanagements

Die Qualität des etablierten Risiko- und Krisenmanagements kann im Anschluss an die Umsetzung des Leitfadens anhand der Checklisten im Anhang überprüft werden. Es ist eine regelmäßige Überprüfung und Bewertung des Risiko- und Krisenmanagements empfehlenswert.

[68] Bundesministerium des Innern Juli 2008, Seite 14ff.

Impressum

Herausgeber:
Bundesministerium des Innern
Alt-Moabit 101 D
10559 Berlin

Redaktion:
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Abteilung II – Notfallvorsorge, Kritische Infrastrukturen,
Internationale Angelegenheiten
Provinzialstraße 93
53127 Bonn
www.bbk.bund.de

Gestaltung und Produktion:
MEDIA CONSULTA Deutschland GmbH

Bildnachweis:
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bundesregierung,
hafenarchiv-hamburg.de, iStockphoto

Druck:
Silber Druck oHG, Niestetal

Stand:
Mai 2011

2. Auflage (überarbeitet):
3.500 Exemplare

Die Broschüre ist kostenlos. Sie kann bestellt werden beim:
Publikationsversand der Bundesregierung
Postfach 48 10 09
18132 Rostock
Telefon: 0 18 05–77 80 90
(Festpreis 14 Cent/Min.; abweichende Preise aus den Mobilfunknetzen möglich)
Telefax: 0 18 05–77 80 94
(Festpreis 14 Cent/Min.; abweichende Preise aus den Mobilfunknetzen möglich)
E-Mail: publikationen@bundesregierung.de
Artikelnummer: BMI07326

Nach Lieferung der gewünschten Publikation werden die von Ihnen angegebenen Daten gelöscht.

www.bmi.bund.de