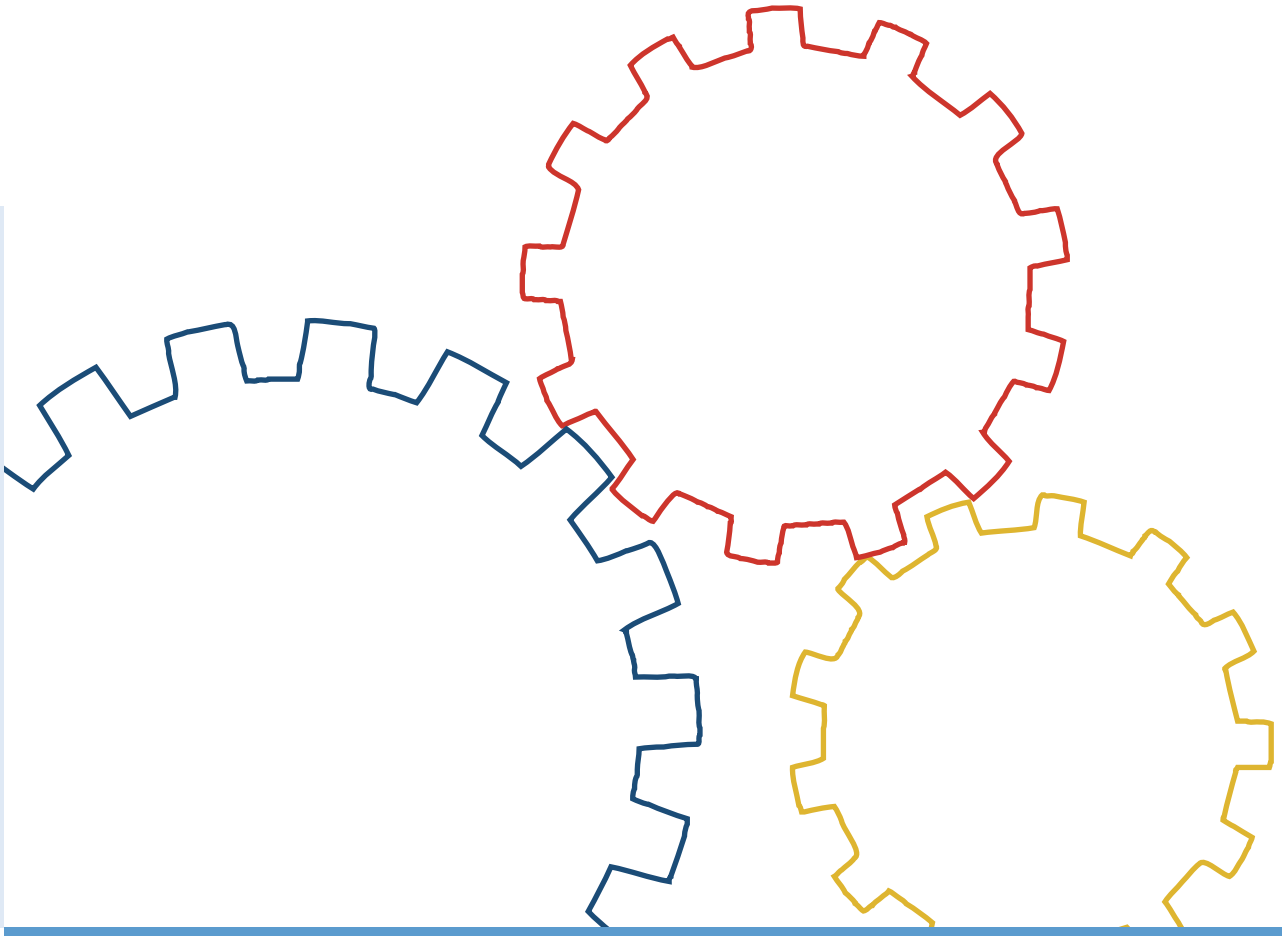
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 100-4

Notfallmanagement



www.bsi.bund.de/gshb

Version 1.0

Inhaltsverzeichnis

1 Einleitung

1.1 Versionshistorie

Stand	Version	Verfasser
November 2008	1.0	BSI

1.2 Zielsetzung

Behörden und Unternehmen sind steigenden Risiken ausgesetzt, die die Produktivität oder die kontinuierliche und zeitnahe Erbringung ihrer Dienstleistungen für die Kunden gefährden. Dazu tragen verschiedene Entwicklungen und Trends in der Gesellschaft und der Wirtschaft bei, wie die wachsende Globalisierung, zunehmende Vernetzung, Zentralisierung, Automatisierung, Outsourcing oder Offshoring (Auslandsverlagerung). Durch die steigende Komplexität der Geschäftsprozesse und deren zunehmenden Abhängigkeit von Informationstechnik und externen Dienstleistern können Ereignisse wie Feuer, Hochwasser oder der Ausfall von Informationstechnik, Dienstleistern, Lieferanten oder Personal große Auswirkungen nach sich ziehen. Zusätzlich nehmen Bedrohungen wie Pandemie, extreme Wetterereignisse oder Terrorismus stetig zu.

Das Notfallmanagement ist ein Managementprozess mit dem Ziel, gravierende Risiken für eine Institution, die das Überleben gefährden, frühzeitig zu erkennen und Maßnahmen dagegen zu etablieren. Um die Funktionsfähigkeit und damit das Überleben eines Unternehmens oder einer Behörde zu sichern, sind geeignete Präventivmaßnahmen zu treffen, die zum einen die Robustheit und Ausfallsicherheit der Geschäftsprozesse erhöhen und zum anderen ein schnelles und zielgerichtetes Reagieren in einem Notfall oder einer Krise ermöglichen. Das Notfallmanagement umfasst das geplante und organisierte Vorgehen, um die Widerstandsfähigkeit der (zeit-)kritischen Geschäftsprozesse einer Institution nachhaltig zu steigern, auf Schadensereignisse angemessen reagieren und die Geschäftstätigkeiten so schnell wie möglich wieder aufnehmen zu können. Das Notfallmanagement wird auch als „Business Continuity Management“ (BCM) oder „betriebliches Kontinuitätsmanagement“ bezeichnet.

Ziel des Notfallmanagements ist es, sicherzustellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz der Institution auch bei einem größeren Schadensereignis gesichert bleibt. Eine ganzheitliche Betrachtung ist daher ausschlaggebend. Es sind alle Aspekte zu betrachten, die zur Fortführung der kritischen Geschäftsprozesse bei Eintritt eines Schadensereignisses erforderlich sind, nicht nur die Ressource Informationstechnik. IT-Notfallmanagement ist ein Teil des Notfallmanagements.

Im vorliegenden BSI-Standard 100-4 wird eine Methodik zur Etablierung und Aufrechterhaltung eines behörden- bzw. unternehmensweiten internen Notfallmanagements vorgestellt. Die hier beschriebene Methodik baut dabei auf der im BSI-Standard 100-2 [BSI2] beschriebenen IT-Grundschutz-Vorgehensweise auf. Bei vollständiger Umsetzung dieses Standards und des korrespondierenden Bausteins in den IT-Grundschutz-Katalogen wird ein Notfallmanagement etabliert, das auch weniger technisch-orientierte Standards wie den British Standard BS 25999 Part 1 und 2 komplett erfüllt.

Der Herausforderung eines Behörden- bzw. Unternehmens-übergreifenden Notfall- oder Krisenmanagements hat sich das Projekt „Schutz Kritischer Infrastrukturen in Deutschland“ [KRI] gestellt und unter anderem in den beiden Plänen „Umsetzungsplan KRITIS“ und „Umsetzungsplan Bund“ konkretisiert. Externes Notfall- und Krisenmanagement im Sinne von Katastrophenschutz ist originäre Aufgabe des „Bundesamt für Bevölkerungsschutz und Katastrophenhilfe“ (BBK) und hat das Ziel, den Bevölkerungs- und Zivilschutz zu garantieren. Beide Gebiete sind nicht Gegenstand dieses BSI-Standards, sondern sind ergänzende Bereiche.

1.3 Adressatenkreis

Dieses Dokument richtet sich an Notfall- bzw. Business Continuity Manager, Krisenstabsmitglieder, Sicherheitsverantwortliche, -beauftragte, -experten und -berater, die mit dem Management von Notfällen und Krisen technischen und nicht-technischen Ursprungs betraut sind. Anwender der in diesem Dokument beschriebenen Methodik sollten mit der IT-Grundschutz-Vorgehensweise, die im BSI-Standard 100-2 beschrieben ist, vertraut sein.

Ein angemessenes Notfallmanagement ist sowohl bei kleinen als auch großen Institutionen erforderlich. Ein effektives und zweckmäßiges Notfallmanagement muss nicht teuer sein. Da kleine und mittlere Institutionen in der Regel weniger komplex, über weniger Standorte verteilt, weniger Geschäftsprozesse haben und weniger Abhängigkeiten unterliegen, sind die Kosten für das Notfallmanagement entsprechend geringer. Doch sind gerade solche Institutionen schon bei geringen Störungen ihrer Geschäftsprozesse oftmals existenziell gefährdet.

Der BSI-Standard 100-4 ist so gefasst, dass die Vorgehensweise von Institutionen beliebiger Art, Größe und Branche genutzt werden kann. Er beschreibt eine vollständige für größere Institutionen ausgerichtete ideale Art und Weise der Umsetzung. Es sollte beachtet werden, dass alle Empfehlungen unter dem Kontext der jeweiligen Institution betrachtet und angemessen umgesetzt werden. Kleine und mittlere Institutionen sollten die essentiellen Teilschritte und –aufgaben angepasst übernehmen.

1.4 Anwendungsweise

Dieses Dokument beschreibt eine Methodik zur Etablierung eines Notfallmanagements, das auf das in BSI-Standard 100-2 [BSI2] beschriebene Vorgehen zur Umsetzung eines Managementsystems für Informationssicherheit aufsetzt und ergänzt. Durch die Verwendung von Informationen, welche bei der Umsetzung von IT-Grundschutz erhoben werden, können Synergieeffekte genutzt und Kostenersparnisse erzielt werden.

Es wird empfohlen, die in den Kapiteln 4 bis 9 dieses Standards beschriebene Methodik Schritt für Schritt anzuwenden. Besonders wird darauf verwiesen, dass Notfallmanagement nicht als Projekt zu betrachten ist, sondern nur bei wiederholter Durchführung der Prozessschritte als wirksam etabliert angesehen werden kann.

Der Begriff „Institution“ wird in diesem Dokument als neutraler Oberbegriff für Unternehmen, Behörden und sonstige öffentliche oder private Organisationen verwendet.

Alle Personalbegriffe in diesem Dokument beziehen sich in gleicher Weise auf Frauen und Männer. Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

1.5 Literaturverzeichnis

[BMIKI] Bundesministerium des Innern (BMI), Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden, www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/Leitfaden__Schutz__kritischer__Infrastrukturen,templateId=raw,property=publicationFile.pdf/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf, Dez. 2007

[BMIKK] BMI, Bundesministerium des Inneren: Krisenkommunikation – Leitfaden für Behörden und Unternehmen, www.bmi.bund.de, 2008

[BSI1] Bundesamt für Sicherheit in der Informationstechnik (BSI), Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.5, Juni 2008, www.bsi.bund.de/

[BSI2] BSI, IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Juni 2008, www.bsi.bund.de/

[BSI3] BSI, Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.5, Juni 2008, www.bsi.bund.de

[BSIHVK] BSI: Hochverfügbarkeitskompendium, Version 1.0, Veröffentlichung 1. Quartal 2009

[BSIKRI] BSI: Schutz Kritischer Infrastrukturen in Deutschland. www.bsi.de/fachthem/kritis/index.htm

[BS259991] British Standards Institute, BS 25999-1:2006 Business Continuity Management, Part 1: Code of practice, www.thebci.org/standards.htm

[BS259992] British Standards Institute, BS 25999-2:2007, Business Continuity Management, Part 2: Specification, www.thebci.org/standards.htm

[GPG08] Business Continuity Institute, Good Practice Guidelines 2008, www.thebci.org/gpgmoreinfo.htm

[GSK] BSI, IT-Grundschutz-Kataloge – Standard-Sicherheitsmaßnahmen, jährlich neu, www.bsi.bund.de/gshb

[HB221] Standards Australia, Business Continuity Management, ISBN 0-7337-6250-6, 2004

[INS24001] Standards Institution of Israel, INS 24001:2007, Security and continuity management systems – Requirements and guidance for use, 2007

[ITIL] Office of Government Commerce, IT Infrastructure Library, Service Management - ITIL (IT Infrastructure Library) www.ogc.gov.uk/guidance_itil.asp, Jan. 2008

[ISO20000] International Organization of Standardization (ISO), ISO/IEC 20000, IT Service-Management; bestehend aus ISO/IEC 20000-1:2005, IT Service-Management - Teil 1: Spezifikation für Service Management ISO/IEC 20000-2:2005, IT Service Management - Teil 2: Allgemeine Verfahrensregeln für Service Management

[ISO22399] ISO, ISO/PAS 22399:2007, Societal security - Guideline for incident preparedness and operational continuity management

[ISO27001] ISO, ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems requirements specification, ISO/IEC JTC1/SC27

[ISO27002] ISO, ISO/IEC 27002:2005 Information technology - Code of practice for information security management, ISO/IEC JTC1/SC27

[NIST34] National Institute of Standards and Technology (NIST), NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, Juni 2002, csrc.nist.gov/publications/nistpubs/

[NFPA1600] National Fire Protection Association, Standard on Disaster/Emergency Management and Business Continuity Programs, 2007, www.nfpa.org

[PAS77] British Standards Institute, PAS 77:2006, IT Service Continuity Management – Code of Practice, www.standardsdirect.org/pas77.htm

[SS540] Singapore Standard, SS 540:2008, Business Continuity Management (BCM), SPRING Singapore, www.spring.gov.sg

2 Notfallmanagement und IT-Grundschutz

2.1 Einordnung in die BSI-Standards

Im BSI-Standard 100-1 [BSI1] werden allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS) festgelegt, zu denen auch generische Anforderungen an ein Notfallmanagement gehören. Im BSI-Standard 100-2 [BSI2] wird die IT-Grundschutz-Vorgehensweise vorgestellt, eine Methode, ein ISMS in der Praxis aufzubauen und zu betreiben. Der Aufbau einer Sicherheitsorganisation und deren Einbettung in die Institution sind dabei wichtige Themen. Dazu gehört auch das Zusammenspiel mit der Aufbauorganisation des Notfallmanagements. Der BSI-Standard 100-3 [BSI3] stellt eine Methode für die Durchführung einer Risikoanalyse vor, die für die Vorgehensweise nach IT-Grundschutz optimiert ist.

Der vorliegende BSI-Standard 100-4 baut auf den vorherigen Standards auf, doch beschreibt er ein eigenständiges Managementsystem für die Geschäftsfortführung und die Notfallbewältigung. Ziel ist es, einen systematischen Weg aufzuzeigen, um bei Notfällen und Krisen der verschiedensten Art und Ursprungs, die zu einer Geschäftsunterbrechung führen können, schnell reagieren zu können. Er beschreibt mehr als IT-Notfallmanagement (IT-Service Continuity Management) und ist daher nicht als Unterbereich des ISMS zu sehen. Der BSI-Standard 100-4 beschreibt, wie die Ergebnisse der klassischen IT-Grundschutz-Vorgehensweise gemäß BSI-Standard 100-2 und der Risikoanalyse gemäß BSI-Standard 100-3 als Basis für angemessene Vorsorge zur Vermeidung von Notfällen wie auch zur Minimierung der Schäden in einem Notfall verwendet werden können. Er verweist auf die Notwendigkeit einer engen Zusammenarbeit mit dem Sicherheitsmanagement, um ein effizientes Notfallmanagement in einer Institution zu etablieren. Je höher die Durchdringung der Geschäftsprozesse mit Informationstechnologie ist, umso stärker können durch die Kooperation mit dem ISMS Synergieeffekte genutzt werden. Eine enge Zusammenarbeit dieser beiden Disziplinen ist aufgrund vieler Überschneidungen zu empfehlen.

Mit der im vorliegenden Standard beschriebenen Business Impact Analyse (BIA) wird ein die Schutzbedarfsfeststellung der IT-Grundschutz-Vorgehensweise ergänzendes Werkzeug eingeführt. Mit Hilfe der BIA werden die kritischen Geschäftsprozesse identifiziert und die Verfügbarkeitsanforderungen an die Prozesse und deren Ressourcen ermittelt.

Der Fokus des Informationssicherheitsmanagements liegt auf dem Schutz der Informationen einer Institution, das Notfallmanagement dagegen fokussiert sich auf die kritischen Geschäftsprozesse. Die Informationen zählen zu den schützenswerten Werten (auch Assets genannt) einer Institution, die kritischen Geschäftsprozesse bilden das Rückgrat. Beiden Managementsystemen ist die ganzheitliche Betrachtungsweise zueigen. Die Treiber des Notfallmanagements sind ebenso wie beim Informationssicherheitsmanagement die Geschäftsbereiche.

2.2 Begriffe

Unterbrechungen von Geschäftsprozessen können unterschiedliche Ursachen und Auswirkungen haben. Um zu verdeutlichen, welche Schadensereignisse im Rahmen eines Notfallmanagements betrachtet werden, folgt hier eine kurze Erläuterung der Begriffe „Störung“, „Notfall“, „Krise“ und „Katastrophe“, wie sie im Rahmen dieses Standards verstanden werden.

Störung

Eine Störung ist eine Situation, in der Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind als gering einzustufen. Ein „geringer“ Schaden ist ein Schaden, welcher im Verhältnis zum Gesamtjahresergebnis eines Unternehmens bzw. zum Haushaltsvolumen einer Behörde zu vernachlässigen ist oder die Aufgabenerfüllung nur unwesentlich beeinträchtigt. Störungen werden durch die im allgemeinen Tagesgeschäft integrierte Störungsbehebung beseitigt. Störungen können sich jedoch zu einem Notfall ausweiten und sind

deshalb genau zu beobachten, sorgfältig zu dokumentieren und zeitnah zu beheben. Dies ist jedoch nicht Teil des Notfallmanagements, sondern Aufgabe des Störungsmanagements.

Notfall

Ein Notfall ist ein Schadensereignis, bei dem Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wieder hergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt. Eventuell vorhandene SLAs (Service Level Agreements) können nicht eingehalten werden. Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf das Gesamtjahresergebnis eines Unternehmens oder die Aufgabenerfüllung einer Behörde auswirken. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation.

Krise

Unter einer Krise wird eine vom Normalzustand abweichende Situation verstanden, die trotz vorbeugender Maßnahmen im Unternehmen bzw. der Behörde jederzeit eintreten und mit der normalen Aufbau- und Ablauforganisation nicht bewältigt werden kann. Das Krisenmanagement wird aktiv. Für die Bewältigung existieren kein Ablaufpläne, sondern lediglich Rahmenanweisungen und –bedingungen. Ein typisches Merkmal einer Krise ist die Einmaligkeit des Ereignisses.

Notfälle, welche die Kontinuität von Geschäftsprozessen beeinträchtigen, können eskalieren und sich zu einer Krise ausweiten. Unter einer Krise wird dann ein verschärfter Notfall verstanden, in dem die Existenz der Institution oder das Leben und die Gesundheit von Personen gefährdet sind. Die Krise konzentriert sich auf das Unternehmen oder die Behörde und beeinträchtigt nicht breitflächig die Umgebung oder das öffentliche Leben. Sie kann, zumindest größtenteils, innerhalb der Institution selbst behoben werden.

Es existiert jedoch eine Vielzahl von Krisen, welche die Geschäftsprozesse nicht direkt betreffen. Beispiele dafür sind Wirtschaftskrisen, Führungskrisen, Liquiditätskrisen, Betrug, Produkterpressung oder -missbrauch, Entführung oder Bombendrohung. Krisen, welche im Rahmen dieses Standards betrachtet werden, stellen eine Untermenge dar.

Katastrophe

Eine Katastrophe ist ein Großschadensereignis, das zeitlich und örtlich kaum begrenzbar ist und großflächige Auswirkungen auf Menschen, Werte und Sachen hat oder haben kann. Die Existenz der Institution oder das Leben und die Gesundheit von Personen sind gefährdet. Auch das öffentliche Leben wird stark beeinträchtigt. Eine Katastrophe kann nicht ausschließlich durch die Institution selbst behoben werden. Durch die geographische Ausbreitung einer Katastrophe und die Auswirkungen für die Bevölkerung ist insbesondere auch der Katastrophenschutz gefordert. Dies ist in Deutschland eine Aufgabe der Länder, die durch den Bund unterstützt und ergänzt werden. Aus der Sicht einer Institution stellt sich eine Katastrophe als Krise dar und wird intern durch die Notfallbewältigung der Institution in Zusammenarbeit mit den externen Hilfsorganisationen bewältigt.

2.3 Weitere Standards für Notfallmanagement

Das Thema Notfallmanagement wird in verschiedenen Normen sowie nationalen und De-facto-Standards behandelt. Einige werden im Folgenden kurz vorgestellt. Die Liste erhebt keinen Anspruch auf Vollständigkeit.

BS 25999-1 / BS 25999-2

Der im November 2006 vom British Standards Institute veröffentlichte BS 25999-1 „Business Continuity Management – Part 1: Code of Practice“ beschreibt den Aufbau eines Management-Systems für das Notfallmanagement [BS259991]. Dazu zählt unter anderem die Organisationsstruktur, die Umsetzung eines Business Continuity Management Prozesses auf Basis von Good Practice

Vorgaben und die Konzeption organisatorischer Maßnahmen. Die detaillierten Arbeitsschritte oder konkrete Maßnahmen für ein Notfallmanagement werden nicht beschrieben. Hierfür wird auf weitere Standards wie ISO 27001, ISO 20000 oder PAS77 verwiesen.

Der britische Standard BS 25999-2 „Business Continuity Management – Part 2: Specification“ legt die Punkte fest, die zur Zertifizierung eines Business Continuity Managements vorhanden sein müssen [BS259992].

Der Kern eines Business Continuity Management nach BS 25999 ist das Programm-Management, das das steuernde Element ist, welches Verantwortlichkeiten zuweist und die permanente Aufrechterhaltung der Geschäftsprozesse sicherstellt. Der Lebenszyklus des BS 25999 besteht aus vier Phasen:

- Umfassendes Verstehen (Transparenz) der eigenen Organisation (z. B. Durchführen einer BIA und Risikoanalyse),
- Entwickeln von BCM-Strategie-Optionen,
- Entwickeln und Implementieren von Reaktionsmaßnahmen und BCM-Plänen und
- Durchführen von BCM-Übungen, Überprüfungen und Weiterentwickeln der BCM-Pläne und -Maßnahmen.

Diese vier Phasen sind durch die Etablierung einer BCM-Kultur in der Institution zu unterstützen.

Good Practice Guidelines (GPG)

Eine weitere BCM-Richtlinie sind die „Good Practice Guidelines” (GPG) des Business Continuity Institute (BCI) [GPG08]. Das BCI wurde 1994 gegründet und hat in mehr als 85 Ländern über 4000 Mitglieder (Stand Februar 2008). Sein Ziel ist es, einen hohen Standard und Kompetenz im Bereich des Business Continuity Management zu setzen.

Im Jahre 2002 wurden zum ersten Mal die „Good Practice Guidelines“ herausgegeben, die von Mitgliedern entwickelt wurden und seitdem regelmäßig aktualisiert und optimiert werden. Die GPG wurden in mehrere Sprachen übersetzt. Die deutsche Übersetzung stammt aus dem Jahre 2005.

Die BCI GPG 2008 sind in sechs Sektionen eingeteilt:

- Sektion 1: BCM Policy & Programme Management (Entwicklen der BCM-Vorgaben und Prozess-Management),
- Sektion 2: Understanding the Organisation (Umfassendes Verstehen der Organisation),
- Sektion 3: Determining BCM Strategy (Festlegen der BCM-Strategie),
- Sektion 4: Developing and Implementing BCM Response (Entwickeln und Implementieren von Reaktionsmaßnahmen),
- Sektion 5: Exercising, Maintaining & Reviewing BCM arrangements (Üben, Betreiben und Überprüfen der BCM-Maßnahmen) und
- Sektion 6: Embedding BCM in the Organisation’s Culture (Einbetten von BCM in der Organisationskultur).

Die GPG des BCI bieten als einer der wenigen Quasi-Standards mit mehr als 120 Seiten eine wirkliche Implementierungshilfe zur Umsetzung eines Business Continuity Managements in einer Institution.

ISO / PAS 22399

Die Vornorm ISO/PAS 22399 „Societal security - Guideline for incident preparedness and operational continuity management“ wurde 2007 veröffentlicht [ISO22399]. Diese Vornorm „Sicherheit und Schutz des Gemeinwesens - Leitfaden für Planung, Vorbereitung und operationelle Kontinuität“ beschreibt in der bekannten generischen Art von ISO-Normen auf 31 Seiten den Prozess und die

Prinzipien für „Incident Preparedness and Operational Continuity Management“ (IPOCM). Der IPOCM-Lifecycle gliedert sich in die Phasen:

- Policy (Richtlinienerstellung),
- Planning (Planung),
- Implementation and operation (Einführung und Betrieb),
- Performance assessment (Performance-Messung) und
- Management review (Überprüfung des Managements),

und beinhaltet alle aus dem BCM-Lifecyle bekannten Teilschritte. Der Begriff „IPOCM“ wird dabei als Erweiterung des Begriffs „BCM“ verstanden.

Die Vornorm basiert auf den Standards NFPA 1600 [NFPA1600], HB 221:2004 [HB221], BS 25999-1:2006 [BS259991], INS 24001:2007 [INS24001] und japanischen Vorschriften. Die Besonderheit ist die Zielgruppe. Es werden Unternehmen adressiert, doch stehen insbesondere private und öffentliche Organisationen sowie die Verwaltung im Fokus.

ISO 27001 / ISO 27002

Aufgrund der Komplexität von Informationstechnik und der Nachfrage nach Zertifizierung sind in den letzten Jahren zahlreiche Anleitungen, Standards und Normen zur Informationssicherheit entstanden. ISO/IEC 27001 "Information technology - Security techniques - Information security management systems requirements specification" [ISO27001] ist die erste internationale Norm zum Management von Informationssicherheit, die auch eine Zertifizierung ermöglicht. ISO/IEC 27001 gibt auf circa 10 Seiten allgemeine Empfehlungen. In einem normativen Anhang wird auf die Sicherheitsempfehlungen (Controls) aus ISO/IEC 27002 verwiesen. Die Leser erhalten jedoch keine Hilfe für die praktische Umsetzung.

Bei der ISO/IEC 27002 (bisher ISO/IEC 17799) "Information technology – Code of practice for information security management" [ISO27002] handelt es sich um eine Sammlung von Erfahrungen, Verfahren und Methoden aus der Praxis. Ihr Ziel ist es, ein Rahmenwerk für das Informationssicherheitsmanagement zu definieren. Die Norm befasst sich daher hauptsächlich mit den erforderlichen Schritten, um ein funktionierendes Sicherheitsmanagement aufzubauen und in der Organisation zu verankern. Die entsprechenden Sicherheitsempfehlungen werden kurz auf den circa 100 Seiten angerissen. Mit dem Thema Business Continuity Management (BCM) beschäftigt sich Kapitel 14 des ISO/IEC 27002. Die fünf Seiten umfassenden Empfehlungen zu BCM im Rahmen des Sicherheitsmanagements sind sehr generisch gehalten und beschreiben auf Management-Ebene die wesentlichen Prozess-Schritte.

NIST SP 800-34

Der vom National Institute of Standards and Technology (NIST) im Jahre 2002 veröffentlichte Standard NIST SP 800-34 "Contingency Planning Guide for Information Technology Systems" ist ein Leitfaden zur Notfallvorsorgeplanung für IT-Systeme [NIST34].

Der Standard NIST SP 800-34 beschreibt auf ca. 60 Seiten eine Methodik zum Aufbau einer IT-Notfallvorsorge-Organisation, der Auswahl und Umsetzung von Maßnahmen zur IT-Notfallvorsorge und Notfallbehebung. In Teilen werden konkrete Lösungsansätze aufgezeigt. Im Anhang befinden sich Vorlagen für zu erstellende Dokumente, wie beispielsweise der Business Impact Analyse oder den IT Contingency Plan.

Der beschriebene Lebenszyklus für das IT-Notfallmanagement besteht aus sieben Phasen:

- Entwickeln einer Leitlinie,
- Durchführen einer Business Impact Analyse,

- Definieren von präventiven Maßnahmen (Notfallvorsorge),
- Entwickeln von Wiederherstellungsstrategien,
- Entwickeln von IT-Notfallplänen,
- Schulen, Üben und Testen von IT-Notfallplänen und
- Aktualisieren der IT-Notfallpläne.

Als Zielgruppe werden primär US-amerikanische Behörden angesprochen. Der Leitfaden ist jedoch für alle Organisationsarten und –größen anwendbar.

PAS 77 / BS 25777

Die Public Available Specification 77:2006 „IT Service Continuity Management - Code of Practice" von der British Standards Institution [PAS77] beschreibt die Prinzipien und Methoden für den Aufbau und die Umsetzung eines IT Service Continuity Managements. Dieser Vor-Standard ist öffentlich verfügbar, jedoch kostenpflichtig. Die PAS 77 kann als ergänzender Part zum BS 25999 für den Bereich Notfallvorsorgeplanung für IT-Services gesehen werden. Er befindet sich aktuell in der Weiterentwicklung zum BS 25777 „ Code of practice for information and communications technology continuity". September 2008 wurde der erste Entwurf mit 38 Seiten zur externen Kommentierung freigegeben und kann kostenpflichtig bezogen werden.

Die Zielgruppe dieser Spezifikation sind die für den Aufbau, die Implementierung und die Aufrechterhaltung des IT Service Continuity verantwortlichen Personen. Ziel ist die Etablierung einer IT-Notfallvorsorge für die kritischen IT-Services. Die entsprechenden Maßnahmen und Pläne sollen Unterbrechungen des IT-Betriebs minimieren bzw. eine rasche Wiederherstellung nach einem Ausfall eines IT-Services gewährleisten.

ISO / IEC 24762

Die Anfang 2008 veröffentlichte Norm ISO/IEC 24762 „Information technology – Security techniques – Guidelines for information and communication technology disaster recovery services" beschäftigt sich mit den Anforderungen an die Wiederanlauf-Services für die Informations- und Kommunikationstechnologie. Die Norm adressiert sowohl interne wie auch externe Service Provider für ICT (Information and Communication Technology) Disaster Recovery (DR) Services und beschreibt die Anforderungen an die Implementierung, den Betrieb, die Überwachung und die Aufrechterhaltung von DR-Services. Die ICT-DR-Services sind Teil des Business Continuity Managements.

ITIL

Die „IT Infrastructure Library" (ITIL) wird vom Office of Government Commerce (OGC), einer britischen Regierungsbehörde, herausgegeben, gepflegt und weiterentwickelt. Die aktuelle Version ITIL V3 ist 2007 erschienen. Sie hat sich inzwischen als weltweit akzeptierter De-facto-Standard für Gestaltung, Implementierung und Management wesentlicher Steuerungsprozesse in der IT etabliert. Es handelt sich dabei um eine Verfahrensbibliothek von Best-Practice-Publikationen, die Methoden für die Planung und Steuerung von IT-Services beschreiben.

Das IT-Service Management ist das zentrale organisatorische Instrument für die Ausrichtung der IT an den Geschäftsanforderungen und für die Steuerung der IT-Services gemäß Kundenanforderungen. Diese Service-Management-Prozesse bilden den Kern von ITIL.

Der IT-Service Continuity Lebenszyklus nach ITIL besteht aus vier Phasen:

- Initiierung des Prozesses: Festlegung der Richtlinien (Policy) und des Umfangs / Geltungsbereichs / IT-Verbunds (Scopes),

- Erfordernisse und Strategie: Business Impact Analysis (BIA), Risikoanalyse und Kontinuitätsstrategie,
- Implementierung: Entwicklung von Kontinuitätsplänen, Wiederherstellungsplänen und Teststrategien,
- Operatives Management: Schulung und Sensibilisierung, Revisionen, Tests und Änderungsmanagement (Change Management).

Das ITIL-Wissen ist in einer Bibliothek von circa 40 englischsprachigen Publikationen verfügbar [ITIL]. Zwei wesentliche Bestandteile von ITIL, die Managementprozesse zur Unterstützung und Lieferung von IT-Services (Service Support, Service Delivery), wurden zudem bereits in einer deutschsprachigen Ausgabe zusammengefasst und überarbeitet.

ISO/IEC 20000

Der Standard ISO/IEC 20000 "IT Service Management" geht auf den British Standard BS 15000 zurück und ermöglicht eine Zertifizierung des IT Service Managements einer Institution. Der Standard besteht aus zwei Teilen. ISO 20000 Part 1 definiert die Mindestanforderungen, die für die Zertifizierung notwendig sind, zusätzliche Anforderungen, Leitlinien und Empfehlungen. Part 2 beinhaltet Best Practices für den Aufbau und Betrieb eines Management-Systems [ISO2000]. Die Implementierungsgrundlagen dafür können aus den ITIL Best Practices abgeleitet werden. Der für IT-Notfallvorsorge relevante Abschnitt “6.3 Service continuity and availability management” legt acht Kontrollziele fest, die zu einer Zertifizierung nach ISO 20000 erfüllt werden müssen. Dies sind:

1. Business plan requirements (Anforderungen aus der Geschäftsplanung),
2. Annual reviews (jährliche Überprüfungen),
3. Re-testing plans (Nachprüfungspläne),
4. Impact of changes (Auswirkungen von Änderungen),
5. Unplanned non-availability (Unplanmäßige Nichtverfügbarkeit),
6. Availability of resources (Verfügbarkeit von Ressourcen),
7. Business needs (Anforderungen der Geschäftsbereiche),
8. Recording tests (Dokumentation der Überprüfungen).

3 Der Notfallmanagement-Prozess

Das Notfallmanagement eines Unternehmens oder einer Behörde ist ein komplexer Prozess, der sowohl die Notfallvorsorge, die Notfallbewältigung wie auch die Notfallnachsorge umfasst. Um einen solchen Prozess etablieren und aufrechterhalten zu können, ist ein effizientes Managementsystem notwendig.

3.1 Überblick

Für die Gestaltung des Notfallmanagements ist ein systematisches Vorgehen erforderlich. Der Notfallmanagement-Prozess besteht aus den folgenden Phasen: Initiierung des Notfallmanagements, Konzeption, Umsetzung des Notfallsvorsorgekonzepts, Notfallbewältigung, Tests und Übungen sowie Aufrechterhaltung und kontinuierliche Verbesserung des Notfallmanagement-Prozesses.

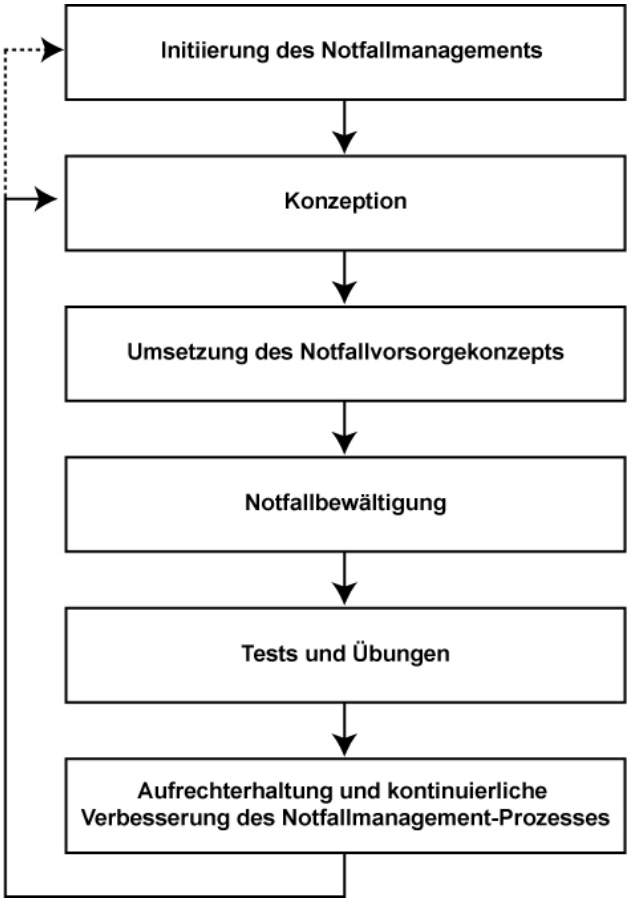


Abbildung 1: Notfallmanagement-Prozess

Bevor ein Notfallmanagement in einer Institution etabliert werden kann, müssen zunächst die Rahmenbedingungen geklärt werden. Es ist eine Leitlinie zum Notfallmanagement zu erstellen, die von der Leitungsebene initiiert, mitentwickelt und freigegeben wird. Zusätzlich sind die organisatorischen Voraussetzungen für das Notfallmanagement zu schaffen. Hierzu müssen die Rollen und Verantwortlichkeiten festgelegt sowie von der Institutionsleitung ein ausreichendes Budget zur Verfügung gestellt werden. Für den Erfolg des Notfallmanagements ist die erfolgreiche Integration des Themas Notfallmanagement in die bestehende Behörden- bzw. Unternehmenskultur ausschlaggebend. Dazu sind die Mitarbeiter in den Prozess mit einzubeziehen und durch Sensibilisierungs- und Schulungsmaßnahmen auf ihre Rollen vorzubereiten.

Grundlage der Konzeption des Notfallmanagements bilden die Informationen, die durch eine sogenannte Business Impact Analyse (BIA) erhoben werden. Im Rahmen der BIA werden die kritischen Geschäftsprozesse der Institution ermittelt und die Prioritäten für den Wiederanlauf festgelegt. Zusätzlich werden die den jeweiligen Geschäftsprozess unterstützenden Ressourcen erhoben und die Mindestanforderungen an einen potenziellen Notbetrieb identifiziert.

Für die ermittelten kritischen Prozessen und Ressourcen wird eine Risikoanalyse durchgeführt. Dabei wird die Frage „Durch was werden meine Prozesse und Ressourcen bedroht?“ beantwortet. Liegen diese Informationen bereits durch andere Managementsysteme vor, kann die Risikoanalyse entfallen.

Auf Basis der Informationen aus der BIA und der Risikoanalyse werden verschiedene Strategieoptionen erarbeitet, aus denen angemessene Kontinuitätsstrategien ausgewählt werden. Diese setzen den Rahmen für die Auswahl der Vorsorgemaßnahmen und den damit verbundenen Investitionen. Anschließend werden die Notfallvorsorgemaßnahmen festgelegt (Notfallvorsorgekonzept) und umgesetzt. Dazu gehört auch die Entwicklung eines Notfallhandbuchs, das die Grundlage und das Hilfsmittel für die Notfallbewältigung bildet.

Zur Aufrechterhaltung und Verbesserung des Notfallmanagements werden Tests und Übungen der Verfahren und Prozeduren, die in den verschiedenen Notfalldokumenten beschrieben werden, Auswertungen der Notfallbewältigung wie auch regelmäßige Überprüfungen durchgeführt. Der dabei ermittelte Änderungs- und Optimierungsbedarf fließt in die stetige Anpassung, Verbesserung und Aktualisierung der Verfahren und der Pläne mit ein. Diese immer wiederkehrende Überarbeitung der Notfallvorsorgemaßnahmen und Notfallplänen sorgt für die permanente Angemessenheit des Notfallmanagements.

3.2 Dokumentation

In den verschiedenen Phasen des Notfallmanagement-Prozesses entstehen verschiedene Konzepte, Prüf- und Testberichte und weitere Dokumente zum Notfallmanagement der Institution. Nur durch eine ausreichende Dokumentation werden getroffene Entscheidungen nachvollziehbar, Handlungen wiederholbar und Schwächen erkannt, so dass sie in Zukunft vermieden werden können.

Die schnelle und effektive Handlungsfähigkeit in einem Notfall hängt entscheidend von der vorhandenen Dokumentation ab. Neben der Qualität und Aktualität der Dokumente spielt auch deren Verfügbarkeit eine entscheidende Rolle. Die in der Notfallbewältigung tätigen Mitarbeiter benötigen schnellen Zugriff auf die für sie relevanten Dokumente.

Beispiele für zu erstellende Dokumente sind:

- Leitlinie zum Notfallmanagement,
- Notfallvorsorgekonzept mit den Berichten zur Business Impact Analyse und Risikoanalyse,
- Notfallhandbuch mit aktuellen Kontaktdaten,
- Übungshandbuch, Übungsplan, Übungskonzepte und -protokolle,
- Schulungs- und Sensibilisierungskonzept,
- Auswertungen von Notfallbewältigungen,
- Revisionsberichte
- sonstige Berichte sowie
- Entscheidungsvorlagen an die Leitungsebene.

3.2.1 Mindestanforderung an die Kennzeichnung der Dokumente zum Notfallmanagement

Die Dokumente, die im Rahmen des Notfallmanagements erstellt, bearbeitet und verwaltet werden, müssen aussagekräftig und für die jeweilige Zielgruppe verständlich sein. Es sollte, soweit sinnvoll, ein einheitlicher Aufbau der Dokumente genutzt werden. Dies dient dem besseren Verständnis und der

einfacheren Handhabung. Die Dokumente müssen so gekennzeichnet sein, dass sie im Bedarfsfall schnell gefunden und zugeordnet werden können. Daher müssen mindestens folgende Angaben vorhanden sein:

- Eindeutige Bezeichnung (aussagekräftiger Titel),
- Ersteller / Autor / Dokumenteninhaber,
- Funktion des Erstellers,
- Versionsnummer,
- letzte Überarbeitung, nächste geplante Überarbeitung,
- freigegeben am / durch,
- Klassifizierung (vertrauliche Inhalte müssen klassifiziert, als solche gekennzeichnet und die Dokumente sicher verwahrt werden) und
- berechtigte Rollen (Verteilerkreis).

Optional können folgende Informationen mit aufgenommen werden:

- Quellenangaben,
- Aufbewahrungszeitraum und
- eine Änderungsübersicht.

3.2.2 Detailtiefe

Für die Detailtiefe der einzelnen Dokumente gilt das Prinzip „dem Ziel und Zweck angemessen". Strategiedokumente, wie die Leitlinie, sollten kurz und prägnant, jedoch aussagekräftig gehalten werden. Die bei der Konzeption anfallenden Dokumente sollten detaillierte Informationen enthalten, um die daraus abgeleiteten Entscheidungen nachvollziehen zu können. Alle Entscheidungen sowie die Informationen, auf denen die Entscheidungen basieren, müssen dokumentiert werden.

Für die Dokumente, die bei der Notfallbewältigung benötigt werden, gilt in besonderem Maße, dass sie klar und verständlich gehalten werden müssen. Der Detaillierungsgrad sollte so sein, dass die Anweisungen für einen sachverständigen Dritten verständlich sind. Ausführliche Handlungsanweisungen für Laien sind hier nicht zu empfehlen, da das Ziel schnelles und zügiges Handeln ist. Oftmals sind für bestimmte Bereiche einfache Checklisten ausreichend. Diese ermöglichen einen schnellen Überblick und helfen dabei, nichts zu vergessen und die Reihenfolge einzelner Schritte einzuhalten.

3.2.3 Änderungsmanagement

Für das Notfallmanagement ist die Aktualität der Informationen von elementarer Bedeutung (z. B. Kontaktinformationen für Meldung und Eskalation oder Ansprechpartner). Um sicherzustellen, dass alle Dokumente zum Notfallmanagement regelmäßig aktualisiert werden, empfiehlt es sich, ein Änderungsmanagement-Verfahren aufzusetzen, mit dem alle Änderungen erfasst, bewertet, freigeben und nachvollzogen werden können. Dazu sind für alle Dokumente klare schriftliche Änderungsmanagement-Anweisungen vorzugeben. Das Verfahren sollte des Weiteren festlegen, wie Anwender Änderungsvorschläge einbringen können und wie diese dann beurteilt und gegebenenfalls berücksichtigt werden. Das Änderungsmanagement des Notfallmanagements ist in das übergreifende Änderungsmanagement der Institution zu integrieren.

Für die Aktualisierung der einzelnen Dokumente sollten Intervalle vorgegeben werden. Für den überwiegenden Teil der Dokumente hat sich eine jährliche Überprüfung bewährt. Für Dokumente, die Angaben zu Personen und Kontaktinformationen enthalten, ist mindestens eine vierteljährliche, besser noch monatliche Überprüfung in Koordination mit den internen Prozessen der Personalverwaltung

anzustreben. Durch die Schnelllebigkeit des heutigen Geschäftslebens empfiehlt es sich, die Business Impact Analyse (BIA) halbjährlich zu überprüfen und gegebenenfalls zu aktualisieren.

Neben den regelmäßigen Überprüfungen sollte auch bei Änderungen von Rahmenbedingungen, Geschäftszielen, Aufgaben oder Strategien eine Aktualisierung der entsprechenden Dokumente veranlasst werden. Es ist sicherzustellen, dass auch kleine, jedoch relevante Änderungen die Anpassung der entsprechenden Dokumente zur Folge hat. Dazu zählen beispielsweise Personalwechsel, Änderungen von Kontaktdaten von im Notfallmanagement involvierten Mitarbeitern, Änderungen in der Raumbelegung, –ausstattung oder IT, sofern es beispielsweise Notfallarbeitsplätze betrifft.

Die Mechanismen, die das Änderungsmanagement anstoßen, sind in die entsprechenden Prozessen (z. B. Personalverwaltung, Hausverwaltung, Inventarisierung) zu integrieren. Der Notfallbeauftragte ist steuernd tätig. Die Verantwortung für die Aktualisierungen und Durchführung der Änderungsanforderungen für ein einzelnes Dokument trägt der jeweilige Dokumenteneigentümer.

3.2.4 Dokumentationsmedium

Dokumente zum Notfallmanagement müssen nicht immer in Papierform vorliegen. Zur Dokumentation können Software-Tools, Internet-Technologien, Notebooks oder auch PDAs genutzt werden. Diese speichern alle nötigen Informationen und sind von verschiedenen Standorten aus nutzbar.

Für das Notfallhandbuch und alle weiteren für die Notfallbewältigung benötigten Unterlagen empfiehlt es sich, diese als Dokumente in Papierform oder/und elektronisch in einem einfachen und gängigen Format (z. B. als PDF- oder HTML-Dateien auf einem USB-Stick inklusive eines entsprechenden Viewers) schnell griffbereit zu halten. Die Lösung muss die Verfügbarkeit im Notfall garantieren, sowohl bei Stromausfall wie auch bei Brandschaden und sonstigen Risiken, die die Dokumente unbrauchbar machen, Daten zerstören oder den Zugriff darauf verhindern können. Daher empfiehlt es sich, Kopien an einem Ausweichort aufzubewahren. Im Krisenfall werden Entscheidungen schnell abgefordert, so dass weder Zeit vorhanden ist, um nach elektronischen Dokumenten auf dem Server oder dem Notfall-Notebook zu suchen, noch um die Dokumente an einer weiter entfernten Lokation abzuholen. Auch die Nutzung von Software-Tools zur Verwaltung der Notfalldokumente, die selten oder nie genutzt werden, kann zusätzlichen Stress erzeugen oder von der eigentlichen Aufgabe ablenken. Es gilt, in Stresssituationen dem Nutzer zusätzliche Sicherheit zu geben.

Das Dokumentationsmedium sollte daher je nach Bedarf (z. B. Lesend oder zur Dokumentation), Phase (Notfallvorsorge oder Notfallbewältigung) oder Teilaufgabe gewählt werden. Auch die Zielpersonen der Dokumente und deren Vertrautheit mit den unterschiedlichen Medien sollte in die Überlegung eingeschlossen werden. Während die einen die Arbeit mit Papier bevorzugen, ist für die anderen das einfache Suchen oder Filtern in elektronischen Dokumenten unverzichtbar.

3.3 Sicherheit und Datenschutz

Da die Dokumente zum Notfallmanagement sowohl sensitive Daten über die Institution als auch personenbezogene Daten beinhalten, muss die Informationssicherheit und der Datenschutz gewährleistet werden. Neben der Verfügbarkeit ist auch die Integrität und insbesondere die Vertraulichkeit der Dokumente zu garantieren. Die verschiedenen Dokumente des Notfallmanagements sollten in Bezug auf ihre Vertraulichkeit eingestuft, entsprechend gekennzeichnet und durch geeignete Maßnahmen geschützt werden.

Die jeweils berechtigten Empfänger sollten in den Dokumenten genannt werden. Der Zugriff auf die Dokumente ist auf die Personen zu beschränken, die die enthaltenen Informationen für ihre Tätigkeit benötigen („Need-to-know-Prinzip“). Eine sinnvolle Modularisierung der Dokumente ist daher empfehlenswert. Das ermöglicht eine auf die Empfänger ausgerichtete Verteilung der Informationen. Es sollte in der Institution einen Überblick über die Anzahl der klassifizierten Dokumente, deren Art (z. B. Papier oder CD) und deren Verteilung geben, wie auch über deren korrekte und vollständige Aktualisierung und Vernichtung bzw. Rücknahme.

Für das Notfallhandbuch und alle weiteren für die Notfallbewältigung benötigten Unterlagen gelten sehr hohe Anforderungen an die Verfügbarkeit (siehe auch Kap. 3.2.4), doch ist die Vertraulichkeit dabei nicht zu vernachlässigen. Beispielsweise ist der Einsatz von USB-Sticks als Speichermedium für Notfallpläne eine gute Wahl, um die schnelle Verfügbarkeit zu garantieren, doch ohne zusätzliche Sicherheitsmaßnahmen, die die Vertraulichkeit gewährleisten, nicht zu empfehlen. Es gilt, Maßnahmen auszuwählen, die die Vertraulichkeit garantieren, aber im Notfall und der Krise die Verfügbarkeit nicht einschränken. Es können sowohl Spezial-Hardware (z. B. Einsatz biometrischer Systeme) für den Zugriffsschutz oder zur Verschlüsselung wie auch Softwarelösungen zum Einsatz kommen, jedoch sollten die Risiken eines Ausfalls dieser Lösung in Notfällen vorab untersucht werden. So kann beispielsweise ein möglicher Ausfall einer benötigten, über das Internet oder Intranet verfügbaren PKI (Public Key Infrastruktur) problematisch sein oder auch die falsche Rückweisung eines autorisierten Benutzers (False Rejection) am Fingerabdruckleser durch feuchte Finger in der Stresssituation.

4 Initiierung des Notfallmanagement-Prozesses

Das oberste Ziel des Notfallmanagements ist es, kritische Geschäftsprozesse aufrecht zu erhalten und die Auswirkungen von Schadensereignissen auf die Institution so gering wie möglich zu halten. Um dieses zu erreichen, sind strategische Entscheidungen zu treffen, Organisationsstrukturen zu etablieren und Maßnahmen umzusetzen. Die ersten Schritte in der Initiierungsphase sind die Übernahme der Verantwortung durch die Behörden- bzw. Unternehmensleitung und die Entwicklung von Leitaussagen zum Notfallmanagement.

4.1 Übernahme von Verantwortung durch die Leitungsebene

Aufgrund der Bedeutung und der weitreichenden Konsequenzen der zu treffenden Entscheidungen muss der Prozess „Notfallmanagement“ von der obersten Leitungsebene der Institution initiiert, gesteuert und kontrolliert werden. Daher ist es von Bedeutung, dass sich diese aktiv mit der Notwendigkeit eines Notfallmanagements für die Institution auseinandersetzt. Die Gründe für eine Einführung eines Notfallmanagements in der Institution sollte der Leitungsebene vermittelt werden.

Die Verantwortung für ein Notfallmanagement ist, ebenso wie beim Informationssicherheitsmanagement [BSI2], auf der obersten Leitungsebene der Institution zu etablieren. Diese ist verantwortlich dafür, dass alle Geschäftsbereiche zielgerichtet und ordnungsgemäß funktionieren und dass Risiken erkannt, reduziert und die Auswirkungen auf die Institution bei Eintreten eines Schadensereignisses minimiert werden.

Ein Mitglied der obersten Leitungsebene sollte als Prozesseigentümer des Notfallmanagements benannt werden, der die volle Verantwortung trägt. Dieses Mitglied der Leitungsebene stellt sicher, dass ein Notfallmanagement in der Institution etabliert und die Vorgaben der Leitlinie eingehalten werden. Dabei sind je nach Organisationsform und Branche verschiedene gesetzliche Regelungen zu beachten.

Die Aufgabe, das Notfallmanagement aufzubauen und aufrecht zu erhalten, wird durch die Leitungsebene typischerweise an einen Notfallbeauftragten delegiert. Eine intensive Beteiligung der Leitungsebene, sowohl bei der Konzeption als auch bei der Bewältigung von Notfällen, ist jedoch erforderlich, da durch strategische Entscheidungen sichergestellt werden muss, dass keine untragbaren Risiken unberücksichtigt bleiben und Ressourcen an der richtigen Stelle investiert werden. Selbst wenn einzelne Aufgaben im Rahmen des Notfallmanagements an Personen oder Organisationseinheiten delegiert werden, die dann für die Umsetzung zuständig sind, verbleibt die nicht delegierbare Gesamtverantwortung bei der Institutionsleitung.

Die Leitungsebene muss dafür sorgen, dass ausreichende Ressourcen (Personal, Zeit, Finanzmittel) für das Notfallmanagement bereitgestellt werden. Sie trägt die Verantwortung dafür, dass die Aspekte des Notfallmanagements in alle relevanten Geschäftsprozesse bzw. Fachverfahren integriert werden und die einzelnen Organisationseinheiten das Notfallmanagement unterstützen.

4.2 Konzeption und Planung des Notfallmanagement-Prozesses

Die Etablierung eines Notfallmanagement-Prozesses ist ein Projekt, das geplant werden muss. Um den Aufwand abschätzen und eine Zeit- und Ressourcenplanung durchführen zu können, sind die Ziele für das Notfallmanagement zu definieren, der Geltungsbereich festzulegen, die Rahmenbedingungen zu ermitteln und die Strategie, mit der die Ziele erreicht werden sollen, festzulegen.

4.2.1 Definition des Notfallmanagements

Die Institutionsleitung muss festlegen, was unter Notfallmanagement verstanden wird und welche Aufgaben und Kompetenzen das Notfallmanagement umfasst. Da in einer Institution in der Regel weitere Managementsysteme wie beispielsweise das IT-Management, das Informationssicherheitsmanagement, das Gebäudemanagement, das Qualitätsmanagement oder das Risikomanagement

etabliert sind, die Schnittstellen oder Überschneidungen zum Notfallmanagement aufweisen, sollten diese ermittelt werden. Die entsprechenden Schnittstellen, Zuständigkeiten und gegebenenfalls Rechte und Pflichten der verschiedenen Disziplinen sollten eindeutig festgelegt und dokumentiert werden.

4.2.2 Festlegung des Geltungsbereichs

Der Geltungsbereich des Notfallmanagements sollte eindeutig festgelegt werden. Dieser kann die gesamte Institution inklusive aller Standorte umfassen, einzelne Standorte oder in Ausnahmefällen auch einzelne Teilbereiche. Der Geltungsbereich sollte in sich abgeschlossen, nicht zu eng gefasst sein und die Wert schöpfenden Geschäftsprozesse bzw. relevanten Fachaufgaben wie auch die relevanten Ressourcen und die benötigten unterstützenden Prozesse vollständig enthalten. Eine Beschreibung des Geltungsbereichs sollte eventuell vorgenommene Einschränkungen und Grenzen des Notfallmanagements enthalten. Optional können die wesentlichen Geschäftsprozesse bzw. Fachaufgaben innerhalb des Geltungsbereichs hervorgehoben werden.

Da das Ziel des Notfallmanagements ist, die Überlebensfähigkeit der Institution zu stabilisieren und zu sichern, ist eine Betrachtung der gesamten Institution anzustreben. Nur so kann ein wirksamer Schutz des Ansehens und der wertschöpfenden Tätigkeiten der Institution und damit der Interessen der wichtigsten Interessensgruppen gewährleistet werden.

4.2.3 Rechtliche Anforderungen und sonstige Vorgaben

Es sind alle relevanten Gesetze, Richtlinien und Vorschriften, die für das Notfallmanagement von Bedeutung sind, zu ermitteln. Um die rechtlich relevanten Anforderungen für die Institution identifizieren zu können, sollte daher zunächst immer die aktuelle Gesetzeslage geprüft werden. Es existiert eine Vielzahl von bereichsspezifischen Vorgaben und branchenspezifische relevante Standards, die gegebenenfalls zu beachten sind. Welche das jeweils sind, hängt unter anderem von der Organisationsform der Institution, der Branche und der Art der Geschäftsprozesse ab. Rechtliche Anforderungen zum Notfallmanagement ergeben sich beispielsweise aus dem Sarbanes-Oxley Act, dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), der Baseler Eigenkapitalvereinbarungen (Basel II), dem Aktiengesetz (AktG), dem Post- und Telekommunikationssicherstellungsgesetz (PTSG), dem Börsengesetz (BörsG), dem Arbeitsschutzgesetz (ArbSchG), der Störfallverordnung (12. BImSchV – StörfallV), der Gefahrstoffverordnung (GefStoffV) oder der Betriebssicherheitsverordnung (BetrSichV).

4.2.4 Zielsetzung und Anforderung an das Notfallmanagement

Die Institutionsleitung hat die strategischen Ziele festzulegen, die mit dem Aufbau und dem Betrieb des Notfallmanagements verfolgt werden. Zur Notfallmanagementstrategie, oder kurz Notfallstrategie, zählen unter anderem

- die Festlegungen, welche Geschäftsziele geschützt werden sollen,
- welche Schadensszenarien ausschlaggebend sind,
- welche Arten von Geschäftsunterbrechungen als Existenz bedrohend angesehen werden,
- welche Bereitschaft besteht, Risiken einzugehen (Risikoappetit), bzw. wie hoch das Risikoakzeptanzniveau für das Unternehmen oder die Behörde liegt,
- in welcher Art und Größenordnung etwas dagegen unternommen werden soll und
- was bei der Notfallbehandlung primäres Ziel ist.

So könnte beispielsweise in der Notfallstrategie festgelegt werden, dass die Abwicklung bestehender Aufträge im Vordergrund steht und kein Neugeschäft angenommen wird, dass alle Geschäftsprozesse mit mindestens 50% der Leistungsfähigkeit oder des Durchsatzes funktionieren sollen, oder dass das primäre Ziel bei der Notfallbehandlung ist, die Ausbreitung des Schadens zu verhindern, insbesondere das Überspringen auf Geschäftspartner, und dies noch vor dem schnellst möglichen Wiederanlauf steht.

Die diesbezüglichen Anforderungen an das Notfallmanagement lassen sich aus den Geschäftsprozessen bzw. Fachaufgaben, den gesetzlichen Rahmenbedingungen und insbesondere den jeweiligen Behörden- bzw. Unternehmenszielen ableiten. Auch kann eine sogenannte Stakeholder-Analyse hilfreich sein. Dabei werden die wichtigsten Interessensgruppen, die Key Stakeholder, identifiziert, die Interesse am und damit Einfluss auf das Notfallmanagement der Institution haben können, sei es aus Eigeninteresse oder um die Interessen Dritter wie der Gesellschaft zu wahren. Zu den möglichen Interessensgruppen zählen beispielsweise Anteilseigner, die Mitarbeiter und deren Angehörigen, Investoren, Kunden, Lieferanten aber auch Versicherer, Aufsichtbehörden, Branchenverbände oder Gesetzgeber.

4.2.5 Planungsprinzip

Der Aufwand, ein Notfallmanagement-Prozess zu konzipieren und zu etablieren, sollte nicht unterschätzt werden. Um die Übersicht und die Motivation dabei nicht zu verlieren, sollten realistische Ziele gesetzt und der Aufbau gegebenenfalls in mehreren Stufen erfolgen. Es empfiehlt sich, sinnvolle Zwischenziele und erreichbare Meilensteine zu setzen. So könnte in einer ersten Stufe eine Fokussierung auf die essentiellen Prozesse erfolgen und die einzelnen Prozessschritte nicht bis in die tiefsten Details ausgefeilt werden. Ist ein erstes Niveau des Notfallmanagements erreicht, erfolgt innerhalb des Notfallprozesses eine kontinuierliche Verbesserung und Anhebung auf höhere Reifegrade durch Verbesserung der Methoden, Ausdehnung der einbezogenen Geschäftsprozesse und einer höheren Detaillierung der einzelnen Prozessschritte.

4.3 Schaffung organisatorischer Voraussetzungen

Das Notfallmanagement kann in die Bereiche Notfallvorsorge und Notfallbewältigung unterteilt werden. Die Notfallvorsorge ist proaktiv tätig, die Notfallbewältigung nach Eintreten eines Notfalls reaktiv.

Beim Notfallmanagement können drei Verantwortungsbereiche unterschieden werden:

- Strategischer Bereich (im angelsächsischen Sprachraum auch als „Gold Team“ bezeichnet),
- Taktischer Bereich („Silber Team“) und
- Operativer Bereich („Bronze Team“).

Der strategische Verantwortungsbereich umfasst die Gesamtverantwortung für die unternehmerischen oder planerischen Handlungen zur Erreichung der Ziele der Institution und ist daher auf der Leitungsebene zu etablieren. Der taktische Verantwortungsbereich beinhaltet die Umsetzung der strategischen Vorgaben für die Organisationseinheiten. Der operative Verantwortungsbereich setzt die Vorgaben der strategischen und taktischen Ebene um.

Die folgende Abbildung gibt einen Überblick über die Rollen in den drei Verantwortungsbereichen und den beiden Phasen Notfallvorsorge und Notfallbewältigung. Die in den beiden folgenden Unterkapiteln enthaltenen Beschreibungen umfassen deren Aufgaben, Verantwortungen, Kompetenzen und Befugnisse.

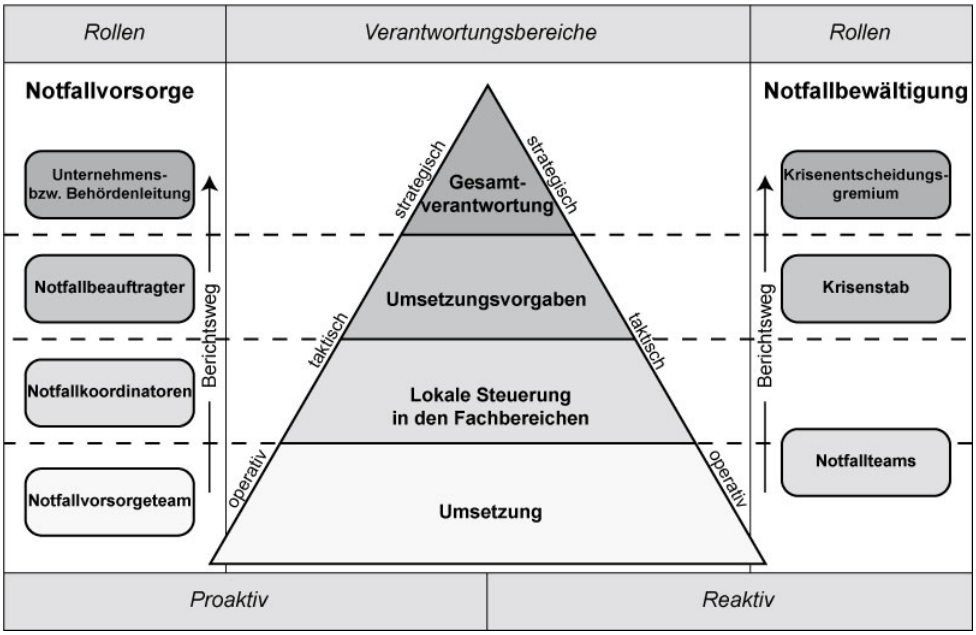


Abbildung 2: Rollen und Verantwortungsbereiche

Nicht jede beschriebene Rolle wird in jeder Institution benötigt. Dies ist von der Größe der Institution, der logischen Organisationsstruktur und der geographischen Verteilung der Organisationseinheiten abhängig. Die Auswahl und Besetzung muss individuell und geeignet gewählt werden. Die gewählte Struktur sollte eindeutig dokumentiert werden. Die Besetzung mehrerer Rollen in Personalunion ist unter der Bedingung möglich, dass der entsprechende Mitarbeiter über die erforderlichen Qualifikationen verfügt und genügend zeitliche Ressourcen zur Verfügung hat. Auch erfordern nicht alle Rollen eine Vollzeitstelle, sondern können als zusätzliche Aufgaben wahrgenommen werden, insbesondere bei kleinen und mittleren Institutionen.

4.3.1 Rollen in der Notfallvorsorgeorganisation

Unternehmens- bzw. Behördenleitung

Die Unternehmens- bzw. Behördenleitung ist für die institutionsweite Sicherstellung des Notfallmanagements verantwortlich. Sie legt die Bedeutung des Notfallmanagements in der Institution fest, bestimmt die strategische Ausrichtung bei der Etablierung und stellt die notwendigen finanziellen und personellen Ressourcen nach wirtschaftlichen Ansätzen zur Verfügung. Die Institutionsleitung beauftragt und ermächtigt den Notfallbeauftragten mit der Planung und Koordinierung aller Aufgaben im Rahmen des Notfallmanagement-Prozesses.

Der Notfallbeauftragte

Der Notfallbeauftragte steuert alle Aktivitäten rund um die Notfallvorsorge und wirkt bei den damit verbundenen Aufgaben mit. Er ist für die Erstellung, Umsetzung, Pflege und Betreuung des institutionsweiten Notfallmanagements und der zugehörigen Dokumente und Regelungen zuständig. Der Notfallbeauftragte koordiniert in Abstimmung mit der Institutionsleitung die Bereitstellung der Ressourcen für die Mitarbeitergruppen, die im Rahmen der Notfallvorsorgeplanung sowie bei Eintritt von Notfällen mitwirken. Er koordiniert die Erstellung des Notfallvorsorgekonzepts und des Notfallhandbuches. Er überprüft die Umsetzung der Maßnahmen, plant Notfallübungen und stimmt die Planung mit der Institutionsleitung ab. Er analysiert den Gesamtablauf der Notfallbewältigung nach einem Schadensereignis, ist verantwortlich für die Auswertung der Übungsergebnisse und erarbeitet in Zusammenarbeit mit den verschiedenen Organisationseinheiten Maßnahmen zur Beseitigung von Mängeln oder Verbesserung des Prozesses. Er benennt Verantwortliche für deren Umsetzung und kontrolliert diese. In seiner Verantwortung liegt die konzeptkonforme Aufrechterhaltung des Notfall-

managements. Änderungen jeglicher Notfalldokumentationen werden unter seiner Verantwortung genehmigt.

Der Notfallbeauftragte ist gegenüber der Institutionsleitung berichtspflichtig. Falls zusätzlich Notfallkoordinatoren eingesetzt sind, initiiert und leitet der Notfallbeauftragte regelmäßige Gremienveranstaltungen. Verteilt arbeitende Notfallkoordinatoren werden durch den Notfallbeauftragten koordiniert. Er ist gegenüber diesen im Rahmen der Notfall-Vorsorgeplanung weisungsbefugt. Der Notfallbeauftragte macht Vorgaben zu Verfahrensweisen, gibt Muster vor, fügt die Arbeiten der Notfallkoordinatoren zusammen und konsolidiert sie zu einem Gesamtergebnis für die Institution.

Es darf nicht vergessen werden, dass der Notfallbeauftragte einen qualifizierten Vertreter benötigt, der stets gut über den aktuellen Sachstand informiert sein sollte.

Notfallkoordinatoren

In größeren Institutionen kann der Notfallbeauftragte durch zusätzliche Notfallkoordinatoren unterstützt werden. Ob und wie viele Notfallkoordinatoren ernannt werden, hängt von der Art und Größe der jeweiligen Institution ab. Es empfiehlt sich, für jede größere logische Organisationseinheit einen Notfallkoordinator zu benennen. Organisationseinheiten können einzelne Standorte oder Regionen der Institution umfassen oder durch die logische Struktur der Institution gebildet werden.

Ein Notfallkoordinator versteht sich als Bindeglied zwischen dem Notfallbeauftragten und der ihm zugewiesenen Organisationseinheit. Er arbeitet eigenverantwortlich und führt die Aktivitäten des Notfallmanagements für seine Organisationseinheit durch. Dazu zählen sowohl die Durchführung der Business Impact Analyse, die fachlich korrekte Erstellung der Geschäftsfortführungspläne als auch die konsequente Festlegung und Umsetzung angemessener Maßnahmen in seiner Organisationseinheit. Der Notfallkoordinator wirkt an der Vorbereitung, Durchführung und Nacharbeitung von Tests und Übungen seines Bereichs mit. Er analysiert die Ergebnisse von regelmäßigen Überprüfungen der Funktionsfähigkeit und Aktualität der Notfalldokumentationen und erarbeitet bei Bedarf Verbesserungen (Überprüfung der Notfallvorsorgeplanung) für seinen Bereich. Er berichtet eigenverantwortlich in regelmäßigen Gremienveranstaltungen an den Notfallbeauftragten und unterstützt diesen bei der Vorbereitung von Entscheidungsvorlagen für die Institutionsleitung.

Notfallvorsorgeteam

Ausgewählte Experten aus den Organisationseinheiten oder für fachbezogene Fragen arbeiten temporär im Notfallvorsorgeteam mit. Sie beraten die Notfallkoordinatoren oder den Notfallbeauftragten zu speziellen Themen oder setzen die Vorgaben und Maßnahmen der strategischen Notfallvorsorgeplanung um. Gegebenenfalls nehmen sie an der Vorbereitung, Durchführung und Nacharbeitung von Tests und Übungen teil.

4.3.2 Rollen in der Notfallbewältigungsorganisation

Die Bewältigung von Notfällen oder Krisen erfordert eine gesonderte Aufbauorganisation, die je nach Art, Umfang und Schwere der Ausnahmesituation in unterschiedlicher Konstellation zusammengesetzt wird. Die Rollen für die Notfallbewältigungsorganisation sind mit ihren Aufgaben, Zuständigkeiten, Verantwortungen, Informationspflichten, Eskalationsstufen aber auch Rechten eindeutig festzulegen und zu dokumentieren. Die Besetzung der Rollen durch Mitarbeiter sollte nach Eignung erfolgen und nicht nach hierarchischer Position in der Institution, da besondere Anforderungen bezüglich physischer und psychischer Belastungen in den extremen Ausnahmesituationen an diese Mitarbeiter gestellt werden. Nicht alle Funktionsträger sind automatisch auch gute Strategen unter hoher Belastung und können im Extremfall die Arbeit eines Krisenstabs daher eher behindern als fördern. Mitglieder der Leitungsebene sind es gewohnt, die vollständige Kontrolle über die Situation zu haben, Entscheidungen vollständig durchzudenken und die Folgen abwägen zu können. Die Grenzerfahrung des “Kontrollverlusts“ in einer Krisensituation oder schnelle Entscheidungen treffen zu müssen, deren Konsequenzen für die eigene Position und Karriere nicht absehbar sind, kann daher zu einem Gefühl der persönlicher Bedrohung bis hin zur völligen Handlungsunfähigkeit führen.

Übernehmen Mitarbeiter einzelne Rollen in der Notfallbewältigung, so sollte in ihren Arbeitsverträgen oder entsprechenden Zusatzverträgen ein Haftungsausschluss oder eine Haftungseinschränkung für den Krisenfall vereinbart werden.

Da Notfall- und Krisensituationen ein schnelles Handeln erfordern, dieses aber eventuell durch besondere Umstände behindert wird, sollten jeweils ein oder gar mehrere Stellvertreter benannt werden.

Krisenentscheidungsgremium

Der strategische Verantwortungsbereich der Notfallbewältigung wird durch das Krisenentscheidungsgremium abgedeckt. Dieses wird üblicherweise durch einen oder mehrere Vertreter der obersten Führungsebene wie Vorstandmitglieder, die Geschäftsführungsebene oder die Amtsleitung in Behörden gestellt. Im Krisenentscheidungsgremium befinden sich die „Denker“, die die strategische Richtung in der Krise vorgeben und weitreichende Entscheidungen treffen, welche über die festgelegte Kompetenzen des Krisenstabsleiters gehen. Dazu zählen beispielsweise strategische Entscheidungen in Krisen, die über den Geltungsbereich des Notfallmanagements hinausgehen, oder Geschäftsfortführungsstrategien, die längerfristige Auswirkungen auf die Institution haben können (z. B. vollständige Einstellung eines Prozesses). Eine weitere Aufgabe des Krisenentscheidungsgremiums während der Notfallbewältigung ist, gegebenenfalls die Verbindung zu den wichtigsten Interessensgruppen herzustellen und zu halten.

Die eigentliche Durchführung der Krisenarbeit sollte jedoch dem Krisenstab überlassen werden. Wie eng das Krisenentscheidungsgremium an den Krisenstab angegliedert ist, hängt von der Art der Institution und deren Größe ab. In manchen, insbesondere kleineren Institutionen, ist die Trennung aufgehoben und das Krisenentscheidungsgremium wird durch einen Vertreter der obersten Leitung im Krisenstab repräsentiert.

Krisenstab

Das zentrale Führungsgremium der Notfallbewältigung ist der Krisenstab. Der Begriff „Krisenstab“ hat sich für dieses Gremium eingebürgert, unabhängig davon, ob es einen Notfall oder eine Krise zu bewältigen gilt. Daher wird auch in diesem Dokument dieser Begriff verwendet.

Der Krisenstab ist ein planendes, koordinierendes, informierendes, beratendes und unterstützendes Organ. Er stellt eine besondere temporäre Aufbauorganisation dar, die die normale Aufbauorganisation zur Bewältigung eines Notfalls durchbricht und abteilungsübergreifende Kompetenzen bündelt. Der Krisenstab funktioniert auf einer hierarchielosen Entscheidungsebene, das bedeutet, alle Stabsmitglieder sind hierarchisch gleichgestellt. Er plant, koordiniert, veranlasst und überwacht die Aktivitäten der Notfallbewältigung und steuert die Bereitstellung aller relevanter Informationen und Ressourcen zur Bewältigung des Schadensereignisses.

Der Krisenstab setzt sich aus einem Leiter, einem Kernteam und einem erweiterten Krisenstabsteam zusammen. Er wird gegebenenfalls durch weitere Fachberater ergänzt. Wie ein Krisenstab im Detail aufgebaut ist, hängt vor allem von der Art, Struktur und Größe der Institution ab. Die Zusammenstellung des Krisenstabs in einer Krise hängt von der Art der Krise ab. Es sollte jedoch gelten: „so klein wie möglich und so ausbaufähig wie nötig“.

Die folgenden Aufgaben sollten in jedem Krisenstab wahrgenommen werden, unabhängig von den Aufgaben der Einrichtung:

- Die Situation muss erfasst und bewertet werden. Alle wichtigen Informationen müssen regelmäßig aktualisiert werden.
- Aufträge zur Notfall-Behebung müssen an die zuständigen Instanzen erteilt und die hierfür erforderlichen Aktivitäten koordiniert werden.
- Die Pressearbeit und die interne Kommunikation müssen koordiniert werden (Krisenkommunikation).

- Die Abstimmung der einzelnen Maßnahmen muss geregelt werden.

Für jedes Mitglied sollte mindestens ein Stellvertreter vorgesehen werden, bei leitenden Funktionen mindestens zwei. Für den Krisenstabsleiter gehen die Empfehlungen bis zu vier Stellvertreter. Die zentrale Anforderung ist, dass der Krisenstab ad hoc handlungsfähig sein muss.

Leiter und Kernteam des Krisenstabs

Das Kernteam wird durch den Krisenstabsleiter und ein bis maximal fünf wichtige Funktionsträger gebildet. Diese sind die ständigen Mitglieder des Teams. Der Leiter des Krisenstabs trifft alle Entscheidungen im Rahmen der Notfallbewältigung. Seine weitreichenden Kompetenzen, der Finanz- und Rechtsrahmen, in dem er agieren kann, sind im Vorfeld festzulegen und treten mit Ausrufung des Notfalls in Kraft.

Ist der Notfall ausgerufen, so entscheidet der Krisenstabsleiter über den Umfang und die ereignisabhängige Zusammensetzung des einzuberufenden Krisenstabs. Er legt den Ort für die Krisenstabsarbeit, den Krisenstabsraum sowie die von der Krise betroffenen Organisationsbereiche der Institution fest, denn nur für diese ist der Krisenstab weisungsbefugt. In nicht betroffenen Organisationseinheiten gilt die normale Kompetenz der Linienorganisation weiter. Für den Fall, dass der Leiter nicht erreichbar sein sollte, ist eine Stellvertreterregelung zu treffen, die in der Regel innerhalb des Krisenstabs erfolgt.

Um in einem Notfall eine erfahrene und koordinierte Vorgehensweise sicherzustellen, sollten im Kernteam möglichst dieselben Personen über einen längeren Zeitraum vertreten sein. Es hat sich bewährt, folgende Funktionen in das Kernteam aufzunehmen:

- die Öffentlichkeitsarbeit vertreten durch die Behörden- bzw. Unternehmenskommunikation sowie
- die Behörden- bzw. Unternehmenssicherheit bestehend aus Informationssicherheit wie auch Betriebssicherheit (also Safety und Security).

Je nach Ausprägung der Institution kann auch ein Vertreter des IT-Betriebs zum Kernteam gehören.

Da die Mitglieder des Krisenstabs in extremen Ausnahmesituationen besonnen und gezielt handeln und dabei viele heikle Aspekte sowie sich ständig ändernde Faktoren gegeneinander abwägen müssen, sollten sie sorgfältig ausgewählt und entsprechend geschult werden. Der Leiter des Krisenstabes sollte die Eigenschaft einer starken Führungspersönlichkeit haben, in Extremsituationen hoch belastbar und stressresistent sein sowie unter Zeitdruck Entscheidungsfreudigkeit bewiesen haben. Teamfähigkeit und soziale Kompetenz sind weitere Eigenschaften, die den Leiter des Krisenstabes auszeichnen sollten.

Erweiterter Krisenstab

Der erweiterte Krisenstab besteht aus designierten Spezialfunktionen oder Unterstützungsgruppen, die je nach Art des Notfalls für den erweiterten Krisenstab aktiviert werden. Daher spricht man auch von den ereignisspezifischen Mitgliedern des Stabes. Dazu zählen beispielsweise:

- IT-Administration / IT-Leiter (sofern nicht schon im Kernteam),
- Standortsicherheit, z. B. Brandschutzbeauftragter, Umweltschutz, Anlagensicherheit, Rettungsdienst,
- Leiter CERT, falls ein CERT (Computer Emergency Response Team) vorhanden ist,
- Justitiariat,
- Personalvertretung,
- Ansprechpartner betroffener Abteilungen und Geschäftsprozesse, z. B. Vertrieb, Logistik, etc.,
- Ansprechpartner aus den Bereichen Beschaffung, Finanzen, Haustechnik, Innerer Dienst, Organisation, Personal,

- Datenschutzbeauftragter sowie
- Geheimschutzbeauftragter.

Eine Sonderstellung nimmt der Notfallbeauftragte ein, der den Krisenstab unterstützt und insbesondere in Fragen der Notfallplanung berät. Neben den Fachvertretern sollte es im Krisenstab ein Sekretariat (Krisenstabsassistenz) zur administrativen Unterstützung sowie einen Protokollführer zur revisionssicheren Protokollierung aller Ereignisse und Entscheidungen geben.

Fachberater im Krisenstab

Der Krisenstab sollte einerseits nicht zu viele Personen umfassen (maximal zehn Personen), um schnell kommunizieren und entscheiden zu können, andererseits sollten alle benötigten Aufgaben und Funktionen des jeweiligen Notfalls wahrgenommen werden können. Eine Möglichkeit, den Krisenstab nicht unnötig auszuweiten, ist die Unterstützung durch externe Spezialisten, die jedoch keine formalen Mitglieder im Krisenstab sind. Das gilt besonders für Krisen, die von der Institution nicht alleine bewältigt werden können, wie beispielsweise Krisen mit kriminellem Hintergrund wie Erpressung, Entführung oder Bombendrohung.

Notfallteams

Der operative Teil der Notfallbewältigung wird durch verschiedene Notfallteams geleistet. Diese sind für den Wiederanlauf bzw. die Wiederherstellung von Geschäftsprozessen, Anwendungen oder Systemen zuständig. Klassische Notfallteams sind Infrastruktur, IT und Fachbereiche. Die Notfallteams sind gegenüber dem Krisenstab im Rahmen der Notfallbewältigung ausschließlich weisungsgebunden.

Das Infrastruktur-Team ist dafür zuständig, die Nutzbarkeit eines Gebäudes und der Arbeitsplätze wiederherzustellen. Dazu zählen die Wiederherstellung der Energie- und Klimaversorgung, die Netzumschaltung, der Aufbau von Ausweicharbeitsplätzen, die Ent- und Versorgung mit Betriebsmitteln, aber auch der Umbau der Verkabelung.

Zu den Aufgaben des IT-Teams gehören unter anderem die Beschaffung von Ausweichsystemen, deren Inbetriebnahme, die Wiederherstellung von Daten oder die Behebung von Störungen der TK-Anlage.

Die Notfallteams für die Fachbereiche oder Organisationseinheiten („Geschäft“) sind für die Maßnahmen vor Ort und den Wiederanlauf der Prozesse bzw. Fachverfahren zuständig. Dazu gehören die Aufnahme der Arbeit an Ausweicharbeitsplätzen, die Aufnehmen von Ausweichverfahren oder eines reduzierten Betriebs und schließlich die Wiederherstellung des Normalbetriebs. Dies geschieht in Zusammenarbeit mit den fachspezifischen Notfallteams. Die Leiter der Notfallteams für die Fachbereiche (Fachbereichskoordinatoren) sind für die ordnungsgemäße Umsetzung der Geschäftsfortführungspläne in der jeweiligen Einheit verantwortlich.

Die Notfallteam-Leiter sind während der Notfallbewältigung gegenüber dem Krisenstab in regelmäßigen Abständen berichtspflichtig. Sie sammeln die Informationen vor Ort, leiten diese an den Krisenstab weiter und koordinieren und kontrollieren die Umsetzung der vom Krisenstab angeordneten Maßnahmen vor Ort. Sie leiten gegebenenfalls Erstmaßnahmen am Schadensort ein und bilden die Kontaktstelle für externe Hilfskräfte wie beispielsweise Polizei, Rettungsdienste oder die Feuerwehr. Anfragen von Medien sollten jedoch an den Krisenstab bzw. die Krisenkommunikationsstelle weitergeleitet werden.

Unterstützendes Zusatzpersonal

Je nach Art der Institution und den möglichen Schadensszenarien kann es sinnvoll sein, Vorsorge für die psychologische Betreuung von Mitarbeitern, Angehörige oder sonstig Betroffene zu treffen. Großschadensereignisse bedeuten oftmals eine besondere psychologische Belastung, insbesondere wenn es zu Personenschäden gekommen ist. Verfügt die Institution hausintern über eigene Psychologen, so

können diese mit Hilfe von Zusatzqualifikationen auf die Betreuung von Personen bei Großschadensereignissen oder auch die Unterstützung und Beratung des Krisenstabs vorbereitet werden.

Mehrere Standorte

Verfügt die Institution über mehrere Standorte, die weltweit verteilt sein können, so gibt es mehrere mögliche Modelle, die Aufbauorganisation der Notfallbewältigung zu organisieren:

- An jedem Standort ist die gesamte Struktur von Krisenentscheidungsgremium bis Notfallteams aufgebaut. Die übergreifende Koordinierung erfolgt durch ein zusätzliches (eventuell internationales) Entscheidungsgremium.
- Jeder Standort verfügt über einen lokalen Krisenstab und lokale Notfallteams. Die übergreifende Koordinierung erfolgt über das zentrale Krisenentscheidungsgremium.
- Sowohl das Entscheidungsgremium als auch der Krisenstab agieren zentral, nur die operativen Notfallteams sind vor Ort.

Welches Modell für die Institution geeignet ist, um eine Standort übergreifende Krise zu meistern, muss individuell entschieden werden und ist im Wesentlichen von der allgemeinen Organisationsstruktur, der Größe der einzelnen Standorte, den Abhängigkeiten zwischen den Standorten wie auch von deren geographischer Verteilung abhängig.

4.3.3 Zusammenspiel mit dem Informationssicherheitsmanagement

Neben den Rollen in der Notfallvorsorge und –bewältigung gibt es in jeder Institution auch die Rollen und Verantwortungsbereiche des Informationssicherheitsmanagements. So sollte es in jeder Institution neben einem Notfallbeauftragten auch einen IT-Sicherheitsbeauftragten geben, der für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Institution zuständig ist.

Da es einige Überschneidungen bei der Konzeption des Notfallmanagements und des Informationssicherheitsmanagements gibt, ist zu klären, inwieweit der Notfallbeauftragte die Rolle des IT-Sicherheitsbeauftragten mit übernehmen kann oder der IT-Sicherheitsbeauftragte eine der Rollen im Notfallmanagement. Diese Rollen schließen sich nicht grundsätzlich aus. Ausschlaggebend sind jedoch die Art und Ausrichtung der Institution, die Durchdringung der Geschäftsprozesse mit IT und die Ausprägung des Sicherheitsmanagements. Je stärker die Abhängigkeit der Geschäftsprozesse von der IT, umso größer ist die Überschneidung beider Disziplinen. Das etablierte Sicherheitsmanagement muss ganzheitlich und prozessorientiert ausgerichtet sein und nicht auf IT fokussiert. Nur unter diesen Bedingungen ist eine Übernahme von der Rolle als IT-Sicherheitsbeauftragter und Notfallbeauftragter in Personalunion sinnvoll.

Es sind allerdings einige Aspekte im Vorfeld zu klären:

- Die Schnittstellen zwischen den verschiedenen Rollen sollten klar definiert und dokumentiert werden. Außerdem sollten auf beiden Seiten direkte Berichtswege nach oben existieren. Idealerweise sind diese Berichtswege identisch wie auch die verantwortliche Person in der obersten Leistungsebene.
- Es sollte überlegt werden, ob bei Eintritt konfliktträchtiger Themen die Innenrevision benachrichtigt werden sollte.
- Es muss sichergestellt sein, dass Personen mit mehreren Rollen ausreichend qualifiziert sind und genügend Ressourcen für ihre Aufgaben zur Verfügung haben.

4.4 Erstellung einer Leitlinie zum Notfallmanagement

Der Stellenwert des Notfallmanagements in der Institution und die strategische Ausrichtung sollten in einer Leitlinie zum Notfallmanagement zusammengefasst werden. Sie legt den Rahmen für die Konzeption, den Aufbau und die Aufrechterhaltung des Notfallmanagements fest. Die Leitlinie

beschreibt auf wenigen Seiten, warum ein Notfallmanagement etabliert werden soll und welche Ziele damit angestrebt werden.

Die Erstellung der Leitlinie wird durch ein entsprechend qualifiziertes Team übernommen. Der Notfallbeauftragte ist dabei koordinierend tätig. Da die Leitlinie zum Notfallmanagement das zentrale Strategiepapier darstellt, sollte es so gestaltet werden, dass sich alle betroffenen Organisationseinheiten mit dem Inhalt identifizieren können. Daher ist es für die allgemeine Akzeptanz sinnvoll, neben der Institutsleitung möglichst viele der Fachbereiche bei der Erstellung zu beteiligen. Es empfiehlt sich, zusätzlich zu den Vertretern der Fachbereiche, die Personalvertretung, Vertreter der Unternehmens- bzw. Behördensicherheit (Informations- und Betriebssicherheit), der Internen Revision, des Risikomanagements, der Unternehmens- bzw. Behördenkommunikation, der Informationstechnologie oder der Rechtsabteilung mit einzubeziehen. Doch kann und muss jede Institution dies für sich individuell entscheiden.

Inhalt der Leitlinie zum Notfallmanagement

Eine Leitlinie zum Notfallmanagement sollte kurz und übersichtlich gehalten werden und mindestens folgende Aspekte enthalten:

- eine Definition für Notfallmanagement,
- den Stellenwert des Notfallmanagements für die Institution,
- die Zielsetzung,
- die Kernaussagen der Notfallstrategie,
- den Geltungsbereich,
- das zugrunde gelegte Vorgehensmodell für das Notfallmanagement bzw. den zugrunde gelegten Standard (beispielsweise BSI-Standard 100-4),
- die Struktur der Aufbauorganisation mit den wichtigsten Rollen und deren Zuständigkeiten,
- die Verpflichtung der Institutionsleitung, durch regelmäßige Überprüfungen, Tests und Übungen das Notfallmanagement zu optimieren,
- die relevanten Gesetze, Richtlinien und Vorschriften, die zu beachten sind, und
- die Übernahme der Verantwortung durch die Institutionsleitung, die zusätzlich durch die explizite Freigabe per Unterschrift dokumentiert wird.

Optional können auch allgemeine Aussagen zur Aufsicht und Erfolgskontrolle des Notfallmanagements genannt werden.

Bekanntgabe der Leitlinie

Die Leitlinie zum Notfallmanagement muss in der Institution veröffentlicht und allen Mitarbeitern und potentiellen Interessensgruppen bekannt gegeben werden. Die Prozessbeteiligten des Notfallmanagements sollten auf die Leitlinie gesondert hingewiesen und die Kenntnisnahme schriftlich bestätigen werden.

Aktualisierung der Leitlinie

Die Leitlinie ist sowohl in regelmäßigen Abständen wie auch anlassbezogen bei Änderungen von Rahmenbedingungen, Geschäftszielen, Aufgaben oder Strategien zu aktualisieren. Für die Durchführung dieser Aufgabe ist der Notfallbeauftragte koordinierend zuständig. Die Aktualisierung sollte gemeinsam mit der Leitungsebene erfolgen. Die aktualisierte Leitlinie muss erneut von der Institutsleitung per Unterschrift freigegeben und kommuniziert werden.

4.5 Bereitstellung von Ressourcen

Der Aufbau und der Betrieb eines Notfallmanagements erfordern finanzielle, personelle und zeitliche Ressourcen. Diese Tatsache sollte schon bei der Festlegung der Notfallstrategie und der angestrebten Absicherung für die kritischen Geschäftsprozesse bedacht werden. Das angestrebte Absicherungsniveau sollte wirtschaftlich sinnvoll ist. Die Höhe der benötigten Ressourcen für ein Notfallmanagement hängt entscheidend von der Größe und der Art der Institution, der Art des Geschäftes aber auch des Standortes, der Umgebung, den Kunden, der eingesetzten Technologien oder der Bereitschaft der Institution, Risiken einzugehen (Risikoappetit), ab.

4.5.1 Kosteneffiziente Notfallstrategie

Für eine kosteneffiziente Notfallstrategie sind die anfallenden Investitionen den Gewinnen, aber auch der Notwendigkeit der Absicherung gegenüber zu stellen. Gewinne sind die Verhinderung von Kosten durch das Eintreten von Risiken bzw. durch den Ausfall oder Störung kritischer Geschäftsprozesse. Damit hat das Notfallmanagement die gleichen Probleme in der Argumentation und der Überzeugung der Leitungsebene wie das Informationssicherheitsmanagement.

Die verhinderten Kosten setzen sich aus direkten Kosten und indirekten Kosten zusammen. Zu den direkten Kosten zählen Kosten wie der Verlust durch geringeren Absatz oder entgangener Aufträge, Produktivitätsausfall, Strafen durch Nichteinhaltung von Verträgen oder Gesetze und die Kosten für die Wiederherstellung der Systeme. Indirekte Kosten sind vielfältiger Natur. Dazu zählen beispielsweise Imageschäden und Verlust von Vertrauen. Diese können wiederum zu Verlust von Kunden oder Schwächung der Marktposition führen und höhere Investitionen für die Gewinnung von Neukunden oder Rückgewinnung von Vertrauen verursachen.

Da bei Start des Projekts zur Etablierung eines Notfallmanagements nur sehr grobe Schätzungen für die Kosten und den Nutzen vorliegen, empfiehlt es sich, die initial festgelegte Notfallstrategie im Laufe des Projekts aber auch im laufenden Betrieb des Notfallmanagements periodisch einer Überprüfung zu unterziehen. Erst dann liegen konkretere Schätzungen für Ausfallkosten und Investitionszahlen vor. Wenn Anspruch und finanzielle Möglichkeiten zu weit auseinander liegen, sollte die Notfallstrategie überdacht werden.

4.5.2 Ressourcen für die Notfallmanagement-Organisation

Der Betrieb und insbesondere der Aufbau eines Notfallmanagements erfordern personelle Ressourcen. Bei der Einrichtung eines Notfallmanagements sollte der Notfallbeauftragte und gegebenenfalls auch die Notfallkoordinatoren von ihren sonstigen Aufgaben freigestellt werden, um eine zügige Umsetzung zu ermöglichen. Je nach Größe der Institution können diese Mitarbeiter ihre Aufgabe im Notfallmanagement neben ihrer originären Aufgabe wahrnehmen. Nur wenige Institutionen werden die Möglichkeit haben, hauptamtliche Stellen für Notfallkoordinatoren oder ein Notfallvorsorgeteam bereitstellen zu können.

Nicht nur in der Notfallvorsorge werden Ressourcen benötigt. Der zeitliche Aufwand für die Mitarbeiter, die bei der Notfallbewältigung zum Einsatz kommen, sollte nicht unterschätzt werden. Hoffentlich weniger im aktiven Einsatz während einer Krise, doch im Rahmen von notwendigen Tests und Übungen ist ihr Einsatz gefordert. Je nach Umfang der für die Institution erforderlichen Übungen ist eine phasenweise Freistellung der Mitarbeiter von ihren originären Aufgaben notwendig.

Es sollten auch ausreichend Ressourcen bereitgestellt werden, damit die Wirksamkeit und Eignung von Notfallmaßnahmen und des Notfallmanagement-Prozesses systematisch und regelmäßig überprüft werden können. Bei der Überprüfung sollte auch die Effizienz der eingesetzten Ressourcen im Verhältnis zum Nutzen betrachtet werden. Stellt sich heraus, dass bestimmte Maßnahmen unwirtschaftlich hohe Kosten verursachen, sollten alternative Maßnahmen gesucht, die Kontinuitätsstrategie (siehe Kapitel 5.4), die Anforderungen aus der Business Impact Analyse oder gar die Notfallstrategie überdacht werden. Auch ist die Einarbeitung und Umsetzung von Verbesserungsvorschlägen sowie die Behebung von festgestellten Mängeln bei der personellen Ressourcenplanung zu berücksichtigen.

In der Praxis fehlt den internen Notfallmanagementverantwortlichen häufig die Zeit, um alle relevanten Einflussfaktoren und Rahmenbedingungen (z. B. gesetzliche Anforderungen oder technische Fragen) zu analysieren. Teilweise fehlen ihnen zu Beginn des Projekts auch die entsprechenden fachlichen Grundlagen. In diesen Fällen kann es sinnvoll sein, auf externe Experten zurückzugreifen. Dies sollte vom Notfallbeauftragten kommuniziert und dokumentiert werden, damit die Leitungsebene die erforderlichen Ressourcen bereitstellt.

4.5.3 Ressourcen für Vorsorgemaßnahmen und deren Betrieb

Zu den Vorsorgemaßnahmen gehören neben personellen Maßnahmen auch organisatorische, infrastrukturelle und technische Maßnahmen. Bei der Auswahl von geeigneten Maßnahmen sollte auf eine sinnvolle Mischung geachtet werden. Häufig sind Investitionen in personelle Ressourcen und organisatorische Regelungen effektiver und effizienter als Investitionen in Technologie. Technologien alleine lösen keine Probleme. So müssen technische und infrastrukturelle Maßnahmen immer in einen geeigneten organisatorischen Rahmen eingebunden werden. Aber auch der zielgerichtete Einsatz von technischen Maßnahmen ist ausschlaggebend. Sowohl die richtige Auswahl, die Administration wie auch regelmäßige Überprüfungen und Tests auf korrekte Funktionsweise sind entscheidend. Investitionen in Technik, welche im Ernstfall versagt, sind verschwendet.

4.5.4 Zusammenarbeit mit anderen Management-Systemen

Wie in den nächsten Kapiteln weiter deutlich werden wird, bestehen einige Überschneidungen des Notfallmanagements mit anderen Management-Systemen wie dem Informationssicherheitsmanagement oder dem (IT-)Risikomanagement. Eine sinnvolle Eingliederung des Notfallmanagements in bestehende Strukturen, eine gute Unternehmens- bzw. Behördenkommunikation zwischen den Disziplinen, aber auch zu den Geschäftsbereichen, der offene, konstruktive Austausch von benötigten Informationen und eine eindeutige Aufgabenteilung ist ein zentraler Faktor für den Erfolg der Management-Systeme, aber auch um die Kosten niedrig zu halten. Durch eine zielgerichtete und zeitnahe Zusammenarbeit in den Schnittbereichen der Management-Systeme können Synergieeffekte genutzt und finanzielle, personelle und zeitliche Ressourcen eingespart werden.

4.6 Einbindung aller Mitarbeiter

Um ein Notfallmanagement erfolgreich einzuführen und aufrechtzuerhalten, sollte dieses, wie andere übergreifende Managementsysteme auch, fest in die Behörden- bzw. Unternehmenskultur verankert werden. Notfallmanagement betrifft ohne Ausnahme alle Mitarbeiter, wenn auch in unterschiedlicher Ausprägung. Jeder Einzelne kann durch verantwortungs- und risikobewusstes Handeln dazu beitragen, Schäden zu vermeiden und den Erfolg des Notfallmanagements zu ermöglichen. Sensibilisierung und Schulung der Mitarbeiter ist dafür eine notwendige Voraussetzung. Der erste Schritt ist die Veröffentlichung der Leitlinie zum Notfallmanagement. Auch das Arbeitsklima, gemeinsame Wertvorstellungen und das Engagement der Mitarbeiter beeinflussen entscheidend die Robustheit von Geschäftsprozessen und damit der Institution.

4.6.1 Sensibilisierung und Schulung

Die Sensibilisierung der Mitarbeiter für das Thema Notfallmanagement hat einen hohen Stellenwert innerhalb des Lebenszyklus des Notfallmanagements. Ein Sensibilisierungs- und Schulungsprogramm sowie themenbezogene Veranstaltungen sollen sicherstellen, dass alle Mitarbeiter der Institution darüber informiert sind, dass ein Notfallmanagement existiert, welche Intention dahinter steckt, wie sie dazu beitragen können, dass das Notfallmanagement erfolgreich umgesetzt und gelebt werden kann, und wie sie sich bei Eintreten eines Notfalls zu verhalten haben. Da nicht alle Mitarbeiter die gleiche Intensität der Sensibilisierung benötigen, sollte Zielgruppen-orientiert und bedarfsgerecht gearbeitet werden. Je nach Bedarf ist die geeignete Tiefe und Form der Sensibilisierung und Schulung zu wählen.

Sowohl die Mitarbeiter der Notfallvorsorge wie auch der Notfallbewältigung, müssen durch Schulungen gezielt auf ihre Aufgaben vorbereitet und qualifiziert werden. Um ein Schulungskonzept zu erstellen, muss im ersten Schritt der Schulungsbedarf ermittelt und dokumentiert werden. Im nächsten Schritt sind die Themen und Inhalte (beispielsweise BIA, Risikoanalyse, Kommunikation mit Medien, Training der Mitglieder der Notfallbewältigungsteams) zu identifizieren. Die zum Einsatz kommenden Schulungs- bzw. Trainingsarten, wie beispielsweise

- computergestütztes oder internetbasiertes Lernen,
- Einzel- oder Gruppentraining oder
- interne oder externe Seminare,

sind festzulegen und zu dokumentieren.

Für die Sensibilisierung sollten schon vorhandene Wege der Behörden- oder Unternehmenskommunikation, wie z. B. Führungskräftetagungen, Jour-Fixe, Einführungsveranstaltungen für neue Mitarbeiter, Veranstaltungen von Organisationseinheiten, Mitarbeiterzeitschriften, Poster oder Newsletter genutzt werden. Ein abgestimmtes Vorgehen und Zusammenarbeit mit den Sensibilisierungsmaßnahmen des Sicherheits- oder Risikomanagements ist sinnvoll.

Die Leiter der Organisationseinheiten sollten die Ausbildung und aktive Teilnahme ihrer Mitarbeiter unterstützen und sie für diese Maßnahmen von ihren alltäglichen Aufgaben freistellen. Nach durchgeführten Sensibilisierungs- und Schulungsmaßnahmen sollte überprüft werden, ob diese von den Mitarbeitern entsprechend aufgenommen und verstanden wurden. Die Umsetzung und die Fortschritte des Schulungs- und Sensibilisierungsprogramms sind entsprechend zu dokumentieren. Der Nachweis über durchgeführte Schulungsmaßnahmen ist entsprechend aufzubewahren. Eine Bewertung der Effizienz der durchgeführten Sensibilisierungs- und Schulungsmaßnahmen ist empfehlenswert. Der Stand der Maßnahmen ist jährlich an die Institutionsleitung zu berichten.

4.6.2 Einbindung, Risikokommunikation und Früherkennung

Um die Widerstandsfähigkeit einer Institution zu erhöhen und auf den Notfall vorbereitet zu sein, müssen die Mitarbeiter nicht nur regelmäßig sensibilisiert werden, sondern es müssen auch geeignete Strukturen geschaffen werden, damit Notfallmanagement aktiv gelebt werden kann. Dazu sind Ansprechpartner und Zuständigkeiten für das Thema festzulegen und bekannt zu machen.

Die Mitarbeiter sind in einen regelmäßigen Informationsfluss über Risiken, Vorfälle und Auswirkungen einzubinden. Erkennen Mitarbeiter im Alltagsbetrieb mögliche Risiken für die Geschäftsfortführung oder besteht auch nur ein Verdacht auf Risiken, so sollte jeder Mitarbeiter wissen, wie er sich zu verhalten hat und wie er diese melden kann. Diese pro-aktive Kommunikation von potentiellen Risiken wird im Bereich des Notfallmanagements auch Risikokommunikation genannt. Sie kann dazu beitragen, dass Risiken frühzeitig erkannt und Gegenmaßnahmen getroffen werden können, um einen Notfall abzuwenden oder schneller einzudämmen.

5 Konzeption

Um ein Notfallkonzept bestehend aus Notfallvorsorgekonzept (siehe Kapitel 5.5) und Notfallhandbuch (siehe Kapitel 7.4) entwickeln zu können, sind verschiedene Vorarbeiten zu leisten. Ziele dabei sind, das Unternehmen bzw. die Behörde und deren „Geschäft“ zu verstehen, die Verfügbarkeitsanforderungen der Geschäftsprozesse zu identifizieren, Schwachstellen zu erkennen, Gegenmaßnahmen zu etablieren und auf die Restrisiken durch eine funktionierende Notfallbewältigung vorbereitet zu sein.

Eine Business Impact Analyse liefert die notwendigen Informationen über die kritischen Geschäftsprozesse und Ressourcen. Eine Risikoanalyse liefert die nötigen Informationen über bestehende Risiken, gegen die sich die Institution absichern sollte. Die Entwicklung von Kontinuitätsstrategieoptionen zeigt mögliche Alternativen für die Umsetzung auf. In einer Managemententscheidung werden die geeigneten Kontinuitätsstrategien ausgewählt, die dann den Rahmen für die Konzept- und Planerstellung bildet.

5.1 Die Business Impact Analyse

Die zentrale Aufgabe einer Business Impact Analyse ist es, zu verstehen, welche Geschäftsprozesse wichtig für die Aufrechterhaltung des Geschäftsbetriebs und damit für die Institution sind, und welche Folgen ein Ausfall haben kann. Diese „kritischen“ Geschäftsprozesse werden im Rahmen des Notfallmanagements besonders abgesichert und Vorsorge für die Krise getroffen.

„Kritisch“ im Sinne des Notfallmanagements bedeutet „zeitkritisch“, also dass dieser Prozess eine schnellere Wiederaufnahme der Tätigkeit erfordert, da sonst ein hoher Schaden für die Institution zu erwarten ist. Der hohe Schaden kann dabei sowohl aus finanziellen Verlusten, Verstößen gegen Gesetze oder Verträge, aus Imageschäden oder weiteren Schadensszenarien entstehen. Ein bei der BIA als „unkritisch“ eingestufter Geschäftsprozess bedeutet nicht, dass dieser für die Institution unwichtig ist, sondern lediglich, dass er eine geringere Priorität in der Wiederherstellung hat.

Um die „kritischen“ Geschäftsprozesse zu identifizieren und geeignete Strategien und Vorsorgemaßnahmen für Schadensereignisse ausarbeiten zu können, müssen zunächst die Auswirkungen von Störungen, Unterbrechungen oder gar der Verlust von Geschäftsprozessen auf die Institution ermittelt werden. Dazu sind die wichtigsten Produkte und Dienstleistungen der Institution und die dazugehörigen Prozesse zu identifizieren. Die kritischen Geschäftsprozesse werden in der Regel zur Erbringung der wichtigsten Dienstleistungen und Erzeugung der Produkte beitragen, doch sollte eine allzu einschränkende Sichtweise ausschließlich auf diese Prozesse vermieden werden.

In dieser Phase des Notfallmanagement-Prozesses ist die Frage nach der Ursache eines Notfalls noch nicht von Interesse, sondern lediglich, welche Konsequenzen für die Institution zu erwarten sind. Hierzu wird eine so genannte Business Impact Analyse (BIA), im Deutschen auch Folgeschädenabschätzung oder Betriebsunterbrechungsanalyse genannt, durchgeführt. Eine BIA ist ein Verfahren, um die Wiederanlaufpunkte der Geschäftsprozesse, eine Priorisierung für den Wiederanlauf und damit die Kritikalität der Geschäftsprozesse festzulegen und die benötigten Ressourcen zu identifizieren.

Es existieren viele Methoden und Wege, eine Business Impact Analyse durchzuführen. Der eine „wahre“ Weg oder „Best Practice“ existiert nicht. Wie die benötigten Ergebnisse ermittelt werden, kann jede Institution für sich entscheiden. In diesem Standard wird eine Methode vorgestellt, die an die Schutzbedarfsfeststellung nach BSI-Standard 100-2 zum Aufbau eines Informationssicherheitsmanagements nach IT-Grundschutz angelehnt ist. Die Business Impact Analyse und die Schutzbedarfsfeststellung nach BSI-Standard 100-2 besitzen einige Gemeinsamkeiten in der Vorgehensweise, so dass Synergieeffekte genutzt werden können und Aufwand eingespart werden kann, wenn eine Zusammenarbeit der beiden Disziplinen erfolgt oder zumindest umfassend Informationen ausgetauscht werden. Wo die Gemeinsamkeiten liegen und wie die Schutzbedarfsfeststellung ergänzt werden kann, um die Ergebnisse einer BIA zu erhalten, wird im Folgenden verdeutlicht.

5.1.1 Überblick

Die Durchführung einer Business Impact Analyse kann in folgende Teilschritte untergliedert werden (siehe Abbildung 3):

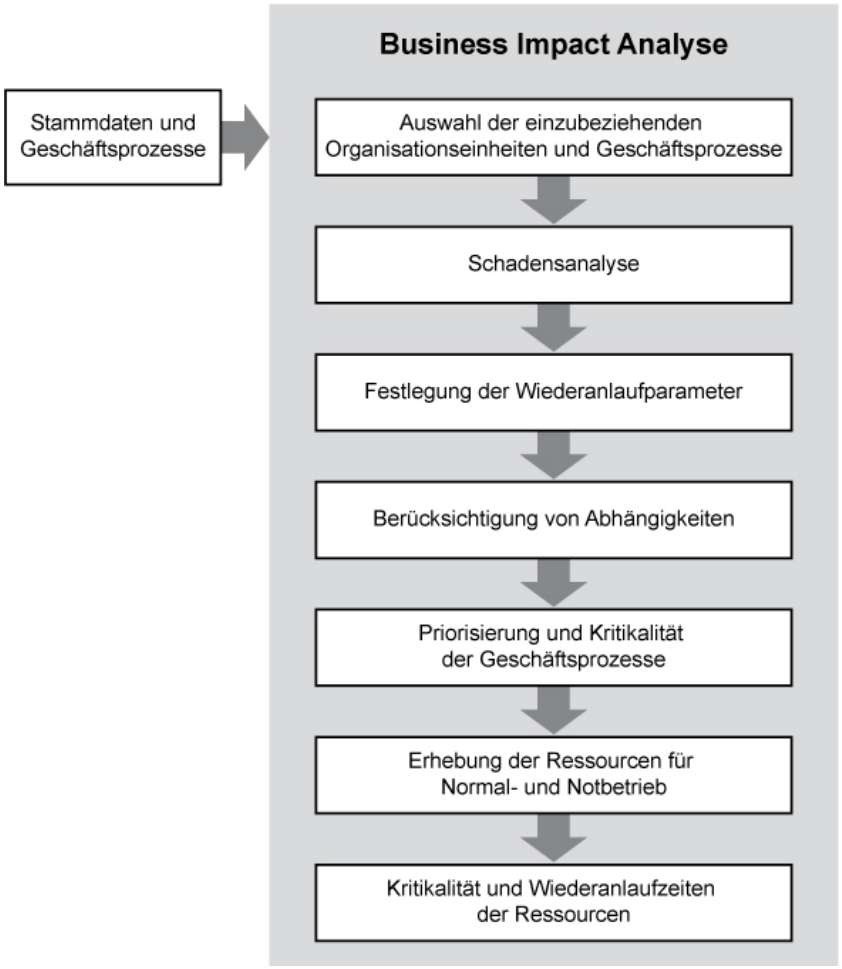


Abbildung 3: Übersicht Business Impact Analyse

0. Schritt: Stammdaten und Geschäftsprozesse

Für die Durchführung einer BIA wird eine Übersicht über alle relevanten Geschäftsprozesse des Unternehmens bzw. aller Fachaufgaben der Behörde mit den jeweils verantwortlichen Ansprechpartnern bzw. Prozessverantwortlichen benötigt. Diese Übersicht sollte neben der Auflistung der Prozesse auch eine Zuordnung zu den Geschäftszielen enthalten sowie die Abhängigkeiten zwischen den einzelnen Prozessen darstellen. Die Geschäftsziele einer Behörde leiten sich meist aus deren gesetzlichen Aufträgen ab. Liegt keine aktuelle Prozess-Übersicht vor, so ist diese als Vorarbeit zur BIA zu erstellen oder zu aktualisieren. Zusätzlich sollten Stammdaten der Institution wie Unternehmensstruktur oder Lokationen bereitgestellt werden.

1. Schritt: Auswahl der einzubeziehenden Organisationseinheiten und Geschäftsprozesse

Ist offensichtlich, dass innerhalb des festgelegten Gültigkeitsbereichs des Notfallmanagements einige Organisationseinheiten oder Geschäftsprozesse eine sehr geringe Bedeutung für das Erreichen der Geschäftsziele und die wertschöpfenden Prozesse der Institution besitzen, so können diese bei der weiteren Betrachtung ausgespart werden.

2. Schritt: Schadensanalyse

Die Schadensanalyse untersucht den Schaden für die Institution, den der Ausfall einzelner Geschäftsprozesse verursachen könnte. Dabei ist nicht nur die Höhe des Schadens, sondern insbesondere die zeitliche Entwicklung des Schadenverlaufs von Interesse. Für die Durchführung der Schadensanalyse sind die Rahmenbedingungen für die Erhebung festzulegen (Schadenskategorien und Schadensszenarien), die Bewertungsperioden sowie die Strategie zur Behandlung besonderer Termine, an denen die Verfügbarkeitsanforderung eines Prozesses von dessen Durchschnitt abweicht. Anschließend wird für jeden einzelnen Prozess und jede Bewertungsperiode der entstehende Schaden bei Ausfall bewertet.

3. Schritt: Festlegung der Wiederanlaufparameter

Anhand des zeitlichen Schadenverlaufs und der zu erwartenden Schadenshöhe werden die maximal tolerierbare Ausfallzeit, die Wiederanlaufzeit und das Wiederanlauf-Niveau für jeden Geschäftsprozess festgelegt. Die Ergebnisse werden anschließend zentral zusammengefasst und konsolidiert.

4. Schritt: Berücksichtigung von Abhängigkeiten

Da die Wiederanlaufparameter in Bezug auf den Einzelprozess festgelegt wurden, sollte anschließend eine Feinabstimmung durchgeführt werden. Dabei werden Prozessabhängigkeiten und strategische Geschäftsziele berücksichtigt und es sind gegebenenfalls Korrekturen an den Parameter durchzuführen.

5. Schritt: Priorisierung und Kritikalität der Geschäftsprozesse

Anhand der vorliegenden Daten für den Wiederanlauf und den Schadensverlauf wird die Reihenfolge der Geschäftsprozesse für den Wiederanlauf und Kritikalität der Prozesse festgelegt. Dazu sind die Kritikalitätskategorien und ihre Abgrenzungen zu definieren.

6. Schritt: Erhebung der Ressourcen für Normal- und Notbetrieb

Um Kontinuitätsstrategien entwickeln und Vorsorgemaßnahmen festlegen zu können, ist es notwendig, die von den kritischen Geschäftsprozessen genutzten Ressourcen zu identifizieren. Es sind die Art der Ressourcen und die benötigte Kapazität für den Normalbetrieb und den Notbetrieb zu erheben. Für die Ressource „Information“ wird zusätzlich der jeweils maximal zulässige Datenverlust, der sich im sogenannten Wiederherstellungspunkt widerspiegelt, festgelegt.

7. Schritt: Kritikalität und Wiederanlaufzeiten der Ressourcen

Im letzten Schritt der BIA werden für die von den kritischen Prozessen verwendeten Ressourcen die Wiederanlauf- und Wiederherstellungszeiten sowie deren Kritikalität ermittelt.

5.1.2 Durchführung einer Business Impact Analyse

In den folgenden Unterkapiteln werden Hinweise und Hilfen gegeben, wie die einzelnen Schritte einer BIA im Detail durchgeführt werden können. Die Erhebung der benötigten Informationen kann dabei mittels Fragebögen, Workshops oder individuellen Interviews erfolgen. Es bietet sich an, eine Kombination dieser Methoden zu wählen, da sie unterschiedliche Vor- und Nachteile besitzen und sich ergänzen. So können Fragebögen, ob in Papierform oder Software-basiert, nur allgemein und für alle Fachbereiche und Geschäftsprozesse gültig formuliert werden. Für die Einführung in das Thema Notfallmanagement und um zu vermitteln, warum und mit welchem Ziel bestimmte Schritte durchgeführt werden müssen, eignen sich Workshops, mit denen ein größerer Kreis erreicht werden kann. Einzelinterviews mit den Leitern der Fachbereiche, den Prozessverantwortlichen oder sonstigen Personen, die Auskunft geben können, sind am zeitaufwendigsten, liefern jedoch konkrete Informationen, da durch gezielte Gesprächsführung und geeignete Fragetechniken Missverständnisse erkannt und behoben, und die essentiellen Informationen in der gewünschten Form ermittelt werden

können. Welche Interview-Partner bei der Durchführung der BIA gewählt werden, hängt sowohl vom jeweiligen Prozessschritt, aber vor allem von der Aufstellung der Institution ab.

Für die Durchführung einer BIA ist die Unterstützung durch die Institutionsleitung von entscheidender Bedeutung. Da breite Mitarbeit sowohl in den Geschäftsbereichen, den Organisationseinheiten wie auch auf der Ressourcen-Ebene (z. B. Administration für die IT) benötigt wird, muss sichergestellt sein, dass der Arbeitsauftrag durch die oberste Ebene getragen und dessen Bedeutung institutionsweit kommuniziert wird.

5.1.2.1 Stammdaten und Geschäftsprozesse

Voraussetzung für die BIA sind umfassende Kenntnisse über das Geschäftsmodell bzw. Aufgaben der Institution und deren Aufbau. Dazu zählen das Wissen über die Geschäftsprozesse bzw. der Fachaufgaben sowie die Stammdaten der Institution. Zu den Stammdaten gehören beispielsweise die Informationen über die Rechtsform, die Branche, die organisatorische Struktur, die Lokationen oder die Lieferanten. Fachaufgaben sind Geschäftsprozesse in Behörden. Werden im Folgenden nur noch die Geschäftsprozesse genannt, so sind die Fachaufgaben implizit gemeint. Das dient ausschließlich der besseren Lesbarkeit.

Jede Institution sollte einen vollständigen, aktuellen und gut dokumentierten Überblick über ihre wesentlichen Prozesse besitzen. Liegt keine Übersicht vor, so ist diese zu erheben oder zu aktualisieren. Dies ist jedoch keine originäre Aufgabe des Notfallmanagements.

Es existieren keine eindeutigen und allgemein gültigen Vorgaben, was unter einem Geschäftsprozess zu verstehen ist (siehe Abbildung 4). Diesem Dokument liegt folgende Vorstellung zugrunde: Eine Wertschöpfungskette umfasst den gesamten Weg eines Produktes oder einer Dienstleistung vom Hersteller bis zum Verbraucher und kann mehrere Institutionen einschließen. Unter einer Wertkette werden die Teile einer Wertschöpfungskette verstanden, die sich innerhalb einer Institution befinden. Sie setzt sich aus mehreren abhängigen Geschäftsprozessen (Prozesskette) zusammen, in der Regel vom Auftrag bis zur Auslieferung und Verrechnung. Ein Geschäftsprozess kann als Abfolge von (Teil-)Prozessen gesehen werden, in denen Aktionen ausgeführt und Entscheidungen getroffen werden. Jeder Teilprozess ist wiederum ein Geschäftsprozess. Ein Prozess benötigt in der Regel Eingaben (Input), der von anderen Geschäftsprozessen geliefert wird. Ein Prozess liefert Ergebnisse (Output) beispielsweise in Form von Produkten, Informationen oder Dienstleistungen, die von Nachfolge-Prozessen verarbeitet werden. In- und Output stellen die Verbindungen zwischen den Prozessen dar. Um die Durchführung einer BIA zu erleichtern, ist es hilfreich, Geschäftsprozesse so festzulegen, dass sie, soweit es sinnvoll ist, vollständig innerhalb einer Organisationseinheit und damit in einem Zuständigkeits- und Verantwortungsbereich liegen.

Geschäftsprozesse werden nach ihrer Art in Kernprozesse und unterstützende Prozesse unterschieden. Kernprozesse sind Prozesse, die direkt einen Beitrag zum Erreichen eines oder mehrerer Geschäftsziele liefern. Diese können weiter kategorisiert werden in strategische Prozesse, die der strategischen Entscheidungsfindung der Institution dienen, und in operative Prozesse, die Bestandteil des operativen Geschäfts sind. Das operative Geschäft kann beispielsweise die Erfüllung der übertragenen staatlichen Aufgaben bei Behörden sein, die Erbringung von Dienstleistungen oder auch die Herstellung eines Produkts.

Unterstützende Prozesse tragen nicht direkt zur Erbringung von Geschäftszielen bei, können jedoch indirekt eine sehr wichtige und damit eine kritische Rolle spielen, da sie der Aufrecherhaltung von Kernprozessen dienen. Zu den klassischen unterstützenden Prozessen zählen das Personalmanagement und die IT-Administration.

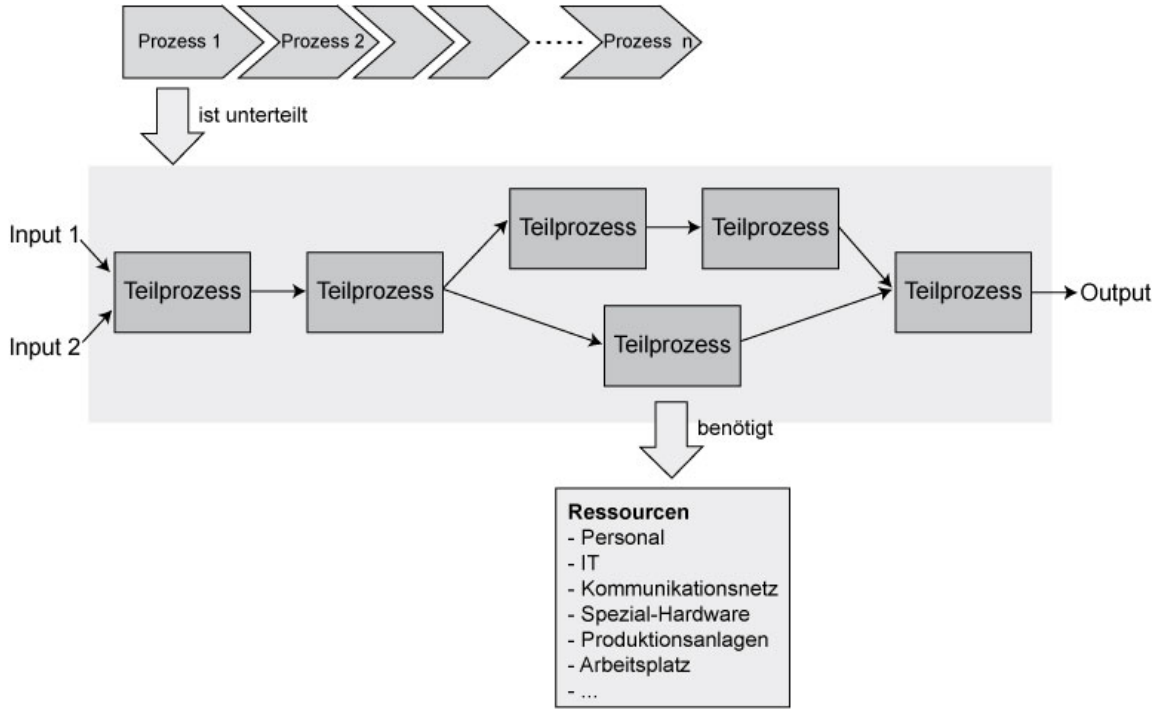


Abbildung 4: Geschäftsprozesse

Die Erarbeitung der Prozessübersicht erfordert zum einen einen Gesamtblick über die Abläufe in der Institution wie auch die Kenntnisse über die Einzelaufgaben. Eine Methode, um Vollständigkeit für die Kernprozesse zu erreichen, ist, die Wertketten vom Auftrag bis zur Auslieferung und Verrechnung zu betrachten. Es empfiehlt sich, die Aufgabe der Erhebung an die jeweiligen Organisationseinheiten zu delegieren. Die einzelnen Organisationseinheiten erarbeiten die Geschäftsprozesse für ihren Bereich. Die Erhebung kann durch den Leiter der Organisationseinheit erfolgen, durch einen dazu ernannten Verantwortlichen oder durch den für diese Organisationseinheit zuständigen Notfallkoordinator. Der Notfallkoordinator sollte über das notwendige Wissen zu Geschäftsprozessen und Ansprechpartner verfügen, da er dieses für seine Tätigkeit im Notfallmanagement benötigt.

Wird die Geschäftsprozesserhebung im Rahmen der Notfallvorsorge durchgeführt, so sollte der Notfallbeauftragte informierend, koordinierend und steuernd diese Aufgabe begleiten. Um vergleichbare Ergebnisse zu erhalten, sollte er Vorgaben zur Methode der Erhebung, Darstellungsweise und Granularität der zu erhebenden Prozesse geben, sowie Klassen und einheitliche Rahmenbedingungen festlegen. Diese sind bei der Erhebung durch die Organisationseinheiten zu nutzen. Der Notfallbeauftragte sollte sich regelmäßig mit den Bearbeitern in den einzelnen Organisationseinheiten abstimmen, um große Unterschiede in den Prozessdarstellungen im Ansatz zu erkennen und gegensteuern zu können. Er führt die Einzelergebnisse zusammen und konsolidiert diese in Zusammenarbeit mit der Leitungsebene. Das Ergebnis sollte eine Prozesslandkarte sein, die die Prozesse listet und die verschiedenen Abhängigkeiten zwischen den einzelnen Geschäftsprozessen aufzeigt. Dazu zählen die Prozess- oder Wertketten wie auch die Abhängigkeiten von unterstützenden Geschäftsprozessen.

Wurden einzelne Geschäftsprozesse, die Teil einer Wertkette der Institution sind, ausgelagert, so sollten diese Prozesse ebenfalls in die Übersicht aufgenommen und entsprechend gekennzeichnet werden. Wichtig ist die Darstellung der Verbindungen zu den internen Geschäftsprozessen und deren Abhängigkeit voneinander.

Als Vorgabe für die Granularität bei der Erhebung der Prozesse sollte ein goldener Mittelweg zwischen zu starker Zusammenfassung von Prozessen und einer zu detaillierten Betrachtung gefunden werden. Eine zu starke Bündelung von Prozessen führt zu einer mangelnden Aussagekraft. Eine zu detaillierte Betrachtung führt zu einer nicht zu bewältigenden Anzahl von zu betrachtenden Prozessen. Die praktische Erfahrung lehrt, dass bei der Erstellung der BIA die Detailtiefe der einzelnen Ge-

schäftsprozesse so grob sein sollte, dass zwar spezifische Anforderungen an bestimmte Applikationen möglich sind, andererseits aber auf eine vollständige Geschäftsprozess-Analyse verzichtet werden kann. Als allgemeine Faustregel kann gelten, dass das Ergebnis der Prozesserhebung in einer Organisationseinheit für das Notfallmanagement fünf bis maximal 15 Prozesse liefern sollte. Dies hat sich in der Praxis als sinnvoll erwiesen, kann jedoch institutions- und aufgabenabhängig durchaus unter- bzw. überschritten werden.

Für jeden (Teil-)Geschäftsprozess sind mindestens folgende Angaben zu erheben:

- ein eindeutiger Bezeichner für den Prozess,
- eine kurze Beschreibung,
- der benötigte Input,
- der Output,
- die Teilprozesse, falls weiter untergliedert wurde,
- die Verknüpfungen zu anderen internen wie auch ausgelagerten Geschäftsprozessen (Vorgänger und Nachfolger) und die Abhängigkeiten zu unterstützenden Prozessen wie beispielsweise von IT-Dienstleistungen,
- den Grad der Abhängigkeit der Geschäftsprozesse (siehe Kap. 5.1.2.5) und
- den Prozessverantwortlichen bzw. den Ansprechpartner für den Prozess.

Die Prozesserhebung kann durch geeignete Tools für die Geschäftsprozessmodellierung unterstützt werden.

5.1.2.2 Auswahl der einzubeziehenden Organisationseinheiten und Geschäftsprozesse

Ist offensichtlich, dass innerhalb des festgelegten Geltungsbereichs des Notfallmanagements Organisationseinheiten oder Geschäftsprozesse existieren, welche eine sehr geringe Kritikalität für die Institution besitzen, so können diese bei der weiteren Betrachtung ausgespart werden. Damit können der Aufwand und auf diese Weise die Kosten etwas reduziert werden. Dabei ist jedoch zu bedenken, dass die Intensität mancher Abhängigkeiten zwischen einzelnen Prozessen nicht immer direkt offensichtlich ist oder unterschätzt wird. Für ausgelagerte Prozesse gelten die gleichen Regeln. Ausgelagerte Prozesse dürfen nur dann von der Betrachtung ausgeschlossen werden, wenn sie eindeutig als unkritisch eingestuft werden können.

Existieren Organisationseinheiten, die aus strategischen Gründen von der Institutionsleitung eine untergeordnete Priorität erhalten, so kann der Umfang der zu betrachtenden Geschäftsprozesse gegebenenfalls weiter eingegrenzt werden. Diese Entscheidung kann jedoch ausschließlich von der obersten Leitungsebene getroffen werden.

Wird das Mittel zur Einschränkung des zu betrachtenden Ausschnittes innerhalb des Geltungsbereichs eingesetzt, so muss die Ausklammerung von einzelnen Geschäftsprozessen oder gar Organisationseinheiten schriftlich und nachvollziehbar begründet werden. Diese Einschränkung ist von der Institutionsleitung zu genehmigen und durch eine Unterschrift zu bestätigen Der Ausschluss sollte spätestens bei der nächsten Aktualisierung der BIA intensiv darauf überprüft werden, ob die Argumentation sich als schlüssig und korrekt erwiesen hat.

5.1.2.3 Schadensanalyse

Durch eine Schadensanalyse wird der Schaden für die Institution untersucht, den der Ausfall einzelner Geschäftsprozesse verursachen könnte. Dabei ist nicht nur die Höhe des Schadens, sondern insbesondere dessen zeitliche Entwicklung von Interesse. Für die Durchführung der Schadensanalyse sind verschiedene Rahmenparameter festzulegen. Dazu gehören die Schadenskategorien, die Schadensszenarien, die zu betrachtenden Bewertungsperioden und die Strategie zur Handhabung besonderer Termine.

A. Festlegung der Schadenskategorien und Schadensszenarien

Der Schaden durch den Ausfall eines Prozesses setzt sich aus direkten (z. B. entgangene Gewinne, Verluste durch Rechtsfolgen) und indirekten Schäden (z. B. Verlust durch entgangene Aufträge, Verlust an Marktanteil, Imageverlust) zusammen. Da nur für wenige der genannten Schadensklassen belastbares Zahlenmaterial existiert, ist es sinnvoll, den Schaden nicht quantitativ zu berechnen, sondern eine qualitative Einstufung in Schadenskategorien vorzunehmen. Jede Institution hat die Anzahl und die Bedeutung der Schadenskategorien individuell festzulegen. Üblicherweise wird mit drei bis fünf Kategorien gearbeitet. Als Beispiel wird in diesem Dokument eine Einteilung in vier Kategorien vorgenommen (siehe Tabelle 1). Die Schadenskategorien sind vergleichbar mit den Schutzbedarfskategorien bei der Schutzbedarfsfeststellung nach IT-Grundschutz [BSI2]. Tabelle 1 zeigt eine Gegenüberstellung von Schadens- und der Schutzbedarfskategorien.

Schadenskategorien		**Schutzbedarfskategorien**	
Bezeichnung	Erläuterung	Bezeichnung	Erläuterung
„niedrig“	Ausfall hat eine geringe, kaum spürbare Auswirkung.		
„normal“	Ausfall hat spürbare Auswirkungen.	"normal"	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Ausfall hat erhebliche Auswirkungen.	"hoch"	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Ausfall oder Beeinträchtigung führen zu existentiell bedrohlichen Auswirkungen.	"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 1: Schadens- und Schutzbedarfskategorien

Die Festlegung und Abgrenzung der einzelnen Schadenskategorien könnte prinzipiell ausschließlich über den direkten monetären Schaden erfolgen, doch ist es sinnvoller, weitere Schadensszenarien in die Bewertung mit einfließen zu lassen. Immaterielle oder indirekte finanzielle Schäden können je nach Branche und Institution höher als der direkte finanzielle Schaden sein. In der Praxis hat sich eine Untermenge der aus der Schutzbedarfsfeststellung bekannten Schadensszenarien bewährt:

- finanzielle Auswirkungen,
- Beeinträchtigung der Aufgabenerfüllung,
- Verstoß gegen Gesetze, Vorschriften und Verträge,
- negative Innen- und Außenwirkung (Imageschaden) und
- Beeinträchtigung der persönlichen Unversehrtheit.

Weitere Beispiele für die frei wählbaren Schadenszenarien sind:

- fehlende Management- oder Steuerungsinformationen oder
- Rückgang der Mitarbeitermotivation.

Eine Institution hat festzulegen, welche Schadensszenarien verwendet werden sollen und eventuell mit welcher Priorität. So wird für die Mehrzahl der Unternehmen die finanziellen Auswirkungen das wichtigste Kriterium sein, doch in manchen Branchen, wie beispielsweise bei Banken oder Versicherungen, spielt auch der Imageschaden eine sehr große Rolle. Bei Behörden könnte die Aufgabenerfüllung an erster Stelle stehen, gefolgt von Imageschaden. Es können beliebige Schadensszenarien gewählt oder neue festgelegt werden.

Um die Schadenskategorien voneinander abgrenzen zu können, sind die Grenzen anhand der Schadensszenarien individuell für die Institution festzulegen (siehe Tabelle 2). Wird die BIA zusammen mit der Schutzbedarfsfeststellung durchgeführt und die vorgeschlagene Untermenge der Schadensszenarien verwendet, so bietet es sich an, die Festlegungen aus der Schutzbedarfsfeststellung

zu übernehmen. Damit entfällt weiterer Arbeitsaufwand. Tabelle 2 zeigt eine Möglichkeit für die vorgeschlagenen Szenarien und Kategorien, die jedoch individuell für jede Institution angepasst werden müssen.

Schadenskategorie „niedrig“	
finanzielle Auswirkungen	keine nennenswerten Auswirkungen (z. B. Verlust geringer als 5% des Umsatzes)
Beeinträchtigung der Aufgabenerfüllung	keine nennenswerten Auswirkungen
Verstoß gegen Gesetze, etc.	keine nennenswerten Auswirkungen
negative Innen- und Außenwirkung	keine nennenswerten Auswirkungen
Schadenskategorie „normal“	
finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel (z. B. Verlust weniger als 5-20% des Umsatzes)
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung wird von Mitarbeitern toleriert / andere Tätigkeiten können vorgezogen werden / Nacharbeit behindert die Aufgabenerfüllung nicht merklich / andere Organisationseinheiten oder Vertragspartner werden in ihrer Arbeit nicht wesentlich gestört
Verstoß gegen Gesetze, etc.	Verstöße gegen Gesetze und Bestimmungen mit geringen Konsequenzen / Verstöße werden nur intern bemerkt
negative Innen- und Außenwirkung	Störungen bzw. Ausfälle werden nur in Einzelfällen bemerkt und von Kunden und Geschäftspartnern als bedeutungslos eingeschätzt / Kunden und Geschäftspartner ziehen keine Konsequenzen / das grundsätzliche Vertrauen in die Institution ist nicht beeinträchtigt / keine wahrnehmbaren Verluste von Marktanteilen
Schadenskategorie „hoch“	
finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend (z. B. Verlust unter 20-30% des Umsatzes)
Beeinträchtigung der Aufgabenerfüllung	Nicht tolerierbare Unterbrechungen bzw. Einschränkungen / Minderung der Arbeitsqualität / Fristversäumnisse nach außen wirksam / Rückstandsaufholung nicht innerhalb der normalen Arbeitszeit möglich / andere Organisationseinheiten oder Vertragspartner werden in ihrer Arbeit erheblich gestört, auch dort müssen Rückstände aufgeholt werden / Konventionalstrafen in akzeptablem Rahmen
Verstoß gegen Gesetze, etc.	Verstoß gegen Gesetze und Bestimmungen mit tolerierbaren Konsequenzen / Verstöße werden auch außerhalb der Institution bemerkt
negative Innen- und Außenwirkung	Störungen bzw. Ausfälle werden von Kunden und Geschäftspartnern deutlich bemerkt und in der Brache wahrgenommen / Image und Vertrauen in die Institution sind bei einzelnen Kunden und Geschäftspartnern beeinträchtig / Image- bzw. Vertrauensverluste sind mit hohem Aufwand wieder auszugleichen / einzelne Kunden und Geschäftspartner ziehen Konsequenzen und beenden die Geschäftsbeziehung / merkliche Verluste von Marktanteilen / Verluste sind mit Aufwand wieder zurückzugewinnen

Schadenskategorie „sehr hoch“	
finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzgefährdend (z. B. wenn der Verlust 30% des Umsatzes überschreitet)
Beeinträchtigung der Aufgabenerfüllung	gravierende Beeinträchtigung der Aufgabenerfüllung / Rückstände können nur mit externer Hilfe oder gar nicht aufgeholt werden / Verzögerte und fehlerhafte Ergebnisse werden extern deutlich bemerkt / schwerwiegende Minderung der Servicequalität / die Arbeit anderer Organisationseinheiten oder Vertragspartner ist nicht möglich / hohe Haftungsansprüche, Konventionalstrafen
Verstoß gegen Gesetze, etc.	Verstoß gegen Gesetze mit Konsequenzen für den Geschäftsbetrieb und einzelne Mitarbeiter
negative Innen- und Außenwirkung	ein erheblicher Teil der Kunden und Geschäftspartner zieht aus den Vorfällen Konsequenzen / Image, Vertrauen und Zuverlässigkeit der Institution sind stark beeinträchtigt und werden grundsätzlich in Zweifel gezogen / Image- und Vertrauensverluste sind schwer oder nicht mehr auszugleichen / starke Verluste von Marktanteilen / Verluste sind schwer oder nicht auszugleichen

Tabelle 2: Beispiel für Abgrenzung der Schadenskategorien

Nach der Festlegung, welche Schadensszenarien in die Bewertung einbezogen werden, können die einzelnen Szenarien im Hinblick auf ihre Bedeutung für die Institution noch gewichtet werden. Eine Gewichtung der Blickwinkel ist dann sinnvoll, wenn die Institution die Schadensszenarien „finanzielle Auswirkungen“, „Beeinträchtigung der Aufgabenerfüllung“, „Verstoß gegen Gesetze und Verträge“, „Gefahr für Leib und Leben“ und „negative Innen- und Außenwirkung“ als für die Institution unterschiedlich bedeutsam werten und einen Schwerpunkt setzten möchte.

B. Festlegung der zu betrachtenden Bewertungsperioden

Bei einer BIA wird im Gegensatz zu einer Schutzbedarfsfeststellung nicht nur bewertet, welche Auswirkungen ein Ausfall eines Prozesses für die Institution hat, sondern auch wie sich der Schaden zeitlich entwickelt. Dazu ist es notwendig, sogenannte Bewertungsperioden festzulegen. Für jede Bewertungsperiode wird der Schaden im Falle eines Ausfalls für den jeweiligen Geschäftsprozess durch die Angabe der Schadenskategorie bewertet.

Die Anzahl der Bewertungsperioden wie auch deren Länge ist individuell für die Institution zu wählen, da diese stark von den Gegebenheiten abhängen. Die Gegebenheiten sind beispielsweise die Art der angebotenen Dienstleistungen, die Vielfältigkeit der Geschäftsprozesse, die Art der erzeugten Produkte oder einfach die Branche mit ihren gesetzlichen Vorgaben. So wird eine Bank die einzelnen Bewertungsperioden wahrscheinlich sehr kurz wählen, während Institutionen mit einem weniger zeitkritischen Geschäftsmodell die Perioden deutlich größer wählen werden. Als Hilfe für die Festlegung der Anzahl wie auch der Dauer der Bewertungsperioden können die Wiederanlaufklassen (siehe Kapitel 5.1.2.6) für die Geschäftsprozesse dienen, sofern diese vorhanden bzw. zu diesem Zeitpunkt abschätzbar sind.

In der Praxis hat sich für eine Institution mit durchschnittlichen Anforderungen bezüglich der Verfügbarkeit eine Einteilung in vier bis zehn Bewertungsperioden bewährt. Folgende Tabelle zeigt verschiedene Beispiele, wie eine Einteilung der Bewertungsperioden aussehen könnte. Die Zeitangaben sind dabei als „bis … Stunden“ zu verstehen.

	Bewertungsperioden (96 Stunden = 4 Tage, 168 Stunden = 1 Woche, 720 Stunden = 1 Monat)									
Zeitperiode	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Beispiel 1	24	72	240	720						
Beispiel 2	8	24	48	72	168	720				
Beispiel 3	1	2	4	8	24	48	96	168	240	720

Tabelle 3: Beispiele für Bewertungsperioden

Gegebenfalls ist es sinnvoll, noch eine weitere Bewertungsperiode einzuführen, beispielsweise für den Zeitraum „≥3 Monate“, die den Fall abdeckt, dass erhebliche Zerstörungen der Infrastruktur vorliegen, der Standort bis auf Weiteres nicht mehr zur Verfügung steht und keine Planungen bezüglich Ausweichstandort getroffen sind. Sind keine Ausweichstandorte vorhanden und keine Vorsorgemaßnahmen diesbezüglich getroffen worden, so nehmen die Wiederherstellungsmaßnahmen, angefangen bei der Suche nach einer geeigneten Lokation, eine erhebliche Zeit in Anspruch.

C. Besondere Termine und Ereignisse

Viele Geschäftsprozesse unterliegen in ihren Verfügbarkeitsanforderungen im Laufe eines Tages, eines Monats oder eines Jahres teilweise erheblichen Schwankungen. Dies kann sowohl ein bestimmtes Zeitintervall (z. B. tägliche Cut-Off Time (Abschluss- oder Stichzeit) in Banken, Redaktionsschluss für die Anzeigen einer Wochenzeitung, das Jahresende für einen Jahresabschluss, die Vorweihnachtszeit für einen Online-Shop oder ein bestimmter Wochentag für den Herausgeber eines Wochenblatts) oder ein bestimmtes Ereignis (z. B. Zinserhöhung für eine Bank oder die Pause einer Fußballübertragung für ein Wasserwerk) sein.

Jede Institution hat die strategische Entscheidung zu treffen und zu dokumentieren, wie mit diesen saisonalen oder ereignisbedingten Einflüssen auf die Verfügbarkeitsanforderungen bei der Schadensanalyse umzugehen ist. Aus diesem Grunde und als Basis für die strategische Entscheidung sollten diese Termine und die möglichen Ereignisse mit deren Eintrittswahrscheinlichkeiten erhoben und eine Grobeinschätzung der Schwankungen in den Verfügbarkeitsanforderungen der entsprechenden Prozesse getroffen werden. Besondere Termine können übersichtlich in einem Kalender graphisch dargestellt werden (siehe Abbildung 5). Besondere Ereignisse, deren Auftreten im Voraus zeitlich nicht festgelegt ist, sind zu listen.

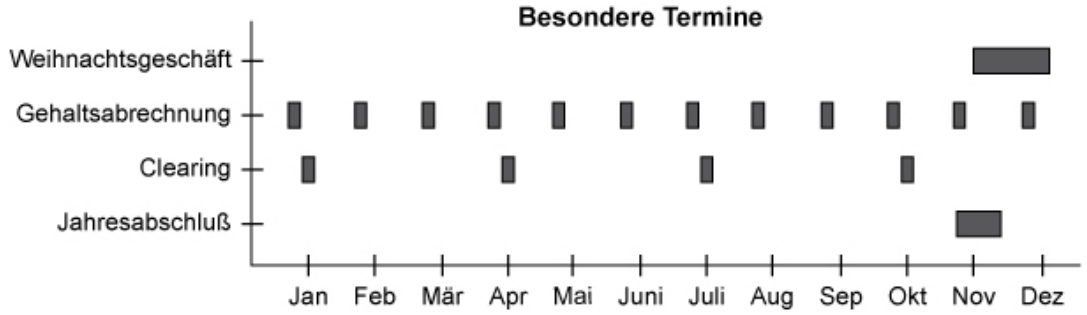


Abbildung 5: Besondere Termine

Das bloße Wissen um die besonderen Termine und Ereignisse kann eine wichtige Information bei Entscheidungen während der Notfallbewältigung sein sowie bei der Planung und Festlegung von Zeiten für Tests und Übungen. Tests und Übungen sollten nicht in die Zeitperioden mit höheren Verfügbarkeitsanforderungen gelegt werden.

Mögliche Varianten für die Strategie zur Behandlung von besonderen Terminen und Ereignissen sind:

- Der Schadensanalyse wird das Worst-Case-Szenario zugrunde gelegt, also die höchste Verfügbarkeitsanforderung des jeweiligen Geschäftsprozesses aus den besonderen Terminen und Ereignissen für den ganzen Zeitraum übernommen.

- Bei der Schadensanalyse werden die verschiedenen Zeitspannen für den jeweils betrachteten Prozess unterschieden und die benötigten Informationen für jede Zeitspanne separat erhoben.
- Der Schadensanalyse wird der Normalfall zugrunde gelegt.

Die erste Variante, die in der Praxis am häufigsten angewendet wird, führt zu Mehraufwand in den Vorsorgemaßnahmen, doch besagt schon Murphys Gesetz, dass „alles, was schief gehen kann, auch schief gehen wird“ und der Notfall immer in der ungünstigsten Situation eintritt. Die zweite Variante bedeutet Mehraufwand bei der Durchführung der BIA, der Priorisierung, der Entwicklung von Notfallplänen bis hin zu den Tests und Übungen. Der Mehraufwand für die zweite Variante steigt überproportional mit der Anzahl der zu unterscheidenden Zeitspannen und sollte nur dann in Betracht gezogen werden, wenn es sich um sehr wenige Zeitspannen handelt. Die dritte Variante bedeutet die Übernahme des Risikos für die besonderen Termine und Zeitspannen, doch sollte diese nur in Ausnahmefällen gewählt werden. Diese Variante kann dann sinnvoll sein, wenn beispielsweise der Mehraufwand für die Vorsorge für die höheren Anforderungen in keinem wirtschaftlichen Verhältnis zum Risiko stehen würde, der durch die Nichtbeachtung der höheren Anforderungen in einem sehr geringen Zeitfenster besteht. Wird diese Variante gewählt, so ist zusätzlich zur Dokumentation der gewählten Strategie das Risiko eindeutig und nachvollziehbar darzustellen und das Vorgehen zu begründen. Die Risikoübernahme ist schriftlich durch die Leitungsebene zu bestätigen.

D. Durchführung der Schadensanalyse

Sind die Vorarbeiten abgeschlossen und die Rahmenbedingungen festgelegt, kann die nicht triviale Aufgabe der eigentlichen Schadensanalyse beginnen. Dabei sind nun für die einzelnen Geschäftsprozesse die Auswirkungen eines Ausfalls für die Institution in den einzelnen Bewertungsperioden anhand der Schadensszenarien abzuschätzen, also der Schadensverlauf zu ermitteln.

Die Aufgabe der Schadensanalyse sollte in den jeweiligen Organisationseinheiten durchgeführt werden, da gute Kenntnisse über die Geschäftsprozesse benötigt werden. Die Notfallkoordinatoren sind für die Durchführung zuständig und erarbeiten in Zusammenarbeit mit den Prozessverantwortlichen und eventuell mit dem Leiter der Organisationseinheit die entsprechenden Informationen.

Die Bewertungen können verbal erfolgen in der Art: „Der Ausfall eines Prozesses führt zu direkten wirtschaftlichen Schäden, die bis 96 Stunden niedrig, bis 168 Stunden normal und ab 720 Stunden hoch sind, während keine Auswirkungen bezüglich Gesetzeskonformität gegeben sind“. Eine in der Praxis oftmals genutzte Form ist die Tabelle. Die tabellarische Form hat den Vorteil, dass ein schneller Überblick gewonnen werden kann. In Tabelle 4 wird ein vereinfachtes Beispiel gegeben, wie die tabellarische Form für die Schadensanalyse eines Prozesses aussehen könnte.

Für die Auswertung des Schadensverlaufs eines Geschäftsprozesses können zusätzlich die einzelnen gewichteten Summen über die Schadensszenarien oder die Zeit gebildet werden (letzte Zeile in Tabelle 4). Die Summen zeigen den jeweiligen Gesamtschaden über alle gewichteten Schadensszenarien für jede einzelne Betrachtungsperiode.

Prozess: *Prozessname*									
Bearbeiter: *Hr. Müller (Notfallkoordinator)*									
Ansprechpartner / Interviewpartner: *Frau Maier (Prozessverantwortliche)*									
Organisationseinheit: *Abteilung 1*									
Datum der Erhebung: *11. Feb. 2008*									
Zeitraum:									
Wiederanlauf:	**Wiederherstellung:**				**Maximal tolerierbare Ausfallzeit:**				
Wiederanlaufniveau:									
Bewertungsperioden / Schadensszenarien	**8 Std.**	**24 Std.**	**48 Std.**	**96 Std.**	**168 Std.**	**720 Std.**	**≥ 720**	**Gew.**	**Anmerkungen**
finanzielle Auswirkungen	*1*	*1*	*1*	*2*	*2*	*3*	*3*	5	
Beeintr. der Aufgabenerfüllung	*1*	*1*	*2*	*2*	*3*	*3*	*4*	3	
Verstoß gegen Gesetze, Verträge	*nicht gegeben für diesen Prozess*							1	
Imageschaden	*1*	*1*	*1*	*1*	*1*	*2*	*3*	1	
Gewichtete ∑	*9*	*9*	*12*	*17*	*20*	*26*	*30*		

Tabelle 4: Beispiel Schadensverlauf eines Geschäftsprozesses (1="niedrig", 2="normal", 3=„hoch", 4="sehr hoch")

Liegen für die finanziellen Auswirkungen genauere Angaben über die Höhe der zu erwartenden Schäden vor (z. B. aus dem Controlling), so können auch diese in der Tabelle aufgenommen werden. Die Angabe von genauen Beträgen suggeriert eine Genauigkeit, die häufig nicht gegeben ist, so dass dieses Mittel nur dann angewendet werden sollte, wenn die Beträge auch stimmig und sinnvoll sind. Als zusätzliche Information zur qualitativen Einschätzung kann es hilfreich sein.

Eine Möglichkeit, einen guten Überblick über alle Geschäftsprozesse zu erhalten, ist, die Ergebnisse der Einzelprozesse in eine Gesamtübersicht zu übernehmen. In Tabelle 5 und 6 werden zwei alternative Darstellungen des Schadensverlaufs mehrerer Geschäftsprozesse im Überblick vorgestellt. Zur besseren Darstellung wurden die Anzahl der Schadensszenarien und der Bewertungsperioden reduziert.

				finanzielle Auswirkung				**Beeinträchtigung der Aufgabenerfüllung**				**Negative Innen- und Außenwirkung**			
				Gewicht: 5				**Gewicht: 3**				**Gewicht: 1**			
Prozesse	**Wiederanlauf**	**Wiederherstellung**	**Max. tol. Ausfall**	**24 Std.**	**48 Std.**	**96 Std.**	**192 Std.**	**24 Std.**	**48 Std.**	**96 Std.**	**192 Std.**	**24 Std.**	**48 Std.**	**96 Std.**	**192 Std.**
P1				1	1	3	4	1	1	2	3	1	1	1	2
P2				1	2	3	4	1	2	3	3	1	1	2	3
P3				1	1	1	2	1	2	3	3	1	2	3	4
…															
P12				1	1	2	4	1	2	3	3	1	1	1	1

Tabelle 5: Beispiel 1 für Gesamtüberblick Schadensbewertungen

Prozess	Wiederanlauf	Wiederherstellung	Max. tol. Ausfall	24 Stunden	48 Stunden	96 Stunden	192 Stunden	Gewicht	Schadensszenario
P1				1	1	3			
				1	1	2			
				1	1	1	2		**Imageschaden**
				9	***9***	***22***	***31***		***Gew. Σ***
P2						3	4	5	**finanzielle Auswirkungen**
						3	3	3	**Beeintr. der Aufgabenerfüllung**
				1	1	2	3	1	**Imageschaden**
				9	***17***	***26***	***32***		***Gew. Σ***
P3				1	1	1	2	5	**finanzielle Auswirkungen**
				1	2	3	3	3	**Beeintr. der Aufgabenerfüllung**
				1	2	3	4	1	**Imageschaden**
				9	***13***	***17***	***23***		***Gew. Σ***
…	…		…	…	…	…	…	…	**…**
P12				1	1	2	4	5	**finanzielle Auswirkungen**
				1	2	3	3	3	**Beeintr. der Aufgabenerfüllung**
				1	1	1	1	1	**Imageschaden**
				9	***12***	***20***	***30***		***Gew. Σ***

Gewichteter Schaden nach 192 Stunden

Schadensanstieg

Tabelle 6: Beispiel 2 für Gesamtüberblick Schadensbewertungen

Bei der Festlegung der Wiederanlauf- und Wiederherstellungszeiten für die einzelnen Prozesse sollte sowohl der Schadensverlauf, der Schaden nach einer bestimmten Zeitspanne (z. B. gewichteter Schaden nach 192 Stunden im Beispiel der Tabelle 6) wie auch die vorhandenen Kapazitäten für den Wiederanlauf bzw. Wiederherstellung in die Betrachtung mit einbezogen werden. Dabei ist sowohl eine Orientierung am Schadensanstieg über alle Schadensszenarien, aber auch am jeweiligen Gesamtschaden möglich.

Die Ergebnisse der Schadensanalyse aus den einzelnen Organisationseinheiten werden durch den Notfallbeauftragten zentral zusammengefügt und konsolidiert.

Mit welcher Methode und in welcher Ausprägung die Schadensanalyse durchgeführt wird, muss jede Institution für sich entscheiden. Eine kleine oder mittlere Institution könnte die Anzahl der Bewertungsperioden und der Schadensszenarien reduzieren und das beschriebene Verfahren anwenden. Der pragmatischste Ansatz für kleine Institutionen, der weder Vollständigkeit garantiert noch objektiv nachvollziehbare Ergebnisse liefert, wäre, in einem Workshop in Zusammenarbeit mit den Verantwortlichen die relevanten Prozesse zu ermitteln, zu klassifizieren bzw. zu priorisieren. Als Minimalanforderung ist eine Liste der Geschäftsprozesse zu erstellen und für diese die Verfügbarkeitsanforderungen festzulegen. Wurde ein Sicherheitskonzept nach BSI-Standard 100-2 erstellt, so liegen diese Informationen für den Großteil der Ressourcen im Wesentlichen vor und können übernommen werden.

5.1.2.4 Festlegung der Wiederanlaufparameter

Bei der Durchführung der Schadensanalyse oder auch im Anschluss daran sind die maximal tolerierbare Ausfallzeit (MTA), die Wiederanlaufzeit (WAZ) und das Wiederanlauf-Niveau für die einzelnen Geschäftsprozesse festzulegen.

Die maximal tolerierbare Ausfallzeit MTA (auf englisch Maximum Tolerable Period of Disruption, MTPD) eines Prozesses bezeichnet den Zeitrahmen, in der der Wiederanlauf spätestens erfolgen muss, damit die Institution nicht in eine Phase gerät, in der kurz- oder langfristig ihre Überlebensfähigkeit gefährdet ist.

Die Wiederanlaufzeit WAZ (englisch Recovery Time Objective, RTO) ist die angestrebte Zeit, in der der Wiederanlauf des Prozesses erfolgen soll. Die Zeit für den Wiederanlauf WAZ muss kleiner als die maximal tolerierbare Ausfallzeit MTA sein.

Der Wiederanlauf eines Prozesses, auch Geschäftsfortführung genannt, kann in einem

- Notbetrieb mit beliebiger Abstufung in der Kapazität und Ressourcen sowohl in der ursprünglichen Umgebung des Normalbetriebs oder
- auf Ausweichressourcen (z. B. an einem Ausweichstandort) erfolgen sowie
- durch einen Alternativprozess mit andersartigen Ressourcen und anderen Abläufen.

Neben dem Zeitpunkt für den Wiederanlauf ist auch das Wiederanlauf-Niveau, die notwendige Kapazität des Prozesses für einen stabilen Notbetrieb (z. B. 60% Kapazität), festzulegen.

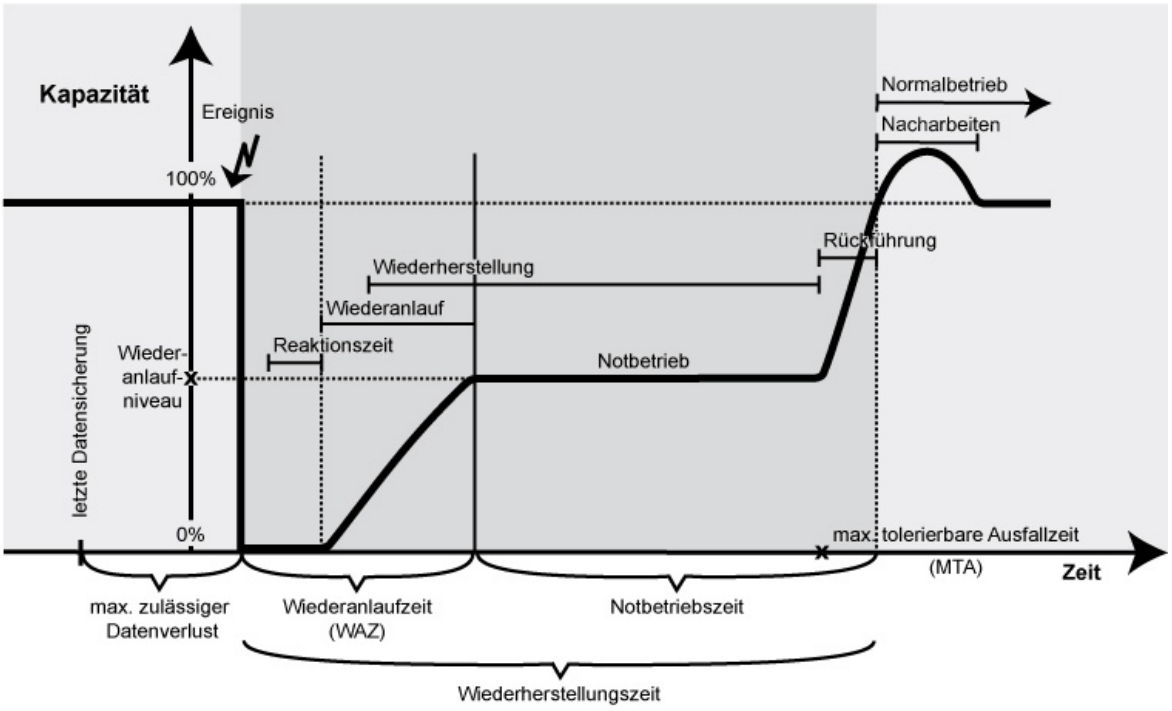


Abbildung 6: Wiederanlaufparameter

Es ist sinnvoll, bei der Betrachtung des zeitlichen Ablaufs eines Notfalls und des Wiederanlaufs eines Prozesses weitere Aktivitäten und deren benötigten Zeitintervalle zu betrachten, festzulegen oder einzurechnen (siehe Abbildung 6). So setzt sich die Wiederanlaufzeit aus der Zeit bis zur Entdeckung des Notfalls, der Reaktionszeit (von der Meldung, über die Eskalation bis zur Einleitung der Maßnahmen zum Wiederanlauf) und der benötigten Zeit für den eigentlichen Wiederanlauf zusammen. Da der Wiederanlauf in den seltensten Fällen sofort in den Normalbetrieb erfolgt, ist es sinnvoll, die maximal tolerierbare Notbetriebszeit (MTN) festzulegen bzw. die maximal tolerierbare Wiederherstellungszeit (MTW). Letztere ergibt sich aus der Wiederanlaufzeit plus der maximal tolerierbaren Notbetriebszeit.

Die Wiederherstellungszeit kann auch größer als die maximal tolerierbare Ausfallzeit MTA sein, da das Eintreten einer existenzgefährdenden Schieflage durch den Notbetrieb zeitlich verschoben wird. Die Zeit für die Rückführung vom Notbetrieb zum Normalbetrieb ist Teil der Notbetriebszeit und mit einzuplanen. Ist der Normalbetrieb erreicht, so sind möglicherweise notwendige Nacharbeiten

durchzuführen, die eine Nacharbeitszeit benötigen und zeitlich zum Normalbetrieb gerechnet werden. Bei der Festlegung des maximal tolerierbaren Notbetriebs sollte die daraus resultierende Nacharbeitszeit mitbetrachtet werden. Werden durch einen zu lange andauernden Notbetrieb die Nacharbeiten so umfangreich, dass sie nicht mehr in einer sinnvollen Zeit durchzuführen sind, so kann dadurch eine weitere Schieflage entstehen.

5.1.2.5 Berücksichtigung von Abhängigkeiten

Die Schadensanalyse und die Festlegung der maximal tolerierbaren Ausfallzeit, der Wiederanlaufzeit und eventuell der Wiederherstellungszeit erfolgen bezogen auf die Einzelprozesse. Der nächste Schritt ist nun, die Abhängigkeiten zwischen den Geschäftsprozessen einzubeziehen und die Verfügbarkeitsanforderungen gegebenenfalls nachzukorrigieren. Optional kann es sinnvoll sein, durch einen zusätzlichen Top-Down-Ansatz die strategischen Behörden- oder Unternehmensziele bei der Priorisierung der Prozesse für den Wiederanlauf mit zu berücksichtigen.

Prozessabhängigkeiten

Abhängigkeiten zwischen den Geschäftsprozessen können bewirken, dass die Wiederanlaufzeiten einzelner Prozesse angepasst werden müssen. Die Höhe der Korrektur ist abhängig vom Grad der jeweiligen Abhängigkeit zwischen den Prozessen. Benötigt ein Geschäftsprozess den Output oder die Dienstleistung eines anderen Prozesses, so wird eine eventuell höhere Verfügbarkeitsanforderung des betrachteten Prozesses an die liefernden Prozesse abgestuft vererbt. Wird vom betrachteten Prozess ein Output generiert, so ist zu untersuchen, in wie weit die Notwendigkeit besteht, dass der erzeugte Output zeitnah vom Nachfolgeprozess konsumiert wird. In diesem Falle ist eine höhere Verfügbarkeitsanforderung auch auf den Nachfolger zu vererben, damit sichergestellt wird, dass es nicht zur „Verstopfung“ in der Prozesskette kommt, da der Output nicht abgegeben werden kann. In die Betrachtung der Prozessabhängigkeiten sind auch die ausgelagerten Prozesse einzubeziehen.

Der Grad der Vererbung und damit die Erhöhung der Wiederanlaufzeit des verbundenen Prozesses hängt vom Grad der Abhängigkeit ab. Das bedeutet, je höher die Abhängigkeit ist, umso stärker ist die Erhöhung oder Angleichung der Wiederanlaufzeit. Daher ist es sinnvoll, nicht nur zwischen „unabhängig“ und „abhängig“ zu unterscheiden, sondern ein abgestuftes Modell zu wählen. Empfehlenswert sind 3-6 Stufen für den Abhängigkeitsgrad. Ein Beispiel mit 4 Abhängigkeitsstufen könnte folgendermaßen aussehen: 1=„sehr hoch“, 2=„hoch“, 3=„mittel“ und 4=„gering“. Der Abhängigkeitsgrad „gering“ bedeutet, dass keine Anpassung notwendig ist, der Abhängigkeitsgrad „sehr hoch“ drückt eine 1-zu-1-Übernahme der Wiederanlaufzeit aus. Für die Zwischenstufen ist die Definition des Abhängigkeitsgrads individuell festzulegen. Abbildung 7 zeigt in sehr vereinfachter Form das Vorgehen. So wird beispielsweise die Wiederanlaufzeit des Prozesses GP5 abgestuft auf den Vorgänger GP4 vererbt, da eine „hohe“ Abhängigkeit zwischen den beiden Prozessen besteht. Die Wiederanlaufzeit des Prozesses GP4 wird dadurch von 168 Stunden auf 48 Stunden reduziert. Neben der Wiederanlaufzeit sollte auch das Wiederanlauf-Niveau der abhängigen Prozesse kontrolliert und gegebenenfalls abgeglichen werden.

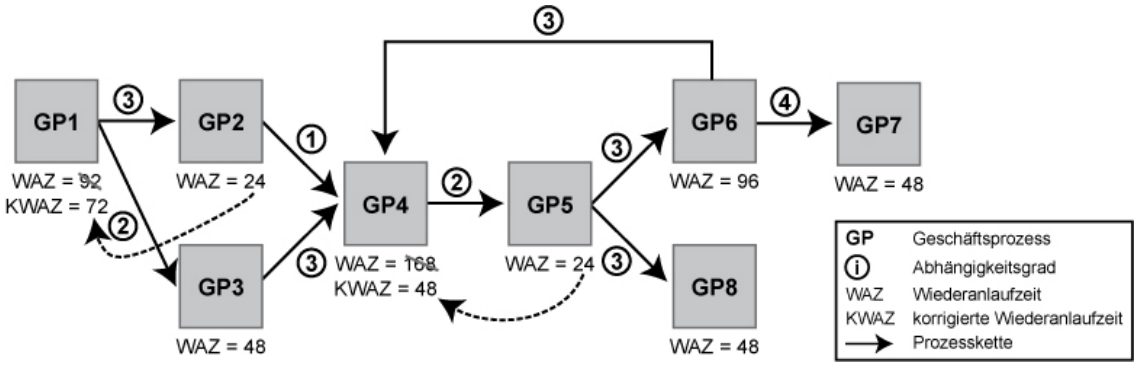


Abbildung 7: Vererbung der Wiederanlaufzeit in Richtung Vorgänger

Dieser Abhängigkeitsgrad ist für beide Richtungen zu ermitteln, also in Richtung Vorgänger und in Richtung Nachfolger. Die Festlegung der jeweiligen Abhängigkeitsgrade zu Vorgänger und Nachfolger sollte durch den Prozesseigentümer vorgenommen werden, sinnvoller Weise bei der Erstellung der Prozesslandkarte im Vorfeld der BIA.

Der Grad der Prozessabhängigkeiten kann im Normal- und im Notbetrieb unterschiedlich sein. Ist in dieser Phase der Konzeption ersichtlich, dass Unterschiede bestehen und ist bekannt, wie der Notbetrieb aussehen wird, so sollten die Abhängigkeiten im Notbetrieb betrachtet werden. Wird die Art des Notbetriebs zu einem späteren Zeitpunkt der Konzeption abgeändert oder erst festgelegt, so sollte eine erneute Überprüfung der entsprechenden Abhängigkeiten und gegebenenfalls Korrekturen vorgenommen werden.

Prozessketten

Bei der Schadensanalyse wurden einzelne Geschäftsprozesse betrachtet und die Schadensauswirkungen bei deren Ausfall. Bei der Betrachtung der Prozessabhängigkeiten wurden die Verfügbarkeitsanforderungen entlang der Prozesskette abhängig vom Abhängigkeitsgrad vererbt. Zusätzlich kann es sinnvoll sein, bei hohen Abhängigkeiten innerhalb einzelnen Prozessketten, diese im Ganzen zu betrachten und den Schaden der einzelnen Geschäftsprozesse aufzusummieren, der bei Ausfall der Gesamt- oder Teilkette entstehen würde, verursacht durch den Ausfall eines oder mehrere essentieller Prozesse. Sollte der Gesamtschaden bei Ausfall einer Prozesskette sehr schnell eine existenzgefährdende Höhe erreichen, so ist zu überprüfen, ob eine weitere Korrektur der einzelnen Wiederanlaufzeiten in dieser Kette nach unten sinnvoll ist.

Geschäftsziele

Es ist sinnvoll, zusätzlich einen „Top-Down"-Ansatz durch die Institutionsleitung einzubringen, bei dem die Geschäftsziele, die Intention einzelner Interessensgruppen und die Kernprozesse unter einem weiteren Blickwinkel betrachtet werden. Die Geschäftsziele einer Behörde leiten sich meist von deren gesetzlichem Auftrag ab. In der Leitungsebene liegt nicht nur das Wissen über die aktuelle Ausrichtung der Institution vor, sondern auch die in die Zukunft weisende Strategie und die damit verbundene Entwicklung der Relevanz und Bedeutung einzelner Geschäftsprozesse, Geschäftszweige, Abteilungen oder gar Unternehmensteile für die Institution.

Für eine zusätzliche Bewertung in einem „Top-Down"-Ansatz priorisiert die Leitungsebene die Interessensgruppen und die Geschäftsziele und damit die Prozessketten, die zum Erreichen dieser Geschäftsziele beitragen. Prozesse, die zur Erreichung mehrerer oder höher priorisierter Geschäftsziele erforderlich sind, werden gegenüber denjenigen, die lediglich zu einem oder weniger wichtigen Geschäftsziel beitragen, höher bewertet. Die zusätzliche Bewertung durch die Leitungsebene fließt in die Gesamtbeurteilung der einzelnen Prozesse und deren Wiederanlaufzeiten ein.

Wird dieser Ansatz verfolgt, sollten jedoch zwei Aspekte beachtet werden:

- Ist ein Prozess Bestandteil mehrerer Prozessketten, so schlägt sich diese Tatsache indirekt auch in der Schadensanalyse nieder.
- Da nur die Prozessketten betrachtet werden, die direkt der Erreichung von Geschäftszielen dienen, werden ausschließlich die Kernprozesse betrachtet. Die unterstützenden Geschäftsprozesse sind aus dieser Betrachtung ausgeschlossen.

Ressourcenabhängigkeit

Bei der Festlegung der Wiederanlaufzeiten für die Geschäftsprozesse sollte ein weiterer Blick den für die Wiederherstellung und den Wiederanlauf genötigten Ressourcen gelten. So ist eventuell der gleichzeitige Wiederanlauf vieler Prozesse zu einem bestimmten Zeitpunkt gefordert, doch mit dem zur Verfügung stehenden Personal nicht umzusetzen. Eine weitere Entzerrung des Wiederanlaufs und Korrektur der Wiederanlaufzeiten kann dadurch notwendig werden.

Beachtung besonderer Termine und Ereignisse

Wurde für die Behandlung von besonderen Terminen die Strategie (siehe Kapitel 5.1.2.3.C) gewählt, die verschiedenen Zeitspannen für den jeweils betrachteten Prozess zu unterscheiden und die benötigten Informationen für jede Zeitspanne in der Schadensanalyse separat zu erheben, so sind diese Geschäftsprozesse bei der Priorisierung besonders zu beachten. Die Unterscheidung von unterschiedlichen Zeitspannen hat sowohl Mehraufwand bei der Vererbung über die Prozessabhängigkeiten zur Folge, wie auch bei der Erstellung unterschiedlicher Prioritätenlisten für die verschiedenen Zeitspannen.

5.1.2.6 Priorisierung und Kritikalität der Geschäftsprozesse

Sind die Wiederanlaufzeiten für die Geschäftsprozesse festgelegt und fein abgestimmt, so liegt damit auch eine Reihenfolge bzw. Priorisierung vor. Die Wiederanlaufzeiten können in der Regel in einzelne Wiederanlaufklassen eingeteilt werden. In den einzelnen Klassen kann zusätzlich eine Reihenfolge für den Wiederanlauf der Prozesse festgelegt werden.

Für die weitere Konzeption ist es nicht notwendig, die Kritikalität festzulegen, doch hilft es im Sprachgebrauch. Für die Festlegung der Kritikalität von Geschäftsprozessen kann die Wiederanlaufzeiten bzw. Wiederanlaufklassen herangezogen werden, da im Notfallmanagement „kritisch“ „zeitkritisch“ bedeutet. Indirekt bedeutet „kritisch“ damit aber auch „schadenskritisch“, da der Wiederanlauf umso schneller erfolgen muss je schneller und höher der Schaden steigt. Für die Festlegung der Kritikalität können neben dem Wiederanlauf beliebige, sinnvolle Kriterien herangezogen werden, wie beispielsweise die maximal tolerierbare Ausfallzeit oder der Gesamtschaden nach x Stunden. Jede Institution kann für sich entscheiden, von welchem Kriterium sie Kritikalität ableitet und welche und wie viele Kritikalitätskategorien sie verwendet. Tabelle 7 zeigt als Beispiel die Einteilung in vier Kritikalitätskategorien und Möglichkeiten einer Festlegung. Die Zahlen sind fiktiv gesetzt und nicht für eine unreflektierte Übernahme geeignete.

Kritikalitäts-kategorie	Wiederanlauf	Maximale tolerierbare Ausfallzeit	Gesamtschaden nach x Stunden	Allgemein
„unkritisch“	> 720 Stunden	> 504 Stunden	„niedrig“	Ausfall hat keine oder nur minimale Auswirkungen.
„wenig kritisch“	≤ 720 Stunden	≤ 504 Stunden	„normal“	Ausfall hat Auswirkungen.
„kritisch“	≤ 168 Stunden	≤ 240 Stunden	„hoch“	Ausfall hat beträchtliche Auswirkungen.
„hoch kritisch“	≤ 4 Stunden	≤ 6 Stunden	„sehr hoch“	Ausfall oder Beeinträchtigung führen zu existentiell bedrohlichen Auswirkungen.

Tabelle 7: Beispiel Kritikalitätskategorien

Sinnvollerweise werden die Kritikalitätskategorien so festgelegt, dass sich die weiteren Arbeiten im Notfallmanagement auf die als mindestens kritisch identifizierten Geschäftsprozesse konzentrieren, um den Aufwand der nun folgenden Arbeitsschritte auf ein sinnvolles Maß zu reduzieren. Wird im Folgenden Text von „kritischen“ Geschäftsprozessen gesprochen, so sind die Geschäftsprozesse gemeint, die im Notfallkonzept weiter betrachtet werden und nicht aufgrund der geringen Zeit- oder Schadenskritikalität nachgeordnete Priorität erhalten haben. Dies ist von der jeweiligen Notfallstrategie der Institution abhängig.

5.1.2.7 Erhebung der Ressourcen für Normal- und Notbetrieb

Für die Durchführung von Geschäftsprozessen wird eine Vielzahl von Ressourcen benötigt. Für die kritischen Geschäftsprozesse wird nun erhoben, welche Ressourcen im Normalbetrieb benötigt werden und welche exklusiv bzw. von mehreren Prozessen genutzt werden. Diese Informationen sind für die Entwicklung von Wiederanlaufplänen relevant und sollten mit Sorgfalt erhoben werden. Liegt ein Sicherheitskonzept nach IT-Grundschutz vor, so kann ein Großteil der benötigten Informationen aus der Strukturanalyse übernommen werden. Einige Informationen über Ressourcen sind zusätzlich zu erheben, da im Notfallmanagement weitere Klassen von Ressourcen von Interesse sind. Zu den betrachteten Ressourcen zählen:

- Personal
  Für die Durchführung von Geschäftsprozessen werden Mitarbeiter benötigt, die Entscheidungen treffen, Maschinen bedienen, Daten eintragen oder sonstige Arbeitsschritte durchführen. Werden für einen Geschäftsprozess spezielle Fachqualifikationen oder -kenntnisse benötigt, so sollte diese Information mit erfasst werden, genauso wie die Information über designierte, mögliche oder fehlende Stellvertreter. Wird für den Wiederanlauf oder die Wiederherstellung Spezialpersonal benötigt, so sollte diese Information ebenfalls erhoben werden.
- Informationen
  Zu Informationen werden sowohl elektronische Daten wie auch Unterlagen in Papierform gezählt, die zur Durchführung von Geschäftsprozessen benötigt werden. Eine grobe Klassifizierung der Bedeutung der Daten für die Geschäftsprozesse und die Identifizierung der essentiellen Daten für die Prozesse ist für die weitere Betrachtung hilfreich.

  > Bei der Erfassung der Ressource „Informationen“ sollte mindestens für die kritischen Daten der maximal zulässige Datenverlust (z. B. in Form von Anzahl von Transaktionen oder Alter der Daten) ermittelt werden. Dieser Wert beeinflusst insbesondere die Datensicherungsstrategie.

- Informationstechnologie
  Unter IT werden beispielsweise Anwendungen, Hardware, Software, Kommunikationsverbindungen, z. B. über Intranet oder Internet, aber auch TK-Anlage, Faxgeräte oder Scanner zusammengefasst.
- Spezialgeräte und –anlagen
  Zu Spezialanlagen zählen unter anderem Produktionsanlagen, Sicherheitsschleusen, medizinische Geräte oder Steuerelemente.
- Dienstleistungen
  Werden interne oder auch externe Dienstleistungen benötigt, die einen Input liefern oder benötigte Ressourcen für einen Prozess bereitstellen, so sind diese zu erheben. Beispiel einer möglichen internen Dienstleistung ist die IT-Administration.
- Infrastruktur
  Zur Infrastruktur zählen beispielsweise Gelände, Gebäude, Lager, Produktionshallen, Parkgaragen, Aktenarchive, Server- oder Büroräume, Arbeitsplatz, aber auch Strom-, Gas-, Wasser- oder Fernwärmeversorgung, Transport- und Verkehrsmittel (PKW, LKW, Züge, Flugzeug, etc.).
- Betriebsmittel
  Unter Betriebsmittel werden alle Ressourcen zusammengefasst, die noch in keiner anderen Kategorie erfasst wurden, wie beispielsweise Rohstoffe oder Materialien für eine Produktion, Büromaterialien oder Büroausstattung.

Ressource			Anwendungen								Hardware					Infrastruktur					…
			E-Mail	Datenbankserver	Office-Anwendung	SAP	EDI	AutoCAD	Kalender	…	Internet-Anbindung	LAN	FileServer1	Fileserver2	…	Arbeitsplatz	Hochlager	…	Telefonanschluß	Fax	…
Geschäfts-prozess		WAZ	4	92	24	…	…	…	…	…	48	…	…	…	…	…	…	…	…	…	…
	WAZ	kWAZ	4	18	24	…	…	…	…	…	48	…	…	…	…	…	…	…	…	…	…
Prozess GP1	92	72	1	1	4	1	3	-	4	…	3	1	1	-	…	1	-	…	1	-	…
Prozess GP4	168	48	3	-	1	-	-	-	3	…	-	1	-	1	…	-	1	…	-	2	…
Prozess GP5	24	24	-	1	1	-	-	1	-	…	-	1	1	-	…	-	-	…	-	-	…

Tabelle 8: Beispiel Ressourcenerfassung mit Angabe des Nutzungsgrads und der Wiederanlaufzeiten

Bei der Erhebung der benötigten Ressourcen für einen kritischen Prozess sollte auch der jeweilige Nutzungsgrad bewertet und dokumentiert werden. Dieser gibt indirekt an, wie sich das Wegfallen dieser Ressource auf die Fortführung des Prozesses auswirken würde. Je höher der Nutzungsgrad ist, umso höher sind die Auswirkungen bei Wegfall. Für den Nutzungsgrad hat sich eine drei- bis fünfstufige Skala bewährt. Mögliche Nutzungsgrade angelehnt an die Abhängigkeitsgrade zwischen Prozessen sind beispielsweise 1=„sehr hoch“ (unentbehrlich für den Prozess), 2=„hoch“ (wesentlich für den Prozess), 3=„mittel“ (wird benötigt) und 4=„gering“ (siehe Tabelle 8).

Spätestens in diesem Schritt werden auch die Single-Points-of-Failure identifiziert, also die sehr kritischen Ressourcen, deren Ausfall einen Komplettausfall des (Teil-)Prozesses verursachen würde. Diese Single-Points-of-Failure sind zu dokumentieren und schnellst möglich Maßnahmen zur Absicherung einzuleiten.

Neben der Erhebung der Ressourcen für den Normalbetrieb sind auch die Ressourcenanforderungen des Notbetriebs zu erfassen. Dabei ist zu beachten, dass

- nicht jeder Geschäftsprozess einen Notbetrieb erlaubt,
- der Notbetrieb darin bestehen kann, dass auf Alternativprozesse gewechselt wird (beispielsweise Ausweichen von IT-Anwendungen auf Papier oder manuelle Bearbeitung) oder
- der Notbetrieb darin bestehen kann, dass der Prozess mit einer reduzierten Kapazität gefahren wird, mit geringerer Ressourcenanforderung, aber auch geringerem In- und Output.

Für jeden kritischen Prozess ist zu dokumentieren, wie der Notbetrieb aussieht und welche Ressourcen dieser benötigt. Erfolgt der Wiederanlauf kaskadierend in mehreren Stufen, so sind für jede Stufe die notwendigen Ressourcen zu erfassen (siehe Tabelle 9).

Prozess D		Notbetrieb			
Ressourcen	Normal-betrieb	≤ 2 Stunden	≤ 24 Stunden	≤ 48 Stunden	≥ 48 Stunden
Arbeitsplatz	8	2	2	4	8
Anwendung H	8	2	2	4	8
Anwendung B	4		1	2	4
Telefonanschluss	8	1	2	2	8
Experte	8	2	2	4	8
…					

Tabelle 9: Beispiel Ressourcenerfassung für Normal- und Notbetrieb

Die Erhebung der benötigten Ressourcen erfordert Sorgfalt und Geschick, denn während Ressourcen wie der Arbeitsplatz-PC oder das Intranet meist offensichtlich sind, werden manche Betriebsmittel erst wahrgenommen, wenn sie nicht mehr zur Verfügung stehen.

Der Schritt der Ressourcenerhebung kann zusammen mit der Schadensanalyse durchgeführt werden oder auch nach der Priorisierung. Der Vorteil der ersten Variante ist, dass keine zweite Erhebung und Befragung kompetenter Ansprechpartner erfolgen muss. Der Vorteil der zweiten Variante ist, dass sich die Ressourcenerhebung auf die kritischen Geschäftsprozesse beschränkt und daher weniger Aufwand bedeutet.

5.1.2.8 Kritikalität und Wiederanlaufzeiten der Ressourcen

Die Kritikalität und die Anforderung an den Wiederanlauf von Ressourcen leiten sich in der Regel von der Kritikalität und den Wiederanlauf-Anforderungen der Prozesse ab, die diese Ressource nutzen. Bei der Vererbung der Kritikalität ist zu beachten, ob die jeweilige Ressource von mehreren Prozessen genutzt wird und welchen Nutzungsgrad sie für die einzelnen Prozesse besitzt (siehe auch Tabelle 8). Damit greifen die gleichen Prinzipien wie bei der Schutzbedarfsvererbung nach BSI-Standard 100-2: Maximumprinzip, Kumulationseffekt und Verteilungseffekt. Die Kritikalität einzelner Ressourcen wie beispielsweise E-Mail können auch durch eine Managemententscheidung hoch gesetzt werden, unabhängig von den Anforderungen durch die Geschäftsprozesse. Bei der Festlegung der Ressourcen-Wiederanlaufzeiten sind einige Randbedingungen zu beachten:

- Ist eine Ressource im Notbetrieb notwendig, so hängt ihre Wiederanlaufzeit von der Wiederanlaufzeit für den Notbetrieb ab. Wird sie im Notbetrieb nicht benötigt, so ist sie von der Anforderung an die späteste Wiederherstellungszeit des Normalbetriebs abhängig.
- Teilweise können die von einem Prozess benötigten Ressourcen parallel wiederhergestellt werden, doch manche erfordern eine bestimmte Reihenfolge. So können beispielsweise Daten erst eingespielt werden, wenn die zugehörigen Anwendungen (z. B. Datenbank) installiert sind. Diese können erst wiederhergestellt werden, wenn die IT vorhanden ist, die ihrerseits erst bei vorhandener Infrastruktur wiederhergestellt werden kann (Infrastruktur-WAZ + IT-WAZ + Anwendungs-WAZ inklusive Datenwiederherstellung ≤ Prozess-Wiederanlauf). Daher sind die Wiederanlaufzeiten der Ressourcen oftmals geringer als die Wiederanlaufzeiten für die Prozesse. Jedoch ist dies abhängig von der Art des Notbetriebs (welche Ressourcen werden für den Notbetrieb benötigt) und dem Niveau der einzelnen Stufen bei kaskadierendem Anlauf (wann werden wie viele Ressourcen benötigt).

Zusätzlich sollte mit den Ressourcen-Verantwortlichen geklärt werden, inwieweit zusätzliche Rüst- und Anlaufzeiten bei den Ressourcen berücksichtigt werden müssen, die zu verkürzten maximalen Ausfallzeiten führen, oder Abhängigkeiten zwischen verschiedenen Ressourcen.

Die Wiederanlauf-Anforderungen der Ressourcen werden oftmals durch den Geschäftsprozess-Verantwortlichen festgelegt. Zusätzlich kann ein Bottom-Up-Ansatz durchgeführt werden, um die Ergebnisse zu evaluieren. Die Praxis hat gezeigt, dass es empfehlenswert ist, für die kritischen Bereiche zusätzlich die Ressourcenverantwortlichen oder Anwender dahin zu befragen, welche Ressourcen aus ihrer Sicht für kritisch zu erachten sind und wie sich der Ausfall von einzelnen Ressourcen bemerkbar macht. Dadurch, dass Prozessverantwortliche über eine idealisierte und auf ihren Geschäftsprozess eingeschränkte Sichtweise verfügen, kann die Sichtweise der Basis, die die Erfahrung aus dem täglichen Geschehen widerspiegelt, eine zusätzliche Hilfe und Kontrolle sein.

5.1.3 BIA-Bericht

Der BIA-Bericht sollte alle wesentlichen Informationen, die im Verlauf der Durchführung der BIA erhoben wurden, inklusive der Begründungen enthalten. Damit sollte ein BIA-Bericht mindestens folgende Informationen enthalten:

- Management-Übersicht
- Vorgehensmodell der BIA (z. B. Verweis auf den BSI-Standard 100-4)

- Prozesslandkarte: Prozesse, Abhängigkeiten, Prozessketten und deren Beitrag zu den Geschäftszielen
- Betrachtete Organisationseinheiten und eventuell ausgeschlossene Geschäftsprozesse
- Rahmenbedingungen, verwendete Methoden und Vorgehensweisen bei der Durchführung der Kritikalitätsbewertung
- Rahmenbedingungen für die Schadensanalyse
- Einzelbewertungen der Prozesse
- Liste der kritischen Prozesse mit Priorisierung für Wiederanlauf
- Ressourcenübersicht der kritischen Geschäftsprozesse und Anforderungen für Wiederanlauf

Die Verantwortung für die Erstellung des Berichts trägt der Notfallbeauftragte. Der Bericht sollte von den Leitern der einzelnen Organisationseinheiten schriftlich freigegeben und der obersten Leitungsebene zur Genehmigung vorgelegt werden.

5.2 Risikoanalyse

Die Risikoanalyse dient im Kontext des Notfallmanagements dazu, die Gefährdungen zu identifizieren, die eine Unterbrechung von Geschäftsprozessen verursachen können, und die damit verbundenen Risiken zu bewerten. Die Ziele sind,

- die bestehenden Risiken gegenüber den Entscheidungsträgern transparent zu machen,
- gegebenenfalls geeignete Strategien und Gegenmaßnahmen zu entwickeln, um diese Risiken im Vorfeld zu reduzieren und die Robustheit der Institution zu stärken, sowie
- die Szenarien zu identifizieren, für die individuelle Notfallpläne zu entwickeln sind.

Die Durchführung einer Risikoanalyse ist im Notfallmanagement optional, da das Ziel der Risikovorsorge im günstigen Fall durch das Risiko- oder das Informationssicherheitsmanagement schon erreicht ist. Wird in keiner anderen Managementdisziplin für die Institution eine Risikoanalyse durchgeführt, die den Geltungsbereich des Notfallmanagements und alle zu betrachtenden Ressourcen vollständig umfasst, so ist im Rahmen des Notfallmanagements eine Risikoanalyse durchzuführen. Der Fokus liegt dabei auf den kritischen Geschäftsprozessen und kritischen Ressourcen.

Die klassische Vorgehensweise bei einer Risikoanalyse ist, die Gefährdungen zu identifizieren, die für die Institution, den Prozess oder die Ressource relevant sind, und eine Risikobewertung durchzuführen. Charakterisiert werden Risiken dabei durch die Auswirkungen eines Schadens, die das Eintreten zur Folge haben kann, und die Eintrittswahrscheinlichkeit. Bei der Durchführung einer Risikoanalyse sollten folgende Aspekte immer berücksichtigt werden:

- Es ist nicht möglich, alle Risiken zu identifizieren. Es existiert immer mindestens ein weiteres Risiko, das nicht berücksichtigt wurde. Daher sollte ein sinnvolles Maß bei der Durchführung der Risikoanalyse gefunden und nicht der Versuch unternommen werden, alle Risiken zu identifizieren, die jemals relevant werden könnten.
- Die Schätzung der Eintrittswahrscheinlichkeit kann nur subjektiv und grob erfolgen. Nur für wenige Risiken im Bereich der operationellen Risiken existieren fundierte und belastbare Zahlen. Ein weiteres Problem ist, dass sich aus Ereignissen in der Vergangenheit häufig keine Schlussfolgerungen für die Zukunft ableiten lassen, da sich die Rahmenbedingungen sehr schnell ändern können.

5.2.1 Risikoidentifizierung

Der erste Schritt bei der Risikoanalyse ist die Identifizierung möglicher Gefährdungen bzw. Risiken für die kritischen Geschäftsprozesse. Unter Gefährdungen werden Bedrohungen verstanden, die konkret auf die Prozesse oder Ressourcen über vorhandene Schwachstellen einwirken können. Im

Unterschied zum Begriff "Gefährdung" umfasst der Begriff „Risiko“ bereits eine Bewertung und drückt somit aus, dass durch diese Gefährdung ein Schaden für die Institution entstehen kann.

Während bei der BIA die Frage beantwortet wird, welche Folgen der Ausfall eines Prozesses für die Institution hat, wird nun die Frage nach den möglichen Ursachen für den Ausfall gestellt. Dabei werden sowohl Risiken auf Prozessebene, als auch Risiken auf Ressourcenebene untersucht. Ein Risiko auf der Prozessebene kann beispielsweise der Ausfall einer oder mehrerer (kritischer) Ressourcen sein. Eine Risikoanalyse auf Ressourcenebene sucht dann die möglichen Ursachen für den Ausfall dieser kritischen Ressourcen.

Risiken lassen sich anhand unterschiedlicher, voneinander unabhängiger Merkmale kategorisieren:

- interne / externe Risiken
- direkt wirkende / indirekt wirkende Risiken
- durch die Institution beeinflussbare / nicht beeinflussbare Risiken

Wichtig bei der Identifizierung der Risiken ist ein strukturiertes und systematisches Vorgehen, das auch die verschiedenen Arten von Risiken in die Betrachtung einbezieht. Dabei können bekannte Methoden, wie die Kollektionsmethoden oder die Suchmethoden, eingesetzt werden. Zu den Kollektionsmethoden zählen beispielsweise Checklisten, SWOT-Analysen („Strengths, Weaknesses, Opportunities and Threats“) oder Interviews. Kollektionsmethoden sind besonders für die Identifizierung von offensichtlichen Risiken gut geeignet. Dagegen werden die Suchmethoden vor allem eingesetzt, um zukünftige oder weniger offensichtliche Risiken zu identifizieren. Dazu zählen FMEA (Fehlermöglichkeits- und Einflussanalyse), HAZOP („Hazard and Operability Study“), Fehlerbaumanalyse, morphologische und statistische Verfahren, aber auch Brainstorming, Brainwriting oder die Delphi-Methode. Da die einzelnen Methoden unterschiedliche Stärken und Schwächen haben, sollten möglichst mehrere, sich ergänzende Methoden eingesetzt werden.

Eine gute Ausgangsbasis für die Risikoidentifizierung bieten die Gefährdungskataloge des IT-Grundschutzes [BSIGK]. Diese enthalten eine breite Auswahl an Gefährdungen für die Gefährdungsklassen

- Höhere Gewalt,
- Organisatorische Mängel,
- Menschliche Fehlhandlungen,
- Technisches Versagen und
- Vorsätzliche Handlungen.

Zur Identifizierung von Informationsrisiken auf Ressourcenebene bietet sich das Vorgehen nach der „Risikoanalyse auf der Basis von IT-Grundschutz“ gemäß BSI-Standard 100-3 [BSI3] an. Wurde ein Sicherheitskonzept nach IT-Grundschutz entwickelt, so können viele Informationen aus den bei dieser Vorgehensweise durchgeführten Analysen übernommen werden. Für die im Notfallmanagement zusätzlich betrachteten Ressourcen, für die keine Ergebnisse aus dem Informationssicherheitsmanagement vorliegen, sollten zusätzliche Risikoanalysen durchgeführt werden.

5.2.2 Risikobewertung

In einem weiteren Schritt sind die identifizierten Risiken auf ihre Relevanz hin zu bewerten. Dazu können die Eintrittswahrscheinlichkeiten sowie die zu erwartenden Schäden geschätzt werden. Dieses Vorgehen weist bekannte Probleme auf. Insbesondere liegen in der Regel nur für bestimmte Teilbereiche, wie beispielsweise Naturkatastrophen, belastbare Zahlen für die Eintrittswahrscheinlichkeiten vor. Daher ist für die Abschätzung der Eintrittswahrscheinlichkeit der qualitative Ansatz vorzuziehen. Als Beispiel zeigt Tabelle 10 eine Kategorisierung der Eintrittswahrscheinlichkeit von Risiken mit vier Stufen sowie deren Abgrenzung untereinander. Sowohl die Anzahl der Stufen als auch die Kriterien sind für jede Institution individuell festzulegen.

Unwahrscheinlich	Möglich	Wahrscheinlich	Sehr wahrscheinlich
alle 10 Jahre oder seltener	etwa einmal pro Jahr	etwa einmal pro Monat	einmal pro Woche oder öfter

Tabelle 10: Beispiel für Wahrscheinlichkeitsstufen

Die Schätzung der zu erwartenden Schäden bei Ausfall von Geschäftsprozessen liegt aus der BIA in qualitativer oder quantitativer Form vor. Falls ein quantitativer Ansatz zur Schadensermittlung angewandt wurde, ist zu beachten, dass die daraus resultierenden Zahlen nur grobe Schätzungen sein können und nur bedingt belastbar sind. Auch bei der Bewertung der potentiellen Schadenshöhe empfiehlt es sich also, einen qualitativen Ansatz zu wählen.

Zur Bewertung der Risiken wird die Wahrscheinlichkeit des Eintretens in Bezug zu den möglichen Schäden gesetzt, der, wie zuvor beschrieben, in „niedrig", „normal", „hoch" und „sehr hoch" kategorisiert ist. Eine Möglichkeit, die Risiken zu kategorisieren, ist als Beispiel in der folgenden Tabelle dargestellt: „niedrig", „mittel", „hoch" und „sehr hoch". Dies ist jedoch für jede Institution individuell festzulegen.

		Auswirkung / Schaden			
		Niedrig	**Normal**	**Hoch**	**Sehr hoch**
Wahrscheinlichkeit	**Sehr wahrscheinlich**	niedrig	mittel	hoch	sehr hoch
	Wahrscheinlich	niedrig	mittel	hoch	hoch
	Möglich	niedrig	niedrig	mittel	mittel
	Unwahrscheinlich	niedrig	niedrig	niedrig	niedrig

Tabelle 11: Beispiel für die Risikoklassifikation

Die Risiken können in unterschiedlicher Form erfasst und dargestellt werden. Eine Tool-Unterstützung kann dabei hilfreich sein. Folgende Tabelle zeigt eine mögliche Erfassung:

Ursache	Risiko	Szenario	Auswirkung	Wahrscheinlichkeit	Risikobewertung	Schwachstellen	Strategie	Maßnahmen	Verantwortlich
Kabelbrand Kurzschluss Erwärmung …	Brand	Ausfall Rechenzentrum	Sehr hoch	Möglich	Mittel	Raumaufteilung Brandschottung zwischen …	…	…	…
Ausfall externe Stromzuführung Ausfall interne Strominfrastruktur …	Stromausfall	Ausfall Rechenzentrum	Hoch	Möglich	Mittel	Dieselmenge nur für 5 Stunden ausreichend, Nur 50% der Server an Notstromversorgung …		Zusätzliche Stromgeneratoren	

Tabelle 12: Beispiel für eine Risikoerfassung

Für eine Übersichtsdarstellung der Risiken wird oftmals eine Risikomatrix verwendet, die bei der Auswahl der jeweiligen Risikostrategie hilfreich sein kann.

5.2.3 Gruppierung und Szenarienbildung

Um die Anzahl der identifizierten Risiken für die weiteren Arbeitsschritte handhabbar zu machen, sollten diese sinnvoll zusammengefasst werden.

Um konkrete Vorsorgemaßnahmen zu identifizieren, muss die hohe Anzahl von Risiken handhabbar gemacht werden. Werden die Risiken auf der Prozessebene untersucht, so kann es zweckmäßig sein, für jeden betrachteten Geschäftsprozess die jeweils relevanten Risiken in eine dem jeweiligen Prozess zugeordnete Gruppe einzuordnen. Auf der Ressourcenebene kann die Anzahl der für eine Ressource relevanten Risiken dadurch reduziert werden, dass ähnlicher Risiken zusammengefasst werden.

Da es nicht möglich ist, für jedes Risiko eigenständige Notfallpläne zu entwickeln, sollten Szenarien entwickelt werden, denen die Risiken zugeordnet werden können. Um die Anzahl der Notfallpläne überschaubar zu halten, sollten allgemeine und praxisnahe Notfallszenarien erarbeitet werden. Die Notfallszenarien orientieren sich dabei an den Auswirkungen der Risiken auf die Geschäftsprozesse. Der Einsatz der Szenario-Technik ist bei der Entwicklung hilfreich. Sie untersucht die unterschiedlichen zeitlichen Entwicklungen und Eskalationsmöglichkeiten der Ereignisse (vom positiven Extrem bis zum negativen Extrem) und ermöglicht es, die mit dem jeweiligen Notfallszenario zusammenhängenden Risiken zu identifizieren. Bei der Auswahl der Szenarien für die Entwicklung spezifischer Notfallpläne ist darauf zu achten, dass jene Notfallszenarien gewählt werden, die hohen Schaden verursachen und deren Eintreten für die eigene Institution am wahrscheinlichsten sind. Als eine in der Praxis handhabbare Anzahl haben sich 5 bis maximal 15 Szenarien erwiesen. Generische Notfallszenarien sind beispielsweise:

- (Teil-)Ausfall eines Standortes (z. B. durch Hochwasser, Großbrand, Gebietssperrung, Ausfall der Zutrittskontrolle)
- Erheblicher Ausfall von Informationstechnik oder der Kommunikationsinfrastruktur
- Erheblicher Ausfall von Systemen oder Anlagen (z. B. in der Produktion)
- Ausfall einer kritischen Anzahl von Mitarbeitern (z. B. bei Pandemie, Lebensmittelvergiftung, Streik)
- Ausfall von Dienstleistern (z. B. Zulieferer, Stromversorger)

Die Entwicklung von Notfallszenarien kann auch vor oder während der Durchführung der Business Impact Analyse durchgeführt werden. Obwohl bei der Abschätzung der Auswirkungen eines Ausfalls eines Geschäftsprozesses die Ursache keine Rolle spielt, kann es für manchen Verantwortlichen hilfreich sein, sich konkrete Notfallszenarien vorzustellen und die Auswirkungen abzuleiten.

5.2.4 Risikostrategie-Optionen identifizieren

Risiken können akzeptiert, transferiert, vermieden oder reduziert werden. Strategieoptionen sind richtungsweisende Entscheidungen bezüglich der Behandlung von Risiken [BSI3]. Für jeden kritischen Geschäftsprozess und jedes Risiko werden die geeigneten Risikostrategie-Optionen bestimmt und dokumentiert. Die anschließende Auswahl der Risikostrategien bildet die Grundlage für die spätere Auswahl der Kontinuitätsstrategien. Das verbleibende Restrisiko nach Umsetzung der jeweiligen Risikostrategie hilft zu entscheiden, für welche Geschäftsprozesse individuelle Notfallpläne erstellt werden sollen.

In die Auswahl der Risikostrategie fließt nicht nur die Risikosituation ein, sondern es müssen unter anderem auch wirtschaftliche, betriebliche und technische Aspekte berücksichtigt werden. Die möglichen Risikostrategien sind im Folgenden genauer beschrieben:

Risikoübernahme

Bei der Risikoübernahme wird das identifizierte Risiko akzeptiert. Diese Strategieoption wird häufig dann gewählt, wenn Ausfallszenarien mit geringer Eintrittswahrscheinlichkeit und geringem Schadenspotential identifiziert wurden. Andere Gründe für diese Entscheidung können beispielsweise

sein, dass gegen die zugrunde liegende Gefährdung keine wirksamen Gegenmaßnahmen bekannt sind oder dass die Gesamtkosten für wirksame Gegenmaßnahmen den zu schützenden Wert überschreiten.

Risikotransfer

Bei einem Risikotransfer wird das Risiko auf eine andere Institution übertragen. Das kann beispielsweise durch das Abschließen einer Versicherung erfolgen oder durch Outsourcing. Durch das Abschließen einer Versicherung kann der direkte finanzielle Schaden gesenkt werden, da entstehende Schäden ganz oder zumindest teilweise ersetzt werden (z. B. bei Feuer, Wasser oder Diebstahl). Nicht ersetzt werden in der Regel jedoch die Folgeschäden, die direkt oder indirekt durch den Ausfall der betroffenen Geschäftsprozesse entstehen. Dies betrifft insbesondere Imageschäden. Bei Abschluss einer Versicherung sollten die besonderen Rahmenbedingungen und etwaige Ausschlussklauseln berücksichtigt werden. Zu beachten ist auch, dass eventuell eine längere Zeitspanne finanziell überbrückt werden muss, bis die Versicherung den Schaden ersetzt.

Eine andere Möglichkeit des Risikotransfers ist das Outsourcing des betroffenen (Teil-)Geschäftsprozesses. Dies ist beispielsweise dann sinnvoll, wenn der Outsourcing-Partner aus wirtschaftlichen oder technischen Gründen eher in der Lage ist, mit dem Risiko umzugehen. Hierbei ist zu beachten, dass Teilrisiken, wie die Rufschädigung und die Einschränkung der Handlungsfähigkeit durch abhängige Prozesse, weiterhin bei der eigenen Institution verbleiben. Außerdem entstehen zusätzliche Risiken durch die neue Abhängigkeit vom beauftragten Dienstleister.

Risikovermeidung

Besitzt ein Geschäftsprozess aufgrund spezieller Abläufe eine hohe Kritikalität, kann es auch eine geeignete Strategie sein, die Prozessabläufe oder die Umgebungsbedingungen so zu verändern, dass die entsprechende Gefährdung nicht mehr relevant ist. Wenn ein Geschäftsprozess aufgrund des identifizierten Risikos für die Institution nicht weiter tragbar ist, kann es sogar notwendig sein, diesen Prozess einzustellen und durch einen vollständig neuen Prozess zu ersetzen. Risikovermeidung bedeutet immer, dass die Eintrittswahrscheinlichkeit oder das Schadensausmaß des jeweils betrachteten Risikos auf Null reduziert wird.

Risikoreduktion

Die am häufigsten gewählte Strategieoption ist die Risikoreduktion, bei der die Eintrittswahrscheinlichkeit oder die Schadenshöhe vermindert wird. Dies kann durch die Umsetzung von Maßnahmen oder durch die Modifikation des Prozessablaufes erfolgen.

Eine sehr hohe Konzentration von Risiken wird beispielsweise durch die Zentralisierung von Geschäftsprozessen in einem Rechenzentrum erzeugt, wie dies heute von vielen Institutionen praktiziert wird. Dem Gewinn durch die damit verbundenen Kosteneinsparungen ist jedoch das höhere Risiko entgegenzusetzen. Eine Maßnahme zur Risikoreduktion kann somit in einer geringeren Zentralisierung bzw. in der Verteilung des Risikos auf mehrere Rechenzentren bestehen.

5.2.5 Risikoanalyse-Bericht

Der Bericht zur Risikoanalyse sollte nicht nur die Ergebnisse dokumentieren, sondern auch die verwendete Methode. Damit ergibt sich als mögliche Struktur:

- Management-Übersicht
- verwendete Methode der Risikoanalyse,
- Liste der Risiken mit eventuell vorgenommenen Gruppierungen,
- Ergebnisse der Risikobewertungen,
- Risikostrategien-Optionen für die kritischen Prozesse.
- Auswahl der Risikostrategien.

Die Verantwortung für die Erstellung des Risikoanalyse-Berichts trägt der Notfallbeauftragte. Der Bericht ist der Leitungsebene vorzulegen und von dieser zu genehmigen.

5.3 Aufnahme des Ist-Zustandes

Mit der Business Impact Analyse wurden die kritischen Prozesse und deren (kritischen) Ressourcen identifiziert. Für die im folgenden Schritt zu entwickelnden Kontinuitätsstrategieoptionen und die Strategieentscheidungen ist die Ermittlung des aktuellen Ist-Zustandes der Notfallvorsorgemaßnahmen und der aktuell möglichen Wiederanlaufzeiten notwendig, damit zum einen für die verschiedenen Strategieoptionen der notwendige Handlungsbedarf und die damit verbundenen Investitionskosten grob abgeschätzt werden können, und zum anderen nach der Strategiefestlegung die noch umzusetzenden Maßnahmen durch eine Soll-Ist-Analyse identifiziert werden können.

Die Aufnahme des Ist-Zustandes kann auf die wesentlichen Ressourcen bzw. Bereiche (z. B. die kritischen Geschäftsprozesse) beschränkt werden. Viele Informationen können aus der Strukturanalyse bei der Sicherheitskonzeption nach BSI-Standard 100-2 entnommen werden. Zu ergänzen sind die im Informationssicherheitsmanagement nicht betrachteten Ressourcen.

5.4 Kontinuitätsstrategien

Die Geschäftsfortführung bzw. der Wiederanlauf kann auf unterschiedliche Weise realisiert werden. Die alternativen Lösungswege, also die Strategieoptionen, unterscheiden sich durch Parameter wie die Wiederanlaufzeit, die Kosten und die Zuverlässigkeit der Lösung. Ziel ist es nun, die wesentlichen Alternativen zu identifizieren und anschließend die für die Institution beste Vorgehensweise auszuwählen. Dazu wird in einem „Top-Down"-Ansatz die im Rahmen der Initiierung des Notfallmanagements entwickelte richtungsweisende institutionsweite Notfallstrategie, die in der Leitlinie zum Notfallmanagement festgehalten ist, auf die Prozess- und Ressourcenebene übertragen und konkretisiert.

5.4.1 Entwicklung von Kontinuitätsstrategien

Die Alternativen für die Kontinuitätsstrategien stellen verschiedene Möglichkeiten dar, die Lücke zwischen dem Soll und dem Ist der Notfallvorsorgemaßnahmen zu schließen. Sie müssen die folgenden Randbedingungen erfüllen:

- regulatorische Vorgaben und
- die festgelegten Wiederanlaufzeiten für die Prozesse und die Ressourcen müssen eingehalten werden, und
- die Kosten der Alternative sollten in einem akzeptablen Verhältnis zum erwartenden Schaden bei einem Ausfall pro gewählter Zeitperiode stehen und damit wirtschaftlich sinnvoll sein.

Abgeleitet von den Zielen der Institution sowie dem Kerngeschäft ist eine grobe institutionsweite Notfallstrategie festgelegt und in der Leitlinie zum Notfallmanagement festgehalten. Diese bildet den Rahmen für die weiteren Überlegungen. Auf der Institutionsebene werden dann Optionen für eine Kontinuitätsstrategie mit allgemeinen Grundsätzen festgelegt. Folgende Tabelle zeigt ein Beispiel dafür.

Strategieoption	Beschreibung	Risikobetrachtung
Minimale Lösung	Nur die Prozesse mit maximaler Kritikalität werden abgesichert. Die Gesamtkosten der Maßnahmen sind auf … zu begrenzen. Die Absicherung des Schadenspotentials erfolgt weitestgehend über Versicherungen.	Hohes Restrisiko
Kleine Lösung	Die Prozesse mit hoher Priorität werden abgesichert. Die Gesamtkosten der Maßnahmen sind auf … zu begrenzen.	Mittleres bis hohes Restrisiko

Strategieoption	Beschreibung	Risikobetrachtung
Mittlere Lösung	Die wichtigsten Kernprozesse werden abgesichert. Bei den Maßnahmen ist darauf zu achten, dass weitestgehend interne Möglichkeiten genutzt werden.	Mittleres Restrisiko
Große Lösung	Die kritischen Geschäftsprozesse werden umfassend abgesichert. Die Einhaltung gesetzlicher Auflagen und Verträge sowie die Vorbeugung vom Imageverlust haben hohe Priorität.	Geringes Restrisiko

Tabelle 13: Beispiele für institutionsweite Strategieoptionen

Ist eine institutionsweite Kontinuitätsstrategie festgelegt, so muss diese auf die Prozess- und Ressourcenebene heruntergebrochen und für die (kritischen) Geschäftsprozesse und Ressourcen in verschiedenen Handlungsmöglichkeiten konkretisiert werden. Die folgende Tabelle zeigt ein unvollständiges Beispiel für Strategieoptionen auf Prozessebene. Ausführlichere Beschreibungen möglicher Handlungsalternativen und weitere Beispiele für alternative Maßnahmen sind in Anhang A zu finden.

	Prozess „Rechenzentrumsbetrieb“	Prozess „Arbeitsplatz-Management“
Minimale Lösung	Dienstleistungsvertrag für den Notbetrieb	Interne Lösung: Freisetzung von weniger kritischen Arbeitsplätzen für die kritischen und Heimarbeitsplätze für die Arbeitsplätze mit höchster Priorität
Kleine Lösung	„Cold-standby“-Ausweich-Rechenzentrum	Lösung mit kooperierenden Partnerschaften
Mittlere Lösung	„Warm-standby“-Ausweich-Rechenzentrum	Kommerzieller Dienstleistungsvertrag „bezugfertiges Bürogebäude“
Große Lösung	„Hot-standby“-Ausweich-Rechenzentrum	Zweites eigenes Bürogebäude

Tabelle 14: Beispiele für Strategieoptionen für Prozesse

5.4.2 Kosten-Nutzen-Analyse

Ein grundlegendes Ziel des Notfallmanagements ist die ausreichende Absicherung der Geschäftsfortführung bei möglichst vertretbaren Kosten. Als Auswahlhilfe einer guten Kontinuitätsstrategie kann eine Kosten-Nutzen-Analyse der verschiedenen Strategieoptionen dienen. Dazu sind die Kosten der Kontinuitätsmaßnahmen zu betrachten und dem Nutzen gegenüberzustellen. Unzählige Einflussfaktoren materieller und nicht materieller Art (siehe auch Kapitel 5.4.3) können den Nutzen einer Strategieoption erhöhen oder auch verringern. Da nicht alle Einflussfaktoren berücksichtigt werden können, sollte die Kosten-Nutzen-Analyse der Kontinuitätsstrategien deshalb mit einem pragmatischen Ansatz durchgeführt werden. Die folgenden Ausführungen geben eine Orientierungshilfe dafür:

Schritt 1: Ermittlung des Schadens eines Prozesses durch einen Notfall

Das Schadenspotential eines Prozessausfalls wurde bereits bei der BIA erhoben, wobei Schaden nicht ausschließlich als finanzieller Schaden angesehen wird, sondern, wie in der BIA festgestellt, allgemein als negative Folgen für die Institution. Der Nutzen einer Kontinuitätsstrategie kann als die Fähigkeit betrachtet werden, die Schäden für die Institution durch eine möglichst schnelle Wiederaufnahme bzw. der Aufrechterhaltung des Prozesses in einem Notfall gering zu halten. Der Nutzen einer Strategieoption ist umso höher, je niedriger der entstandene Schaden bis zum Wiederanlauf bzw. der Wiederherstellung ist. Abbildung 8 zeigt ein Beispiel für einen möglichen Schadensverlauf (gestrichelte Linie), den bei der BIA für die einzelnen Bewertungsperioden generalisierten Schadensverlauf sowie die Wiederanlaufpunkte W_{Si} für die unterschiedlichen Strategieoptionen.

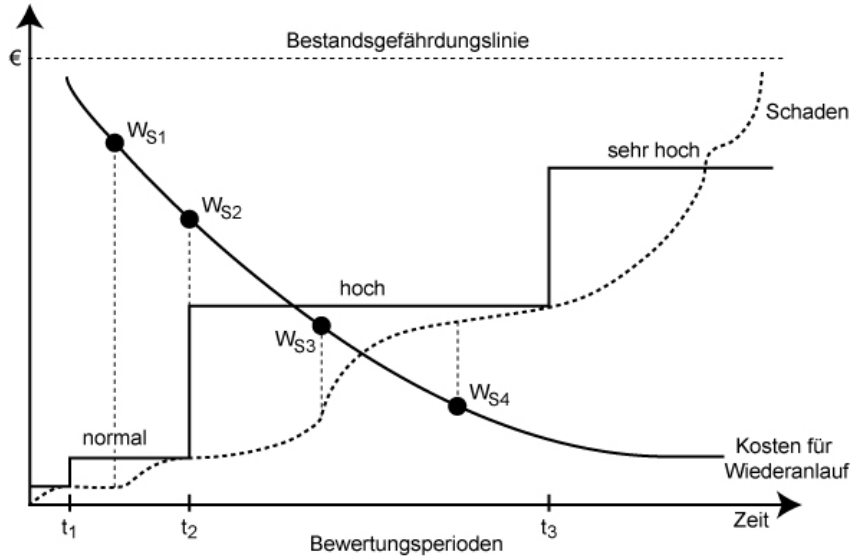


Abbildung 8: Schadensverlauf und Kosten für einen Wiederanlauf

Schritt 2: Ermittlung der Kosten der Kontinuitätsstrategie

Im zweiten Schritt werden die Kosten der einzelnen Strategieoptionen erfasst. Kosten von Kontinuitätsstrategien sollten unter den anerkannten Verfahren der Finanzplanung in der Institution ermittelt bzw. abgeschätzt werden. Dazu zählen neben den Anschaffungskosten auch die fortlaufenden Kosten für regelmäßige Wartungen, Schulungen, Mietkosten oder eventuelle Vertragskosten (z. B. für die Vorhaltung von Ausweicharbeitsplätzen bei einem externen Dienstleister). Eine wichtige Rolle spielen dabei der aktuelle Ist-Zustand der Notfallmaßnahmen und die gegebenenfalls zu schließenden Lücken, die durch einen Soll-Ist-Vergleich für die einzelnen Strategieoptionen zu ermitteln sind.

Schritt 3: Aufarbeitung der Kosten-Nutzen-Analyse

Abschließend werden die Ergebnisse der beiden vorangegangenen Schritte zu einer Entscheidungshilfe zusammengefasst. Diese soll darstellen, welche Kosten notwendig sind, um einen bestimmten Nutzen zu erhalten. In der Regel bedeuten kürzere Wiederanlaufzeiten geringere Schäden aber auch höhere Investitionskosten, doch können Strategieoptionen mit einschränkenden Randbedingungen diese Regel durchbrechen. Folgende Beispiele mit fiktiven Zahlen sollen einen möglichen Aufbau einer Entscheidungshilfe skizzieren. Sie decken nicht alle Möglichkeiten zur Absicherung eines Rechenzentrums bzw. von Arbeitsplätzen ab, und sind auch nicht vollständig spezifiziert. Eine ausführlichere Beschreibung alternativer Absicherungsmöglichkeiten für ein Rechenzentrum ist in Anhang A zu finden.

Prozess „Rechenzentrumsbetrieb“ MTA = 10 Tage	Wieder-anlauf-zeit	Kosten	Schaden bis zum Wieder-anlauf	Zuverlässigkeit / Randbedingungen / Einschränkungen
S1: Stand-by-Rechenzentrum / „Hot“-Lösung: komplette, redundante IT-Infrastruktur	< 6 Std.	5 Mio. €	gering	sehr hoch
S2: „Warm“-Lösung: eigenes Rechenzentrum; vollständige IT vorhanden; Einspielen von Sicherungen im Notfall notwendig	6-24 Std.	3 Mio. €	gering bis mittel	hoch
S3: „Cold“-Lösung: im Notfall teilweise Beschaffung von Hardware notwendig; Installation der Software	2-10 Tage	1-1,2 Mio. €	mittel-hoch	Restrisiko: Hardware-Beschaffung; max. WAZ von 10 Tagen entspricht

Prozess „Rechenzentrumsbetrieb“ MTA = 10 Tage	Wieder-anlauf-zeit	Kosten	Schaden bis zum Wieder-anlauf	Zuverlässigkeit / Randbedingungen / Einschränkungen
und Anwendungen und Einspielen von Sicherungskopien				der MTA und damit kein Restpuffer vorhanden.
S4: Dienstleistungsvertrag „Notfall-Rechenzentrum“ mit Dienstleister A	2 Tage	700.000,- €	mittel	Restrisiko: verfügbare Kapazitäten des Dienstleisters im Notfall
		1,3 Mio €	mittel	Vertrag mit Vorrangsbehandlung
S5: Dienstleistungsvertrag „Notfall-Rechenzentrum“ mit Dienstleister B	2 Tage	500.000,- €	mittel	Restrisiko: verfügbare Kapazitäten des Dienstleisters im Notfall; Restrisiko: Zuverlässigkeit und Image des Anbieters nicht ausreichend

Tabelle 15: Beispiel 1 Entscheidungshilfe Kosten-Nutzen-Analyse

Prozess „Arbeitsplatz-Management“ MTA = 14 Tage	Wieder-anlauf-zeit	Kosten	Schaden bis zum Wieder-anlauf	Zuverlässigkeit / Randbedingungen / Einschränkungen
S1: Angemieteter Standort	2 Tage	2000,- € / Arbeitsplatz	mittel	
S2: Anschaffung von Containern bei Bedarf	7-12 Tage	700,- € / Arbeitsplatz	hoch	Restrisiko: Aufstell-möglichkeit nur auf dem Betriebsgelände und damit für den Falle der Nicht-Verfügbarkeit des Betriebsgeländes keine Lösung.
S3: Heimarbeitsplätze	12 Std.	200,- € / Arbeitsplatz	gering	Aktuell für maximal 10% der Arbeitsplätze geeignet. Restrisiko: Verfügbar-keit der Internetver-bindung und des Ein-wahlknotens, Rechner und Unterlagen befinden sich am Büroarbeitsplatz und nicht am Heim-arbeitsplatz.

Tabelle 16: Beispiel 2 Entscheidungshilfe Kosten-Nutzen-Analyse

Achtung: Die in den Beispielen genannten Wiederanlaufzeiten und Kosten sind fiktive Zahlen, um das Vorgehen zu verdeutlichen. Jede Institution muss für ihre konkreten Anwendungsfälle und ihre Bedürfnisse in Bezug auf die Ausgestaltung von Arbeitsplätzen geeignete Werte ermitteln oder abschätzen!

5.4.3 Konsolidierung und Auswahl der Kontinuitätsstrategien

Zielsetzung der Kosten-Nutzen-Analyse ist eine zur Entscheidungsfindung geeignete Aufstellung der möglichen Kontinuitätsstrategien. Die Kosten von Kontinuitätsstrategien und der durch diese möglicherweise verhinderten Schäden sollten aber aufgrund äußerer Faktoren und innerbetrieblicher Abhängigkeiten nicht als alleinige Kriterien zur Entscheidung herangezogen werden. Randbedingungen, Einschränkungen und Verfügbarkeitseinschätzungen sollten immer in die Entscheidungsfindung mit einbezogen werden.

Innere Abhängigkeiten können in internen Abstimmungen identifiziert werden. So erfordert die Nutzung interner Lösungen als Kontinuitätsstrategie eine detaillierte Betrachtung. Eine ausführliche Soll-Ist-Analyse sollte dabei mindestens folgende Punkte untersuchen:

- Werden die erforderlichen Wiederanlaufzeiten im Notfall garantiert erfüllt?
- Gibt es Abhängigkeiten von Ressourcen, die gleichzeitig in mehreren Prozessen benötigt werden?

Äußere Faktoren wie beispielsweise die Mehrfachnutzung von Räumlichkeiten durch benachbarte Institutionen oder die Bedeutung von besonderen Terminen mit erhöhten Wiederanlauf-Anforderungen für einzelne Geschäftsprozesse können eine eventuelle Neueinstufung einer Kontinuitätsstrategie nach sich ziehen. Äußere Faktoren sollten mit der Institutionsleitung besprochen und ausgearbeitet werden. So kann sich z. B. eine schlechte Reputation eines vermeintlich günstigen Dienstleisters in der Folge einer unzulänglichen Notfallbewältigung auf die eigene Institution übertragen. Die daraus resultierenden Folgekosten in diesem Fall würden dann die Entscheidung für eine kostenintensivere Lösung rechtfertigen. Zusätzlich können einzelne Kontinuitätsstrategien einen vom Notfallmanagement unabhängigen Mehrwert bieten, zum Beispiel durch die Schaffung von neuen Lagerräumen.

Sobald die inneren Abhängigkeiten und äußeren Faktoren identifiziert sind, ist eine Entscheidungsvorlage zu erstellen und der Institutionsleitung vorzulegen. Die Entscheidungsvorlage kann auch Empfehlungen enthalten. Die Leitungsebene hat die Aufgabe, die aus ihrer Sicht besten Strategien festzulegen. Diese Entscheidung ist zu dokumentieren und von der Institutionsleitung schriftlich zu bestätigen. Alle weiteren Maßnahmen im Notfallmanagement müssen sich an diesen gewählten Strategien ausrichten und sind im Notfallvorsorgekonzept zu konkretisieren.

Die Strategie-Entwicklung und Strategie-Festlegung unterliegt einem regelmäßigen Überarbeitungsprozess. Werden neue Strategie-Optionen oder etwaige Änderungen von äußeren Einflüssen identifiziert, sollten eine neue Kosten-Nutzen-Analyse bzw. ein Konsolidierungsgespräch durchgeführt werden.

5.5 Notfallvorsorgekonzept

Das Notfallvorsorgekonzept bildet die Grundlage zur Umsetzung der Kontinuitätsstrategien. Es beschreibt die vorliegenden Bedingungen und beinhaltet alle bei der Konzeption anfallenden Informationen. Alle organisatorischen und konzeptuellen Aspekte sowie alle Maßnahmen und Tätigkeiten des Notfallmanagements, die nicht zur direkten Bewältigung eines Notfalls beitragen, sollten im Notfallvorsorgekonzept beschrieben werden. Dazu zählen

- vorbeugende Maßnahmen, die den Schaden oder die Eintrittswahrscheinlichkeit von Risiken reduzieren und die Widerstandsfähigkeit der Institution durch Anheben der Krisenschwelle erhöhen, wie auch
- Maßnahmen, um ein schnelles und sinnvolles Reagieren auf einen Vorfall zu ermöglichen.

Aus diesem Grund muss ein Notfallvorsorgekonzept sorgfältig geplant, umgesetzt sowie regelmäßig überarbeitet werden. Die direkt für die Bewältigung eines Notfalls benötigten Informationen wie beispielsweise Kontaktinformationen oder Handlungsanweisungen sind im Notfallhandbuch beschrieben (siehe Kapitel 7.4). Zusammen bilden sie das Notfallkonzept.

5.5.1 Feinkonzeption, Sicherheit und Kontrollen

Die einzelnen Vorsorgemaßnahmen zur Prävention und Umsetzung der Kontinuitätsstrategien sind festzulegen. Neben den Lösungen für den Notbetrieb sind auch der Wechsel zurück in den Normalbetrieb und die Nacharbeitsphase nach Aufnahme des Normalbetriebs auszuarbeiten.

Bei der Feinkonzeption wie auch bei der Erstellung des Notfallhandbuchs sollten die beiden Aspekte Sicherheit und Datenschutz eine wichtige Rolle spielen. Unter Sicherheit ist sowohl Informationssicherheit, personelle Sicherheit wie auch Betriebssicherheit zu verstehen. Werden Verschlusssachen in den betroffenen Geschäftsprozessen verarbeitet, so ist auch der Geheimschutzbeauftragte zu involvieren. Es ist sicherzustellen, dass sowohl im Notbetrieb wie auch beim Wechsel zurück in den Normalbetrieb die Sicherheit gewährleistet ist, wie beispielsweise die Einhaltung der gesetzlichen Vorgaben zum Schutze der Mitarbeiter oder die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Daher ist es sinnvoll, mit den jeweils verantwortlichen Sicherheitsbeauftragten (z. B. IT-Sicherheitsbeauftragter, Verantwortlicher für Betriebssicherheit) eng zusammenzuarbeiten. Die Erstellung eines Sicherheitskonzepts für den Notbetrieb ist keine originäre Aufgabe des Notfallmanagements bzw. des Notfallbeauftragten.

Für den Bereich der IT ist federführend durch den IT-Sicherheitsbeauftragten ein entsprechendes Informationssicherheitskonzept für die Prozesse, Systeme und Maßnahmen des Notfallmanagements zu erstellen und umzusetzen, sofern es nicht schon Bestandteil des aktuellen Sicherheitskonzeptes ist. In diesem werden die für den Notbetrieb vorgesehenen Notprozesse aber auch die Wiederanlaufphase, die Prozesse für die Rückführung und die Nacharbeiten betrachtet und die Vertraulichkeit und Integrität der Prozesse sowie der verarbeiteten Informationen für jeden Zwischenschritt sichergestellt. Für Wiederherstellungs- bzw. Wiederanlaufpläne kann dies beispielsweise bedeuten, dass eine bestimmte Reihenfolge der Arbeitsschritte eingehalten werden muss. So darf z. B. die Wiederherstellung vertraulicher Daten in einer Anwendung erst erfolgen, wenn die Netzsicherheit durch ein vollständig wiederhergestelltes Sicherheitsgateway und weiteren Sicherheitsmaßnahmen gewährleistet ist. Sind in den Phasen des Wiederanlaufs, des Notbetriebs oder der Rückführung in Bezug auf Informationssicherheit oder Datenschutz Abstriche oder Kompromisse zu machen, so ist dieses zu dokumentieren, die dadurch entstehenden Risiken aufzuzeigen und von der Institutionsleitung durch Unterschrift zu genehmigen.

Zusätzlich sollten bei der Feinkonzeption die Vorgaben durch die Innenrevision der Institution beachtet werden. Es ist zu überprüfen, in wieweit Kontrollen, die im Normalbetrieb zur Einhaltung eines ordnungsgemäßen Betriebs, zur Abwehr von Wirtschaftsspionage oder Aufdeckung von Missbrauch etabliert sind, im Notbetrieb unabdingbar oder entbehrlich sind. Eine Zusammenarbeit mit der Innenrevision ist daher zu empfehlen, damit diese die Prozesse des Notbetriebs daraufhin überprüft und freigibt.

5.5.2 Inhalt

Das Notfallvorsorgekonzept wird durch den Notfallbeauftragten in Zusammenarbeit mit den Notfallkoordinatoren und dem Notfallvorsorgeteam erstellt. Die Verantwortung für die darin festgehaltenen Strategien liegt jedoch bei der Institutionsleitung und muss daher auch von dieser genehmigt und freigeben werden.

Das Notfallvorsorgekonzept sollte mindestens die folgenden Punkte beinhalten:

Vorgehensmodell und Umsetzung

Mit dem Notfallvorsorgekonzept wird ein klar definierter Rahmen vorgegeben, wie die Fähigkeit zur Geschäftsfortführung in einem Notfall hergestellt, aufgebaut und überwacht werden soll. Es ist genau zu beschreiben, wie die einzelnen Phasen des Notfallmanagements in die bestehenden Strukturen der Institution eingebunden und wie die Aktivitäten des Notfallmanagements gesteuert und kontrolliert werden. Das Notfallmanagement muss regelmäßig auf seine Effektivität und Effizienz hin überprüft werden. Zu diesem Zweck ist ein unabhängiges Überprüfungsverfahren vorzusehen.

Definition Störung – Notfall – Krise

Sobald ein Notfall ausgerufen wird, werden für den betroffenen Bereich die normalen Geschäftsabläufe durch die der Notfallbewältigung abgelöst. Nicht alles, was in der ersten Aufregung als Notfall betrachtet wird, stellt jedoch tatsächlich einen Notfall dar. Es ist aber wichtig, dass jede Institution für sich selber definiert, wann eine Störung, ein Notfall oder eine Krise vorliegt und wer in der Institution autorisiert ist, dies zu entscheiden.

Vorsorgemaßnahmen

Die festgelegten Vorsorgemaßnahmen, wie beispielsweise die Meldetechnik, Ausweichstandorte oder im Notfall relevante Vereinbarungen mit externen Dienstleistern (siehe auch Anhang B), sind zu dokumentieren. Vorsorgemaßnahmen, welche für das Notfallmanagement relevant sind, jedoch schon durch das Informationssicherheitskonzept abgedeckt werden, sollten aufgeführt und auf die entsprechenden Dokumente des Informationssicherheits- oder auch Risikomanagements verwiesen werden.

Glossar

Es ist essentiell, ein gemeinsames Verständnis für die Ziele und Maßnahmen des Notfallmanagements in einer Institution herzustellen. Dazu gehört auch die Definition und Dokumentation einheitlicher und klar verständlicher Begriffe. Hierfür sollte frühzeitig ein Glossar mit den wichtigsten Begriffen rund um das Notfallmanagement erstellt werden.

Inhalt des Notfallvorsorgekonzepts

Das Notfallvorsorgekonzept sollte mindestens die folgenden Punkte beinhalten:

Allgemeines

- Festlegung des Dokumentverantwortlichen
- Klassifizierung des Dokuments und des Genehmigungsverfahrens
- Geltungsbereich, Versionsbezeichnung
- Dokumentenempfänger und Verteilungswege
- Dokumentenstruktur und Zusammenhänge mit anderen relevanten Dokumenten
- Abkürzungsverzeichnis, Glossar

Organisation und Vorgehensmodell

- Definition Störung, Notfall, Krise
- Übernahme von Verantwortung durch die Leitungsebene
- Ziele, Zuständigkeiten, Kompetenzen und Einordnung in andere Managementsysteme der Institution
- Integration des Notfallmanagements in alle relevanten Geschäftsprozesse bzw. Fachverfahren und Projekte
- Beschreibung der Notfallvorsorge- und Notfallbewältigungsorganisation
- Beschreibung der Ablauforganisation und der Umsetzung

Geschäftsprozess- und Schadensanalyse

- Notfallszenarien und ihre Auswirkungen
- Kritische Geschäftsprozesse und deren Wiederanlauf-Anforderungen
- Prioritätenliste

- Kontinuitätsstrategien
- Kosten für die Notfallvorsorge
- verbleibende Restrisiken

Organisatorische und technische Vorsorgemaßnahmen

- Festlegung von generellen Ausweichstandorten und deren Anforderungen
- Alarmierungsverfahren
- Beschreibung risiko-reduzierender Maßnahmen
- Datensicherung
- Meldetechnik
- Vereinbarungen mit externen Dienstleistern
- …

Nachhaltiges Einbinden des Notfallmanagements in die Behörden- bzw. Unternehmenskultur

- Sensibilisierung und Schulung der Mitarbeiter
- Einbindung von Wartungs-, Test- und Monitoringprozesse in die bestehende interne Prozesswert

Aufrechterhaltung und Kontrolle

- Kontinuierliche Verbesserung des Notfallmanagements durch Übungen und Testläufe
- Pflege und Überarbeitung der Notfallvorsorge- und Notfallbewältigungsmaßnahmen
- Beschreibung der Steuerung und Kontrolle des Notfallmanagements

Im Vorfeld der Erstellung des Notfallvorsorgekonzepts sollte über die Strukturierung und Aufteilung des Notfallvorsorgekonzeptes in einzelne Module nachgedacht werden. Bei der Aufteilung kann die jeweilige Zielgruppe betrachtet werden, die einzelne Teile für die Umsetzung benötigt. Auch kann überlegt werden, ob eine Einteilung in einen allgemeinen und in einen Hauptteil sinnvoll ist. Der allgemeine Teil enthält ausschließlich allgemeine Grundsätze des Notfallmanagements und ist somit zusätzlich für die Akquise von Kunden oder Kooperationspartnern geeignet. Der Hauptteil enthält die internen und sensiblen Detailinformationen, die für die Umsetzung notwendig sind.

5.5.3 Bekanntgabe und Verteilung des Notfallvorsorgekonzepts

Das Notfallvorsorgekonzept wird durch die Leitungsebene freigegeben und durch den Notfallbeauftragten veröffentlicht sowie an den autorisierten Empfängerkreis weitergegeben. Es ist wichtig, dass alle an der Notfallvorsorge beteiligten Personen die Inhalte des Notfallvorsorgekonzepts kennen und jederzeit nachvollziehen können. Es ist zu prüfen, ob weitere Personen, beispielsweise aus der Notfallbewältigung oder Kooperationspartner, das Notfallvorsorgekonzept vollständig oder in Auszügen für ihre Arbeit benötigen.

Da ein Notfallvorsorgekonzept einerseits vertrauliche Informationen enthalten kann, andererseits aber für die Absicherung vieler Geschäftsprozesse relevant ist, muss geregelt werden, an wen das Notfallvorsorgekonzept verteilt und wie es klassifiziert werden soll. Beide Punkte können je nach Institution sehr unterschiedlich ausfallen.

5.5.4 Aktualisierung des Notfallvorsorgekonzepts

Der Notfallbeauftragte ist dafür verantwortlich, das Notfallvorsorgekonzept fortlaufend aktuell und vollständig zu halten. Das Notfallvorsorgekonzept sollte in regelmäßigen Abständen auf Aktualität hin überprüft und gegebenenfalls angepasst werden. Hierbei sollte auch überprüft werden, ob sich

Geschäftsziele oder Aufgaben und damit Geschäftsprozesse oder Produktionsverfahren geändert haben oder ob die Organisationsstruktur neu ausgerichtet wurde.

6 Umsetzung des Notfallvorsorgekonzepts

In diesem Kapitel wird beschrieben, wie die Umsetzung der Notfallvorsorgemaßnahmen geplant, durchgeführt, begleitet und überwacht werden kann. Da es einige Überschneidungen zwischen den Notfallvorsorgemaßnahmen und den Sicherheitsmaßnahmen gibt, sollte, wie schon bei der Konzeptentwicklung, auch bei der Umsetzung eine Koordinierung mit dem Informationssicherheitsmanagement stattfinden.

Für die Umsetzung der Maßnahmen stehen in der Regel nur beschränkte Ressourcen an Geld und Personal zur Verfügung. Ziel der nachfolgend beschriebenen Schritte ist daher, eine möglichst effiziente Umsetzung der vorgesehenen Maßnahmen zu erreichen.

6.1 Kosten- und Aufwandsschätzung

Eine erste grobe Kostenabschätzung für die Vorsorgemaßnahmen wurde bei der Entwicklung der Kontinuitätsstrategieoptionen schon durchgeführt. Nach der Entscheidung für eine bestimmte Strategie und deren Konkretisierung im Notfallvorsorgekonzept kann nun eine detaillierte Aufstellung der zu erwartenden Kosten vorgenommen werden.

Da das Budget zur Umsetzung von Vorsorgemaßnahmen praktisch immer begrenzt ist, sollte für jede umzusetzende Maßnahme festgehalten werden, welche Investitionskosten dafür benötigt werden und wie hoch der Personalaufwand ist. Hierbei sollte zwischen einmaligen und wiederkehrenden Investitionskosten bzw. Personalaufwand unterschieden werden.

Wird in dieser Phase deutlich, dass ausgewählte Maßnahmen nicht wirtschaftlich umsetzbar sind, so sollten Überlegungen angestellt werden, durch welche kostengünstigere Maßnahmen sie ersetzt werden könnten oder ob das Restrisiko, das durch die nicht umgesetzten Maßnahmen entstehen würde, tragbar ist.

Stehen für die Umsetzung des Notfallvorsorgekonzepts nicht genügend Ressourcen zur Verfügung, bietet es sich an, für die Entscheidungsebene eine Präsentation vorzubereiten, in der die Ergebnisse der BIA und der Risikoanalyse dargestellt werden. Geordnet nach Priorität der Geschäftsprozesse sollten die Auswirkungen fehlender Vorsorgemaßnahmen vorgestellt werden. Dabei spielen sowohl der aktuelle Stand der Absicherung des jeweiligen Geschäftsprozesses als auch die verbleibenden Restrisiken bei Nicht-Absicherung eine wichtige Rolle. Darüber hinaus bietet es sich an, die für die Realisierung der fehlenden Maßnahmen anfallenden Kosten und den zu erwartenden Aufwand aufzubereiten. Das entstehende Restrisiko sollte beschrieben und der Leitungsebene zur Entscheidung vorgelegt werden. Im Anschluss an diese Präsentation sollte eine Entscheidung über das Budget wie auch über die Priorisierung der Geschäftsprozesse bei der Umsetzung erfolgen. Da die Leitungsebene die Verantwortung für die Konsequenzen tragen muss, erfolgen weitere Schritte erst nach der Entscheidung der Leitungsebene, ob das Restrisiko für die Institution tragbar ist.

6.2 Festlegung der Umsetzungsreihenfolge der Maßnahmen

Wenn das vorhandene Budget oder die personellen Ressourcen nicht ausreichen, um sämtliche Maßnahmen sofort umsetzen zu können, muss eine Umsetzungsreihenfolge festgelegt werden. Bei der Festlegung der Umsetzungsreihenfolge der Maßnahmen ist die festgelegte Priorisierung bei der Absicherung der Geschäftsprozesse zu berücksichtigen. Zusätzlich sollten folgende Aspekte berücksichtigt werden:

- Enthält ein Geschäftsprozess einen Single-Point-of-Failure, also eine mögliche Fehlerstelle, die bei einem Ausfall den Komplettausfall des Geschäftsprozesses nach sich zieht, so ist dieser mit höchster Priorität zu beseitigen bzw. abzusichern.
- Enthält ein Geschäftsprozess einzelne Teilprozesse, welche wesentlich geringer abgesichert sind als die restlichen Teilprozesse, so sollten diese bevorzugt behandelt werden, um ein einheitliches Niveau innerhalb eines Prozesses zu erhalten.

- Bei einigen Maßnahmen ergibt sich durch logische Zusammenhänge eine zwingende zeitliche Reihenfolge.
- Manche Maßnahmen erzielen eine große Breitenwirkung, manche eine eingeschränkte lokale Wirkung. Oft ist es sinnvoll, zuerst auf die Breitenwirkung zu achten.

Die Entscheidung, welche Vorsorgemaßnahmen sofort ergriffen oder verschoben werden und wo Restrisiken akzeptiert werden, sollte auch aus juristischen Gründen sorgfältig dokumentiert werden. In Zweifelsfällen sollten hierfür weitere Meinungen eingeholt und diese ebenfalls dokumentiert werden, um in späteren Streitfällen die Beachtung der erforderlichen Sorgfaltspflicht belegen zu können. Der aus fachlicher Sicht getroffene Vorschlag für die Auswahl und Reihenfolge der Maßnahmen ist von der Entscheidungsebene zu überprüfen und schriftlich zu bestätigen.

6.3 Festlegung der Aufgaben und der Verantwortung

Es muss festgelegt werden, wer bis wann welche Vorsorgemaßnahmen umzusetzen hat. Ohne eine solche Festlegung verzögert sich die Realisierung erfahrungsgemäß erheblich bzw. unterbleibt ganz. Dabei ist darauf zu achten, dass der als verantwortlich Benannte ausreichende Fähigkeiten und Kompetenzen zur Umsetzung der Maßnahmen besitzt und dass ihm die erforderlichen Ressourcen zur Verfügung gestellt werden.

Ebenso ist festzulegen, wer für die Überwachung der Realisierung verantwortlich ist bzw. an wen der Abschluss der Realisierung der einzelnen Maßnahmen zu melden ist. Typischerweise wird die Meldung an den Notfallbeauftragten erfolgen. Es sollte regelmäßig nachgeprüft werden, welche Fortschritte bei der Maßnahmenrealisierung erreicht wurden, damit die Realisierungsaufträge nicht verschleppt werden.

Der nun fertig gestellte Realisierungsplan sollte mindestens folgende Informationen umfassen:

- Maßnahmenbeschreibung,
- Terminplanung für die Umsetzung,
- Budget-Rahmen,
- Verantwortliche für die Umsetzung und
- Verantwortliche für die Überwachung der Realisierung.

6.4 Realisierungsbegleitende Maßnahmen

Überaus wichtig ist es, notwendige realisierungsbegleitende Maßnahmen rechtzeitig zu konzipieren und für die Realisierung mit einzuplanen. Zu diesen Maßnahmen gehören insbesondere Sensibilisierungs- und Schulungsmaßnahmen. Diese sollen den Mitarbeitern die Notwendigkeit des Notfallmanagements und seine Rolle verdeutlichen.

Sind die Mitarbeiter unzureichend geschult, so verzögern sie eventuell die Reaktionen bei der Notfallbehandlung. Fühlen sich die Mitarbeiter unzureichend informiert, führt dies oft zu einer ablehnenden Haltung.

7 Notfallbewältigung und Krisenmanagement

Da auch durch risiko-reduzierende Maßnahmen nicht alle Risiken vollständig eliminiert werden können, muss für das verbleibende Restrisiko Vorsorge getroffen werden. Dies erfolgt durch den Aufbau einer Notfall- und Krisenbewältigung (auch Krisenmanagement genannt), die bei Eintritt eines Notfalls bzw. einer Krise aktiviert werden. Diese beinhalten die Identifikation und Analyse von möglichen Notfall- und Krisensituationen, die Entwicklung von Bewältigungsstrategien, sowie die Einleitung und Verfolgung von Gegenmaßnahmen. Tritt ein Schadensereignis ein, das die Geschäftsfortführung beeinträchtigt, wird je nach Ausmaß des Ereignisses die lokale Notfallbewältigung oder das Krisenmanagement aktiviert. Das Krisenmanagement im Rahmen des Notfallmanagements ist Teil des institutionsweiten allgemeinen Krisenmanagements und stellt eine höhere Eskalationsstufe der Notfallbewältigung dar.

Eine funktionierende Notfallbewältigung und das Krisenmanagement erfordern eine Aufbau- und eine Ablauforganisation. Die Aufbauorganisation wurde in Kapitel 4.3.2 vorgestellt. Sowohl für die Notfallbewältigung wie auch für das Krisenmanagement wird ein Krisenstab benötigt. Der Unterschied liegt in der Zuständigkeit und in der Arbeitsweise. Während ein Notfall überwiegend mit Hilfe von Notfallplänen bewältigt werden kann, erfordert eine Krise eine andere Arbeitsweise. Durch die Einmaligkeit einer Krise sind in der Krise im Gegensatz zu einem Notfall höhere Anforderungen an die Krisenstabsarbeit gestellt. Große Institutionen unterscheiden daher gelegentlich zwischen Notfall- und Krisenstäben. Hier wird zur Vereinfachung darauf verzichtet und der Notfallstab als lokaler Krisenstab verstanden.

Die Beschreibung der Ablauforganisation beinhaltet das Vorgehen nach Eintreten eines Schadensereignisses, von der Meldung über die Eskalation und Wiederherstellung bis hin zur Deeskalation. Im Folgenden werden die wichtigsten Strukturen und Schritte bei der Notfallbewältigung und dem Krisenmanagement beschrieben. Dabei ist zu beachten, dass bei Eintritt eines Schadensereignisses das Vorgehen nicht starr, sondern der jeweiligen Situation angepasst erfolgen muss. Dies spiegelt sich sowohl in der aktivierten Aufbaustruktur wie auch im Ablauf wider.

7.1 Ablauforganisation

Die groben Teilschritte und Aufgaben bei Eintritt eines Notfalls oder einer Krise stellen sich wie folgt dar:

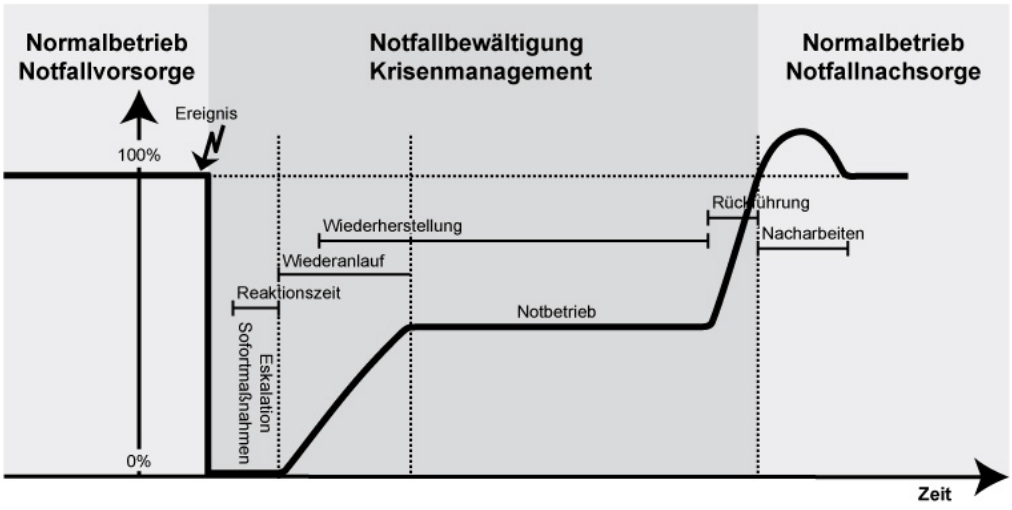


Abbildung 9: Phasen der Notfall- und Krisenbewältigung

Nach Eintritt eines Schadensereignisses löst eine Meldung den Notfall- oder Krisenbewältigungsprozess aus. Es werden gegebenenfalls Sofortmaßnahmen eingeleitet und bei Überschreitung einer Notfall- oder Krisenschwelle an den Krisenstabsleiter eskaliert. Dieser beurteilt die Lage, stellt fest,

was sich ereignet hat und welche Auswirkungen zu erwarten sind. Je nach Schwere des Ereignisses wird zur Behebung einer Störung an die Fachabteilung verwiesen, zur Bewältigung eines Notfalls die lokalen Notfallteams aktiviert oder der Krisenstab einberufen, um die Krise zu managen (siehe Abbildung 10).

Tritt der Krisenstab zusammen, trifft dieser Entscheidungen mit dem Ziel, den Schaden zu minimieren und den Betrieb schnell wieder aufnehmen zu können. Er erteilt entsprechende Anweisungen an die Notfallteams und überwacht die Lage. Auch stellt er die interne wie auch externe Krisenkommunikation sicher. Nach Wiederaufnahme- des Betriebs bzw. Wiederherstellung der Normallage deeskaliert er die Notfallbewältigung und der Normalbetrieb mit der entsprechenden Aufbauorganisation tritt wieder in Kraft.

7.1.1 Meldung, Alarmierung und Eskalation

In einem Notfall oder einer Krise ist ein schneller und geeigneter Informationsfluss mitentscheidend für die erfolgreiche Bewältigung. Daher ist die Festlegung von Wegen und Verfahren für Meldung, Eskalation und Alarmierung von Ereignissen von entscheidender Bedeutung.

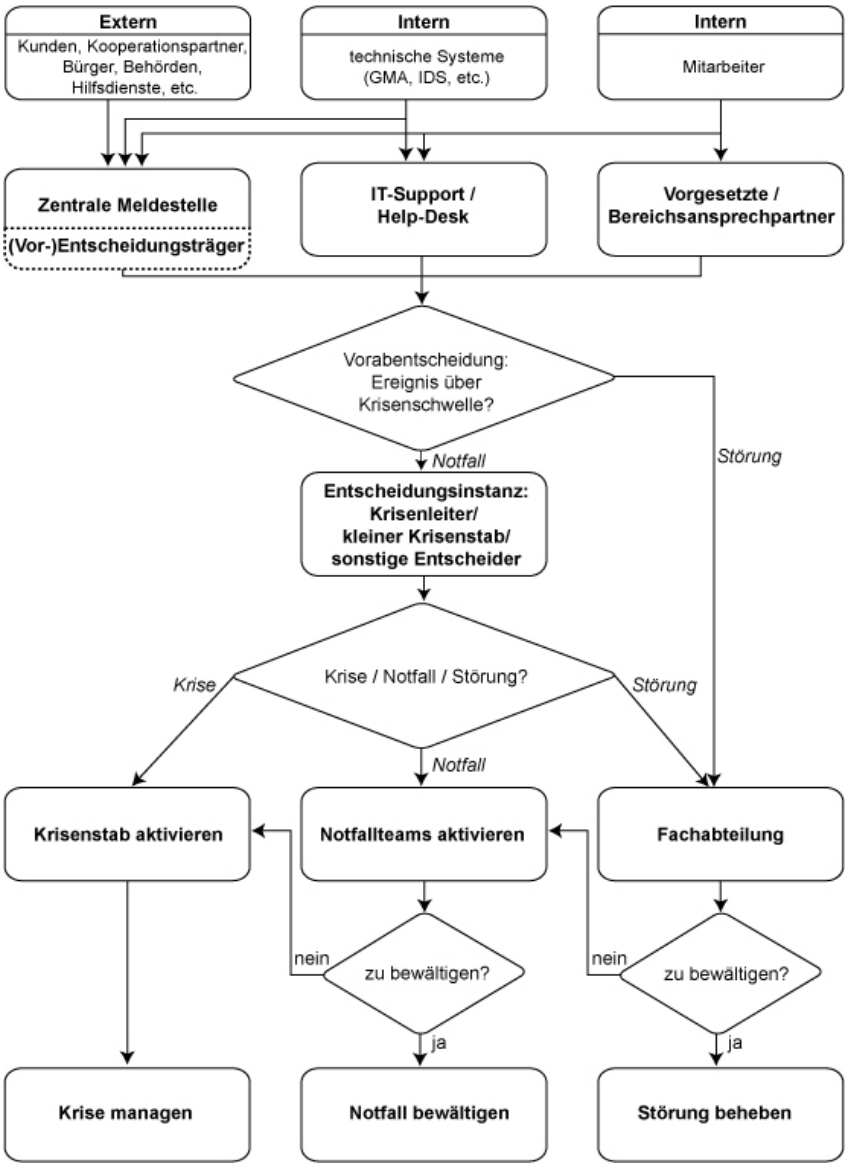


Abbildung 10: Alarmierung und Eskalation

Zentrale Meldestelle

Die Meldung über außergewöhnliche, kritische Ereignisse kann von Außen oder von Innen erfolgen. Die Meldewege sind eindeutig festzulegen, so dass sichergestellt ist, dass alle Meldungen an einer dafür zuständigen, zentral festgelegten Stelle zusammenlaufen. Dabei kann es sich um eine Stelle oder auch um unterschiedliche Stellen (CERT, IT-Support, Empfang, Bereichsverantwortlicher, Leitstelle, Notfallstelle, etc.) für unterschiedliche Ereignistypen (z. B. Feueralarm, Ausfall Dienstleister, Finanzkrise, IT-Krise) handeln. Sie müssen jedoch eindeutig festgelegt und allen Mitarbeitern und gegebenenfalls Externen bekannt gegeben werden.

Die zentrale Meldestelle sollte rund um die Uhr erreichbar sein. Außerhalb der regulären Arbeitszeiten kann dies durch unterschiedliche Maßnahmen wie beispielsweise Schichtdienst, Outsourcing oder durch automatische Weiterleitung an eine Person in Bereitschaftsdienst umgesetzt werden.

Bei internen Meldungen kann unterschieden werden zwischen Meldungen, die von Mitarbeitern generiert und solchen, die durch technische Systeme (z. B. Gefahrenmeldeanlagen) erzeugt werden. Externe Störungsmeldungen erfolgen typischerweise durch Kunden, Geschäftspartner, Bürger, Behörden oder auch Hilfsdienste.

Die Erfassung der von Personen gemeldeten Meldungen in der zentralen Meldestellen sollte in einem zuvor festgelegten Format erfolgen, um sicherzustellen, dass die für die Erstbewertung erforderlichen Informationen enthalten sind. Die Meldungen sollten kurz gefasst werden, deutlich die Tatsachen von Vermutungen getrennt darstellen und mindestens folgende Angaben enthalten:

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

Die zentrale Meldestelle leitet gegebenenfalls Sofortmaßnahmen ein, wie beispielsweise die Alarmierung von Rettungsdiensten oder über akustische und/oder visuelle Signalisierung der Mitarbeiter.

Alarm- oder Eskalationsstufen

Sobald ein Schadensereignis eine gewisse Schwelle übersteigt, wird dessen Bewältigung an die dafür Zuständigen eskaliert. Grundlage für die Entscheidung zur Eskalation bilden sogenannte Alarm- oder Eskalationsstufen. Diese sind im Vorfeld zu definieren, Kriterien und Schwellenwerte festzulegen und Entscheidungshilfen zu entwickeln. Im Extremfall kann eine Institution beschließen, nur mit einer Eskalationsstufe zu arbeiten, also direkt vom Normalbetrieb inklusive Störungsmanagement zu einer Krise überzugehen. Typischerweise wird aber mit einem Eskalationsmodell gearbeitet, bei dem mehrere Stufen definiert sind. Dies ermöglicht es, gezielter auf Vorfälle reagieren zu können.

Eskalationsstufen können beispielsweise folgendermaßen aussehen:

Eskalationsstufe			Beispiele
1	Grün	Normalbetrieb	--
2	Gelb	Störmeldungen	Ereignisse, die gemeldet, geprüft, dokumentiert und gegebenenfalls behoben werden müssen.
3	Orange	Voralarm	Ereignisse, die bereits erste Gefahren abwehrende oder Risiko reduzierende Maßnahmen erfordern, z. B. singulärer Brandlöschung.
4	Rot	Notfall	Ereignisse, die den Geschäftsbetrieb stark beeinträchtigt und nicht mehr innerhalb der geforderten Zeit behoben werden können.

Eskalationsstufe			Beispiele
5	Rot	Krise	Ereignisse mit Krisenpotential, die eine übergeordnete Koordinierung erfordern und die Existenz der Institution oder Leben gefährden.
6	Rot	Katastrophe	Großschadensereignisse, die nicht auf die Institution beschränkt sind.

Tabelle 17: Mögliche Eskalationsstufen

Alarmierungs- und Eskalationsverfahren

Bei der Festlegung des Eskalations- und Alarmierungsverfahrens ist zu definieren, wer eskaliert, an wen zu eskalieren ist und wer wen alarmiert. Je nach Qualifikation der zentralen Meldestelle entscheidet diese anhand von Entscheidungshilfen, welche Eskalationsstufe vorliegt, oder informiert einen Entscheidungsträger, der dann diese Vorentscheidung trifft. Liegt eine Störung vor, so wird an die entsprechende Fachabteilung eskaliert. Wird eine Notfallschwelle überschritten, so wird an eine Entscheidungsinstanz für die Notfallbewältigung eskaliert. Diese Eskalation zur Notfallbewältigung kann auch durch die Fachabteilungen, wie beispielsweise das Störungsmanagement in der IT, oder durch Geschäftsprozess-Verantwortliche erfolgen. Dabei handelt es sich überwiegend um schleichende Störungen, welche eine Schwelle überschritten und sich zum Notfall entwickelt haben.

Wurde zur Entscheidungsinstanz eskaliert, so hat diese die Entscheidung zu treffen, ob doch nur eine Störung, ein Notfall oder eine Krise vorliegt. Die Entscheidungsinstanz kann der Krisenstabsleiter, eine beliebig andere eindeutig benannte Person (z. B. aus der Geschäftsführung oder dem Vorstand) oder eine kleine Gruppe, beispielsweise aus dem Krisenstab, sein. Für den Krisenstabsleiter spricht, dass eine weitere Eskalationsstufe entfällt und das nötige Wissen und die Kompetenz zur Einschätzung von Situationen vorhanden ist. Bedenken gegen diese Lösung bestehen darin, dass der Krisenstabsleitung die Krise ausrufen und damit die „Macht“ in der Institution übernehmen könnte. Dieser hypothetischen Problematik kann dadurch entgegen gewirkt werden, dass als Sicherungsmaßnahme eine oder mehrere Kontrollinstanzen eingeführt werden, die die Feststellung der Krise überprüfen, widerrufen und deeskalieren können. Die Überprüfung kann von jeder Person angestoßen werden.

Ist die Entscheidung der Entscheidungsinstanz, dass es sich um eine Störung handelt, wird an die entsprechende Fachabteilung zur Behebung deeskaliert. Bei Vorliegen eines Notfalls, also einem lokal begrenzten Schadensereignis, werden die benötigten Notfallteams und die lokale Notfallbewältigung alarmiert, welche den Notfall bewältigen. Handelt es sich um ein Schadensereignis größeren Ausmaßes, das übergreifende Koordination erfordert und nicht ausschließlich mithilfe der Notfallpläne behoben werden kann, so wird der Krisenstab situationsangepasst einberufen. Eventuell sind noch weitere Stellen, wie beispielsweise andere Niederlassungen, Partnerbehörden, Gesundheitsdienst, zu informieren. Der Leiter des Krisenstabs entscheidet auch, ob eine weitere Eskalation an höhere Managementhierarchien erforderlich ist.

Für die Durchführung der Alarmierung und Eskalation müssen Pläne der Eskalationswege und Erreichbarkeiten der Krisenstabs-Mitglieder sowie der zu informierenden externen Stellen vorliegen. Dies beinhaltet auch Beschreibungen, wie zu verfahren ist, falls einzelne Mitglieder des Krisenstabs oder der Notfallteams nicht zu erreichen sind. Eine graphische Aufbereitung der relevanten Informationen (beispielsweise als Datenflussdiagramm) erleichtert das intuitive Erfassen der Informationen und verbessert die Übersicht. Dies kann gerade in einer Stresssituation von Vorteil sein. Die notwendige Alarmierung interner Mitglieder sowie externer Stellen sollte möglichst schnell erfolgen, so dass bei größeren Unternehmen bzw. höherer Anzahl von zu informierender Stellen eine Toolunterstützung in Betracht zu ziehen ist.

Art und Weise

Es ist festzulegen, wie die Eskalation und Alarmierung durchzuführen ist. Das kann in Form einer Kette erfolgen, bei der eine Person eine oder mehrere weitere benachrichtigt, oder sternförmig durch

eine zentrale Stelle. Ebenso ist festzulegen, zu welchem Zeitpunkt die Meldung weitergegeben sowie wann der Krisenstab lediglich informiert und wann er alarmiert wird.

Es sollten bei der Alarmierung einige Grundsätze beachtet und eingehalten werden. Die Benachrichtigung der für die Notfallbewältigung verantwortlichen Personen sollte kurz und präzise sein. Diskussionen und längere Ausführungen zur Lage sind bei der Alarmierung zu vermeiden. Aus der Nachricht sollte klar erkennbar sein, welche nächsten Schritte der Alarmierte zu unternehmen hat, beispielsweise sind im Krisenstabsraum einzufinden. Der Alarmierte hat dem Aufruf zwingend zeitnah zu folgen. Leben im Haushalt des Alarmierten weitere Personen, die den Anruf entgegen nehmen könnten, so sind diese im Vorfeld nachdrücklich durch die Notfallvorsorgeorganisation zu instruieren, was im Falle einer Alarmierung zu unternehmen ist, falls sie die Nachricht entgegennehmen. Der Alarmierende hat die Alarmierung vollständig zu dokumentieren. Dazu gehören die Angaben,

- wer wurde alarmiert,
- wer hat alarmiert,
- wann wurde alarmiert,
- wer wurde erreicht und
- was ist das Resultat.

Die Durchführung einer Alarmierung erfordert technische Unterstützung, die insbesondere für den Notfall und die Krise sichergestellt sein muss. Zum Einsatz kommen in der Regel Festnetz-Telefone, Mobiltelefone, Internettelefone (VoIP), Funkmeldeempfänger (auch Pager genannt), Funk- oder Satellitenkommunikationsgeräte. Dabei sind Systeme für die Erstalarmierung zu bevorzugen, die erkennen können, ob die Zielperson erreicht und die Nachricht entgegengenommen worden ist. Die Nutzung von SMS (Short Message Service) ist nur bedingt für die Alarmierung geeignet, da hierbei nur eine zeitverzögerte Rückmeldung möglich ist und es auch keine garantierte Übertragungsdauer gibt.

Für Katastrophenfälle, in denen die Infrastrukturen Telekommunikation oder/und Internet gestört sein könnten, sollten alternative Kommunikations- und Alarmierungswege überlegt und vorgesehen werden, da gängige Alarmierungssysteme, je nach dem, ob sie als eigenes internes System realisiert oder als Service durch Drittanbieter genutzt werden, entweder das Internet oder das Telefonnetz benötigen oder gar beide.

7.1.2 Sofortmaßnahmen

Nachdem ein Ereignis gemeldet wurde, ist der erste Schritt der Notfallbewältigung die Einleitung von Sofortmaßnahmen, sofern welche erforderlich sind. Unter Sofortmaßnahmen werden beispielsweise Löschen von Bränden, Evakuierung oder Retten von Personen verstanden. Diese Maßnahmen werden noch vor einer Eskalation des Notfalls eingeleitet. Hier gilt es, größere Schäden insbesondere von Personen zu vermeiden, die durch Zeitverlust sonst entstehen könnten.

Entsprechende Anweisungen und konkrete Aufgaben sind im Vorfeld festzulegen und zu dokumentieren. Es ist klar zu regeln, wer welche Sofortmaßnahmen anstoßen oder durchführen darf. Rollen für den Notfall wie beispielsweise Ersthelfer, Betriebssanitäter, Brandhelfer, Evakuierungshelfer oder Einsatzteam sind festzulegen und zu besetzen. Diese werden direkt alarmiert und agieren selbstständig am Einsatzort.

Da entsprechende gesetzliche Vorgaben durch die Berufsgenossenschaften existieren und in jeder Institution umzusetzen sind, sollten entsprechende Anweisungen für Sofortmaßnahmen in jeder Institution schon vorhanden sein. Die entsprechenden organisatorischen Maßnahmen sind in geeigneter Form in die Ablauforganisation der Notfallbewältigung zu integrieren. Die benötigten Informationen und Anweisungen sind in das Notfallhandbuch einzubinden.

7.1.3 Krisenstabsraum

Bei einer Eskalation zu einer Krise werden die Mitglieder des Krisenstabs umgehend informiert und treffen sich an einem zuvor festgelegten Ort, dem Krisenstabsraum. Diese Räumlichkeiten, auch Lagezentrum genannt, dienen dem Krisenstab als Arbeitsumgebung, für die besondere Anforderungen bezüglich des Standortes und der Ausstattung gelten.

Für die Lage des Krisenstabsraumes gilt, dass er so ausgewählt sein sollte, dass er in einem Notfall oder einer Krise von den Mitgliedern des Krisenstabes gut erreicht werden kann. Er sollte zentral zum Haupt-Standort der Institution liegen. Für den Fall, dass am Haupt-Standort der Krisenstabsraum ausfällt, sollte ein Alternativ-Standort existieren, welcher unter Beachtung möglicher Notfallszenarien räumlich ausreichend weit vom Haupt-Standort entfernt sein sollte. Als Standort bieten sich, falls vorhanden, Zweigstellen an, aber auch angemietete Räumlichkeiten, Büro-Container oder mobile Alternativen. Bei der Wahl und der Ausstattung des Krisenstabsraums sollten unter anderem folgende Punkte beachtet werden:

- Ausreichend Platz: Die Räumlichkeiten sollten sowohl über ausreichend Arbeitsplätze als auch über abgetrennte Besprechungszonen verfügen, welche für Präsentationen abgedunkelt werden können. Für länger andauernde Krisen sollten soziale Bereiche wie Ess- und Ruhebereiche, Toiletten, Waschräume sowie gegebenenfalls eine Raucherzone vorhanden sein. Die Größe der Räumlichkeiten sollte nicht zu knapp bemessen sein, da keine genaue Vorhersage über die Anzahl des ereignisspezifischen Zusatzpersonals gemacht werden kann.
- Zugang: Der Zugang zu den Räumlichkeiten muss auch außerhalb der regulären Bürozeiten möglich sein.
- Sicherheit: Der Zugang zu den Räumlichkeiten ist durch einen geeigneten Zutrittsschutz zu sichern. Je nach Art der Krise kann die Vertraulichkeit der eintreffenden Informationen und der Besprechungen eine mehr oder minder wichtige Rolle spielen. Daher sollte der Krisenstabsraum über Sichtschutz verfügen sowie gegebenenfalls abhörsicher gestaltet sein.
- Technische Ausstattung: Zur Informationsbeschaffung, -verarbeitung und -darstellung ist eine entsprechende technische Ausstattung mit unter anderem vernetzten Rechnern, Beamer, Scanner, Kopierer, Drucker sowie mobilen Speichermedien für den Transport und Austausch von Informationen notwendig. Die IT-Infrastruktur des Krisenstabsraums sollte unabhängig von dem eventuell nicht mehr zur Verfügung stehenden Intranet sein, wie beispielsweise dem E-Mail-Server, der Public-Key-Infrastruktur oder auch Datenbanken mit benötigten Informationen. Aber auch Faxgeräte, Radio, Fernsehen oder Videorekorder sind sinnvolle Hilfsgeräte. Neben den normalen Telefonen sollten Mobiltelefone, eventuell analoge, stromunabhängige Telefone oder, falls in einem Katastrophenfall Mobil- und Festnetz ausfallen, Satellitentelefone vorhanden sein.
- Klimaanlage: Eine Klimaanlage verbessert die Arbeitsbedingungen und reduziert zusätzlichen Stress. Die Möglichkeit zu Regulierung sollte zu allen Zeiten gegeben sein.
- Redundante Stromversorgung: Für die technischen Geräte inklusiv der Telefone sollte eine redundante Stromversorgung vorgehalten werden.
- Redundante Telekommunikations- und Internetanbindung: Um Informationen aus dem Intranet oder auch Internet abrufen zu können, ist eine redundante Anbindung an das Internet und die Verwendung verschiedener Kommunikationswege empfehlenswert.
- Sonstige Ausstattung: Neben der technischen Ausstattung werden Büromaterialien, Verbrauchsmaterialien (z. B. Druckerpatronen, Batterien) und Arbeitsmittel zur Informationsdarstellung (z. B. Flipcharts, Tafeln), Informationsbearbeitung sowie Informationsbeschaffung (z. B. Karten, Nachschlagewerke, Telefonbücher) benötigt. Für die Vernichtung vertraulicher Unterlagen sollte ein Schredder vorhanden sein. Je nach identifizierten möglichen Schadensereignissen (z. B. Freisetzung von Chemikalien) ist gegebenenfalls eine ausreichende Schutzausrüstung notwendig.
- Verpflegung und Müllentsorgung: Die Verpflegung des Krisenstabs sollte ebenso wie die Müllentsorgung geregelt sein.

Der Raum und dessen Ausstattung sind regelmäßig auf ihre Funktionsfähigkeit zu überprüfen.

Eine besondere Herausforderung stellen Krisen dar, in denen ein Zusammenarbeiten der Krisenstabsmitglieder in einem Krisenstabsraum eingeschränkt möglich, wenig sinnvoll oder gar unerwünscht ist, beispielsweise im Falle einer Pandemie. Für diesen Fall ist eine Alternative zu entwickeln, die das gemeinsame, jedoch verteilte Arbeiten ermöglicht.

7.1.4 Aufgaben und Kompetenzen des Krisenstabs

Wurde ein Ereignis eskaliert und der Krisenstab aktiviert, so beginnt mit dessem Zusammentreten im Krisenstabsraum die eigentliche Notfall- oder Krisenbewältigung. Der Krisenstab legt den von der Krise betroffenen Bereich (z. B. Gebäude, Niederlassung, mehrere Standorte) fest. Er ist ausschließlich gegenüber diesem Bereich weisungsbefugt.

Zu den Kernaufgaben des Krisenstabs gehört es, Entscheidungen zu treffen und Notfallteams zu koordinieren, um den Notfall bzw. die Krise zu bewältigen. Der wesentliche Unterschied zwischen einem Notfall und einer Krise besteht darin, dass ein Notfall im Wesentlichen mit Hilfe von Notfallplänen gemeistert werden kann. Eine Krise erfordert weitergehende Kompetenzen. Sie ist einzigartig, kann auf kein vorgedachtes Muster aufsetzen und erfordert schnelle und kompetente Entscheidungen.

Zu den wesentlichen Teilaufgaben des Krisenstabs gehören:

- Informationsbeschaffung, –auswertung und –aufbereitung,
- Erfassen und Bewerten der aktuellen Lage,
- Entwickeln von Handlungsoptionen und Bewerten in Bezug auf Erfolgsaussichten, Folgerisiken und Rahmenbedingungen,
- Festlegung von Maßnahmen,
- Beauftragung der Notfallteams mit der Durchführung und Kontrolle der einzelnen Notfallmaßnahmen,
- Überprüfung der Wirksamkeit dieser Maßnahmen und gegebenenfalls Korrekturen, wenn diese nicht den gewünschten Erfolg erzielen, und
- Kommunikation mit Partnern, Mitarbeitern, Behörden und Medien.

Bei längerer Dauer des Notfalls muss der Krisenstab seine Abläufe und Strukturen, aber auch die notwendige Infrastruktur selbstständig organisieren. Dazu gehört unter anderem die Organisation von Schichtwechseln und die Versorgung mit Verpflegung und Verbrauchsmitteln.

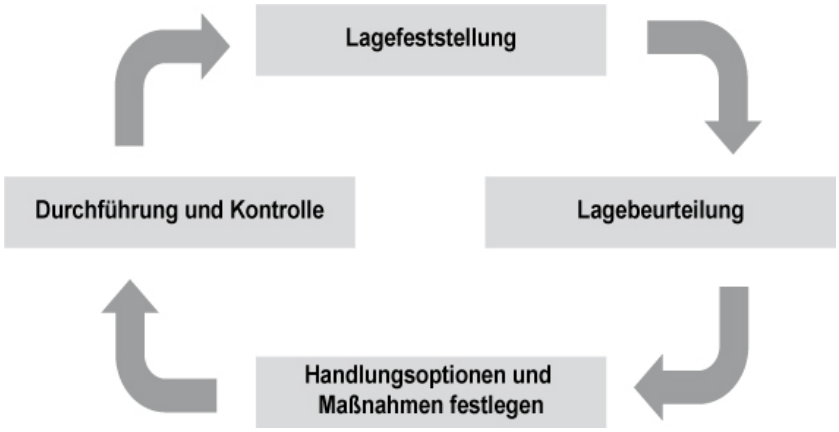


Abbildung 11: Bewältigungsprozess

Lagefeststellung und Informationsgewinnung

Für die Lagefeststellung werden umfassende Informationen benötigt. Eine Lage bezeichnet dabei die Faktoren und Gegebenheiten, die das Schadensereignis und die Schadensabwehr beschreiben, wie beispielsweise Art und Umfang der Beeinträchtigungen, Schäden sowie ihre voraussichtliche Entwicklung, die Zahl der Betroffenen, akute Gefahren, Zeitpunkt des Geschehens, Zustand des Versorgungs- und Verkehrsnetzes.

Für die Lagefeststellung stellt der Krisenstab bzw. Hilfspersonal zuerst alle relevanten Informationen über den Vorfall zusammen, um sich ein Bild der Ereignisse machen zu können. Dafür ist es wichtig, dass eine möglichst genaue Beschreibung der Art des Vorfalls, des Umfanges und der Abläufe der Ereignisse vorliegt. Darüber hinaus werden Informationen über bereits ergriffene Maßnahmen wie auch über deren Auswirkungen auf die Lage benötigt.

Diese Informationen können durch den Krisenstab selbst ermittelt werden, aus bereitgestellten Unterlagen entnommen werden oder aus eingetroffenen Meldungen stammen. Meldungen können von geschultem, eigenen Personal, Erkundungstrupps, externen Helfern oder auch aus der Bevölkerung stammen. Für die Aufarbeitung der Meldungen ist es hilfreich, wenn bei deren Erstellung folgende Grundsätze beachtet wurde:

- Meldungen sollten klar, sachlich und kurzgefasst werden, aber vollständig sein.
- Meldungen sollten aktuell sein und müssen daher unverzüglich erfolgen. Der Zeitpunkt der Feststellung ist zu vermerken.
- Die Darstellung des Ereignisses darf weder über- noch untertrieben sein.
- Es sollte erkennbar sein, wie und durch wen die Feststellung erfolgte: durch die eigene Wahrnehmung oder durch Aussage von Dritten. Die Trennung von Tatsachen und Vermutungen sollte klar und deutlich sein. Die Herkunft der Meldungen sollte erkennbar sein.

Für die Lagefeststellung sind die einzelnen Meldungen relevant. Diese sind je nach Absender unterschiedlich zu bewerten und einzuschätzen, besonders im Falle widersprüchlicher Informationen. Bei der Erstellung des Gesamtbildes der Lage sind daher auch die Reihenfolge der Meldungen und die meldenden Personen zu berücksichtigen.

Je nach Art der Lage können für deren Einschätzung beliebige Zusatzinformationen beispielsweise über die räumliche und geographische Umgebung, klimatische Rahmenbedingungen oder den aktuellen Informationsstand betroffener Personen von Interesse sein. Dazu benötigt der Krisenstab einen Zugriff auf diverse Materialien, die im Normalbetrieb typischerweise von verschiedenen Organisationseinheiten verwaltet werden. Dazu gehören beispielsweise Gebäudepläne, Lagepläne der genutzten Räumlichkeiten, Raumbelegungspläne, Übersichten über die Versorgungsleitungen (Strom, Gas, Wasser) und Netzpläne der Informations- und Kommunikationseinrichtungen. Es muss sichergestellt sein, dass dem Krisenstab die aktuellsten Versionen zur Verfügung stehen.

Lagebeurteilung

Der Krisenstab trifft anhand der vorliegenden Informationen eine gemeinsame Einschätzung der aktuellen Lage und welche Folgeereignisse diese noch nach sich ziehen könnten. Mögliche Fragen bei der Lagebeurteilung sind somit:

- Was kann als nächstes noch geschehen? Was noch im Weiteren?
- Welche Auswirkungen sind möglicherweise zu erwarten?
- Wie kann die weitere Ausbreitung des Schadens eingeschränkt werden?
- Wie kann der schon entstandene Schaden behoben werden?

Handlungsoptionen und Maßnahmenfestlegung

Anhand der Lagebeurteilung werden mögliche Vorgehensweisen zur Bewältigung der konkreten Situation entwickelt. Diese Optionen werden auf ihre Erfolgsaussichten hin bewertet, Vor- und Nachteile gegeneinander abgewogen, die Effektivität eingeschätzt und mögliche positive und negative Auswirkungen und Handlungsrisiken ermittelt, die die getroffenen Notfallmaßnahmen nach sich ziehen könnten. Es gilt, eine Strategie zur Bewältigung der Krise festzulegen und die richtigen Mittel zur richtigen Zeit am richtigen Ort zu finden. Dabei sind auch das strategische Ziel der Notfallbehandlung und die für die Notfall- oder Krisenbewältigung zur Verfügung stehenden Ressourcen zu berücksichtigen.

Die Entscheidungen für bestimmte Handlungsoptionen und damit für bestimmte Maßnahmen werden gemeinsam im Krisenstab getroffen. Dabei ist eine konstruktive Zusammenarbeit ausschlaggebend, um schnell zu einem Konsens zu kommen. Herrscht keine Einigung im Krisenstab, so trifft der Krisenstabsleiter die Entscheidung.

Für die Geschäftsfortführung wird eine der ersten Entscheidungen sein, welche Notfallteams benötigt werden und diese dann zu aktivieren. Es ist unter anderem zu entscheiden, welche aufeinander abgestimmten Teilpläne aktiviert werden und damit, welche konkreten Maßnahmen getroffen werden.

Wichtig ist auch die Entscheidung, wer innerhalb der Institution und vor allem wer außerhalb informiert werden muss. Der Krisenstab bzw. in letzter Instanz der Krisenstabsleiter trifft die Entscheidungen über die durchzuführenden Maßnahmen und erteilt entsprechende Anweisungen.

Durchführung von Maßnahmen und Kontrolle

Es gilt, die bei der Lagebeurteilung entwickelte Lösung in einzelne Aufgaben aufzuteilen. Der Krisenstab erteilt die Anweisungen an die verschiedenen Notfall- und Hilfsteams zur Durchführung von Maßnahmen, die geeignet sind, die Ursachen und die vorhandenen Schäden zu beseitigen. Er überwacht die zeitgerechte Umsetzung der Maßnahmen.

Die Auswirkungen der getroffenen Maßnahmen sollten regelmäßig kontrolliert und deren Effektivität bewertet werden. Die aktuelle Situation ist mit Hilfe der vorliegenden Informationen in regelmäßigen Abständen neu zu bewerten und die aktuellen Informationen sind in die Lagefeststellung einzubringen. Eine Neubewertung der Lage führt solange zu weiteren Maßnahmen, bis der Normalzustand erreicht ist.

Schichtbetrieb und Übergabe

Krisenmanagement erfolgt unter Stress und ist physisch wie psychisch belastend. Daher sollte für die Krisenstabsarbeit Schichtbetrieb vorgesehen werden. Eine Schicht sollte nicht mehr als 8 Stunden dauern, da dann die Konzentrationsfähigkeit erheblich nachlässt. Daher sind zum einen mehrere Teams vorzusehen und zum anderen der Ablauf des Schichtbetriebs organisatorisch zu regeln.

Für die Organisation des Schichtbetriebs bieten sich prinzipiell zwei verschiedene Modelle an: ein kontinuierlicher Austausch des Personals oder ein Gesamtwechsel. Der Vorteil des kontinuierlichen Austausches ist, dass das Wissen über die aktuelle Situation weiter im Krisenstab vorhanden ist. Doch erfordert jeder einzelne Austausch eine Übergabe und verursacht damit auch eine kontinuierliche Unruhe in der Gruppe. Jedoch kann in der Übergabephase parallel weitergearbeitet werden. Damit sind auch die Vor- und Nachteile eines Gesamtaustausches klar: Vorteil ist, dass weniger Unruhe herrscht, da pro Schichtwechsel nur eine einzige Übergabephase existiert. Andererseits geht bei jedem Wechsel viel Hintergrundwissen über die aktuelle Lage und die Krisenbewältigung verloren. Ein weiterer Nachteil ist, dass in der Übergabephase der gesamte oder überwiegende Teil des Krisenstabes nicht für die eigentliche Krisenbewältigung zur Verfügung steht.

Die Übergabephase sollte kurz und überschaubar gehalten werden und 15 bis 20 Minuten nicht überschreiten. In dieser Zeit sind alle notwendigen und wichtigen Informationen auszutauschen. Das beinhaltet eine Übersicht über die aktuelle Lage, die getroffenen Entscheidungen und die durchgeführten, eingeleiteten und ausstehenden Maßnahmen. Alle Mitglieder des Stabes müssen anschließend

über den gleichen Kenntnisstand über die Lage verfügen. Mitglieder des Krisenstabs mit Spezialaufgaben oder –rollen übergeben ihre speziellen Kenntnisse der Situation einzeln an die Ablösung dieser Rollen. Um eine straffe Übergabe zu ermöglichen, sollten in der Konzeptionsphase Kriterien und Verhaltensanweisungen dafür festgelegt werden.

Deeskalation

Ist der Notfall bzw. die Krise überstanden, so wird deeskaliert, der Krisenstab formal aufgelöst und seine Sonderbefugnisse damit beendet. Wie für die Eskalation sind auch für die Deeskalation Kriterien zu definieren. Die Maßnahmen zur Rückkehr in den Normalbetrieb werden veranlasst und die normale Organisationsstruktur übernimmt wieder den Betrieb.

7.1.5 Geschäftsfortführung, Wiederanlauf und Wiederherstellung

Oberstes Ziel in der Notfallbewältigung und dem Krisenmanagement ist die Geschäftsfortführung. Es gilt, die beeinträchtigten Geschäftsprozesse in irgendeiner Art und Weise zügig wieder in Betrieb zu nehmen. Die Geschäftsfortführung beinhaltet daher konkrete Maßnahmen und Verfahren, die eine Wiederaufnahme der Tätigkeiten innerhalb der für die jeweiligen Geschäftsprozesse vorab festgelegten Wiederanlaufzeit ermöglichen. Der Notbetrieb kann durch einen mit reduzierten Ressourcen arbeitenden „Normalbetrieb“ realisiert werden, einem reduziert arbeitenden Betrieb mit Ausweichressourcen oder durch einen Alternativbetrieb.

Wurde ein Geschäftsprozess unterbrochen, so kann im günstigsten Fall die Geschäftsfortführung durch einen Wiederanlauf der nicht beschädigten Ressourcen erfolgen. Wurden Ressourcen zerstört oder stehen aus sonstigen Gründen nicht mehr zur Verfügung, müssen diese wiederhergestellt werden. Je nach Art der Ressourcen bedeutet dies, dass diese ersetzt, neu installiert und eingerichtet werden müssen.

Bei der Notfallbewältigung wird die aktuelle Situation analysiert und eine Entscheidung getroffen, welche der Geschäftsfortführungsalternativen für die einzelnen Prozesse möglich, sinnvoll und bei der Gesamtbetrachtung der Situation die schnellste und beste ist.

Sobald alle Wiederherstellungs- bzw. Wiederanlaufmaßnahmen durchgeführt worden sind, sollte eine Meldung an den Krisenstab erfolgen, unabhängig davon, ob erfolgreich oder nicht. Solange nicht alle Punkte des Wiederherstellungsplans erfolgreich umgesetzt worden sind, kann der Normalbetrieb nicht wieder aufgenommen werden. Die Institution verbleibt dann weiterhin in der Phase des Notbetriebs.

7.1.6 Rückführung und Nacharbeiten

Stehen die benötigten Ressourcen für den Normalbetrieb von Geschäftsprozessen wieder zur Verfügung, so ist der Notbetrieb in den Normalbetrieb zu überführen. Da zwischen den Geschäftsprozessen zu beachtende Abhängigkeiten existieren, sollte die Rückführung geordnet ablaufen, um Unstimmigkeiten zwischen oder innerhalb der Geschäftsprozesse zu vermeiden. Daher ist durch den Krisenstab festzulegen, in welcher Reihenfolge und zu welchem Zeitpunkt die einzelnen Geschäftsprozesse in den Normalbetrieb zurückgeführt werden, und die Rückführung zu koordinieren. Dadurch wird verhindert, dass bei der Rückführung größere Probleme auftreten, welche zu einem erneuten Zusammenbruch der Geschäftstätigkeit führen könnten.

Durch den eventuell mit weniger Ressourcen durchgeführten Notbetrieb entstehen in der Regel Arbeitsrückstände. Um diese kontrolliert und zeitnah abarbeiten zu können, sollten in den Geschäftsfortführungsplänen für jede Organisationseinheit Verantwortliche benannt werden, die eine Übersicht über die jeweiligen Arbeitsrückstände zusammenstellen und einen Abarbeitungsplan festzulegen haben. Bei der Aufstellung des Abarbeitungsplans sollte die aktuell anliegende Arbeitsbelastung, die Arbeitsbelastung während des Notbetriebs und die arbeitsrechtlichen Auflagen berücksichtigt werden. Strategische Vorgaben, wie der zusätzliche Aufwand geleistet werden soll, um die Arbeitsrückstände abzuarbeiten (z. B. durch Überstunden, Schichtarbeit oder zusätzlichem Personal), sollten bei der Notfallvorsorge festgelegt und mit der Personalvertretung abgestimmt sein.

Die Nacharbeiten sollten von den Notfallkoordinatoren der jeweiligen Organisationseinheiten begleitet werden. Es ist festzulegen, wer den Status der Nacharbeiten zu welchen Zeitpunkten an wen berichtet.

7.1.7 Analyse der Notfallbewältigung

Nach Abschluss der Notfallbewältigung und Deeskalation sollte die Notfallbewältigung analysiert werden, um aufgrund erkannter Schwachstellen Verbesserungsmaßnahmen ergreifen zu können. Die Analyse sollte in Zusammenarbeit von Notfallbeauftragtem und gegebenenfalls den betroffenen Notfallkoordinatoren mit den Verantwortlichen aus der Notfallbewältigung erfolgen. Dabei werden Verbesserungsvorschläge erarbeitet.

Bei der Notfallbewältigung kann sich aber auch zeigen, dass in den Organisationsstrukturen, der IT oder den Geschäftsprozessen Verbesserungsbedarf besteht. In solchen Fällen sollte sich der Notfallbeauftragte mit den für den jeweiligen Bereich Zuständigen zusammensetzen und gemeinsam Verbesserungsvorschläge ausarbeiten. Beispielsweise könnten Änderungen beim Brandschutz oder der Informationssicherheit sinnvoll sein.

Für die Umsetzung der Verbesserungsvorschläge sind Umsetzungsverantwortliche zu benennen und Umsetzungstermine festzulegen. Der Notfallbeauftragte sollte die zeitgerechte Umsetzung der Verbesserungsmaßnahmen überwachen und in vorgegebenen Zeitabständen an die Institutionsleitung berichten. Die angewandten Pläne und Verfahren sollten bei Mängeln durch die jeweiligen verantwortlichen Organisationseinheiten überarbeitet und aktualisiert werden. Die Funktionalität und Effizienz der neu umgesetzten Maßnahmen und Verfahren sollte durch Übungen verifiziert werden.

Zusätzlich zu den Verbesserungsvorschlägen ist bei der Nachbereitung der Notfallbewältigung ein Gesamtmanagementbericht zu erstellen, der zeitnah und als „vertraulich“ eingestuft an die Leitungsebene übergeben wird. Der Bericht dient unter anderem auch als Grundlage zur Beurteilung eventueller Rechtsfolgen für oder gegenüber der Institution bzw. einzelnen Personen, die aus dem Notfall oder der Krise erwachsen können.

7.1.8 Dokumentation in der Notfallbewältigung

Während der Notfall- oder Krisenbewältigung sind im Krisenstab aus rechtlichen Gründen alle wesentlichen durchgeführten Aktivitäten und Entscheidungen revisionssicher in einem sogenannten Einsatztagebuch zu protokollieren. Zusätzlich sollten Ein- und Ausgangsnachweise der Meldungen sowie Anwesenheitslisten der Krisenstabsmitarbeiter geführt werden. Dies kann in elektronischer oder in Papierform erfolgen.

Die Protokollierung sollte so erfolgen, dass die Mitglieder des Krisenstabs, insbesondere aber der Krisenstabsleiter, schnell einen Überblick über die aktuelle Situation erhalten können. Die Dokumentation dient der Lagebeurteilung, aber vor allem auch der Nachbereitung des Notfalls bzw. der Krise für die Beurteilung und Verbesserung des Notfallbewältigungsprozesses. Gegebenenfalls müssen Finanzierungs-, Versicherungs- und Rechtsangelegenheiten aus den Aufzeichnungen dargelegt und durchgesetzt werden können. Es sind unter anderem folgende Punkte zu dokumentieren:

- Zeitpunkt der Arbeit des Krisenstabes,
- Lage (Art, Umfang und Abläufe der Ereignisse),
- Eckpunkte aller getroffenen Entscheidungen sowie Namen und Rollen der daran Beteiligten und
- beschlossene Maßnahmen, Verantwortliche für deren Umsetzung, Fertigstellungstermine und jeweiliger Umsetzungsstatus (Aufgabenüberwachung).

Standardisierte Formblätter und Vordrucke beispielsweise für Ein- und Ausgangsnachweise, Ereignis-Tagebücher oder Meldeprotokolle können dabei helfen, im Krisenfall eine ausreichende und zielgerichtete Dokumentation sicherzustellen. Die Hilfsmittel sind im Vorfeld einer Krise in Ruhe zu erarbeiten und abzustimmen.

Die Protokolle sind nach erfolgter Bewältigung von den Mitgliedern des Krisenstabs zu unterschreiben und revisionssicher aufzubewahren.

7.2 Psychologische Aspekte bei der Krisenstabsarbeit

Jede Krise bedeutet enormen mentalen Stress für die Beteiligten, doch gleichzeitig stellt sie ein komplexes Problem dar, das es zu lösen gilt. Krisen besitzen eine Einmaligkeit, hohe Dynamik und Komplexität sowie viele Variablen und Parameter. Die starke Vernetzung heutiger Systeme erschwert es, die Interaktion der einzelnen Teile, die Kaskadeneffekte und Nebenwirkungen von Entscheidungen zu überblicken. Unter diesen erschwerenden Bedingungen sind weitreichende Entscheidungen zu treffen, die nicht nur finanzielle Auswirkungen auf die Institution haben, sondern auch direkt oder indirekt Menschenleben betreffen können.

Die Stressursachen in einer Krise sind unterschiedlichster Natur. Sie reichen vom Schock über die Ereignisse, über Angst vor dem eigenen Versagen, Angst um Angehörige, emotionale Belastung, Angst vor dem Unbekannten, Reizüberflutung durch zu viel Informationen, widersprüchliche Informationen, unzureichenden Informationen, Zeitdruck, störenden Umgebungsbedingungen wie Lärm, Wärme oder Kälte, Hektik bis hin zu Hunger, Durst oder Schlafmangel. Der Körper reagiert darauf wie in der Urzeit mit Reduzierung der Denkleistung und Aktivierung der körperlichen Fluchtreaktionen. Adrenalin wird ausgeschüttet, der Blutdruck steigt, Verspannungen, Kopfschmerzen, Herz- und Kreislauf-Störungen treten auf. Dies kann zu Folgen führen wie Hektik, Konzentrationsmangel, Vergesslichkeit, zirkulärem Denken, Blackouts, überschießendem Aktionismus, unzureichender Problemanalyse und Tunnelblick, der das Sichtfeld einschränkt und die Wahrnehmung verändert. Aber auch Aggressivität bis hin zu völligem Kontrollverlust kann Folge von Stress sein.

Doch Stress hat nicht nur negative Seiten, sondern auch positive. Stress kann Antriebsfeder sein und Menschen zu Höchstleistungen motivieren. Es gilt daher, bei der Vorbereitung auf die Krisenstabsarbeit auch diesen Faktor zu berücksichtigen. Krisenstabsmitglieder sollten daher von Grund auf eine gewisse Stressresistenz und Selbstvertrauen besitzen. Doch weitere Vorkehrungen zur Prävention sind sinnvoll. Dazu zählen beispielsweise:

- Fachliche Schulungen stärken die Selbstsicherheit und reduzieren Stress, der z. B. durch Unsicherheit entstehen kann.
- Kenntnisse über allgemeine Problemlösungsstrategien und eigene Fähigkeiten bzw. Handlungsmuster erlauben ein schnelles und geordnetes Vorgehen zur Entscheidungsfindung.
- Durch Schulungen können die Mitgliedern des Krisenstabs darauf vorbereitet werden, die eigene Stressresistenz zu erhöhen, gegebenenfalls den Stress durch spezielle Techniken abzubauen und in positive Bahnen zu lenken sowie die Emotionalisierung der Situation zu reduzieren. Dies kann notwendig werden, um eine Stressspirale zu verhindern, in der durch Stress verursachte Fehleinschätzungen und -entscheidungen zu immer weiter ansteigendem Stress und damit zur weiteren Fehlentscheidungen führen.
- Weiterbildungen zu psychologischen und gruppendynamischen Aspekten der Krisenstabsarbeit erhöht die Effektivität der Zusammenarbeit im Krisenstab.
- Die Vorbereitung des Teams durch Übungen auf die Zusammenarbeit in der Krise hilft, eine gemeinsame Arbeitsweise und ein gemeinsames Denkmodell zu entwickeln. Faktoren wie Vertrautheit, Entwicklung einer gemeinsamen Sprache als Grundlage für die Kommunikation im Krisenstab, ein gutes Arbeitsklima und die Fähigkeit, die anderen Teammitglieder in einem gewissen Grade einschätzen zu können, reduzieren den Stress.
- Die externen Stressfaktoren können reduziert werden, indem ein positives Arbeitsumfeld und -bedingungen (z. B. Verpflegung, Raumklima, Rückzugs- und Schlafmöglichkeit) geschaffen werden.

7.3 Krisenkommunikation

Krisenkommunikation ist einer der zentralen Erfolgsfaktoren des Krisenmanagements. Krisenkommunikation ist die Kommunikation während und nach einer Krise mit den verschiedenen Interessensgruppen mit dem Ziel, die Krise zu bewältigen, weiteren Schaden zu verhindern, zu informieren und Vertrauens- und Imageverluste zu vermeiden. Es kann zwischen interner und externer Krisenkommunikation unterschieden werden. In diesem Dokument wird unter der internen Krisenkommunikation jegliche Kommunikation, die der Bewältigung des Notfalls oder der Krise dient, verstanden. Externe Krisenkommunikation hat das Ziel zu informieren. Die Zielgruppen sind dabei sowohl innerhalb der Institution wie auch außerhalb zu finden.

7.3.1 Interne Krisenkommunikation

Zur internen Krisenkommunikation gehört sowohl die Meldung, Eskalation und Alarmierung, aber auch sämtliche Kommunikation zur Informationsbeschaffung, der Koordinierung der Notfallteams oder die Kooperation mit externen Stellen wie Geschäftspartner, Kunden, Rettungsdienste, Hilfsorganisationen, Feuerwehr, Polizei oder Technisches Hilfswerk zur Bewältigung der Krise.

Falls der Krisenfall nicht intern begrenzt ist, kann es notwendig sein, externe Stellen wie Geschäftspartner oder Kunden, die ebenfalls davon betroffen sein könnten, darüber zu informieren und mit ihnen zusammenzuarbeiten, um die Schadensausbreitung zu verhindern. Im Falle eines Sicherheitsvorfalles kann dies bedeuten, mit den externen Stellen die möglichen Sicherheitsprobleme und Gegenmaßnahmen zur Eindämmung der Auswirkungen zu besprechen. Sollte diese Informationsweitergabe und Kooperation nicht erfolgen, kann dies die weitere konstruktive Zusammenarbeit mit den externen Stellen nachhaltig stören und das bestehende Vertrauensverhältnis beeinträchtigen, wenn diese über andere Kanäle über die Sicherheitsprobleme informiert werden.

Neben den organisatorischen Festlegungen, wer, wem, wann meldet, eskaliert, alarmiert (siehe Kapitel 7.1.1) und informiert, ist auch festzulegen,

- wer für die einzelnen Informationsflüsse zwischen den verschiedenen Parteien und Rollen bei der Notfall- und Krisenbewältigung zuständig ist,
- wann und in welchen zeitlichen Abständen berichtet wird und
- in welcher Art und Weise die Kommunikation erfolgt.

Dazu gehört beispielsweise der Informationsfluss vom Schadensort oder den Notfallteams zum Krisenstab und zurück. Ein besonderer Augenmerk sollte dabei auf die technischen und logistischen Aspekte der Krisenkommunikation gelegt werden. Dabei sind unter anderem folgende Fragen zu beantworten:

- Wie sehen die erforderlichen Kommunikationsprozesse zur Bewältigung des Notfalls aus (Sprache, Text, Daten, Video und Bilder)?
- Welche Kommunikationssysteme (Endgeräte und Verbindungen) stehen grundsätzlich und alternativ an den verschiedenen Lokationen zur Verfügung?
- Welche Ausfall-Risiken bestehen für die einzelnen Kommunikationslösungen?
- Welche Maßnahmen sind hinsichtlich der Verfügbarkeit der in Notfällen benötigten Kommunikationssysteme zu ergreifen?

In Krisenfällen wird eine zuverlässige und sichere Kommunikation benötigt, daher ist eine hohe Verfügbarkeit der Kommunikationssysteme in der Krise sicherzustellen. Zu den möglichen Vorsorgemaßnahmen zählen sowohl eine ausreichende Anzahl von Endgeräten, gesicherte Stromversorgung für die Endgeräte und insbesondere die Bereitstellung alternativer Kommunikationswege (z. B. Internet, Festnetz, Mobilkommunikation, Satellitenkommunikation). Doch auch die Aspekte der Vertraulichkeit und Integrität der Kommunikation und der Authentizität der Kommunikationspartner sollte in die Betrachtung und die Auswahl der Systeme mit einbezogen werden.

7.3.2 Externe Krisenkommunikation

Jede Krise ist immer auch eine Kommunikationskrise, da die Wahrnehmung der Krise, der Krisenbewältigung und des Managementverhaltens in der Öffentlichkeit ausschlaggebend ist. Die Öffentlichkeit entscheidet mit über das Ausmaß der Krise. Es gilt, einen Flächenbrand zu vermeiden, Emotionen zu kanalisieren und Ängste nicht entstehen zu lassen bzw. abzubauen. Daher ist es von essentieller Bedeutung, dass eine eindeutige Verantwortung und Strategie für die externe Krisenkommunikation, auch Krisen-PR (Public Relation) genannt, festgelegt ist.

Organisatorische Strukturen

Die Verantwortung für die externe Krisenkommunikation trägt ausschließlich der im Krisenstab vertretene Leiter der Krisenkommunikation. Alle Medienkontakte sollten ausschließlich über ihn laufen bzw. von ihm koordiniert werden. Dieser kann durch Mitarbeiter unterstützt werden, die Spezialaufgaben übernehmen und ausführen, wie den Kontakt zu den Medien halten, Pressekonferenzen leiten oder die Redaktion der Online-Information übernehmen. Hilfreich im Team der Krisenkommunikation sind folgende Rollen: ein Krisensprecher, der an die Öffentlichkeit tritt, ein Fachexperte, der wissenschaftliche und Sachfragen bewertet, ein juristischer Experte für juristische Sachfragen und ein Experte für Presse- und Öffentlichkeitsarbeit, der für die Beobachtung der Medien zuständig ist.

Die Mitglieder im Team der externen Krisenkommunikation sollten durch entsprechende, regelmäßige Trainings- oder Schulungsmaßnahmen (z. B. Medientraining) auf die Tätigkeit vorbereitet werden, damit sie auch auf unvorhergesehene Fragen angemessen reagieren und dem extremen Zeitdruck und Stress standhalten können. Sie müssen lernen, sich nicht zu unüberlegten Äußerungen provozieren zu lassen und die Ruhe zu bewahren. Es gilt, sich kritischen Fragen, die oftmals das eigene Versagen thematisieren, zu stellen und niemals aggressiv zu reagieren. Krisenkommunikation ist eine anspruchsvolle und komplexe Aufgabe. Um diese professionell wahrnehmen zu können, sind Spezialisten gefragt. Schulungen dieser Art werden unter anderem von Agenturen durchgeführt, die auf Krisenkommunikation spezialisiert sind.

Stehen nicht genügend interne Ressourcen zur Verfügung, ist zu überlegen, ob es sinnvoll ist, einen externen Krisenkommunikationsexperten in der Krise hinzuziehen. Dieser sollte im Vorfeld ausgewählt, vertraglich gebunden und mit der Institution und deren Begrifflichkeiten vertraut gemacht werden.

Es ist sicherzustellen, dass der Leiter der Krisenkommunikation über ausreichende Informationen zum Krisenfall, über die möglichen Schäden, die durchgeführten sowie geplanten Gegenmaßnahmen (ohne Details) und über die bereits benachrichtigten Stellen verfügt. Er überprüft und genehmigt sämtliche Informationen zur Krise, die zu Informationszwecken weitergegeben werden. Ist ein Vertreter der Leitungsebene mit Teilaufgaben der Krisenkommunikation betraut, wie beispielsweise den Kontakt zu wichtigen Interessensgruppen zu halten, so sind seine Aufgaben und Kompetenzen eindeutig festzulegen, um Missverständnissen vorzubeugen.

Kommunikationsstrategie

Es sollte eine klare Kommunikationsstrategie und –linie festgelegt werden, die ein inhaltlich und argumentativ einheitliches Auftreten in der Krise garantiert. Die Krisenkommunikationsstrategie gibt den Rahmen und die Grundsätze für die Kommunikation sowie Sprachregelungen vor. Sie legt fest, wer die Informationen für die Krisenkommunikation erstellt, welche Zielgruppen welche Informationen erhalten und zu welchem Zeitpunkt der Krise diese in welcher Informationstiefe auf welchen Weg bzw. über welches Medium verteilt werden. Diese Strategie ist in einem Krisenkommunikationsplan zu konkretisieren.

Bei der Entwicklung einer Krisenkommunikationsstrategie ist es hilfreich, die in der Krise relevanten Interessensgruppen, deren Bedürfnisse, Werte, Ziele und mögliches Interesse an den Informationen zu identifizieren. Als Ausgangsbasis kann die Analyse der Interessensgruppen, die bei der Initiierung des Notfallmanagements durchgeführt wurde, dienen. Neben den schon bekannten Interessensgruppen wie Anteilseigner, Investoren, Management, Mitarbeiter, Lieferanten und Kunden spielen für die

Krisenkommunikation weitere Interessensgruppen eine wichtige Rolle. Dazu zählen beispielsweise Familienmitglieder, Anwohner, nicht direkt betroffene Öffentlichkeit, Aufsichtsbehörden, politische Vertreter, Konkurrenten, Umweltverbände, Bürgerinitiativen, Protestgruppen und insbesondere die verschiedenen Medien. Die Gruppen können unterschieden werden in institutionsintern, direkt oder indirekt betroffene Externe und weitere Interessensgruppen (siehe Abbildung 12).

Abbildung 12: Zielgruppen Krisenkommunikation

Ziel der Analyse ist, die verschiedenen Interessen an Informationen über die Krise und Motive der Gruppen zu identifizieren und Strategien und Maßnahmen für den Umgang mit diesen Gruppen zu entwickeln. Es ist sinnvoll, dabei auch den Einfluss der verschiedenen Interessensgruppen und deren Möglichkeiten für Sanktionen (z. B. Protestaktionen, Boykott, rechtliche Schritte) sowie die daraus zu erwartenden Implikationen für die Institution in die Überlegungen mit einzubeziehen. Für die zielgruppenorientierte Aufbereitung von Informationen spielt auch der jeweilige Informations- und Wissensstand der jeweiligen Gruppe eine wichtige Rolle.

Grundsätze

Bei der externen Krisenkommunikation bzw. der Festlegung der Kommunikationsstrategie sollten einige Grundsätze beachtet werden:

- Jede größere Krise einer Institution wird früher oder später öffentlich. Daher ist es notwendig oder ratsam, die Öffentlichkeit rechtzeitig zu informieren. Der Kontakt zu den Medien sollte überlegt und frühzeitig erfolgen, um die Wahrnehmung der Krise und des Krisenmanagements in der Öffentlichkeit möglichst im eigenen Sinne beeinflussen zu können. Denn wer schweigt, hat unrecht.
- Auch wenn die Öffentlichkeit oder Externe nicht im vollen Umfang bzw. über alle Details informiert werden, so gilt für die Krisenkommunikation vor allem, dass die gemachten Aussagen wahr sein müssen.
- Es sollte eine Faktenkommunikation sein, doch bis zu einem bestimmten Maße auch Empathie und die innere Anteilnahme ausdrücken. Die Kommunikation muss der Situation angemessen sein.
- Mutmaßungen und Spekulationen sind zu vermeiden.
- Auch sollten negative Nachrichten nicht einfach verschwiegen werden, denn heutzutage lassen sich Nachrichten nur begrenzt verstecken. Halbwahrheiten, Verschwiegenes, kleinlaute oder erzwungene Rückzieher erzeugen Defensive.
- Die Kommunikation sollte die Ereignisse vereinfacht darstellen, ohne sie zu verfälschen, denn Unverständnis erzeugt Angst.

- Die Informationen für die Öffentlichkeit sollten so weit abstrahiert werden, dass keine Nachahmer animiert werden oder Konkurrenten Vorteile daraus ableiten könnten.

Informationswege

Es sollte eine zentrale Stelle eingerichtet werden, bei der in der Krise alle externen Anfragen gebündelt angenommen und nach Vorgaben beantwortet werden können, also z. B. eine zentrale Hotline. Diese Stelle kann durch die Organisationseinheit Unternehmens- bzw. Behörden-kommunikation, Öffentlichkeitsarbeit oder Pressestelle unterstützt werden. Sie sollte feste Telefon- und Fax-Rufnummern sowie E-Mail-Adressen haben, die in geeigneter Weise bekanntzugeben sind. Zu überlegen ist die Einrichtung einer kostenfreien telefonischen Krisen-Hotline. Je nach Branche und der Größe der Institution und der zu erwartenden Krisen kann es sinnvoll sein, einen spezialisierten, professionellen Anbieter (z. B. ein Call Center) zu beauftragen, um die Flut von Anfragen in einer Krisensituation zu bewältigen. Dieser Anbieter sollte jedoch bereits im Vorfeld ausgewählt, entsprechend vertraglich eingebunden und für Krisenkommunikation geschult werden. Auch für die Mitarbeiter sowie deren Angehörige sollte eine zentrale Anlaufstelle benannt sein, an der sie weitergehende Informationen erhalten. Wichtig für jegliche Anlaufstellen ist, bei allen Personen, die Informationen über die Vorfälle oder die Lage einholen wollen, deren Identität zu überprüfen.

Neben den Anlaufstellen, um Informationen abfragen zu können, sollten Wege vorbereitet werden, um Informationen über die Krise und deren Bewältigung pro-aktiv verbreiten zu können. Dazu zählen zum einen Internetseiten, aber auch Kontakte zu Journalisten oder Pressekonferenzen. Medienvertreter stehen in einem harten Wettbewerb. Es gilt, die beste Story zu veröffentlichen, die den menschlichen Faktor betont und Emotionen erzeugt. Daher sollte das Ziel sein, die Medienvertreter und den Ansturm vor Ort zu kanalisieren. Die Medienvertreter sollten schnellstmöglich informiert, ständig auf dem Laufenden gehalten und mit Informationen versorgt werden. Für den direkten Weg zu den Medien werden die Kontaktdaten benötigt, die im Vorfeld zu erheben und zu pflegen sind. Hilfreich ist es, ein Kontaktnetzwerk zu lokalen wie auch regionalen oder gar nationalen Medien aufzubauen und persönliche und belastbare Kontakte zu Journalisten und Fachmedien zu pflegen.

Eine breite Wirkung kann auch mit nutzerfreundlichen Online-Seiten erzielt werden. Vorbereitete und in der Krise angepasste und frei geschaltete Informationsseiten im Internet können beispielsweise über den aktuellen Status informieren. Um schnell reagieren zu können, sind die Kriseninformationsseiten, als sogenannte "Dark–Sites", für den Webserver der Institution im Vorfeld vorzubereiten, um in der Krise kein Fachpersonal für die Erstellung von Webseiten zu benötigen. Werden spezielle ziel-gruppen-orientierte Seiten beispielsweise im Intranet für Mitarbeiter oder im Internet für deren Ange-hörige oder Medien geschaltet, so ist sicherzustellen, dass der Zugriff nur autorisiert erfolgen kann.

Hilfsmittel und Technik

Um eine schnelle und angemessene Kommunikation sicherzustellen, sollten schon im Vorfeld Vorlagen, vorformulierte Ausführungen und Textfragmente für zu erwartende Situationen erstellt werden. Auch speziell vorbereitetes und ausgesuchtes Hintergrundmaterial kann nützlich sein, um es individuell und situationsangepasst in Pressemappen den Medien zukommen lassen zu können. Bei der Krisenkommunikation gilt: nie in die Defensive gehen.

Es werden für den Krisenfall geeignete, funktionierende Kommunikationsmittel benötigt. Diese, wie auch die Technik und die Räumlichkeiten für Pressekonferenzen, sind bei der Notfallvorsorge einzuplanen und vorzubereiten.

Ausführliche Informationen zu externer Krisenkommunikation insbesondere für Behörden sind in [BMIKK] zu finden.

7.4 Notfallhandbuch

Das Notfallhandbuch ist die Gesamtheit aller für die Notfallbewältigung benötigter (Teil-)Dokumente und fasst die benötigten Strukturen, Informationen sowie die erforderlichen Maßnahmen und Aktionen nach Eintritt eines Notfalles und zur Wiederaufnahme des Geschäfts zusammen. Es ist zusammen und

abgestimmt mit dem Notfallvorsorgekonzept im Vorfeld zu erstellen. Die wesentlichen Teile des Notfallhandbuchs sind der Plan für die Sofortmaßnahmen, der Krisenstabsleitfaden, der Krisenkommunikationsplan, die Geschäftsfortführungspläne und die Wiederanlaufpläne. Je nach Größe und Komplexität der Institution kann es sich dabei um ein oder mehrere Dokumente handeln. Eine kleine oder mittlere Institution kann alle im Notfall benötigten Informationen in einem Dokument zusammenfassen. Für größere Institutionen empfiehlt sich jedoch eine Aufteilung in mehrere Dokumente. Diese sind aufeinander abzustimmen, um Konflikte zu vermeiden und ein geordnetes Handeln verschiedener Gruppen in der Krise zu garantieren. Um eine Einheitlichkeit im Aufbau und bessere Handhabbarkeit zu gewährleisten, sollten für die verschiedenen Teildokumente des Notfallhandbuchs eine gemeinsame Dokumentenvorlage und –struktur erstellt werden.

Zweck eines Notfallhandbuches ist es, eine dokumentierte Vorgehensweise bzw. Hilfestellung bereitzustellen, mit deren Unterstützung eine Institution den Notfall oder die Krise bewältigen und ihre kritischen Geschäftsprozesse fortführen kann. Das Notfallhandbuch sollte so aufgebaut sein, dass es einfache und schnelle Handlungsanweisungen bietet.

Für den Aufbau eines Notfallhandbuchs bieten sich mehrere Möglichkeiten der Gliederung an:

- eine Gliederung nach Phasen, die den zeitlichen Ablauf der Notfallbewältigung widerspiegelt,
- eine Gliederung nach Verantwortungsebenen, -bereichen und / oder Rollen, die sich an den Aufgaben von Bearbeitern orientiert, oder
- eine Gliederung nach Prozessen, die auf die einzelnen Geschäftsprozesse oder Gruppen von Prozessen zielt.

Welche Gliederung und Modularisierung für eine Institution zweckmäßig ist, hängt von deren Größe und Struktur ab. Beliebige Mischformen sind möglich, doch sollten einige Grundprinzipien beachtet werden:

- Informationen, die sich häufig ändern, sollten an zentraler Stelle der Notfalldokumentation zusammengefasst werden, damit sich die Aktualisierung einfacher gestaltet.
- Ein modularer Aufbau sollte garantieren, dass die verantwortlichen Mitarbeiter schnell und gezielt den für sie relevanten Teil finden bzw. dieser Teil ihnen gezielt ausgehändigt werden kann.
- Es ist darauf zu achten, dass die Notfalldokumentation aktuell und präzise gefasst ist, damit im Notfall die notwendigen Maßnahmen schnell abgearbeitet werden können und keine wichtige Aufgabe in der Stress-Situation eines Notfalls vergessen wird.

Ein Beispiel für ein Inhaltsverzeichnis für ein Notfallhandbuch ist in Anhang C zu finden. Dabei ist jedoch zu beachten, dass ein Notfallplan speziell auf die jeweilige Institution, deren Organisationsstruktur und Anforderungen bezüglich Geschäftsfortführung abgestimmt sein sollte und daher keine allgemein gültige Vorlage existieren kann. Das Beispiel ist ausschließlich als Anregung zu verstehen.

7.4.1 Sofortmaßnahmenplan

Als erste Schritte bei der Notfall- und Krisenbewältigung sind die Sicherheit und Unversehrtheit von Personen zu gewährleisten. Daher sind alle Sofortmaßnahmen wie Bergen, Retten oder Evakuieren von Personen in einem entsprechenden Plan zusammenzufassen.

7.4.2 Krisenstabsleitfaden

Im Krisenstabsleitfaden, manchmal auch als Krisenmanagementleitfaden oder Krisenmanagementhandbuch bezeichnet, sind Zielsetzungen, Grundsätze und Rahmenbedingungen für das strategische und taktische Handeln in Krisen jeglicher Art festgelegt. Der Krisenstabsleitfaden deckt überwiegend die Krisenfälle ab, für die auf Grund ihrer Einmaligkeit oder Unvorhersehbarkeit keine Aktionspläne vorliegen. Dazu zählen insbesondere die Krisen, welche nicht aus Schadensereignissen resultieren und die Geschäftsfortführung nicht beeinträchtigen. Zielgruppe ist daher der Krisenstab des unternehmens-

bzw. behördenweiten Krisenmanagements. Aus diesem Grunde sollte dieser Teilplan im Rahmen des institutionsweiten Krisenmanagements entwickelt werden oder zumindest mit diesem abgestimmt werden.

Für den Bereich des Notfall- und Krisenbewältigung, wie es im vorliegenden Dokument beschrieben ist, bietet der Krisenstabsleitfaden unter anderem Entscheidungshilfen zur Beurteilung der Lage und zur Auswahl von geeigneten Unterplänen und Optionen zur Geschäftsfortführung. Dabei gilt es, die Belange der verschiedenen Interessensgruppen zu wahren. Der Krisenstabsleitfaden beinhaltet weiter grundlegende Informationen zur Aufbauorganisation (Rollen, Aufgaben und Rechte), der Ablauforganisation sowie der Ansprechpartner mit Kontaktinformationen insbesondere der Personen und Firmen, die von zentraler Bedeutung bei der Krisenbewältigung sind.

7.4.3 Krisenkommunikationsplan

Im Krisenkommunikationsplan ist geregelt, wie die interne und externe Kommunikation in einer Krise (siehe Kapitel 7.3) erfolgen soll. Dazu zählen die Kommunikation mit den Mitarbeitern und deren Angehörigen, mit den wichtigsten Interessensgruppen und vor allem mit der Öffentlichkeit und den Medien. Im Krisenkommunikationsplan ist unter anderem festgelegt, wer welche Informationen an wen weitergeben darf und in welcher Art und Weise. Der Krisenkommunikationsplan kann auch als ein Bestandteil in den Krisenstabsleitfaden aufgenommen werden.

7.4.4 Geschäftsfortführungspläne

Die Geschäftsfortführungspläne fassen die Reaktionen der Institution auf eine Geschäftsunterbrechung nach einem Schadensfall auf der Prozessebene zusammen. Sie dienen dazu, die Situation zu analysieren und geeignete Strategien zur schnellen Wiederaufnahme der kritischen Geschäftsprozesse zu entwickeln. Es hat sich bewährt, für jede logische Organisationseinheit einen Geschäftsfortführungsplan zu entwickeln. Zweck der Geschäftsfortführungspläne ist die Bereitstellung einer dokumentierten Vorgehensweise, mit deren Hilfe die kritischen Geschäftsprozesse innerhalb der festgelegten Wiederanlaufzeiten fortgesetzt werden können. Sie enthalten die Beschreibung des Notbetriebs, ob an der ursprünglichen oder der Ausweich-Lokation, im Standardablauf oder als Alternativprozess mit reduzierter Kapazität.

Die Geschäftsfortführungspläne der einzelnen Organisationseinheiten sind zu konsolidieren und zeitlich, personell und inhaltlich aufeinander abzustimmen. Sie bilden zusammen einen Gesamt-Geschäftsfortführungsplan.

Ein Geschäftsfortführungsplan sollte mindestens folgende Punkte beinhalten:

- den Geltungsbereich,
- eine Darstellung der Kontinuitätsstrategien und Optionen für die Prozesse für verschiedene Schadensszenarien,
- eine Auflistung der Zuständigkeiten,
- Auflistung der Notfallteams mit den Kontaktinformationen,
- Kriterien für die Aktivierung und Deaktivierung des Plans,
- die Alarmierung und Eskalation dieser Teams,
- die Wiederanlauf-Anforderungen für die Geschäftsprozesse im Überblick,
- die Priorisierung der Prozesse und
- Anweisungen für die Koordinierung der Nacharbeiten.

Für die einzelnen Prozesse sollte der Geschäftsfortführungsplan mindestens folgende Informationen enthalten:

- Maßnahmen zur schnellen Aktivierung der Geschäftsfortführung,

- Prozessbeschreibungen für den Notbetrieb oder die verschiedenen Alternativen (z. B. Aufsetzen auf hausinterne Ausweichressourcen, Aufnahme eines Alternativprozesses), inklusive der gegebenenfalls erforderlichen Hilfsmittel,
- Rollenbeschreibungen,
- Maßnahmen für die Rückführung in den Normalzustand und
- Maßnahmen für die Nacharbeiten.

Die Geschäftsprozesse sind entsprechend der festgelegten Prioritäten sortiert aufzulisten. Die in den Plänen beschriebenen Verfahren und Maßnahmen sollten die während der BIA definierten Leistungsanforderungen für die Fortführung der kritischen Geschäftprozesse gewährleisten können.

Ein Beispiel für ein Inhaltsverzeichnis für einen Geschäftsfortführungsplan ist in Anhang D zu finden.

7.4.5 Wiederanlaufpläne

Die Wiederanlaufpläne enthalten die spezifische Handlungsanweisungen und notwendigen Informationen für die Wiederherstellung und den Wiederanlauf von Ressourcen. Sie ergänzen somit die Geschäftsfortführungspläne und dienen als Arbeitsgrundlage für die entsprechenden Notfallteams.

Die Wiederanlaufpläne enthalten sowohl Informationen für einzelne Ressourcen, aber auch übergreifende Pläne, die den Ausfall mehrerer Systeme gleichzeitig abdeckt. Beispiel dafür ist der Ausfall eines Rechenzentrums. Der entsprechende übergreifende Wiederanlaufplan enthält den Schwenk auf ein Ausweichrechenzentrum und dessen Inbetriebnahme.

Die Wiederanlaufpläne sollten auch einen Überblick über die Priorisierung der Ressourcen und damit die Reihenfolge für den Wiederanlauf enthalten. Für die einzelnen Ressourcen sollten unter anderem folgende Informationen festgehalten werden:

- die Kritikalität,
- Wiederanlaufzeit und gegebenenfalls besondere Termine,
- die Schnittstellen und abhängige Ressourcen,
- eine Kurzbeschreibung,
- die Maßnahmen zur Fehlerbehebung, den Wiederanlauf, die Wiederherstellung, den Notbetrieb und die Rückführung in den Normalbetrieb und
- die Ansprechpartner, also z. B. Fachverantwortliche für Geschäftsprozesse.

8 Tests und Übungen

Um die Angemessenheit, Effizienz und Aktualität der Notfallvorsorgeplanung und der Notfall- und Krisenbewältigung sicherzustellen, sind die Vorsorgemaßnahmen, die organisatorischen Strukturen und die unterschiedlichen Pläne regelmäßig in Tests und Übungen zu überprüfen.

Tests und Übungen verifizieren die dem Konzept zugrunde gelegten Annahmen. Einzelne Maßnahmen oder Maßnahmenbündel werden auf korrekte Umsetzung geprüft und die Technik auf ihre Funktionsfähigkeit hin getestet. Übungen zeigen auch, ob die Notfalldokumentation brauchbar ist und die Beteiligten die ihnen zugedachten Aufgaben in einem Notfall auch wahrnehmen können.

Übungen trainieren die in den Plänen beschriebenen Abläufe, schaffen routinierte Handlungsabläufe und verifizieren die effiziente Funktionalität der Lösungen. Sie verbessern die Reaktionsfähigkeit sowie die Handlungssicherheit der Mitarbeiter. Da Menschen in Krisensituation und dem damit verbundenen Stress dazu neigen, unüberlegt, überhastet und vor allen falsch und irrational zu reagieren, sollten die zuletzt genannten Ziele von Übungen nicht unterschätzt werden.

Tests und Übungen sind mit Aufwand und Kosten verbunden. Um die Investitionen in Tests und Übungen zielgerichtet einzusetzen, ist eine sinnvolle Planung erforderlich. Daher sollte ein Übungskonzept, ein Übungsplan sowie ein Übungskonzept erstellt werden. Die Planung sollte unterschiedliche Test- und Übungsarten berücksichtigen. Einige Beispiele sind im folgenden Unterkapitel beschrieben. Die Wahl der Test- und Übungsarten hängt von der Art und der Größe der Institution sowie der vorhandenen Umgebung ab und ist individuell zu entscheiden.

8.1 Test- und Übungsarten

Im Folgenden werden einige Test- und Übungsarten aufgezeigt. Diese reichen von der einfachen Überprüfung von Einzelmaßnahmen bis hin zur komplexen Ernstfallübung. Einfache Überprüfungen werden in diesem Dokument oftmals Tests genannt, komplexere Überprüfungen, denen ein Szenario hinterlegt ist, Übungen. Eine scharfe Trennung der Begriffe ist jedoch nicht möglich. Viele Aussagen gelten für beide Arten von Überprüfungen.

Test der technischen Vorsorgemaßnahmen

Um die Angemessenheit und die Funktionsfähigkeit der technischen Lösungen sicherzustellen, müssen diese getestet werden. Hierzu zählen beispielsweise Tests von redundant ausgelegten Leitungen, der Stromversorgung, der Wiederherstellung von Datensicherungen, der Ausfallsicherheit von Clustern, der eingesetzten Meldetechnik, der technischen Infrastruktur oder einzelner IT-Komponenten. Einzelne Komponenten und ihre Funktion sollten regelmäßig sowie anlassbezogen bei größeren Veränderungen der Systeme oder der jeweiligen Systemumgebung getestet werden, um das Zusammenspiel zu überprüfen.

Funktionstest

Mit dieser Übungsart werden die Prozeduren, Teilprozesse und Systemgruppen auf ihre Funktionalität überprüft, die in den verschiedenen Teilplänen des Notfallhandbuchs festgelegt sind. Dabei werden zum einen Abläufe, aber vor allem auch das Zusammenspiel und die Abhängigkeiten verschiedener Komponenten oder Maßnahmen überprüft. Dazu zählen Wiederanlaufpläne, Wiederherstellungspläne, wie auch die Notfallpläne für die Sofortmaßnahmen (z. B. zur Evakuierung der Belegschaft bei Feueralarm).

Plan-Review

Ziel von Plan-Reviews ist, die einzelnen Pläne der Notfall- und Krisenbewältigung zu überprüfen. Die Teilnehmer gehen bei dieser Testart die Pläne theoretisch durch und überprüfen die Plausibilität der Inhalte und der getroffenen Annahmen. Die Funktionsfähigkeit der beschriebenen Inhalte wird dabei augenscheinlich bewertet.

Planbesprechung

Die Planbesprechung wird dazu verwendet, am „grünen Tisch“ – daher auch der Name „Table Top Exercise“ – Probleme und Szenarien durchzudenken. In dieser Übungsart wird ein Szenario vorgegeben und theoretisch durchgespielt. Diese Testart ist noch relativ einfach umzusetzen und dient einer ersten Validierung. Unstimmigkeiten und Missverständnisse können so aufgedeckt werden, bevor ein kostenintensiver operativer Aufwand betrieben wird. Während der Etablierungsphase des Notfallmanagements sollte diese Überprüfungsart häufiger wiederholt werden.

Stabsübungen

Eine besondere Form von Planbesprechung sind die sogenannten Stabsübungen. Dabei wird die Zusammenarbeit im Krisenstab geübt.

Stabsrahmenübungen

Eine weitere Form der Planbesprechung sind die Stabsrahmenübungen. Sie stellen eine erweiterte Form der Stabsübung dar. Sie dienen dazu, neben der Zusammenarbeit im Krisenstab auch die Zusammenarbeit zwischen dem Krisenstab und den operativen Teams zu überprüfen und zu üben. In der Regel werden die stabsnahen Strukturen praktisch geübt, während die operative Umsetzung theoretisch simuliert wird.

Kommunikations- und Alarmierungsübung

Ein neuralgischer Punkt der Notfall- und Krisenbewältigung ist die Meldung und Alarmierung des Krisenstabs und weiterer Verantwortlicher. Daher sind die Verfahren zur Meldung, Eskalation und Alarmierung regelmäßig zu überprüfen. Dieser Test umfasst einfache Überprüfungen der Kommunikationsmittel bis hin zum Zusammentreten des Krisenstabs im Krisenstabsraum. Es werden dabei die in den Plänen hinterlegten Zuständigkeiten und Rufnummern wie auch die Verfahren, die Eskalationsstrategie, die Erreichbarkeiten und die Stellvertreterregelungen getestet. Es wird überprüft, ob die vorliegenden Pläne aktuell, verständlich und handhabbar, die Verfahren praktikabel und die zu nutzende Technologien (z. B. Alarmierungssystem, Notfall-Telefon, SMS, Pager, Internet, Funk- oder Satellitenkommunikationsgeräte) funktionsbereit, effektiv und angemessen sind.

Simulation von Szenarien

Durch eine realitätsnahe Simulation werden die festgelegten Prozeduren und Maßnahmen für die Bewältigung von Notfallszenarien oder -ereignissen auf ihre Zweckmäßigkeit, Angemessenheit und Funktionalität getestet. Dabei werden sowohl die Alarmierung und Eskalation, die Notfallbewältigungsorganisation, die Arbeit des Krisenstabs und die Zusammenarbeit aller beteiligten Stellen erprobt. Solche Übungen könnten als Funktions- oder Bereichsübungen und in einer weiteren Stufe bereichsübergreifend organisiert werden.

Ernstfall- oder Vollübung

Die aufwendigste Art einer Simulation ist die Ernstfall- oder Vollübung. Je nach Szenario sind dabei auch Externe, wie beispielsweise die Feuerwehr, Hilfsorganisationen, Behörden etc., einzubeziehen. Diese Übungsart kann und sollte erst in einem fortgeschrittenen Stadium durchgeführt werden.

Die Vollübung orientiert sich an der Wirklichkeit und bezieht alle Hierarchieebenen vom Management bis zum einzelnen Mitarbeiter mit ein. Der Vorbereitungs-, Durchführungs- und Nachbereitungsaufwand ist nicht zu unterschätzen. Dennoch sollte bei hohen Anforderungen der Institution an das Notfallmanagement nicht darauf verzichtet werden. Auch Ernstfallübungen sollten regelmäßig in größeren zeitlichen Abständen durchgeführt werden.

Vergleich der Übungsarten

Die Tests und Übungen können nach verschiedenen Kriterien unterschieden werden: nach Ablaufart oder nach Zielgruppe, nach Umfang oder Aufwand. Der Ablauf kann diskussionsbasiert oder

handlungsorientiert sein. Bei den Zielgruppen können die drei Verantwortungsbereiche strategisch, taktisch und operativ unterschieden werden. Übungen auf der taktischen Ebene überprüfen die Koordinierung, die Zusammenarbeit der einzelnen Bereiche und die Abläufe bei der Lageerfassung und –bewertung. Auf der operativen Ebene stehen die Abläufe und die konkreten Arbeiten zur Behebung des Notfalls im Fokus (siehe Tabelle 18).

Übungsart	Zielgruppe			Ablauf		Aufwand/ Umfang
	strategisch	taktisch	operativ	diskussions-basiert	handlungs-orientiert	niedrig/-mittel/ hoch/ sehr hoch
Test der technischen Vorsorgemaßnahmen			X		X	niedrig
Funktionstest			X		X	mittel
Plan-Review		x	x	X		niedrig
Planbesprechung		X	x	X		niedrig-mittel
Stabsübung	x	X		X		niedrig-mittel
Stabsrahmenübung	x	X	x	X	x	mittel-hoch
Kommunikations- und Alarmierungsübung		x	X		X	niedrig
Simulation von Szenarien		X	X		X	hoch
Ernstfall- oder Vollübung	X	X	X		X	sehr hoch

Tabelle 18: Übungsarten

8.2 Dokumente

Für die Planung und Durchführung von Übungen und Tests ist es hilfreich, verschiedene Arten von Dokumenten anzulegen: das Übungskonzept, den Übungsplan, das Übungskonzept und das Übungsprotokoll.

8.2.1 Übungshandbuch

Für alle Tests und Übungen des Notfallmanagements in einer Institution sollte gelten, dass sie geplant und vorbereitet ablaufen. Daher und um Störungen des Wirkbetriebs so gering wie möglich zu halten, sind zusammen mit der Institutionsleitung strategische Entscheidungen, grundsätzliche Festlegungen, Rahmenbedingungen und Vereinbarungen für alle durchzuführenden Tests und Übungen zu treffen. Diese werden im Übungshandbuch zusammengefasst und bilden die Grundlage für die generelle Übungsplanung und die Planung der einzelnen Übungen.

Das Übungshandbuch sollte unter anderem folgende Fragen beantworten:

- Welche strategische Bedeutung haben die Notfalltests und –übungen für die Institution?
- Was sind die Ziele, die mit der Durchführung von Tests und Übungen erreicht werden sollen?
- Welchen Stellenwert haben die Tests und Übungen?
- Welche Arten von Tests werden in der Institution unterschieden? Welcher Aufwand und welche groben Kosten sind mit den einzelnen Arten verbunden?
- Was sind die Ziele der einzelnen Übungsarten in der Institution?
- Wie viele Tests und Übungen sollten durchgeführt werden? Existieren gesetzliche oder aufsichtsrechtliche Vorgaben bezüglich der Häufigkeit?
- Welche Rollen werden bei der Planung und Durchführung von Tests und Übungen unterschieden? Welche Aufgaben, Rechte und Verantwortlichkeiten haben diese?

- Welche Bereiche sollen getestet werden: Kenntnisse und Fähigkeiten der Beteiligten und Mitarbeiter, Abläufe des Notfallmanagements, Mechanismen und eingesetzte Technologien, Notfalldokumentation, Einsatzbereitschaft zentraler Ressourcen, Maßnahmenpläne etc.?
- Welche Methoden von Übungen werden eingesetzt (z. B. angekündigt, nicht angekündigt)?
- Wie ist für die Durchführung von Übungen die Schnittstelle zum operativen Tagesgeschäft festzulegen? Welcher Grad der Beeinflussung des Tagesgeschäfts durch die Übung ist erlaubt, sofern dieser nicht garantiert auszuschließen ist?
- Wie sind die Tests und Übungen zu dokumentieren? Mit welcher Detailgenauigkeit?
- Wie ist die Auswertung der Übungsergebnisse durchzuführen?

Das Übungshandbuch umfasst neben den strategischen Grundsätzen auch Hilfsmittel, welche für die Feinplanung, die Durchführung und die Nachbereitung von Übungen und Tests hilfreich sind. Dazu zählen beispielsweise Dokumentenvorlagen für Einladungsschreiben, Ankündigungen, Protokolle oder Auswertefragebögen, die für konkrete Übungen ausgefüllt oder angepasst werden müssen.

8.2.2 Übungsplan

Es ist sinnvoll, nicht nur die jeweils nächste durchzuführende Übung zu betrachten, sondern eine aufeinander abgestimmte Reihe von Tests und Übungen zu planen, die in der Gesamtheit alle Bereiche der Institution sowie aller Teile der Notfallpläne, die zu beüben sind, abdeckt. In der Übungsplanung werden daher für einen Planungszeitraum über wenige Jahre die Termine, die Reihenfolge und die groben Eckdaten der geplanten Tests und Übungen festgelegt. Dabei sollten alle Test- und Übungsarten von einfachen Systemtests bis mindestens zur Simulation von Szenarien eingeplant werden. Es ist nicht ausreichend, ausschließlich einzelne Notfallvorsorgemaßnahmen im Rahmen des Changemanagements zu testen.

Bei der Terminfestlegung für Tests und Übungen sind Randbedingungen wie beispielsweise Urlaubszeiten, in denen Mitarbeiter nicht zur Verfügung stehen, oder besondere Termine für die Institution und Geschäftsprozesse zu beachten. Für die Reihenfolge der Tests und Übungen hat sich bewährt, diese vom Einfachen zum Komplexen zu steigern. Tests ohne großen Vorbereitungsaufwand sollten häufiger durchgeführt werden. Die Häufigkeit und der Umfang der Übungen sollten sich an der Gefährdungslage der jeweiligen Organisationseinheiten orientieren. Eine risikoorientierte Vorgehensweise ist zu empfehlen. Je kritischer ein Prozess oder System für die Geschäftsfortführung ist, desto häufiger sollten die Notfallvorsorgemaßnahmen und Pläne getestet werden.

Für Tests und einfache Übungen hat sich ein jährlicher Rhythmus bewährt. So sollte pro Jahr mindestens eine Übung, wie beispielsweise eine Gebäuderäumung, durchgeführt werden. Institutionen mit hohen Verfügbarkeitsanforderungen an Geschäftsprozesse sollten umfangreiche Ernstfallübungen, wie den Bezug eines Ausweichstandortes und Funktionstests der Notfallarbeitsplätze, mindestens alle 2 bis 3 Jahre durchführen. Je nach Branche der Institution sind dabei gesetzliche oder aufsichtsrechtliche Vorgaben zur Durchführung, Art oder Anzahl von Übungen zu beachten.

Im Übungsplan wird für jeden Test und jede Übung das geplante Szenario, die Übungsart, der Zweck und das verfolgte Ziel, ob angekündigt oder nicht-angekündigt sowie die geplanten Teilnehmer (Rollen), der Zeitpunkt und die voraussichtliche Dauer der jeweiligen Übungen festgelegt. Auch sollte eine grobe Abschätzung der benötigten personellen, materiellen und finanziellen Ressourcen erfolgen.

Der Plan sollte sowohl mit der Personalvertretung wie auch mit der Institutionsleitung abgestimmt und von dieser freigegeben werden.

8.2.3 Test- und Übungskonzept

Für jeden einzelnen Test und jede Übung ist ein separates Test- bzw. Übungskonzept zu erarbeiten. Dieses beinhaltet die Detailplanung für die Durchführung. Ein Testkonzept beschreibt mit welcher Methode ein System zu prüfen ist, welche Tools zur Anwendung kommen und welche Randbedingungen vorgegeben sind. Ein Übungskonzept beschreibt unter anderem den Teilnehmerkreis, die

jeweilige Rolle der einzelnen Teilnehmer in der Übung, den zeitlichen Rahmen und die Kriterien für den Abbruch der Übung. Es enthält somit mindestens folgende Angaben:

- Name der Übung,
- Datum, Zeit und geplante Dauer,
- Ort der Übung,
- Art der Übung,
- Ziele,
- Übungsleitung,
- Teilnehmer, Übungsbeobachter, Protokollführer,
- Einweisung (das sogenannte Briefing) der Teilnehmer und
- das Szenario.

Die Erstellung eines Übungskonzepts sollte zweistufig erfolgen. Zuerst wird ein Grobkonzept erstellt, das der Leitungsebene zur Genehmigung vorgelegt wird. Erst anschließend wird die Feinkonzeption durchgeführt. Bei länger andauernden Großübungen wie Ernst- und Vollübungen sollte dabei auf weitere Punkte geachtet werden. Dazu zählen beispielsweise Sicherheitsvorkehrungen für die Beteiligten während der Übung oder die Verpflegung.

Übungsdrehbuch

Bei einem umfangreicheren Übungsszenario ist ein Übungsdrehbuch zu erstellen. In diesem werden die Ausgangslage, der konkrete zeitliche Ablauf der Übung, die vordefinierten Ereignisse und deren Ablaufreihenfolge so detailliert wie möglich beschrieben. Es ist auch festzulegen, wie und durch wen die jeweilige Information an die Teilnehmer übermittelt wird. Das Drehbuch unterstützt die Moderatoren der Übung bei der Gestaltung des Übungsablaufs.

Bei der Entwicklung eines Übungsdrehbuches wird als Methode meist die Szenariotechnik eingesetzt. Dabei werden ausgehend von einem möglichen Schadensereignis die realistischen Entwicklungsmöglichkeiten der Situation für die Institution aufgezeigt. Um Gewöhnungseffekte zu vermeiden und die Teilnehmer immer wieder neu zu motivieren, sollte jedes Übungsszenario und damit die Übung individuell gestaltet werden.

Die Ausgangslage wird in der sogenannten „Blauen Lage“ dokumentiert. Diese dient dazu, die Übungsteilnehmer zu Beginn der Übung über die aktuelle Situation zu informieren. Sie beinhaltet eine Beschreibung der Normalsituation, den Eintritt eines Schadensereignisses, alle benötigten Informationen zur aktuellen Lage und endet mit dem „Auftrag“, der der realen Alarmierung entspricht. Die Bezeichnung "Blaue Lage" geht darauf zurück, dass typischerweise alle schriftlichen Informationen zur Übungsausgangslage auf blaues Papier gedruckt werden, damit sie nicht mit anderen Dokumenten verwechselt werden können.

Eine Darstellungsmöglichkeit für ein Übungsdrehbuch ist eine Tabelle. In dieser können neben einer laufenden Nummer für eine Einzelaktivität (auch Einlagen genannt), der Zeitpunkt, eine Kurzbeschreibung des Ereignisses, das Testziel bzw. die erwartete Reaktion, die Akteure und verwendete Hilfsmittel oder Werkzeuge festgehalten werden (siehe Tabelle 19).

Übung: XYZ											
Nr.	Real-Zeit	Szenario-Zeit	Stichwort	Aktivität	Ziel/ erwartete Reaktion	Ein-spielender	Akteure				Hilfsmittel/ Werkzeug/ Art der Einspielung
							A	B	C	…	
1	…		…		…		…	…	…	…	…
2	10:10		Meldung an LZ	*(Beschreibung der Einlage mit Hintergrundin-formationen)*	Überprüfung der Meldung, Eskalation	Hr. Jansen		X	X		Handy
3	…		…	…	…		…	…	…	…	…

Tabelle 19: Beispiel Übungsdrehbuch

8.2.4 Test- und Übungsprotokoll

Die Durchführung und der Ablauf von Tests und Übungen sind in sogenannten Test- bzw. Übungsprotokollen sorgsam zu dokumentieren. Darin wird festgehalten, welcher Ablaufplan zugrunde liegt, wie die Vorgehensweise der Teilnehmer bei der Durchführung war, mit welchen Methoden gearbeitet wurde, welche Werkzeuge mit welcher Konfiguration genutzt und welche Resultate erzielt wurden. Insbesondere sollten aufgetretene Probleme oder Abweichungen vom Test- bzw. Übungsablaufplan oder den erwarteten Ziele festgehalten werden. Das Test- bzw. Übungsprotokoll bildet die Grundlage für die an den Test oder Übung anschließende Auswertung, der Ermittlung der Schwachstellen und Verbesserungsvorschläge.

8.3 Durchführung von Tests und Übungen

8.3.1 Grundsätze

Bei der Durchführung von Tests und Übungen sind einige Grundsätze zu beachten. So sollten sie unter anderem den normalen Betriebsablauf nicht oder so wenig wie möglich stören. Bei der Wahl eines Durchführungszeitpunkts sollte daher berücksichtigt werden, dass ein Test oder eine Übung direkten Einfluss auf den operativen Betrieb haben könnte. Zu testende Systeme stehen gegebenenfalls während eines Tests nicht oder nur mit verringerter Leistung für den Produktivbetrieb zur Verfügung. Aus diesem Grunde ist es meist empfehlenswert, Tests und Übungen nach Möglichkeit außerhalb der regulären Geschäftszeit durchzuführen, um den Einfluss auf den laufenden Geschäftsbetrieb möglichst zu minimieren.

Die in die Übung einbezogenen Mitarbeiter müssen während der Übungsphase ihr Tagesgeschäft ruhen lassen. Geleistete Arbeitsstunden müssen dem Arbeitszeitkonto gutgeschrieben werden. Werden Tests und Übungen außerhalb der regulären Arbeitszeiten durchgeführt, so sind entsprechende Vereinbarungen mit der Personalvertretung zu treffen.

Es sind Maßnahmen zu planen, die sicherstellen, dass der Übungsablauf unter Kontrolle der Durchführenden bleibt und selbst keine Störungen hervorruft. Für unerwartete Störungen durch die Übung sind Abbruchkriterien festzulegen, sowie Fallback-Lösungen zur schnellstmöglichen Rückkehr in den normalen Geschäftsbetrieb zu planen. Ein Abbruchkriterium für eine Übung kann beispielsweise das Überschreiten einer Zeitspanne sein oder die Erkenntnis, dass die umgesetzten Maßnahmen nicht den erwarteten Erfolg bringen.

8.3.2 Rollen

Sowohl bei der Planung, der Vorbereitung wie auch bei der Durchführung von Übungen fallen umfangreiche Arbeiten an. Daher sind die Rollen für die Übungsvorbereitung und –durchführung mit ihren Aufgaben und Rechten festzulegen.

Übungsautor

Für die Vorbereitung von Übungen sollte ein Übungsautor benannt werden. Seine Aufgabe umfasst sowohl die Entwicklung des Übungsplans als auch die Konzeption der einzelnen Übungen von der Festlegung des Szenarios und der Auswahl der Teilnehmer bis hin zur Vorbereitung der Umgebung für die Übungsdurchführung. Diese Aufgaben sollten nicht unterschätzt werden und erfordern je nach Übungsart weniger oder mehr Aufwand. Der Übungsautor sollte mit dem Notfallvorsorgekonzept wie auch mit den einzelnen Notfall-, Wiederanlauf- und Wiederherstellungsplänen gut vertraut sein. Diese Rolle kann auch in Personalunion durch den Notfallbeauftragten oder den Leiter des Krisenstabs wahrgenommen werden.

Vorbereitungsteam

Für die Erstellung und Ausarbeitung von Übungskonzepten und Übungsdrehbücher benötigt der Übungsautor die Mithilfe durch ein Vorbereitungsteam. Zum Vorbereitungsteam können Leiter von Organisationseinheiten oder Prozessverantwortliche gehören, welche ihr Fachwissen mit einbringen.

Übungsleiter / Moderator

Die zentrale Rolle bei der Durchführung einer Übung ist die des Übungsleiters oder Moderators. Zu seinen Aufgaben gehört es unter anderem, die Übung zu eröffnen, die Einlagen zu koordinieren, Entscheidungen über Alternativen oder Abweichungen von der Planung zu treffen und die Übung offiziell als beendet zu erklären.

Kernteam

Der Übungsleiter wird durch die Rahmenleitungsgruppe unterstützt. Ihre Aufgaben umfassen die fachliche Beratung, die Beantwortung von Anfragen von Übungsteilnehmern oder das Einspielen von Einlagen zur Lagedarstellung in die Übungsszene. Ergänzend dazu gehören ein oder mehrere Protokollanten, der Übungsautor, der Notfallbeauftragte und gegebenenfalls Beobachter zum Kernteam.

Protokollant

Ein Protokollant hat die wichtige Aufgabe, den Ablauf der Übung detailliert zu erfassen. Je nach Umfang der Übung, Anzahl der Lokationen, vertretene Interessensgruppen und anderen Faktoren können auch mehrere Protokollanten notwendig sein, die teilweise aus unterschiedlicher Perspektive die Situation erfassen und schriftlich festhalten.

Beobachter

Neben den Protokollanten können zusätzliche Beobachter zugelassen werden. Zu den Beobachtern können beispielsweise Mitglieder der Internen Revision zählen, aber auch Mitarbeiter aus anderen Bereichen, externe Experten oder Vertreter von Behörden oder Hilfsorganisationen. Sie verhalten sich während der Übungsdurchführung neutral und greifen nicht in das Geschehen ein. Doch sollte auch diese Gruppe in die Auswertung der Übung einbezogen werden, indem deren Beobachtungen und Einschätzungen eingeholt werden.

Akteure

Zu der Gruppe der Akteure können Prozessverantwortliche, Verantwortliche von Organisationseinheiten, Vertreter der Mitarbeiter und des Managements, aber auch Kunden, Dienstleister, Zulieferer oder andere Externe zählen. Solange sich das Notfallmanagement noch im Aufbau befindet, sollte von der Einbindung Externer jedoch abgesehen werden.

8.3.3 Ablauf

Die Durchführung einer Übung kann grundsätzlich in vier Phasen untergliedert werden:

Planung und Freigabe

Die Durchführung eines Tests und einer Übung ist wie ein Projekt zu planen. Dazu gehören die Zeit- und die Personalplanung für die gesamte Dauer von der Konzeption der Übung bis zur Nacharbeit. Es werden das Szenario ausgearbeitet und die bei der Durchführung der Übung benötigten Dokumente erstellt.

Das Übungskonzept ist von der Leitung der Institution zu genehmigen und freizugeben. Das kann nach der Planung erfolgen, doch kann es sinnvoll sein, schon einen groben Zwischenentwurf des Übungskonzepts genehmigen zu lassen, um aufwendige Fehlplanungen zu vermeiden.

Vorbereitung

In der direkten Vorbereitungsphase werden die Voraussetzungen für die Übung geschaffen. Dazu gehören beispielsweise die Einrichtung der Umgebung und eventuell notwendige Vorsichts- oder Sicherheitsmaßnahmen wie eine zusätzliche Datensicherung, Bereitstellung von Ersatzsystemen oder das Informieren von Rettungsdiensten, Behörden oder der lokalen Presse, um Fehlalarme durch Missverständnisse zu vermeiden. Es gilt grundsätzlich, dass die Ressourcen für die Übungen gemäß den Wiederanlaufplänen bereitzustellen sind.

Je nach Kenntnisstand der Teilnehmer empfiehlt es sich, diese allgemein über die Durchführung von Übungen, den Sinn, die Maßnahmen und den Ablauf zu informieren. Zeitnah zur eigentlichen Übung erfolgt die Einsatzbesprechung, auch Briefing genannt. Dabei werden unter anderem die aktuellen Rollen erläutert, der Zeitplan vorgestellt und die Ansprechpartner und Telefonlisten bekanntgegeben. Je nach Übungsart und Übungsziel sind nicht alle Beteiligten vollständig zu informieren. Wer wann welche Informationen über den Ablauf im Vorfeld erhalten soll, ist bei der Planung der Übung festzulegen.

Durchführung

Eine Übung wird zu einem vordefinierten Zeitpunkt durch den Übungsleiter gestartet. Dieser koordiniert den Ablauf und entscheidet, ob und wie von der Planung abgewichen werden kann.

Die Akteure sollten durch den Übungsleiter angeleitet werden, um ein Abdriften ins Chaos zu verhindern, jedoch ohne deren kreatives Handeln zu sehr zu behindern. Um den Fortschritt der Übungen am Laufen zu halten, werden die im Übungsdrehbuch festgehaltenen Aktivitäten durch die entsprechenden Akteure eingespielt.

Der oder die benannten Protokollanten führen das Übungsprotokoll. Im Protokoll sollte der Übungsablauf, die erreichten Ziele sowie Schwierigkeiten bei der Bewältigung von Übungsaktivitäten durch die Übungsteilnehmer festgehalten werden. Der Eintrag sollte die Beobachtung, Datum und Uhrzeit der Anmerkungen sowie den Namen des Beobachters enthalten. Das Übungsprotokoll ist Basis der später durchzuführenden Auswertung der Übung. Das Protokoll dient weiterhin als Nachweis für durchgeführte Übungen für interne oder externe Revisionsprüfungen.

Jede Übung sollte offiziell durch den Übungsleiter beendet werden. Die eventuell für die Übung geschaffene Übungsumgebung ist anschließend in den Normalzustand zurückzuversetzen. Bei verteilt durchgeführten Übungen sind die angefallenen Unterlagen und Protokolle zentral zu sammeln.

Nach dem Ende der Übung sollte mit allen Teilnehmern eine kurze Abschlussbesprechung durchgeführt werden. Inhalt der Abschlussbesprechung ist die Zusammenfassung der Übungsabläufe und gegebenenfalls eine Vorab-Bewertung.

Nachbereitung

Die Auswertung der Übung sollte in einem vordefinierten Teilnehmerkreis stattfinden. Während der Auswertung wird das erreichte Ergebnis mit den festgelegten Zielen verglichen und der protokollierte

Ablauf auf Schwachstellen analysiert. Ziel ist es, sowohl für die Notfallvorsorge, die Notfallbewältigung aber auch für die Durchführung von Übungen Verbesserungspotential zu identifizieren. Grundlage bilden die Übungsprotokolle aber auch die Einschätzungen der Übungsteilnehmer und -beobachter.

Die Auswertung der Übung ist zu dokumentieren. Der Übungsleiter fertigt einen Abschlussbericht über die durchgeführte Übung und der Ergebnisse, und kommuniziert diesen an die Institutionsleitung.

Es sind Verantwortlichkeiten und Maßnahmen zur Beseitigung der festgestellten Mängel sowie Umsetzungstermine für die Maßnahmen festzulegen. Die Umsetzung der Maßnahmen ist durch den Notfallbeauftragten zu kontrollieren. Spätestens während der nächsten Übung sollte die Wirksamkeit der Maßnahmen überprüft werden.

9 Aufrechterhaltung und kontinuierliche Verbesserung

Um das Notfallmanagement aufrecht zu erhalten und kontinuierlich verbessern zu können, müssen nicht nur angemessene Vorsorgemaßnahmen umgesetzt und Dokumente fortlaufend aktualisiert werden, sondern auch der Notfallmanagement-Prozess selbst muss regelmäßig auf seine Wirksamkeit und Effizienz hin überprüft werden. Dabei sollte regelmäßig eine Kontrolle und Bewertung des Prozesses durch die Leitungsebene stattfinden (Managementbewertung). Alle Ergebnisse und Beschlüsse müssen nachvollziehbar dokumentiert werden.

9.1 Aufrechterhaltung

Um die Effektivität des Notfallmanagements und der umgesetzten Notfallvorsorgemaßnahmen zu erhalten, sollte dies kontinuierlich überwacht, gesteuert und aktualisiert werden. Die Überwachung ermöglicht das frühzeitige Erkennen von Verbesserungspotentialen innerhalb des Notfallmanagements. Als Grundlage sollten für die jeweilige Institution geeignete Mess- und Bewertungskriterien entwickelt werden. Diese Messgrößen sind dann regelmäßig zu ermitteln und die Entwicklung der Werte zu beobachten. Bei negativer Entwicklung der Werte sollten die Ursachen ermittelt und Verbesserungsmaßnahmen definiert, Umsetzungsverantwortliche benannt und Anpassungen vorgenommen werden. Die Ergebnisse sollten in Berichtsform aufbereitet und zur Sensibilisierung an die Institutionsleitung kommuniziert werden. Verantwortlich für die Durchführung der hier beschriebenen Schritte ist der Notfallbeauftragte.

Geeignete Mess- und Bewertungskriterien könnten beispielsweise sein:

- Anzahl durchgeführter Übungen (erfolgreich/nicht erfolgreich),
- Anzahl durchgeführter Tests (erfolgreich/nicht erfolgreich),
- Anzahl aufgetretener Notfälle (davon erfolgreich bewältigt),
- Anzahl durchgeführter Schulungen (Anzahl Teilnehmer / Anzahl Stunden),
- erforderliche Zeit zur Alarmierung des Krisenstabs oder
- Anzahl reduzierter Risiken im Vergleich zur Gesamtanzahl der Risiken.

Neben der Überwachung und Steuerung des Notfallmanagement-Prozesses spielt die Aktualität der Maßnahmen, insbesondere der Dokumente, eine entscheidende Rolle. Um deren Aktualität aufrecht erhalten zu können, ist das Setzen von Änderungstriggern in verschiedenen Geschäftsprozessen notwendig. Die Trigger sollten aktiviert werden, wenn sich Änderungen ergeben

- in der strategischen Ausrichtung der Institution, der Geschäftsfelder oder der Priorisierung der Interessensgruppen,
- den Rahmenbedingungen wie gesetzliche oder sonstige Auflagen,
- der Umgebung, wie Lage der Institution oder Umzüge innerhalb der Institution (z. B. von Notarbeitsplätzen),
- den Geschäftsprozessen,
- im Personal,
- in der verwendeten Technologie oder auch
- nur beim Software-Release eines Systems, sofern dieses Teil des Notfallvorsorgekonzeptes ist.

Daraufhin ist der entsprechende Teil des Notfallmanagements zu überprüfen und gegebenenfalls über das Änderungsmanagement Anpassungsmaßnahmen anzustoßen.

9.2 Überprüfungen

Nur durch regelmäßige Überprüfungen des Notfallmanagementprozesses und der Notfallvorsorgemaßnahmen kann die Fähigkeit der Institution, Notfälle und Krisen bewältigen zu können, beurteilt werden. Ziel ist es, die Funktionsfähigkeit, die Effektivität, die Angemessenheit und Effizienz des Notfallmanagements sicherzustellen. Dazu werden Verbesserungsmöglichkeiten und Mängel aufgezeigt und Empfehlungen ausgesprochen.

Die Überprüfung des Notfallmanagements sollte auf unterschiedlichen Ebenen erfolgen. Die innerste Ebene bilden Selbstbewertungen (Self-Assessments), bei denen der Notfallbeauftragte und die Notfallkoordinatoren die korrekte Umsetzung ihrer Vorgaben, den aktuellen Abdeckungsgrad, die Effizienz und den Reifegrad des Notfallmanagements überprüfen oder überprüfen lassen. Dabei wird unter anderem kontrolliert, ob die Umsetzung von Maßnahmen korrekt nach den Vorgaben erfolgte, wie viele der Vorgaben umgesetzt sind und ob die vorgegebenen Prozesse gelebt werden.

Die nächste Stufe ist die Durchführung von unabhängigen Revisionen durch die unabhängige Innenrevision nach den anerkannten Grundsätzen des Berufsstandes. Interne Revisionen werden durch die Institutionsleitung in Auftrag gegeben. Durch die Durchführung von internen Revisionen wird unter anderem dokumentiert, dass die Leitungsebene ihre Überprüfungspflicht wahrnimmt. Die Prüfer sollten kompetent und unabhängig sein, was gegebenenfalls zu überprüfen ist. Bei einer internen Revision wird ein besonderer Augenmerk auf die Einhaltung von internen und externen Richtlinien sowie dem Vergleich zu Standards und Best Practices (Compliance) gelegen. Jedoch sind auch Effektivität und Angemessenheit der Notfallmanagement-Prozesse zu überprüfen.

Die Planung der internen Revisionen des Notfallmanagements sollte auf Basis eines risikoorientierten Ansatzes vorgenommen werden und ist mit der Institutionsleitung abzustimmen. Der Prüfungsplan legt die Ziele, die Art, den Umfang und die Inhalte der Prüfungen sowie die Rollen bei den Prüfungen fest. Während der Durchführung einer Revision sind alle relevanten Feststellungen von den Prüfenden zu dokumentieren und in der Nacharbeitung auszuwerten. Als Prüfungsmethoden können beispielsweise Dokumentenprüfungen, Interviews und Begehungen eingesetzt werden. Die Ergebnisse sind in einem Revisionsbericht festzuhalten, der die Feststellungen und den Handlungsbedarf enthält. Der Revisionsbericht ist an den Notfallbeauftragten und die Institutionsleitung zu kommunizieren.

Externe Revisoren werden von außen durch Aufsichtsorgane initiiert. Mit der Durchführung von externen Revisionen in Unternehmen werden typischerweise Wirtschaftsprüfer oder Beratungsunternehmen beauftragt. Die Methoden und die Vorgehensweise sind durch Vorgaben und Standards der Berufsverbände, wie beispielsweise des IDW (Institut der Wirtschaftsprüfer in Deutschland e.V.), geregelt. In Behörden werden externe Revisoren üblicherweise durch Rechnungshöfe durchgeführt.

Die regelmäßigen Überprüfungen des Notfallmanagements in den verschiedenen Stufen sind zu planen, durchzuführen und die Ergebnisse zu dokumentieren. Die bei einer Überprüfung erkannten Probleme müssen schnellstmöglich abgestellt werden. Daher sind durch den Notfallbeauftragten erforderliche Korrekturmaßnahmen auszuarbeiten und in Form eines Umsetzungsplans festzuhalten. Dieser enthält eine Zeitplanung, eine Ressourcenplanung, die Benennung von Verantwortlichkeiten sowie Vorgaben zur Überprüfung des Umsetzungsstandes. Der Notfallbeauftragte ist auch für die Umsetzung der Korrekturmaßnahmen und den angemessenen Einsatz der notwendigen Ressourcen verantwortlich.

9.3 Informationsfluss und Managementbewertung

Damit die Institutionsleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des Notfallmanagement-Prozesses treffen kann, benötigt sie Informationen über den aktuellen Stand und die Entwicklung des Notfallmanagements. Die Leitungsebene muss von der Notfallvorsorge-Organisation regelmäßig in Management-Berichten in angemessener Form über die Ergebnisse der Überprüfungen und den Status des Notfallmanagement-Prozesses informiert werden. Dabei sollten Probleme, Erfolge und Verbesserungsmöglichkeiten aufgezeigt werden. Die Leitungsebene nimmt die Management-Berichte zur Kenntnis, bewertet den Status und veranlasst eventuell notwendige Korrekturmaßnahmen. In diese Bewertung sollten folgende Aspekte einfließen:

- Ergebnisse von Revisionsüberprüfungen (auch von Dienstleistern und Lieferanten),
- Test- und Übungsergebnisse,
- Vorschläge zu Maßnahmen nach bewältigten Notfällen,
- Maßnahmenstatus (präventive Maßnahmen, reaktive Maßnahmen),
- Risiken (Restrisiken, akzeptierte Risiken, nicht berücksichtigte Bedrohungen und Schwachstellen),
- neue Lösungen (Produkte, Verfahren) zur Verbesserung der Effektivität (beispielsweise Tool gestützte Alarmierung),
- Ergebnisse des Schulungs- und Sensibilisierungsprogramms,
- neue Standards oder Best Practices (zum Notfallmanagement),
- alle Veränderungen, die Einfluss auf das Notfallmanagement haben könnten (beispielsweise an Dienstleister ausgelagerte Prozesse) und
- Umsetzungsstatus der beschlossenen Maßnahmen aus der letzten Managementbewertung.

Obwohl damit jetzt schon viele verschiedene Aspekte aufgelistet sind, sollten die Management-Bewertungen kurz und übersichtlich gehalten werden.

Die Bewertungen sollten Verbesserungen in Form von korrektiven Maßnahmen nach sich ziehen. Diese können präventiver Natur sein oder auch Bestandteile des Notfallmanagementprozesses verändern. Darunter fallen beispielsweise:

- Anpassung des zur Verfügung gestellten Budgets,
- Anpassung der angestrebten Ziele und der Leitlinie,
- Veränderung der Strategien (für einzelne Ressourcen oder der Gesamtstrategie),
- Anpassung des organisatorischen Aufbaus der Notfallorganisation,
- Veränderungen der Verfahren, um auf interne sowie externe Anforderungen zu reagieren,
- Anforderungen der Geschäftsprozesse,
- Anforderungen an die Ausfallsicherheit,
- regulatorische oder vertragliche Anforderungen und
- veränderte Risikobereitschaft.

Es empfiehlt sich, dass die Notfallvorsorge-Organisation daher in den Management-Bewertungen der Leitungsebene bereits konkrete Maßnahmenvorschläge vorlegt, um die Entscheidungsfindung zu unterstützen. Das Ziel der Institutionsleitung sollte es sein, die Effektivität des Notfallmanagements auf Basis der Informationen aus den Management-Bewertungen kontinuierlich zu verbessern. Daher sind die Ergebnisse der Bewertung und die beschlossenen Maßnahmen zu dokumentieren und in der nächsten Bewertung der Umsetzungsstatus der Maßnahmen zu prüfen. Die Notfallvorsorge-Organisation sollte die Wirksamkeit der neu umgesetzten Maßnahmen überprüfen und erforderlichenfalls weiter verbessern.

10 Outsourcing und Notfallmanagement

Die Auslagerung (Outsourcing) von Dienstleistungen bzw. Geschäftsprozessen hat viele Motive, von der Konzentration auf die wesentlichen Kernkompetenzen, der Kostenersparnis bis hin zur Verlagerung von Risiken. Die Entwicklungen zeigen, dass der noch immer andauernde Trend zu einer immer komplexeren Vernetzung der Unternehmen und Behörden mit Outsourcing-Dienstleistern und Zulieferer mit unterschiedlichsten Verträgen, Schnittstellen und Ansprechpartnern führt. Doch den aus wirtschaftlicher Sicht positiven Gründen wie Kosteneinsparungen oder Konzentration auf das Kerngeschäft stehen spezifische Risiken für die Geschäftsfortführung oder Sicherheit gegenüber, die nicht zu unterschätzen sind. Jedes Outsourcing-Projekt unterliegt einer Reihe von Sicherheitsrisiken. Weitere Ausführungen dazu sind beispielsweise in Baustein „B1.11 Outsourcing“ der IT-Grundschutz-Kataloge [GSK] zu finden.

Aus Sicht des Notfallmanagements bedeutet die Auslagerung von Geschäftsprozessen, dass für die eigene Institution die Anzahl der Risiken steigt, die außerhalb des eigenen Einflussbereiches liegen. Damit verbunden ist ein Verlust an Kontrolle. Zusätzlich steigen die Risiken für die internen Geschäftsprozesse, die von diesen Dienstleistern abhängig sind. Um diesem entgegen zu wirken, sind sowohl bei der Planung und Vertragsgestaltung neuer Outsourcing-Projekte oder Liefervereinbarungen wie auch bei laufenden Outsourcing-Projekten in Bezug auf das Notfallmanagement diverse Punkte zu beachten. Im Folgenden werden einige kurz angerissen.

10.1 Planung und Vertragsgestaltung

Bei der Planung von Outsourcing-Projekten sollte neben dem Sicherheitsmanagement auch das Notfallmanagement involviert werden. Es ist zu prüfen, welche Kritikalität die geplante Dienstleistung oder die zu liefernden Produkte besitzen und welche Risiken durch die Auslagerung neu entstehen. Die Aufgabe des Notfallbeauftragten ist es, sicherzustellen, dass die Anforderungen durch das Notfallmanagement an den auszulagernden Geschäftsprozess in den Verträgen entsprechend berücksichtigt werden.

Wird die Dienstleistung als kritisch oder hoch kritisch eingestuft, so sollten weitere Schritte unternommen werden. Dazu zählen je nach konkreter Kritikalitätseinstufung die Überprüfung des Dienstleisters auf dessen Notfallmanagement-Fähigkeit und die Integration von speziellen Klauseln oder Zusätzen für das Notfallmanagement in den Verträgen.

Neben der zu erbringenden Leistung sind die konkreten Anforderungen an die Verfügbarkeit der auszulagernden Geschäftsprozesse, die sich aus der BIA ergeben, ausführlich zu analysieren und zu beschreiben. Ebenso ist die benötigte Notfall- und Krisenmanagement-Fähigkeit des Outsourcing-Dienstleisters detailliert zu spezifizieren. Es ist zu fordern, dass die Dienstleisters Wiederanlauf- und Wiederherstellungspläne für die ausgelagerten Prozesse erstellen. Vom Notfallmanagement des Auftraggebers müssen diese auf ihre Funktionsfähigkeit überprüft werden. Abhängig von den ausgelagerten Prozessen und den Schnittstellen zwischen Institution und Dienstleister kann es notwendig sein, gemeinsame Notfall-Übungen durchzuführen. Die Bereitschaft dazu wie auch die Kostenaufteilung für die Übungen sollten in den Outsourcing-Verträgen berücksichtigt sein. Zusätzlich zu den gemeinsamen Übungen sollte der Dienstleister seine allgemeine Notfall- und Krisenmanagement-Fähigkeit insbesondere in Bezug auf die ausgelagerten Prozesse durch weitere regelmäßige Tests und Übungen nachweisen können. Ist eine Beeinträchtigung der ausgelagerten Prozesse durch die internen Übungen beim Dienstleister zu erwarten, so sollte dieses dem Auftraggeber rechtzeitig mitgeteilt werden. Die Zusammenarbeit in einem Notfall oder einer Krise ist festzulegen. Zusätzlich sind die Rechte wie auch die Pflichten vertraglich festzulegen. Einige wichtige Rechte und Pflichten sind beispielsweise:

- Die eigene Institution benötigt Informations- und Prüfungsrechte beim Outsourcing-Dienstleister, damit die Interne Revision oder durch die Institution benannte externe Prüfer dort Revisionen durchführen können.

- Die Meldepflichten des Dienstleisters sind festzulegen und zu konkretisieren. So sind beispielweise Änderungen im Notfallmanagement, in den Notfallkonzepten oder bei den Ansprechpartnern, die die ausgelagerten Prozesse betreffen, dem Auftraggeber mitzuteilen. Ebenso muss aber auch der Auftraggeber den Dienstleister über Änderungen bei sich informieren, die die ausgelagerten Prozesse betreffen.
- Der Dienstleister muss regelmäßig über den aktuellen Stand und Vorkommnisse berichten, wie Ergebnisse von Revisionen oder aufgetretene Probleme mit Bezug zum Notfallmanagement.
- Der Auftragnehmer sollte Daten über die Dienstleistungsgüte kontinuierlich bereitstellen (z. B. aus dem Help-Desk) oder dem Auftraggeber entsprechende Rechte zum Monitoring einräumen.
- Der Dienstleister ist verpflichtet, den Auftraggeber über Entwicklungen bei sich zu informieren, die die ordnungsgemäße Erledigung der ausgelagerten Prozesse beeinträchtigen könnten,
- Es muss festgelegt werden, welche Priorität die Informationssicherheit gegenüber der Geschäftsfortführung im Krisenfall hat, damit der Dienstleister entsprechend darauf reagieren kann.
- Zwischen den Outsourcing-Partnern müssen klare Eskalationsstufen und –wege festgelegt werden, damit es in Notfällen zu keinen Verzögerungen oder Missverständnissen kommt.
- Mit dem Dienstleister müssen Reaktions- und Verfügbarkeitsgarantien vereinbart werden, inklusive einer 24-stündigen Erreichbarkeit des Dienstleisters für Notfälle.
- Der Auftraggeber benötigt im Not- oder Krisenfall gegebenenfalls Weisungsrechte gegenüber dem Dienstleister (bezogen auf die ausgelagerten Prozesse).
- Es sind zwischen den Outsourcing-Partnern Regelungen über die Möglichkeit und Modalitäten einer Weiterverlagerung zu treffen.
- Im Vertrag sollte ein außerordentliches Kündigungsrecht des Auftraggebers bei Verstößen oder Nicht-Einhaltung der spezifizierten Anforderungen vorgesehen werden.

Bei der Vertragsgestaltung sind die Ausschlussklauseln, beispielsweise für höhere Gewalt, genau zu überprüfen, um zu verhindern, dass gerade für Krisensituationen die Leistungserbringung aus der Haftung ausgeschlossen werden.

Bei der Auswahl eines Dienstleisters sollte darauf geachtet werden, dass die Erbringung der Dienstleistung auch im Notfall beim Auftraggeber möglich und die Kompatibilität mit den Notfallvorsorge-Maßnahmen des Auftraggebers gewährleistet ist. Dazu gehört beispielsweise, dass ein Dienstleister auch am oder für den Ausweichstandort des Auftraggebers seine Dienstleistung erbringen kann.

10.2 Berücksichtigung bei der Konzeption

Beim Aufbau und der Konzeption des Notfallmanagements sind die ausgelagerten Geschäftsprozesse wie auch die Zulieferer in den einzelnen Arbeitsschritten zu berücksichtigen. Sie sind sowohl bei der Durchführung der Business Impact Analyse zu beachten wie auch bei der Risikoanalyse. Das Ziel bei der BIA im Hinblick auf Outsourcing ist, die Anforderungen bezüglich des Wiederanlaufs und der Wiederherstellung an die ausgelagerten Prozesse zu identifizieren und mit den vorliegenden Verträgen abzugleichen, um eventuell vorhandene Lücken bei der Leistungsbeschreibung (z. B. maximale Ausfallzeit, Wiederanlauf-Niveau, maximale Wiederherstellungszeit) zu entdecken.

Bei der Risikoanalyse sind sowohl die Schnittstellen zwischen den ausgelagerten Anteilen und den innerhalb der Institution betriebenen Geschäftsprozessen wie auch die ausgelagerten Prozesse zu betrachten und die betreffenden Risiken zu identifizieren. Dabei stellen sowohl die ausgelagerten Prozesse selbst als auch die Schnittstellen zum internen Betrieb mögliche Risiken dar. Es ist zu untersuchen, welche Auswirkungen eine zeitweise Unterbrechung eines ausgelagerten Prozesses haben kann. Dies sollte in verschiedenen Abstufungen bis hin zu einem Totalausfall eines Outsourcing-Dienstleisters durchleuchtet werden. Darauf aufbauend sind entsprechende Vorkehrungen

und Sicherungsmaßnahmen zu entwickeln. Die Risikobetrachtung sollte sich dabei nicht ausschließlich auf die Betriebsphase beschränken, also nur laufende Outsourcing-Verträge einbeziehen, sondern auch die Migrationsphase von Prozessen zu einem neuen Dienstleister sowie die Phase eines eventuellen Insourcing betrachten.

Bei der Erstellung von Notfallplänen sind die Schnittstellen von internen zu ausgelagerten Prozessen genau zu definieren und die Pläne aufeinander abzustimmen. Die Notfall-Prozeduren des Outsourcing-Dienstleisters müssen kompatibel mit denen des Auftraggebers sein. Dieses sollte bei gemeinsamen Tests und Übungen des Auftraggebers und des Dienstleisters überprüft werden.

Die Notfallbewältigung erfordert je nach Schadensszenario eine enge Zusammenarbeit mit den Dienstleistern. Daher sollte die Leistungsbeschreibung der Verträge auch Regelungen zur Eskalation, Aktivierung der Notfallbewältigung und der Krisenbewältigung enthalten. Es sollte in der Konzeption des eigenen Notfallmanagements eindeutig geregelt werden, wie die Kommunikation zur Bewältigung der Krise erfolgen soll und wie die Zuständigkeiten bei der externen Krisenkommunikation verteilt sind.

Bei der regelmäßigen Überprüfung des Notfallmanagementprozesses und der Notfallvorsorge-maßnahmen sind auch die ausgelagerten Geschäftsprozesse und die externen Dienstleister einzubeziehen. Der Nachweis der Notfall- und Krisenmanagement-Fähigkeit des Dienstleisters durch eine Zertifizierung oder eine andere unabhängige Prüfung ist möglich, doch sollte der Auftraggeber genau darauf achten, ob seine ausgelagerten Geschäftsprozesse im Geltungsbereich der Zertifizierung enthalten, er zu den Key-Stakeholdern gerechnet wurde, die Kritikalität der Geschäftsprozesse nach den Vorgaben im Vertrag eingestuft und in den Notfallplänen des Dienstleisters berücksichtigt sind.

Je nach Komplexität und Kritikalität der ausgelagerten Geschäftsprozesse ist es daher notwendig, ein Outsourcing-Management zu etablieren. Die Verantwortung ist in der Leitungsebene der eigenen Institution zu verankern. Auf beiden Seiten ist ein verantwortlicher Ansprechpartner zu benennen.

11 Tool-Unterstützung

Für die verschiedenen Aufgaben und Phasen des Notfallmanagement-Prozesses steht eine Reihe von Software-Werkzeugen zur Verfügung. Die am Markt verfügbaren Tools decken verschiedene Aspekte des Notfallmanagement-Prozesses ab. Zu deren Leistungsmerkmalen gehören unter anderem Unterstützung bei der Erfassung der Geschäftsprozesse, der Durchführung und Auswertung der Business Impact Analyse, der Durchführung der Risikoanalyse, der Erstellung und Aktualisierung eines Notfallhandbuchs, der Revision, der Durchführung von Tests und Übungen, der Alarmierung bis hin zur Unterstützung der reaktiven Notfallbewältigung bei der Protokollierung und Lagebewertung. Beispielsweise kann, je nach eingesetzter Software,

- die Erstellung und Aktualisierung von Plänen für das Notfallmanagement unterstützt werden,
- die Versionierung und damit eindeutige Zuordnung von Dokumenten erfolgen, die beim Notfallmanagement relevant sind,
- ein Aktualisierungszyklus der erstellten Dokumente über automatische Erinnerungsmails gesteuert werden,
- eine Übersicht über vorhandene Pläne für die kritischen Geschäftsprozesse erzeugt werden,
- ein Bezug zu einzelnen Wiederanlauf-Plänen und unterstützten Ressourcen (Anwendungen und Systeme) automatisch hergestellt werden (so dass im Notfall eine schnelle und eindeutige Zuordnung vorliegt),
- die Alarmierung automatisiert und ohne Zeitverzögerung erfolgen oder
- eine revisionssichere Protokollierung im Krisenstab durchgeführt werden.

Der Einsatz geeigneter Software-Werkzeuge kann die Tätigkeiten der an der Notfallorganisation beteiligten Personen erheblich erleichtern. Einige Softwareprodukte geben dabei eigene Methoden und Vorgehensmodelle vor, an denen sich die Benutzer orientieren können, beispielsweise für die Business Impact Analyse oder Risikoanalyse. Entsprechende Frage- und Auswertungsschemata sind vorgegeben und können ohne größere Aufwände sofort umgesetzt und genutzt werden.

Bei der Auswahl des Werkzeugs sollte darauf geachtet werden, dass die Größe und die Art der eigenen Institution unterstützt wird. Weitere Kriterien bei der Auswahl können neben den allgemeinen Leistungsmerkmalen und den Kosten für das Tool, den Support und eventuell notwendige Schulungen die Folgenden sein:

- die unterstützten Plattformen bzw. Plattformunabhängigkeit durch Web-Technologien,
- Schnittstellen zu anderen Tools, die in der Institution schon vorhanden sind, beispielsweise für das Störungsmanagement (Help-Desk), Alarmierungstools oder auch Inventarisierungs- oder Personalmanagement-Tools,
- die Bedienungsfreundlichkeit, insbesondere der Dokumentationswerkzeuge,
- die Möglichkeit, individuelle Sichten zu erstellen, je nach Bedarf, Situation oder Rolle des Nutzers,
- Sicherheit und Datenschutz für die darin verwalteten und gespeicherten Daten (z. B. private Telefonnummern, Adressen),
- die Verfügbarkeit in der Krise (z. B. Zugriff über das Internet) oder
- die Robustheit, die in Krisensituationen besonders wichtig ist, da durch die Stresssituation mit einer erhöhten Fehlerquote zu rechnen ist.

Aus dem Blickwinkel der Informationssicherheit sind zentrale Anforderungen an Notfallmanagement-Tools, dass

- Hard- und Software so ausgelegt sind, dass die Anforderungen an die Verfügbarkeit und die Integrität der Daten erfüllt werden können,
- die Kommunikation über sichere Protokolle möglich ist, z. B. bei der Administration und bei Remote-Zugriffen,
- die Benutzerverwaltung es erlaubt, das organisationsweite Rollenkonzept für das Notfallmanagement abzubilden,
- eine verlässliche Zugriffskontrolle möglich ist,
- der Hersteller zeitnah auf bekannt gewordene Sicherheitsmängel reagiert und regelmäßige Updates und schnell verfügbare Sicherheitspatches anbietet,
- dass es möglich ist, besonders sensitive Daten zu verschlüsseln.

Nachfolgend werden einige Aspekte für die oben genannten sicherheitsrelevanten Auswahlkriterien aufgelistet:

- Unterstützt das Tool sichere Protokolle zur Kommunikation? Damit Daten sicher ausgetauscht werden können, müssen netzfähige Tools sichere Protokolle unterstützen, bei einer Browser-basierten Konfiguration beispielsweise SSL/TLS.
- Hat das Tool geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer?
- Unterstützt das Tool die verschlüsselte Speicherung von Passwörtern oder anderer genutzter Authentisierungsmerkmale? Tools, bei denen Passwörter unverschlüsselt gespeichert werden, sollten nicht mehr beschafft werden.
- Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?
- Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden? Ein Wartungsvertrag ist nur dann geeignet, wenn mit den garantierten Reaktions- und Wiederinbetriebnahmezeiten die festgelegten Ansprüche an die Verfügbarkeit der Geräte abgedeckt werden können.
- Bietet der Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen? Dieser Punkt sollte Bestandteil des abgeschlossenen Wartungsvertrags sein. Beim Abschluss des Vertrags ist auf die Sprache der zur Verfügung gestellten Hotline des Herstellers zu achten.
- Wie zuverlässig und ausfallsicher ist das Produkt? Der Hersteller sollte Erfahrungswerte bezüglich der Zuverlässigkeit liefern können.
- Ist der Detailgrad der Protokollierung konfigurierbar? Werden durch die Protokollierung alle relevanten Daten erfasst? Ist der Zugriff auf die Protokolldaten mit einem Zugriffsschutz versehen? Die angebotenen Möglichkeiten zur Protokollierung müssen mindestens die in der Sicherheitsrichtlinie festgelegten Anforderungen erfüllen.

Sind alle Anforderungen an das zu beschaffende Produkt erfasst, so sollten die am Markt erhältlichen Produkte dahin gehend untersucht werden, inwieweit sie diese Anforderungen erfüllen. Nicht jedes Produkt erfüllt alle Anforderungen gleichzeitig oder gleich gut. Daher sollten die einzelnen Anforderungen daraufhin gewichtet werden, wie entscheidend die Erfüllung der jeweiligen Anforderung ist. Auf dieser Grundlage kann dann eine fundierte Kaufentscheidung getroffen werden.

12 Glossar

Abkürzungen / Begriffe	Definitionen
Alarmierung	Ziel der Alarmierung ist es, verantwortliche Entscheider und Akteure möglichst schnell nach Eintritt Schadensereignisses zu informieren und damit die Bewältigung des Notfalls oder der Krise einzuleiten.
BCM	Business Continuity Management Ganzheitlicher Managementprozess zur Fortführung der kritischen Geschäftsprozesse bei Eintritt eines Notfalls.
BIA	Business Impact Analyse, Folgeschädenabschätzung Analyse zur Ermittlung von potentiellen direkten und indirekten Folgeschäden für eine Institution, die durch das Auftreten eines Notfalls oder einer Krise und Ausfall eines oder mehrerer Geschäftsprozesse verursacht werden.
CERT	Computer Emergency Response Team Spezielles Team von Sicherheitsfachleuten, das bei der Lösung von konkreten Sicherheitsvorfällen als koordinierende Instanz mitwirkt, Warnungen vor Sicherheitslücken herausgibt und Lösungsansätze anbietet (sogenannte Advisories).
Fachaufgabe	Eine Fachaufgabe ist der in Behörden verwendete Begriff für einen Geschäftsprozess.
Institution	Der Begriff „Institution“ wird als Oberbegriff für eine Behörde, ein Unternehmen oder sonstige Organisationen verwendet.
Heißer Standort (hot site)	"Heiße Standorte" werden kontinuierlich aktiv betrieben. Bei Ausfall eines Standortes kann eine „hot site“ ohne zeitliche Verzögerung unmittelbar aktiv werden.
Kalter Standort (cold site)	Als "kalte Standorte" werden Standorte bezeichnet, die zwar alle Voraussetzungen bieten, um die erforderliche Betriebsausstattung wie IT-Systeme aufzunehmen, diese aber noch nicht betriebsbereit installiert sind.
KPI	Key Performance Indicator Kennzahlen, anhand derer der Fortschritt oder der Erfüllungsgrad hinsichtlich einer Zielsetzungen gemessen werden kann.
Krisenmanagement	Schaffung von konzeptionellen, organisatorischen und technischen Voraussetzungen, die eine schnellstmögliche Zurückführung der eingetretenen Schadenssituation in den Normalzustand unterstützen. Ziel ist, die Entscheidungsfähigkeit der Institution sicherzustellen und eine zielgerichtete und koordinierte Bewältigung der Krise zu ermöglichen. Das institutionsweite Krisenmanagement ist für alle Arten von Krisen zuständig. Krisen im Sinne des vorliegenden Standards zum Notfallmanagement stellen eine Untermenge dar. Die Bewältigung einer Krise im Rahmen des betrieblichen Kontinuitätsmanagement umfasst somit nicht ein vollständiges Krisenmanagement.
Kritikalität eines Geschäftsprozesses	Skalierbare Wertung (Klassifizierung) von Geschäftsprozessen anhand ihrer Bedeutung für die Wertschöpfung einer Institution. Die Klassifizierung erfolgt meist anhand der Wiederanlauf-Anforderung an den Geschäftsprozess oder des über die Dauer der Ausfallzeit zu erwartenden Schadens, kann jedoch durch weitere Kriterien ergänzt werden.
Kritische Ressource	Ressource einer Institution, welche bei Ausfall zur Unterbrechung bzw. Ausfall eines (kritischen) Geschäftsprozesses führt.

Abkürzungen / Begriffe	Definitionen
Lagezentrum	Krisenstabsraum Räumlichkeiten, die dem Krisenstab als Arbeitsumgebung dienen und für die besondere Anforderungen bezüglich des Standortes und der Ausstattung gelten.
MTN	Maximal tolerierbarer Notbetrieb
MTPD	Maximum Tolerable Period of Disruption Maximal tolerierbare Ausfallzeit, bei deren Überschreitung die Lebensfähigkeit des Prozesses bzw. der Institution mittel- bis langfristig ernsthaft bedroht ist.
Notfallhandbuch	Das Notfallhandbuch beinhaltet alle Informationen, die während und für die Notfall- und Krisenbewältigung benötigt werden. Es umfasst somit alle Notfallpläne wie den Krisenkommunikationsplan, den Krisenstabsleitfaden, die Wiederanlauf- und Wiederherstellungpläne.
Notfallkonzept	Das Notfallkonzept umfasst das Notfallvorsorgekonzept und das Notfallhandbuch.
Notfallvorsorge-konzept	Das Notfallvorsorgekonzept beinhaltet alle bei der Konzeption des Notfallmanagement anfallenden Informationen, die nicht direkt für die Notfallbewältigung benötigt werden.
Organisationseinheit	Logische Einheit einer Institution. Dabei kann es sich beispielsweise um einen Standort, eine Abteilung, einen Fachbereich oder sonstige Einheit der Institutionsstruktur handeln.
RTO	Recovery Time Objective Die Wiederanlaufzeit eines Prozesses oder der benötigten Ressourcen. Die maximale Zeit für den Wiederanlauf muss kleiner als die maximal tolerierbare Ausfallzeit sein.
SLA	Service Level Agreement
Warmer Standort (warm site)	Ein "warmer Standort" besitzt eine vorbereitete Hardwareumgebung inklusive aller Versorgungseinrichtungen, so dass diese im Notfall nur noch geeignet konfiguriert oder anderweitig vorbereitet werden müssen.
WAZ	Wiederanlaufzeit Zeitspanne von der Unterbrechung eines Prozesses bis zum Beginn des Notbetriebs.
Wertkette	Unter einer Wertkette wird der Teil einer Wertschöpfungskette verstanden, der sich innerhalb der Organisation befindet. Eine Wertschöpfungskette umfasst den gesamten Weg eines Produktes oder einer Dienstleistung vom Hersteller bis zum Verbraucher und kann daher mehrere Institutionen umfassen.
Wiederherstellungszeit (WHZ)	Die Wiederherstellungszeit ist die Zeitspanne von der Unterbrechung des Prozesses bis zum Start des Normalbetriebs. Die Wiederherstellungszeit muss kleiner oder gleich der festgelegten Wiederanlaufzeit plus dem maximal tolerierbaren Notbetrieb sein (WHZ ≤ WAZ+MTN).

Weitere im Dokument verwendete Begriffe und Abkürzungen finden Sie im Glossar der IT-Grundschutz-Kataloge.

Anhang A Strategieoptionen

Die folgenden Erläuterungen zeigen die wesentlichen Optionen für einzelne Ressourcenklassen auf. Sie können nur einen groben Überblick geben. In jedem Fall sollte eine detaillierte Betrachtung der Umgebungsvariablen des jeweiligen Unternehmens oder der Behörde in die Bewertung und Auswahl mit einbezogen werden. Dazu gehören beispielsweise neben ortsansässigen Dienstleistern auch behörden- bzw. unternehmensbezogene Risiken.

Für den überwiegenden Teil der Ressourcenklassen können folgende generischen Strategien verfolgt werden:

- Nutzung interner Kapazitäten,
- Kooperative Partnerschaften und
- Nutzung kommerzieller Kapazitäten und Lösungen.

A.1 Arbeitsplätze

In die Kontinuitätsüberlegungen für Arbeitsplätze sollten sowohl die für die Geschäftsprozesse benötigten Büroarbeitsplätze wie auch die Arbeitsplätze in der Produktion inklusive deren speziellen Anforderungen an die Ausstattung einbezogen werden. Ausschlaggebend für die Wahl ist die jeweils benötigte Wiederanlaufzeit und die identifizierten Schadensszenarien.

Verteilte Geschäftstätigkeit

Werden Prozesse mit einer sehr geringen Wiederanlaufzeit betrieben, so ist zu überlegen, diese auf mehrere redundante Standorte aufzuteilen. Solche redundanten Standorte betreiben die Geschäftsfunktion in gleicher oder sehr ähnlicher Weise. Die notwendigen Ressourcen inklusive des Personals sind dort kontinuierlich vorhanden. Die jeweils genutzten Ressourcen sind äquivalent. Bei Eintritt eines Notfalls übernimmt der jeweils andere Standort die Arbeit des ausgefallenen zusätzlich. Der Wechsel von Personal zum Ausweichstandort ist daher nicht notwendig. Damit die Aufgabenübernahme reibungslos funktioniert, muss die Verteilung der Geschäftstätigkeit vorbereitet sein. Dazu gehört beispielsweise die redundante Datenhaltung oder die Datenübertragung im Notfall. Diese Alternative ist ideal für sehr geringe Wiederanlaufzeit und um die Zeit bis zum Aufbau alternativer Arbeitsplätze zu überbrücken, jedoch nur bedingt geeignet als längerfristige Lösungsmöglichkeit.

Dedizierte interne Ausweicharbeitsplätze

Eine aufwendige Alternative ist das Bereithalten von eigenen Ausweicharbeitsplätzen an einer Ausweichlokation. Dies bedeutet, dass an einer weiteren Lokation Arbeitsplätze bereit stehen und sofort genutzt werden können. Je nach Ausprägung, ob „warm“ oder „heiß“, entstehen erhebliche Investitions- und laufende Kosten zur Aufrechterhaltung der Einsatzfähigkeit.

Nicht-dedizierte interne Lösung

Sind Räumlichkeiten vorhanden, die für die Aufrechterhaltung des Kerngeschäfts nicht unbedingt notwendig sind oder nur temporär genutzt werden, können diese kurzfristig als Ausweicharbeitsplätze zweckentfremdet werden. Dies könnten zum Beispiel Schulungs- und Besprechungsräume oder auch eine Cafeteria sein.

Freisetzung

Bei Notfällen werden für die kritischen Prozesse Ressourcen von anderen, nicht vom Notfall betroffenen Prozessen, die eine niedrigere Kritikalität haben, eingesetzt. Die Prozesse der niedrigeren Priorität werden gestrafft oder gar vollständig stillgelegt. Die dabei entstandenen Ressourcen könnten kurzfristig für kritische Prozesse verwendet werden.

Telearbeitsplätze und Fernzugriff

Ist die Ausführung einer Prozesstätigkeit nicht an einen individuellen Standort gebunden, können Mitarbeiter mit der entsprechenden Ausstattung und einem Internetzugang von einem beliebigen Arbeitsplatz aus, zum Beispiel von einem Heimarbeitsplatz, arbeiten. Kapazitätseinschränkungen der Internetverbindung durch Netzüberlastungen oder am Einwahlpunkt der Institution sollten beobachtet und gegebenenfalls überprüft werden. Auch weitere Rahmenbedingungen müssen dabei beachtet werden. Werden diese Arbeitsplätze schon als Heimarbeitsplätze genutzt, so sind organisatorische Aspekte wie Sicherheitsaspekte, Software-Updates oder auch die Nutzung und der Austausch von benötigten Dokumenten geregelt. Jedoch sollte das für die Arbeiten erforderliche Equipment vollständig am Telearbeitsplatz dupliziert sein. Notebooks, die sowohl am Arbeitsplatz in der Institution wie auch am Telearbeitsplatz zum Einsatz kommen, sind nur bedingt geeignet, da sie gegebenenfalls im Notfall unerreichbar in der Institution und nicht am Telearbeitsplatz zur Verfügung stehen.

Kooperierende Partnerschaft

Durch Partnerschaften mit benachbarten Institutionen können Krisensituationen überbrückt werden, indem auf Ressourcen der anderen Institution zugegriffen wird, die diese kurzfristig zur Verfügung stellt. Kooperierende Institutionen sollten ähnliche Strukturen besitzen.

Die grundlegende Bereitschaft für Kooperationen in Notfällen muss auf Leitungsebene vereinbart werden. Im Vorfeld muss geprüft werden, in wie weit in Notfällen kurzfristig Raumressourcen der Partner genutzt werden können, wo sich diese befinden und mit welcher Rechner- und Leitungskapazität diese ausgestattet sind. Die Notfall-Kooperation sollte im Vorfeld konzeptioniert und einzelne Hilfsoptionen mit den betroffenen Organisationseinheiten in Bezug auf ihre Machbarkeit durchgespielt werden. Die Details hierzu können dann vom Notfallmanagement ausgearbeitet werden. Es empfiehlt sich jedoch, einen gemeinsamen Arbeitskreis der Notfallmanagement-Verantwortlichen aller kooperierenden Institutionen zu gründen. Dies bietet gleichzeitig eine Möglichkeit, sich über aktuelle Bedrohungen und Strategien auszutauschen. Die Risikosituation, die Marktsituation und anderer Rahmenbedingungen müssen ständig neu evaluiert und in die Vereinbarung eingearbeitet werden. Eine entsprechende Verpflichtung sollte vertraglich festgehalten und regelmäßig auf Aktualität geprüft werden.

Eine wechselseitige Vereinbarung ist aufgrund der häufig zwischen Nachbarunternehmen herrschenden Wettbewerbssituationen (z. B. bei Anbietern der gleichen Produktsparte) oftmals schwer zu treffen. Schutzmaßnahmen gegen Konkurrenzspionage und ähnliche Bedrohungsszenarien sind in jedem Falle zu treffen.

Kommerzielle Lösungen von speziellen Dienstleistern

Eine häufig gewählte Variante ist, die Angebote externer Dienstleister zu nutzen, die sich auf die Bereitstellung von Ausweichstandorten oder –dienstleistungen spezialisiert haben. Diese stellen in einem Notfall zuvor vertraglich zugesagte Ressourcen zur Verfügung, um Geschäftsprozesse im Notfall ganz oder teilweise auf Ausweichstandorte auszulagern zu können. In einem Vertrag müssen die vereinbarten Leistungen detailliert festgelegt werden. Auch Konventionalstrafen müssen festgelegt werden, falls die vertraglichen Verpflichtungen nicht in der vereinbarten Weise erbracht werden können. Da diese Ressourcen kontinuierlich im vereinbarten Leistungsumfang bereitgehalten werden, entstehen bei dieser Lösung fortlaufende Kosten. Diese und die Verfügbarkeitskriterien bestimmen vor allem die Entscheidung. Die Verfügbarkeitskriterien setzen sich dabei zum Beispiel aus der geographischen Lage, anderen Institutionen, die ebenfalls diesen Standort im Notfall nutzen, und der Größe der benötigten Büroflächen zusammen.

Es können folgende Alternativen von kommerziellen Lösungen unterschieden werden:

- **Fest zugeordneter Ausweichstandort**
  Ein fest zugeordneter Ausweichstandort bei einem externen Dienstleister kann an die individuellen Bedingungen der Institution angepasst werden. Er hat den Vorteil, dass abhängig von den

Vertragsbedingungen eine hohe Verfügbarkeit gewährleistet wird. Die Verfügbarkeitsanforderungen und sonstige Vertragsbedingungen sind dabei aus den Ergebnissen der BIA und der Risikoanalyse abzuleiten. Diese Variante ist kostenintensiv, garantiert aber im Gegenzug einen exklusiven Standort, der im Notfall ohne Einschränkung zur Verfügung steht.

- **Geteilter Ausweichstandort**
  Im Unterschied zu einem fest zugeordneten wird ein geteilter Ausweichstandort durch weitere Institutionen genutzt. Je nach Art und Auswirkung des Notfalls kann es zu der Situation kommen, dass mehrere von dem Notfall betroffene Institutionen den Ausweichstandort gleichzeitig nutzen möchten. Aufgrund von Überlastungen steht der Ausweichstandort in einem solchen Fall nur eingeschränkt oder gar nicht zur Verfügung. Aus diesem Grund muss bei den Vertragsvereinbarungen geklärt werden, ob und unter welchen Rahmenbedingungen der gewählte Standort auch anderen Kunden zugänglich ist. Es ist notwendig, Angaben über die anderen nutzenden Institutionen einzufordern, wie z. B. Nutzungsprioritäten, Branche und Größe der anderen Institutionen. Wenn mit dem Dienstleister nicht eindeutig geklärt werden kann, dass in einem Notfall der eigenen Institution die erforderlichen Raumkapazitäten zur Verfügung stehen, sollte von einer gemeinsamen Nutzung mit benachbarten Institutionen abgesehen werden.

- **Mobiler Ausweichstandort**
  Als mobile Ausweichstandorte werden beispielsweise im Notfall bereitgestellte Büro-Container oder speziell ausgerüstete Groß-Fahrzeuge bezeichnet. Die mobilen Ausweichstandorte sind eine kostengünstige Büroalternative zur Überbrückung eines Verlustes von Arbeitsplätzen. Deren Raumkapazität ist in der Regel allerdings sehr begrenzt. Im Vorfeld müssen unbedingt geeignete Aufstellungsorte festgelegt werden. Es ist außerdem zu überprüfen, ob in einem Notfall die erforderlichen Versorgungsleitungen wie Strom- und Kommunikationsanbindungen vom Dienstleister gewährleistet werden können oder ob sie vom Auftraggeber selbst bereitgestellt werden müssen.

Im Notfall kann es erforderlich sein, dass Mitarbeiter an einen entfernten Ausweichstandort arbeiten müssen. Hierfür ist zu klären, wie der Transport schnell und reibungslos organisiert werden kann. Ist der Mitarbeitertransfer an den entfernten Ausweichstandort über längere Zeit notwendig und müssen unternehmens- bzw. behördeneigene Mitarbeiter am Ausweichstandort für eine längere Zeit anstelle ihres üblichen Arbeitsplatzes arbeiten, sollte im Vorfeld die Zustimmung der Personalvertretung eingeholt werden. Es sollten Regelungen bezüglich des zusätzlichen zeitlichen und finanziellen Aufwands der Mitarbeiter für den Anfahrtsweg getroffen werden. Gegebenenfalls sind sogar Anpassungen im bestehenden Arbeitsvertrag erforderlich und umzusetzen.

A.2 Personal

Fachlich gut ausgebildetes Personal bildet die Basis, um die Geschäftsprozesse erfolgreich umsetzen zu können. Durch geeignete Maßnahmen muss sichergestellt werden, dass das Schlüsselpersonal in Notfällen zur Verfügung steht. Dazu gehören Vertreterregelungen wie auch Vorkehrungen, dass das benötigte Personal die Ausweichstandorte im Notfall erreichen kann. Weitere Ausführungen hierzu finden sich auch in den Bausteinen Organisation und Personal der IT-Grundschutz-Kataloge [GSK].

Es empfiehlt sich zum einen, für das Schlüsselpersonal Stellenbeschreibungen mit den erforderlichen Qualifikationen zu erstellen, und zum anderen einen Überblick über Mitarbeiter mit Fachqualifikationen zur Unterstützung der Notfallteams oder notfallbezogenen Fähigkeiten anzufertigen. Dazu zählen beispielsweise Erfahrung mit

- Personenschäden (z. B. Erste-Hilfe-Training),
- Schäden an Gebäuden (z. B. Experten für Brandschutz oder Gebäudetechnik) oder

Schäden an IT oder Kommunikationsnetzen (z. B. fundierte IT-Fachkenntnisse).

Stellvertreter durch Vielseitigkeits- und Cross-Training

Ein Programm, in dem Mitarbeiter in verschiedenartigen Arbeitsbereichen geschult werden, ermöglicht eine flexible Rollenbesetzung in einem Notfall. Die Fähigkeit zur Aufrechterhaltung laufender Prozesse wird somit auf mehrere Mitarbeiter der Institution verteilt. Eine Abhängigkeit von wenigen Wissensträgern kann damit vermieden werden.

Fachpersonal durch Nutzung externer Anbieter
Manchmal ist es notwendig, in Notfällen kurzfristig externes Fachpersonal einzusetzen. Es empfiehlt sich, spezielle Stellenanforderungen oder -profile des Schlüsselpersonals im Vorfeld mit den entsprechenden Dienstleistern abzustimmen und gegebenenfalls die erforderlichen Bereitstellungszeiten vertraglich festzuhalten. Wird fremdes Personal nur zeitweise eingesetzt, sollte eine entsprechende Risikobetrachtung durchgeführt und die passenden Sicherheitsmaßnahmen umgesetzt werden.

Wissensmanagement
Um eigenes oder externes Personal in ihnen bisher unbekannte Prozesse einbinden zu können, ist ein funktionstüchtiges und gelebtes Wissensmanagement erforderlich. Es empfiehlt sich, hierzu spezielle an der Praxis orientierte Handlungsanweisungen und Problemlösungen bereitzustellen. Die gesammelten Informationen sollten entsprechend ihres Schutzbedarfs eingestuft und angemessen Sicherheitsmaßnahmen umgesetzt werden. Die Verfügbarkeit der Daten sollten durch Datensicherungsmaßnahmen abgesichert werden.

A.3 Informationstechnik

Die meisten Geschäftsprozesse sind von Informations- und Kommunikationstechnik abhängig. Dabei haben vor allem die IT-Komponenten einen besonders kritischen Stellenwert. Die folgenden Erläuterungen geben einen Überblick über mögliche Kontinuitätsstrategien für die Informationstechnik, vor allem beim Betrieb von Rechenzentren.

Eingeschränkter IT-Betrieb
Bei der Durchführung der BIA wurden die Minimalanforderungen an die Ressourcen in einem Notfall sowie die Prioritäten der für den Wiederanlauf notwendigen Ressourcen erfasst und schriftlich festgehalten. Die Geschäftsprozesse werden mit einer geringeren Kapazität und damit mit einer geringeren Anzahl von Ressourcen betrieben.

Redundante IT-Standorte
Für die Aufstellung der zentralen IT-Komponenten werden besondere Räumlichkeiten wie Serverräume und Rechenzentren benötigt. Redundante IT-Standorte können je nach Wiederanlaufzeit verschiedene Ausprägungen besitzen:

Kalter Standort („Cold Site“)
Mit dem Begriff "Kalter Standort" werden Ausweichstandorte beschrieben, die den Standort bereitstellen, jedoch noch nicht mit den erforderlichen IT-Komponenten ausgestattet sind. Sie bieten die notwendigen Voraussetzungen, um diese aufzunehmen, wie beispielsweise eine angemessene Klimatisierung oder Stromversorgung, die die besonderen Beschaffenheiten der einzelnen IT-Komponenten berücksichtigen. Im Notfall werden dann Hardware, Software und Daten dorthin geschafft und installiert, benötigte Kommunikationsverbindungen werden geschaltet.

Warmer Standort („Warm Site“)
Als "Warmer Standort" wird ein Ausweichstandort bezeichnet, der eine vorinstallierte Hardwareumgebung inklusive aller Versorgungseinrichtungen besitzen. Die Hardware ist so ausgelegt, dass sie im Notfall lediglich aktiviert und gegebenenfalls die Konfigurationseinstellung angepasst werden muss. Die Datenbasis ist noch einzuspielen. Je nach Komplexität und Datenmenge kann eine Inbetriebnahme einer Warm-Site daher einige Stunden in Anspruch nehmen.

Heißer Standort („Hot Site“)
Als "Heißer Standort" wird ein Ausweichstandort bezeichnet, mit einer vollständigen, funktionsfähigen Infrastruktur mit aktueller Datenbasis. Bei Ausfall des Hauptstandortes kann ein heißer Standort unmittelbar aktiviert werden (eventuell durch Fernaktivierung) und mit minimaler zeitlicher Verzögerung die Aufgaben übernehmen. In der Regel ist es jedoch notwendig, dass das notwendige Personal vom Hauptstandort zum Ausweichstandort umsiedelt.

Hinweise für die Festlegung einer geeigneten Entfernung des redundanten Rechenzentrums vom Hauptstandort sind in der BSI-Publikation „Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren“ zu finden.

Verteilte IT-Standorte
Eine Alternative zu einem redundanten Standort ist die Verteilung der Prozesse auf zwei oder gar mehrere Standorte. Der alternative Standort wird nicht erst im Notfall aktiviert, sondern beide Standorte werden parallel betrieben und sind produktiv. Dadurch wird sowohl das Risiko reduziert wie auch der Zeitverlust durch die Aktivierung eines Ausweichstandortes weiter reduziert.

A.4 Komponentenausfälle

Bei Ausfall einzelner Komponenten gibt es neben der Reparatur verschiedene Optionen, um die Verfügbarkeit zu erhöhen und die Betriebsfähigkeit so schnell wie möglich wieder herzustellen. Komponenten können beispielsweise Server, Arbeitsplatzcomputer, Drucker, Kopierer oder Telefone sein, aber auch Klimageräte, Notstromaggregate oder Teile einer Produktionsanlage.

Lagerung von Komponenten
Für besonders kritische Komponenten können in geeigneter Anzahl Ersatzgeräte oder –komponenten vorgehalten werden. Hierbei sind allerdings einige Punkte zu beachten. Es wird zusätzlicher Lagerraum benötigt, der für die IT- oder andere Hardware-Komponenten, wie z. B. Teile von Produktionsanlagen, geeignet sein muss. Das Lager für die Ersatzsysteme sollte sich möglichst nicht in denselben Gebäudeteilen oder zumindest in einem anderen Brandabschnitt befinden. Die gelagerten Komponenten müssen denen im Produktivbetrieb entsprechen oder kompatibel sein, und sind daher regelmäßig zu aktualisieren. Die Vorratshaltung ist teuer und fehleranfällig.

Ersatzbeschaffung
Wenn ausgefallene Komponenten nicht in einer tolerablen Zeitspanne wieder hergestellt werden können, sollte Ersatz beschafft werden. Um diesen Vorgang zu beschleunigen, sollte ein aktueller Ersatzbeschaffungsplan vorliegen, der für jede wichtige Komponente ausreichende Angaben über die Leistungsbeschreibung der Komponenten sowie Hersteller- und Lieferantenangaben enthält. Lassen sich für eine Komponente mehrere Hersteller oder Lieferanten benennen, so sind möglichst alle aufzuführen, um in Notfällen den schnellsten Lieferanten wählen zu können.

Lieferantenvereinbarungen
Viele Hardware-Anbieter bieten spezielle Verträge an, die eine zeitnahe Anlieferung von Ersatz-Hardware auch außerhalb der allgemein üblichen Geschäftszeiten garantieren. Die Vereinbarungen sollten Aussagen über die festgelegten Wiederanlaufzeiten enthalten. Falls ein solcher Vertrag abgeschlossen wird, sollte die geographische Risikoausbreitung beachtet werden. Benachbarte Institutionen können bei Katastrophen dem gleichen Krisen-Szenario ausgesetzt sein und benötigen möglicherweise die gleiche Hardware, so dass es zu Lieferengpässen trotz vertraglicher Vereinbarungen kommen kann. Bei hohen Verfügbarkeitsanforderungen sollten daher die Verträge zusätzliche Anlieferungswege vorsehen, z. B. per Schiff- oder Luftfracht. Es ist jedoch zu überprüfen, ob der Lieferant überhaupt in der Lage ist, Ersatzhardware von unterschiedlichen Standorten aus zu liefern.

A.5 Informationen

Informationen finden sich in Unternehmen und Behörden in Papierdokumenten, in elektronischen Daten, in den Köpfen der Mitarbeiter, in abgestimmten Vorgehensweisen oder auch in der Bauart von Produktionsanlagen. Für die Kontinuitätsoptionen werden die digital gespeicherten Informationen und Papierdokumente betrachtet.

Grundwerte der Informationssicherheit
Informationen nehmen eine Sonderstellung ein, daher sollten in die Kontinuitätsüberlegungen die klassischen Grundwerte der Informationssicherheit mit einfließen:

- Vertraulichkeit
  In einem Notfall kann nicht nur die Verfügbarkeit, sondern auch die Vertraulichkeit von Informationen gefährdet sein. So liegen beispielsweise bei einem Brand oftmals die Prioritäten auf dem Schutz von Personen und Gebäuden, nicht aber auf dem Schutz der Informationen. Daher könnte es passieren, dass vertrauliche Informationen bei Rettungsarbeiten auf der Strasse oder anderen Bereichen zwischengelagert werden, wodurch Unbefugte Zugriff darauf nehmen könnten. Ebenso muss sichergestellt sein, dass auch durch im Notfall kurzfristig eingesetztes Fremdpersonal kein unberechtigter Zugriff auf vertrauliche Informationen möglich ist.
- Integrität
  Durch einen Notfall kann auch die Integrität von Informationen bedroht sein. Eine nach einem Notfall wiedereingespielte Datensicherung kann eventuell Fehler enthalten. Besonders Datenbanken sind hierfür anfällig, wenn Transaktions-Logs nicht oder nicht vollständig mitgesichert wurden und folglich korrupte Datenbestände entstanden sind. Aber auch durch die Zerstörung von Papierdokumenten (z. B. durch Brand- oder Wasserschäden) können anschließend Lücken innerhalb der Dokumentation auftreten.
- Verfügbarkeit
  Im Notfall müssen Informationen, die Aufschluss über die Geschäftsprozesse der Institution und deren Wiederherstellungsprozesse geben, schnell verfügbar sein. Die Notfalldokumentation sollte deshalb durch geeignete Maßnahmen verfügbar gehalten werden, zum Beispiel indem sie redundant an verschiedenen Standorten vorrätig gehalten wird.

Datensicherung, Datenlagerung und Archivierung
Je nach Kritikalität der Datenbestände und der Verfügbarkeitsanforderungen, sind verschiedenen Anforderungen an die Datensicherung zu stellen.

Bei sehr kurzen Wiederaufsetzpunkten sind verschiedene Redundanz-Maßnahmen (siehe auch Baustein B 1.4 Datensicherungskonzept in [GSK]) sinnvoll, wie Mirror- oder Spiegelverfahren (Shadowing). Sie bieten auch synchrone bzw. asynchrone Datenübertragungen zu redundanten Standorten oder Speichersystemen. Weitere Optionen zur redundanten Datenhaltung, die auch dazu beitragen können, dass gesetzliche oder vertragliche Auflagen, die Anforderungen an die Archivierung von Informationen stellen, eingehalten werden, sind:

- Analoge Informationen
  Analoge Informationen wie Papierdokumente oder Mikrofilme können zum Beispiel kopiert werden und in ausgelagerten Lagerstätten aufbewahrt werden. Eine geeignete Maßnahme, um Papierdokumente redundant aufzubewahren, ist, diese zu digitalisieren und in elektronischen Archivsystemen zu speichern.
- Digitale Informationen
  Digitale Informationen können auf kostengünstige Speichermedien kopiert und anschließend ausgelagert werden. Dabei ist darauf zu achten, dass der Auslagerungsort so gewählt ist, dass er einerseits ausreichend weit vom Hauptstandort entfernt ist, aber nah genug, um die Daten innerhalb der festgelegten Wiederanlaufzeiten erreichen und wiederherstellen zu können. Archivräume für Datensicherungen sollten die gleichen Anforderungen erfüllen wie die Räumlichkeiten, in denen die Original-Daten verarbeitet werden.

A.6 Externe Dienstleister und Lieferanten

An vielen Stellen sind externe Dienstleister und Lieferanten so in die Geschäftsprozesse eingebunden, dass diese nicht wie vorgesehen durchgeführt werden können, wenn ein Dienstleister kurzfristig ausfällt. Dieses kann durch einen Notfall bedingt sein, aber auch durch Insolvenz des Dienstleisters oder kurzfristiger Kündigung des Vertrags, z. B. wegen unzureichender Leistung. Mögliche Kontinuitätsstrategien dafür sind:

- Transfer von externen zu internen Dienstleistungen
  Können Dienstleistungen, die durch Externe erbracht werden, auch durch internes Personal erbracht werden, kann ein kurzfristiger Transfer der Dienstleistung in die eigene Institution nützlich sein. Hierfür muss das interne Personal allerdings die notwendigen Kenntnisse besitzen und von anderen Aufgaben freigestellt werden, auch muss die notwendige Infrastruktur für die Prozesse vorhanden sein.
- Redundante und alternative Anbieter
  Dienstleistungen, die für die Fortführung des Geschäftbetriebs besonders kritisch sind, wie zum Beispiel Kommunikationsanbindungen oder die Energieversorgung, können durch die Nutzung von redundanten oder alternativen Anbietern mit gleicher Ausprägung gesichert werden. Hierbei ist die geographische Unabhängigkeit der Anbieter und Erfüllung der festgelegten Wiederanlaufzeit in die Entscheidung einzubeziehen.

Anhang B Präventive Maßnahmen

Zur Vorbeugung können Institutionen verschiedene Arten von Maßnahmen ergreifen. Einige dieser Möglichkeiten sind im Folgenden aufgezählt.

B.1 Meldetechnik

Für die Früherkennung von verschiedenen Gefahren existieren verschiedene Arten von automatisierten Gefahrenmeldetechniken. Hierzu gehören beispielsweise Rauch-, Brand-, Wasser- oder Einbruchmelder.

Automatisierte Meldetechnik hat zur Aufgabe, etwaige Parameter, die in einem direkten oder indirekten Zusammenhang mit einem Schadensereignis stehen, so früh wie möglich zu erfassen und weiterzumelden, um rechtzeitige Abwehrmaßnahmen gegen die Ursachen einleiten zu können. Das erkannte Ereignis wird dann an eine zentrale Stelle, z. B. eine Leitstelle in der Institution oder einem Dienstleister, gemeldet. Je nach Art der Gefahr kann auch eine Alarmierung der direkten Umgebung sinnvoll sein, beispielsweise bei Feuer.

Bei der Konzeption der Meldetechnik sollte das Ziel verfolgt werden, die Wahrscheinlichkeit einer Entdeckung zu erhöhen, den Zusammenhang zwischen Meldungen und auslösenden Ereignissen schnell zu erkennen und gegebenenfalls ein abgestuftes Reaktionsverfahren für die verschiedenen Bereiche zu ermöglichen. Die Meldetechnik sollte daher die folgenden drei Bereiche einschließen:

- Freigelände-Überwachung
  Das Freigelände kann durch drei wesentliche Sensorenarten überwacht werden. Dazu gehören die Liniensensoren (zum Beispiel Infrarotüberwachung, hermetische Videoüberwachung), Zaunmelder und Bodensensoren (zum Beispiel Erschütterungsmelder).
- Innenraum-Überwachung
  Die Innenraumüberwachung sichert den Bereich von der Gebäude-Außenhaut bis zum eigentlichen Schutzobjekt ab. Die Anforderungen für die jeweiligen zu überwachenden Bereiche sollten dokumentiert und mit den einzurichtenden Meldesensoren erfüllt werden.
- Objekt-Überwachung
  Einzelne Objekte erfordern eine individuelle Überwachung, wie beispielsweise Serverschränke auf Temperaturänderungen oder IT-Komponenten auf ihre Performanz.

Meldesysteme sind speziell den jeweiligen Überwachungsaufgaben bezüglich Einsatzort, Funktion und Anforderung zugeordnet. Vor Einrichtung eines Meldesystems sollten daher folgende Punkte berücksichtigt werden:

- Umgebungsparameter
- Energieversorgung
- Störeinflüsse
- Überwindbarkeit
- Bedien- und Wartungsfreundlichkeit

Eine Gefahrenmeldeanlage (GMA) besteht aus einer Vielzahl lokaler Melder, die mit einer Zentrale kommunizieren, über die auch der Alarm ausgelöst wird. Ist eine Gefahrenmeldeanlage für Einbruch, Brand, Wasser oder auch Gas vorhanden, sollten zumindest die Kernbereiche der Institution in die Überwachung mit eingebunden werden, damit Gefährdungen frühzeitig erkannt und Gegenmaßnahmen eingeleitet werden können. Die Meldungen müssen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, etc.) weitergeleitet werden. Dabei muss sichergestellt sein, dass diese Stelle auch in der Lage ist, technisch und personell auf den Alarm zu reagieren.

Eine Gefahrenmeldeanlage ist ein komplexes Gesamtsystem, das einerseits an die Gebäude sowie die einzelnen Geschäftsprozesse angepasst und andererseits im Hinblick auf die zu erwartenden Risiken der jeweiligen Institution geplant und installiert werden muss.

Die Übertragung von Alarmen sollte an eine zentrale Leitstelle erfolgen. Zur Unterstützung dieser Leitstelle ist ein Leit- und Kommunikationssystem in der Institution zu integrieren. Je nach den installierten Überwachungssensoren und äußeren Parametern sollten die Mitarbeiter in der Leitstelle einer Institution auf die folgenden technischen Einrichtungen zugreifen können:

- Lageplan aller Melder
- Monitore der Videoüberwachung
- Rechner mit großen Displays für die Protokollierung, um eine geringere Fehleranfälligkeit beim Ablesen von Informationen in der Stresssituation zu gewährleisten
- Telefon- und Faxanbindung
- Eventuell Telefonanlage mit Direktschaltung zu Sicherheitskräften (Feuerwehr, Polizei)
- Funk-Basisstation mit direkter Anbindung an mobile Einsatzgeräte der Sicherheitskräfte (Reserve-Funkgeräte für zusätzliche Sicherheitskräfte im Notfall)
- Archiv für Pläne, Zeichnungen und objektspezifische Unterlagen (Liegenschaftspläne)

Um zukünftige Maßnahmen zu planen und deren Wirksamkeit zu messen, ist eine ausführliche Dokumentation von Sicherheitsvorfällen bzw. Meldungen innerhalb der Meldetechnik notwendig. Diese Informationen können sowohl über Personen (durch Rundgänge oder ähnliches) als auch über Informationssysteme erhoben werden. Zu den zu dokumentierenden Informationen gehören:

- Aktuelle Statusmeldungen durch Personen oder Sensoren
- Berichte über Schadensereignisse und Schadensbearbeitung
- Alarmmeldungen
- Angeordnete Maßnahmen zur Reaktion
- Objekt- und funktionsbezogene Hilfsinformationen (zum Beispiel Pläne und Checklisten)

Außerdem sollten historische Referenzdaten aus vergangenen Schadensereignissen dokumentiert werden, um Erkenntnisse aus vergleichbaren Vorfällen ziehen zu können.

B.2 Datensicherung

Informationen stellen einen wichtigen Wert für jede Institution dar, egal ob sie analog oder digital vorliegen. Wenn materielle Ressourcen zerstört oder unbrauchbar werden, können sie in den meisten Fällen durch Lieferanten, externe Dienstleister oder andere Beschaffungswege wiederhergestellt werden. Dagegen sind die auf Datenträgern gespeicherten Informationen als individuelles Gut für immer verloren, wenn die Datenträger zerstört oder beschädigt werden. Deshalb ist es notwendig, spezielle Maßnahmen zur Sicherung der Daten zu implementieren.

Wie im Baustein B 1.4 *Datensicherungskonzept* der IT-Grundschutz-Kataloge [GSK] beschrieben, ist es erforderlich, innerhalb einer Institution entsprechende Datensicherungskonzepte zu erstellen.

B.3 Vereinbarungen mit externen Dienstleistern

Wurde als eine Kontinuitätsstrategie festgelegt, bei der Notfallbewältigung zur Unterstützung auf kommerzielle Anbieter von Notfall-Dienstleistungen zuzugreifen, so sind bei deren Auswahl und Vertragsgestaltung ähnliche Kriterien wie beim Outsourcing zu beachten. Die wesentlichen Punkte hierfür sind in den IT-Grundschutz-Katalogen [GSK] in Baustein B 1.11 *Outsourcing* beschrieben.

Es gibt eine Vielzahl von Dienstleistungen, die zur Vorbereitung auf einen Notfall angeboten werden. Dazu gehört z. B. der Betrieb eines Ausweich-Rechenzentrums, einzelner Applikationen oder IT-Komponenten, es können aber auch Ausweich-Arbeitsplätze oder geschultes Personal für bestimmte Bereiche zur Verfügung gestellt werden. Wenn die Institution sich zur Inanspruchnahme von Notfall-Dienstleistungen entschieden hat, müssen zunächst die wesentlichen Anforderungen an diese festgelegt werden. Diese Anforderungen bilden die Basis für die Auswahl geeigneter Anbieter.

Es ist deshalb wichtig, innerhalb des Prozesses zur Anbieter-Auswahl geeignete Prüfungspunkte zu erarbeiten. Auf dieser Basis sollten anschließend Verträge mit denjenigen Dienstleistern abgeschlossen werden, die alle diese Kriterien erfüllen.

Hierzu sollten zunächst Angebote von unterschiedlichen Anbietern eingeholt werden. Hierfür sollten die Eckpunkte des geplanten Auftrags in einem Anforderungsprofil und einem darauf aufbauenden Pflichtenheft skizziert werden. Dieses Pflichtenheft bildet später die Basis für die Bewertung und Auswahl der angebotenen Dienstleistungen. Hieran orientieren sich auch alle zukünftigen vertraglichen Vereinbarungen. Es ist deshalb notwendig, detaillierte Informationen über die erwartetenden Leistungen aufzulisten. Damit gewährleistet ist, dass die vereinbarten Leistungen alle kritischen Geschäftsprozesse vollständig abdecken, müssen alle relevanten Organisationseinheiten und Rollen in die Abstimmung des Pflichtenhefts eingebunden werden. Diese Organisationseinheiten und Rollen können zum Beispiel sein:

- Gebäudemanagement
- Verantwortliche für die Notfallplanung
- Mitarbeiter der Informationstechnik
- Beschaffung und Einkauf
- Rechtsabteilung

Es wird empfohlen, Fragenkataloge zusammenzustellen, die die Anforderungen an einen Dienstleister auflisten. Dabei sollten zum Beispiel folgende Punkte aufgenommen werden:

- Erfahrungsgebiete, Größe und Standort des Anbieters
- Referenzen des Anbieters
- Qualitätsnachweise bzw. eine Zertifizierung, z. B. nach ISO 27001 auf Basis von IT-Grundschutz
- Service und Unterstützung innerhalb des Notfallmanagementprozesses/-bewältigung
- Test- und Übungsmöglichkeiten
- Initiale Kosten, jährliche Kosten, Kosten bei Inanspruchnahme, Kosten für Beteiligung an Tests und Übungen
- Anpassungsfähigkeit des Anbieters an die Gegebenheiten des Auftraggebers
- Ressourcenbedingte Anforderungen (garantierte Zeitfenster, Reaktionszeiten etc.)
- Kommunikationsschnittstellen
- Fundiertes Sicherheits- und Notfallvorsorgekonzept des Anbieters
- Prüfmöglichkeiten der eigenen Revision

Das Anforderungsprofil hängt stark davon ab, welche Art von Notfall-Dienstleistungen genutzt werden sollen. Daher sind die Bewertungskriterien an die speziellen Gegebenheiten anzupassen und individuell zu gewichten.

Nachdem die Entscheidung für einen der Anbieter getroffen wurde, sollten alle für das Notfallmanagement relevanten Kriterien vertraglich zugesichert werden. In diesem Vertrag müssen auch die genauen Modalitäten der Zusammenarbeit geklärt sein, z. B. Ansprechpartner, Vertreterregelung, Reaktionszeiten, IT-Anbindung, Kontrolle der Leistungen, Ausgestaltung der IT-

Sicherheitsvorkehrungen, Umgang mit vertraulichen Informationen, Verwertungsrechte, Dokumentationsverpflichtung, Weitergabe von Information an Dritte.

B.4 Festlegung von Ausweichstandorten und deren Anforderungen

Während der Planungen im Rahmen der Notfallvorsorge sind für einige Szenarien einer oder mehrere Ausweichstandorte, sowohl für die Büro- oder Produktionsgebäude, als auch für den IT-Betrieb, auszuwählen.

Bei der Erstellung des Notfallvorsorgekonzepts sind mindestens die nachfolgenden Punkte zu berücksichtigen:

- Erreichbarkeit des Ausweichstandortes (Verkehrsmittel und –wege) und gegebenenfalls Transport der Mitarbeiter zum Ausweichstandort
- Ausstattung des Standortes (Platzbedarf, Infrastruktur, Sicherungsmaßnahmen wie zum Beispiel Zutrittsschutz)
- Kommunikationswege und –mittel (Wie viele Telefonkanäle werden benötigt? Wer schaltet die Telefone bzw. Faxgeräte um? Wie viele Telefon- und Faxanschlüsse und -geräte müssen mindestens vorgehalten werden?)
- Netzanbindung des Standortes (z. B. WAN-Anbindung an ein eigenes Rechenzentrum oder IT-Anbindung über Internet). Hierbei ist unter anderem die Bandbreite, IP-Adressen, Sicherheitsmaßnahmen wie Art und Konfiguration des Firewall-Systems, etc. zu klären.
- Erreichbarkeit der Mitarbeiter und deren Vertreter am Ausweichstandort und/oder zuhause (Telefon-, Handynummern, E-Mail)
- Maßnahmen und Verantwortlichkeiten zur Inbetriebnahme des Ausweichstandorts, so dass der Ausweichstandort in der geforderten Zeit bezugs- und funktionsfähig ist
- Maßnahmen und Verantwortlichkeiten zum Rückbau des Ausweichstandorts nach Bewältigung eines Notfalls, also wer dafür zuständig ist und wie der Ausweichstandort in den Zustand versetzt wird, den er vor dem Bezug hatte. Hierzu gehört z. B. das Zurückschalten der Telefone oder das Umleiten von IP-Adressen.

Anhang C Gliederung Notfallhandbuch

Ein Notfallhandbuch ist so zu gestalten, dass ein sachverständiger Dritter in der Lage ist, die im Handbuch spezifizierten Notfallmaßnahmen durchzuführen. Nachfolgend wird beispielhaft ein Inhaltsverzeichnis eines Notfallhandbuchs zur Orientierung aufgeführt. Welche Teile dieses Vorschlags übernommen werden können, ist abhängig von der vorhandenen System- und Anwendungsdokumentation und kann daher nur individuell entschieden werden.

Hinweis: Ein sinnvoller Aufbau und die Gliederung eines Notfallhandbuchs für eine Institution ist von deren Größe und der Struktur abhängig. Dieses Beispiel kann lediglich als Anregung dienen und muss an die jeweiligen Bedingungen der Institution angepasst werden.

1 Einleitung

- 1.1 Allgemeine Informationen: Name der Organisation, Geltungsbereich, etc.
- 1.2 Dokumentenkontrolle: Version, Verteiler, Festlegung des Dokumentverantwortlichen, Klassifizierung des Dokuments, etc.
- 1.3 Abkürzungsverzeichnis
- …

2 Sofortmaßnahmen

- 2.1 Konkrete Aufgaben für einzelne Personen/Rollen im Notfall
- 2.2 Handlungsanweisungen für spezielle Notfälle
- …

3 Krisenmanagement

- 3.1 Rollen, Zuständigkeiten und Kompetenzen
- 3.2 Meldewege und Eskalation
- 3.3 Krisenstabsraum / Lagezentrum
  - 3.3.1 Standorte, Erreichbarkeiten. …
  - 3.3.2 Vorbereitung des Notfalltreffpunkts
  - …
- 3.4 Krisenstabsarbeit
- 3.5 Lagebeurteilung
- 3.6 Dokumentation im Krisenstab
- 3.7 Deeskalation
- 3.8 Analyse und Bewertung der Notfallbewältigung

4 Kommunikation und Öffentlichkeitsarbeit im Krisenfall

- …

5 Wiederherstellung

- 5.1 Wiederherstellung der Bürofläche
- 5.2 Wiederherstellung der Infrastruktur
- 5.3 Wiederherstellung der IT
- 5.4 Wiederherstellung der Kommunikationsanbindungen
- …

6 Geschäftsfortführung

- 6.1 Verfügbarkeitsanforderungen der Organisationseinheiten
- 6.2 Geschäftsfortführungspläne
  - 6.2.1 Organisationseinheiten Kritikalität A
  - 6.2.2 Organisationseinheiten Kritikalität B
  - 6.2.3 Organisationseinheiten Kritikalität C
  - …
- 6.3 Analyse des Wiederanlaufs und der Wiederherstellung
- …

7 Anhang

- 7.1 Erreichbarkeit der Notfallteam-Mitarbeiter
- 7.2 Notrufnummern (z. B. Feuerwehr, Polizei, Notarzt, Wasser- und Stromversorger, Ausweich-Rechenzentrum, externes Datenträgerarchiv, externe Telekommunikationsanbieter)
- 7.3 Weitere/unterstützende Pläne und Listen

Anhang D Gliederung Geschäftsfortführungsplan

Als Beispiel wird im Folgenden ein mögliches Inhaltsverzeichnis eines Geschäftsfortführungsplans aufgeführt. Abhängig vom Aufbau der Institution und der Geschäftsprozesse muss individuell entschieden werden, welche Teile dieses Vorschlags übernommen werden.

1 Einleitung

- Allgemeine Informationen: Name der Organisation, Name des Plans, Ziel des Plans, Geltungsbereich, etc.
- Aktivierung und Deaktivierung des Plans
- Dokumentenkontrolle: Version, Verteiler, Festlegung des Dokumentverantwortlichen, Klassifizierung des Dokuments, etc.
- Abkürzungsverzeichnis
- Relevante und zugehörige Dokumente

2 Notbesetzung der Organisationseinheit

- Verantwortlicher
- Notfallteams, Pflichten und Kompetenzen
- Alarmierung und Eskalation

3 Wiederanlauf der Geschäftsprozesse

- Wiederanlaufstrategie
- Wiederanlaufziele und maximale Dauer des Notbetriebs
- Ressourcenanforderungen der Prozesse
- Alternativen für Not- und Alternativbetrieb
- Rückführung
- Nacharbeiten

4 Szenarien

- Szenario "Ausfall eines Standorts"
  - Anforderungen an den Ausweichstandort
  - Am Ausweichstandort benötigte Ressourcen
  - Reaktive Maßnahmen für den Wiederanlauf
  - Änderungen an Arbeitsabläufen im Notbetrieb
  - Maßnahmen zur Wiederherstellung und Rückführung in den Normalbetrieb
  - …
- Szenario "Ausfall Informationstechnologie"
  - Folgeszenarien
  - Anforderungen an den Notbetrieb
  - „Betrachtung der jeweiligen Anwendung / des jeweiligen Systems“
  - Ersatzbeschaffungsplan
  - …

- Szenario "Ausfall von Personal"
    - Folgeszenarien
    - Anforderungen an den Notbetrieb
    - Reaktive Maßnahmen für den Wiederanlauf
    - Änderungen an Arbeitsabläufen im Notbetrieb
    - Maßnahmen zur Wiederherstellung und Rückführung in den Normalbetrieb
- Szenario "Ausfall eines Dienstleisters"
    - Folgeszenarien
    - Reaktive Maßnahmen für den Wiederanlauf
    - Änderungen an Prozessabläufen im Notbetrieb
    - Maßnahmen zur Wiederherstellung und Rückführung in den Normalbetrieb

…

5 Zusatzinformationen

- Standorte
- Anfahrtspläne
- …

6 Kontaktinformationen

- Mitarbeiterlisten
- Dienstleister
- …

7 Anhang

- Formulare, Vorlagen, Checklisten

Referenzdokumente

Dankesworte

Bei der Entwicklung des Leitfadens wurde das Bundesamt für Sicherheit in der Informationstechnik durch Experten aus der Praxis unterstützt. Es sei allen gedankt, die dieses Werk ermöglicht und begleitet haben.

Der BSI-Standard 100-4 basiert auf einem Entwurf, der von der Firma HiSolutions AG im Auftrag des BSI erstellt wurde. Es sei hiermit den Autoren Robert Kallwies, Timo Kob, Stefan Nees und Björn Schmelter gedankt, die dieses Werk mit ermöglicht haben.

Wir danken außerdem folgenden Experten und Institutionen, die mit ihren Beiträgen, ihrer Unterstützung bei der Qualitätssicherung und hilfreichen Diskussionen diesem Standard wesentliche Impulse gegeben haben. Ihnen gebührt besonderer Dank, da ihr Engagement die Entstehung und Weiterentwicklung des BSI-Standards erst ermöglicht hat.

- Thomas Bittl, Bundesanstalt für Post und Telekommunikation
- consequa GmbH
- Ulrich Dreyer, 3R-Kontext
- Ingo Geisler, Vodafone D2 GmbH
- Matthias Hämmerle, KPMG AG
- Dr. Armin Hampel, Hewlett-Packard GmbH
- Dr. Wolfgang Mahr, Axept AG
- Michael Müller, KPMG AG
- Uwe Naujoks, UKN Management Consulting
- Markus Riedl, Bayer. Staatsministerium des Innern
- Thomas Teichmann, Schmitz & Teichmann Betriebsberatung GmbH
- Astrid Wiesendorf, Vodafone D2 GmbH

An der Erstellung des BSI-Standards 100-4 waren folgende Mitarbeiter des BSI beteiligt: Dr. Marie-Luise Moschgath, Isabel Münch, Dr. Harald Niggemann.