IT-Notfallplan

Cyber

MARKEL

VORWORT UND BEARBEITUNGSHINWEISE

Institutionen – Unternehmen, aber auch sonstige Einrichtungen – müssen bei internen IT-Notfällen, wie z. B. bei Hackerangriffen, Datenrechtsverletzungen oder Bedienfehlern am Computersystem, weiter ihre Kernaufgaben erfüllen und können schneller und effektiver auf Notfälle reagieren, wenn sie sich hinreichend auf Ausnahmesituationen vorbereitet haben. Hierbei helfen beispielsweise folgende Fragen:
Was kann präventiv getan werden, damit Institutionen IT-Notfälle möglichst unbeschadet überstehen?
Was ist zu tun, um bei der Unterbrechung wichtiger Prozesse deren raschen Wiederanlauf und die Wiederherstellung der Systeme, Anwendungen oder Daten zu bewerkstelligen?
Was sind überhaupt die kritischen Ressourcen und Prozesse einer Institution?

Zur Beantwortung derartiger Fragen trägt der BSI-Standard 100-4 bei. Er beschreibt eine Vorgehensweise für die Einführung, den Betrieb und die kontinuierliche Verbesserung eines Notfallmanagements in einer Institution. Für die in den jeweiligen Phasen anstehenden Aufgaben wird eine Fülle von Empfehlungen gegeben.

Das Notfallmanagement beinhaltet die benötigten Prozeduren, Informationen sowie die erforderlichen Reaktionsmaßnahmen, die nach Eintritt eines IT-Notfalls bis zur Wiederaufnahme des Geschäftsbetriebs erforderlich sind.

Ziel eines IT-Notfallplans ist es, eine dokumentierte Vorgehensweise bzw. Hilfestellung für alle Phasen der Notfallbewältigung bereitzustellen, mit deren Unterstützung eine Institution einen Notfall bewältigen und ihre kritischen Geschäftsprozesse fortführen kann. Der IT-Notfallplan sollte so aufgebaut sein, dass er schnelle und eindeutige Handlungsanweisungen bietet. Er dient primär als strukturierter Handlungsleitfaden zur Bewältigung eines IT-Notfalls unter Leitung eines Notfallstabs.

Das vorliegende Muster wird Ihnen als Dokumentvorlage zur Erstellung Ihres eigenen IT-Notfallplans zur Verfügung gestellt. Die Grundlage des Muster-IT-Notfallplans ist das Modul „Notfallhandbuch“ des Umsetzungsrahmenwerks zum Notfallmanagement nach dem BSI-Standard 100-4. Dieses wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben. Alle hierzu vom BSI angebotenen Hilfestellungen und Dokumentvorlagen lassen sich ebenfalls über die Webseiten des BSI abrufen.

Der BSI-Standard 100-4 beschreibt ein umfangreiches Notfallmanagement und umfasst damit deutlich mehr Elemente als dieses Muster eines IT-Notfallplans, das sich auf mögliche Szenarien im Zusammenhang mit dem Ausfall von IT-Infrastruktureinrichtungen und Gefahren bei der Nutzung von IT-Systemen beschränkt. Notfälle durch andere Gefahren, die auch Auswirkungen auf die IT-Infrastruktur haben können, wie Feuer oder Überschwemmung, werden hier nicht betrachtet. Für ein ganzheitliches Notfallmanagement empfehlen wir Ihnen aber, auch andere Gefahren in Ihrem Risikomanagement zu berücksichtigen.

Bei der Nutzung dieser Vorlage sind zudem die folgenden Hinweise zu beachten:

- Das Kapitel „Vorwort und Bearbeitungshinweise“ dient der Erläuterung und Einführung in den Muster-IT-Notfallplan und ist bei Übernahme dieser Dokumentvorlage zu entfernen.
- Der Muster-IT-Notfallplan dient lediglich als Anregung und muss zwingend an die jeweiligen Bedingungen der Institution angepasst werden.
- Beschreibungen, Funktionsbezeichnungen, Namen etc. sind den konkreten Verhältnissen der Institution anzupassen.

- Verweise auf andere Kapitel innerhalb dieses Musters sind bei Verwendung der Dokumentvorlage zu überprüfen und anzupassen.
- Erläuternde Texte in den jeweiligen Abschnitten sind kursiv gedruckt. Diese Erläuterungen sollten im fertiggestellten Dokument entfernt werden.
- Die Begrifflichkeit „Computersystem“ umfasst in diesem Dokument die direkt oder indirekt miteinander verbundene Gesamtheit von informations- und telekommunikationstechnischen Geräten und Bauteilen, einschließlich der darauf befugt gespeicherten Programme und sonstigen Daten.
- Aus Gründen der besseren Lesbarkeit wird im vorliegenden Muster-IT-Notfallplan auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für beide Geschlechter.
- **Wichtiger Hinweis:** Dieser Muster-IT-Notfallplan dient nur zur Unterstützung/zu Informationszwecken und enthält/berücksichtigt keine rechtlichen Belange. Die Markel Insurance SE übernimmt daher keinerlei Haftung für die Inhalte der Mustertexte. Dieser Muster-IT-Notfallplan überträgt keine Rechte an den Besitzer dieses Dokuments und sonstige Dritte.

Dokumentinformationen			
Klassifikation:			
Versionsnummer:			
Dokumenttitel:			
Dokument-verantwortlicher:			
Erstellt am:		**Erstellt von:**	
		Funktion des Erstellers:	
Letzte Überarbeitung:		**Nächste Überarbeitung:**	
Freigabe am:		**Freigabe von:**	

Berechtigte Rolle (Dokumentverteiler) Bitte die Rolle/Funktionsbezeichnung angeben

Versionsverlauf			
Datum	**Version**	**Beschreibung**	**Verändert durch**

Mitgeltende Dokumente Bitte mitgeltende Dokumente eintragen
z. B. betriebliche Richtlinie/Anweisungen (Ersthelfer, Meldezentrale, Notarzt), siehe Kapitel 2.1

INHALTSVERZEICHNIS

1. Einleitung

1.1 Leitlinie IT-Notfallmanagement

In diesem Kapitel werden die Leitgedanken der Unternehmensführung zur Wichtigkeit einer funktionierenden Informationstechnik für das Unternehmen benannt.

Beispieltext

Die Geschäftsführung der ist sich bewusst, dass der kurz- und langfristige Geschäftserfolg in hohem Maße von der einwandfreien Funktion der gesamten IT-Infrastruktur abhängt. Zur Gewährleistung dieses Zieles ist es notwendig, bei Ausfällen der IT-Infrastruktur oder von IT-Prozessen die Auswirkungen auf die Geschäftstätigkeit so gering wie möglich zu halten. Aus diesem Grund hat sich die Geschäftsführung dazu entschlossen, ein IT-Notfallhandbuch zu entwickeln, das die Abläufe und Zuständigkeiten während der Bewältigung eines IT-Notfalls regelt.

1.2 Allgemeine Informationen

In diesem Kapitel sind die Funktion, die Struktur und das Ziel der Notfallbewältigung für die jeweilige Institution zu beschreiben und ist auf ergänzende oder mitgeltende Dokumente hinzuweisen.

Beispieltext

Das Notfallhandbuch soll die Verantwortlichen der in die Lage versetzen, wieder den Normalbetrieb zu erreichen, ggf. mit dem Zwischenschritt eines stabilen Notbetriebs. Es dient als ein strukturierter Handlungsleitfaden zur Bewältigung des Notfalls unter Leitung eines Notfallstabs.

- Dieses Notfallhandbuch betrachtet vorrangig Notfälle, die durch sachschadenunabhängige Ereignisse entstanden sind, d. h. insbesondere:
- IT-Sicherheitsvorfälle (mit und ohne Erpressung)
- Datenschutzvorfälle
- Ausfall der Stromversorgung
- Ausfall der Telefon- oder Internetanbindung
- Ausfall von externen IT- oder Cloud-Dienstleistungen
- Bedienfehler der eigenen Mitarbeiter an der unternehmenseigenen IT-Infrastruktur

1.3 Komponenten des Notfallhandbuchs

In diesem Kapitel werden zur schnellen Orientierung die wichtigsten Elemente des Notfallhandbuchs aufgelistet.

Beispieltext

- Sofortmaßnahmen zur unmittelbaren Abwehr von Gefahren
- Beschreibung der Notfallorganisation
- Regelungen für die interne und externe Kommunikation
- Beschreibung der Wiederherstellung von Ressourcen
- Kontaktadressen von allen internen und externen Personen und Institutionen, die zur Bewältigung des Notfalls benötigt werden könnten

1.4 Geltungsbereich

Das Notfallhandbuch kann bei einer zentralen oder relativ einheitlichen IT-Organisation für das ganze Unternehmen gelten. Wenn sich die IT-Infrastrukturen oder IT-unterstützte Prozesse jedoch von Standort zu Standort stark unterscheiden, könnte es dagegen sinnvoll sein, wenn es spezifische Notfallhandbücher für einzelne Standorte oder sogar Organisationseinheiten gibt.

Beispieltext

Das Notfallhandbuch ist gültig für alle Mitarbeiter der . Die im Handbuch beschriebenen Aspekte beziehen sich auf den Standort .

1.5 Definitionen

Es sollten die wesentlichen Begrifflichkeiten im Notfallhandbuch definiert sein, deren Verständnis für eine geordnete Notfallbewältigung bei allen Beteiligten vorausgesetzt wird. Sofern die Begriffe „Störung" oder „Notfall" bereits in anderen Notfallhandbüchern definiert wurden, sollten die Definitionen im IT-Notfallhandbuch übernommen werden.
Weitere relevante Begriffe sind bei Bedarf selbstständig durch die Institution zu ergänzen. Die Definition muss klar und leicht verständlich für den Leser beschrieben sein.

1.5.1 Definition „Störung"

Es ist zu definieren, was in der Institution unter einer Störung zu verstehen ist. Zusätzlich ist zu erklären, was in der Institution unter einer Störungsbewältigung und -eskalation verstanden wird.

Beispieltext

Eine Störung ist eine Situation, in der bestimmte Bereiche, Prozesse oder Ressourcen der nicht wie vorgesehen funktionieren, sodass hierdurch Schäden entstehen können. Diese werden aber nicht als schwerwiegend eingestuft, da sie im Verhältnis zum Gesamtjahresergebnis zu vernachlässigen sind. Eine Störung ist ein Ereignis, dessen Schaden ohne ein Hinzuziehen von Strukturen des IT-Notfallmanagements im Regelfall vom IT-Helpdesk oder IT-Dienstleister im Tagesgeschäft innerhalb der definierten kritischen Wiederanlaufzeiten behoben werden kann. Die Pläne zur Störungsbewältigung sowie die Behebung von Störungen liegen in der Verantwortung der jeweiligen Geschäftsbereiche.

Alle Ereignisse, die von Anfang an nicht als Notfall bewertet werden, stellen Störungen dar. Störungen können jedoch schnell zu einem Notfall eskalieren und sind deshalb genau zu beobachten und zeitnah zu beheben. Bei Störungen mit Notfallpotenzial ist der Notfallbeauftragte zeitnah in Kenntnis zu setzen.

1.5.2 Definition „Notfall"

Es ist zu definieren, was in der Institution unter einem Notfall zu verstehen ist. Zusätzlich ist zu erklären, was in der Institution unter einer Notfallbewältigung und -eskalation verstanden wird.

Beispieltext

Ein Notfall ist eine Situation, in der wesentliche Bereiche, Prozesse oder Ressourcen der nicht wie vorgesehen funktionieren oder deren Verfügbarkeit innerhalb der geforderten Zeit nicht wiederhergestellt werden kann. Dadurch können sehr hohe Schäden entstehen, die sich signifikant auf das Gesamtjahresergebnis oder die Aufgabenerfüllung auswirken können. Ein Notfall kann ohne ein Hinzuziehen von Strukturen des IT-Notfallmanagements nicht bzw. nicht mehr in der Art und Weise behoben werden, wie es für den Fortbestand der günstig wäre.

Alle Ereignisse mit Auswirkungen oberhalb einer Störung stellen Notfälle dar.

Ein Notfall wird durch die reaktive Notfallorganisation außerhalb des Tagesgeschäfts abgewickelt. Hierzu koordiniert ein Notfallstab alle Maßnahmen zur Notfallbewältigung.

1.5.3 Definition „Stabiler Notbetrieb“

Der stabile Notbetrieb ist eine Betriebsweise, die es der Institution ermöglicht, die Bedürfnisse der wichtigsten internen oder externen Kunden auf einem Leistungsniveau zu befriedigen, bei dem keine oder nur eine geringe Gefahr besteht, dass Aufträge oder Kunden in nennenswertem Ausmaß verloren gehen.
Abhängig von der Wichtigkeit des betroffenen Prozesses für den Unternehmenserfolg wird der stabile Notbetrieb bei 50 bis 70 % des Normalbetriebs angesetzt.

Beispieltext

Falls die vollständige Funktionsfähigkeit der IT-Infrastruktur inklusive der sie umgebenden Sicherheits- und Managementprozesse nicht in einem Schritt erreichbar ist, soll der stabile IT-Notbetrieb als Zwischenstufe angestrebt werden. Dieses Betriebsniveau stellt sicher, dass die Lieferfähigkeit der bezüglich der wichtigsten internen und externen Kundenaufträge weitestgehend erhalten wird.
Der stabile Notbetrieb der folgenden IT-Prozesse liegt bei:

- Warenwirtschaftssystem %
- Callcenter %

2 Sofortmaßnahmen

2.1 Grundsätze

Sofortmaßnahmen dienen dem Ziel – nachdem ein Schadenereignis erkannt worden ist –, weiteren Schaden von der Institution abzuwenden und eine schnellstmögliche Wiederaufnahme der kritischen Geschäftsprozesse durch die reaktive Notfallorganisation sicherzustellen.
Die Sofortmaßnahmen sind grundsätzlich von jeder Person, die ein Schadenereignis bemerkt, auszuführen. Damit auch Personen ohne Kenntnisse im Notfallmanagement je nach Situation die erforderlichen Sofortmaßnahmen einleiten können, sollten diese im Notfallhandbuch klar und leicht verständlich beschrieben sein.

Beispieltext

Bei Gefahr für Leib und Leben sind ZUERST:

- Maßnahmen zu ergreifen, um die Unfall- oder Gefahrenstelle zu sichern,
- ggf. betroffene Personen mit Maßnahmen der Ersten Hilfe zu versorgen und
- das Ereignis entsprechend der betrieblichen Richtlinie/Anweisung XXX (Ersthelfer, Meldezentrale, Notarzt) zu melden.

Besteht die Gefahr, dass infolge eines Angriffs oder einer Fehlmanipulation die Funktionsfähigkeit des IT-Systems Schaden nimmt, ist der Mitarbeiter aufgefordert, eigenständig „spezielle Sofortmaßnahmen“ durchzuführen.

Bei allen anderen Ereignissen erfolgt eine Meldung an .

2.2 Meldung eines Ereignisses und Eskalation

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

Beispieltext

Alle Mitarbeiter der sind aufgefordert, jede Störung bei Anwendungen der informations- und telekommunikationstechnischen Systeme oder jedes anormale/merkwürdige Verhalten der IT-Infrastruktur an zu melden. Diese Meldung hat auch zu erfolgen, wenn Mitarbeiter von Externen (z. B. Dienstleistern) Informationen entgegennehmen, die auf eine Störung hindeuten.

Ist nicht verfügbar und es besteht gleichzeitig der Verdacht, dass es sich um ein notfallrelevantes Ereignis handelt, ist oder ggf. dessen Stellvertreter zu alarmieren.

Die Kontaktdaten der genannten Meldestelle(n) befinden sich im Anhang.

prüft, welche Anwendungen und Technologien von dem gemeldeten Ereignis betroffen sind. bzw. sind unverzüglich zu informieren, wenn

- die Wahrscheinlichkeit besteht, dass die in Kapitel 4.1 aufgelisteten wichtigen IT-Anwendungen und IT-Systeme betroffen sein können, oder
- sich der Verdacht erhärtet, dass die Auswirkungen des Ereignisses anderweitig einen Notfall auslösen können.

Kommt bzw. nach erneuter Betrachtung des Ereignisses und der möglichen Folgen zu dem Schluss, dass es sich um einen Notfall handelt, ist unverzüglich die Geschäftsführung zu unterrichten.

Die Entscheidung, ob ein IT-Notfall ausgerufen und der Notfallstab eingesetzt wird, wird nach Beratung mit dem Notfallbeauftragten von getroffen. Ist die Geschäftsführung in angemessener Zeit nicht erreichbar, entscheidet bzw. .

2.3 Beschaffung von Zugangsdaten

Sind für die Durchführung von besonderen Sofortmaßnahmen geschützte Zugangsdaten notwendig, sind diese auf folgendem Weg zu beschaffen.

Beispieltext

Sind zur Wiederherstellung von IT-Systemen Medien oder Passwörter notwendig, sind folgende Personen zur Herausgabe anzusprechen:

Für IT-System	Name, Vorname	Telefon dienstlich
z. B. Back-up-Datenträger		
z._B. Passwörter für		
z._B. Bankschließfach		

2.4 Spezielle Sofortmaßnahmen

Hier sind die Sofortmaßnahmen für bestimmte Gefahrensituationen zu beschreiben, die jeder Mitarbeiter unverzüglich durchführen soll, um den Schaden für die Institution zu minimieren.
Zu den speziellen Sofortmaßnahmen gehören auch Hinweise für IT-Fachleute, welche Maßnahmen durchzuführen bzw. ggf. zu unterlassen sind, um forensische Analysen zu ermöglichen.

2.4.1 Grundlegende Verhaltensweisen für

Beispieltext

Zur Erhaltung der Möglichkeit einer forensischen Analyse sind folgende Verhaltensregeln zu beachten:

Nr.	Aktivität
1	Verbindungen des Unternehmensnetzwerks nach außen trennen
2	Auf KEINEN Fall die betroffenen IT-Systemen von der Stromversorgung trennen
3	KEINE Datei löschen, selbst wenn sie von Malware infiziert sein könnte
4	Möglichst kurzfristig eine Datensicherung erstellen, die eine forensische Analyse erlaubt (forensische Duplikation) (Sofern das Know-how in forensischer Duplikation nicht vorhanden ist, sollte grundsätzlich die 24-Stunden-Soforthilfe-Hotline zur Unterstützung kontaktiert werden.)

2.4.2 Anormale bzw. ungewöhnliche Erscheinungen am Computersystem

Beispieltext

Nr.	Aktivität	Verantwortlich Betroffener Mitarbeiter
1	Sofort die Verbindung vom betroffenen IT-Gerät zum Netzwerk trennen ACHTUNG: Auf KEINEN Fall die IT-Geräte von der der Stromversorgung trennen	
2	Auf jeden Fall Fehlerbild merken; falls möglich, den Bildschirm mit einem Smartphone fotografieren	
3 4	Danach sofortige Meldung an das IT-Helpdesk Besteht auch für das IT-Helpdesk der Verdacht auf einen Angriff auf die Informationssicherheit: Abschalten der Netzwerk- und sonstiger Verbindungen Falls sicherheitstechnisch vertretbar: Einstellen einer unternehmensweiten Warnung per Pop-up an alle Endgeräte, bis auf Weiteres keine Mails zu öffnen mobile Dienstgeräte weder in privaten noch in einem der Netze der Institution noch in einem Kundennetz anzumelden ALLE am Netzwerk angeschlossenen USB-Massenspeichergeräte (Sticks, Kameras, Mobiltelefone etc.) vom Unternehmensnetz zu entkoppeln, nicht mehr zu benutzen und nicht vom Arbeitsplatz zu entfernen nicht mit externen Dritten über das Problem zu kommunizieren Falls ein externer IT- oder Cloud-Dienstleister involviert ist, (z. B. bei SaaS): sofortige Meldung an Ansprechpartner bei IT-/Cloud-Dienstleister (siehe Liste in Kapitel 5.3) Ggf. weitere erforderliche Maßnahmen	
5	Parallel oder sofort danach: Meldung an Notfallbeauftragten bzw. Stellvertreter	

2.4.3 Eingang einer Online-Erpressernachricht

Beispieltext

Nr.	Aktivität	Verantwortlich Betroffener Mitarbeiter
1	Sofort die Verbindung vom IT-Gerät zum Netzwerk trennen Nachricht NICHT weiterleiten oder wegklicken, sondern so belassen, wie sie ist	
2	Screenshot erzeugen bzw. Bildschirm mit einem Smartphone fotografieren; danach keine weiteren Aktionen am IT-Gerät durchführen	
3	Sofortige Meldung an IT-Helpdesk UND Notfallbeauftragten bzw. Stellvertreter	
4	Einstellen einer unternehmensweiten Warnung per Pop-up an alle Endgeräte, bis auf Weiteres Stillschweigen über das Problem gegenüber externen Dritten zu bewahren	

2.4.4 Bedienfehler am Computersystem

Beispieltext

Die folgenden Maßnahmen sind zu treffen, wenn Systeme betroffen sind, die als unternehmenskritisch definiert sind (siehe Kapitel 4.1):

Nr.	Aktivität	Verantwortlich Meldender Mitarbeiter
1	Keine eigenmächtigen „Reparaturversuche“ ohne Nachfrage beim Spezialisten für die betroffenen Systeme – es sei denn, dass der Verursacher selbst dieser Spezialist ist	
2	Meldung an	
3	Erfassen der Situation und ggf. Behebung des technischen Problems	
4	Meldung an den Spezialisten UND Notfallbeauftragten bzw. Stellvertreter	

2.5 Allgemeine Sofortmaßnahmen

2.5.1 Ausfall Stromversorgung von extern

Beispieltext

Aktivität	**Adressat/Ausführender**	**Verantwortlich** Meldender Mitarbeiter
Erstmeldung an:	– wenn nicht erreichbar: – –	
Klären der Situation und Behebung des Problems:	– ggf. Energieversorger –	
Kann das Problem nicht in kurzer Zeit oder nur mit Fremdunterstützung behoben werden, Meldung an:		
Ggf. Beauftragung von:		

2.5.2 Ausfall der IKT-Geräte bzw. des Netzwerks

Beispieltext

Aktivität	**Adressat/Ausführender**	**Verantwortlich** Meldender Mitarbeiter
Erstmeldung an:	– wenn nicht erreichbar: – –	
Klären der Situation und Behebung des Problems:	Mitarbeiter von	
Kann das Problem nicht in kurzer Zeit oder nur mit Fremdunterstützung behoben werden, Meldung an:		
Ggf. Beauftragung von:		

2.5.3 Ausfall der Internetverbindung

Beispieltext

Aktivität	**Adressat/Ausführender**	**Verantwortlich** Meldender Mitarbeiter
Erstmeldung an:	– wenn nicht erreichbar: – –	
Klären der Situation und Behebung des Problems:	Mitarbeiter von ggf. –	
Kann das Problem nicht in kurzer Zeit oder nur mit Fremdunterstützung behoben werden, Meldung an:	–	
Ggf. Beauftragung von:	–	

2.5.4 Ausfall eines externen IT- bzw. Cloud-Dienstleisters

Beispieltext

Aktivität	**Adressat/Ausführender**	**Verantwortlich** Meldender Mitarbeiter
Erstmeldung an:	– wenn nicht erreichbar: – –	
Klären der Situation und Behebung des Problems:	Mitarbeiter von – –	
Kann das Problem nicht in kurzer Zeit oder nur mit Fremdunterstützung behoben werden, Meldung an:	–	
Ggf. Beauftragung von:	–	

2.5.5 Datenschutzvorfall

Beispieltext

Aktivität	**Adressat/Ausführender**	**Verantwortlich** Meldender Mitarbeiter
Erstmeldung an:	– wenn nicht erreichbar: – –	
Klären der Situation und Behebung des Problems:	Mitarbeiter von	
Meldung an:	–	
Kann das Problem nicht in kurzer Zeit oder nur mit Fremdunterstützung behoben werden, Meldung an:	–	
Ggf. Beauftragung von:	–	

2.5.6 DoS-Attacke

Beispieltext

Aktivität	**Adressat/Ausführender**	**Verantwortlich** Meldender Mitarbeiter
Erstmeldung an:	– wenn nicht erreichbar: – –	
Klären der Situation und Behebung des Problems:	Mitarbeiter von	
Kann das Problem nicht in kurzer Zeit oder nur mit Fremdunterstützung behoben werden, Meldung an:	–	
Ggf. Beauftragung von:	–	
	–	

2.5.7 Ausfall der Webseite

Beispieltext

Aktivität	**Adressat/Ausführender**	**Verantwortlich** Meldender Mitarbeiter
Erstmeldung an:	– wenn nicht erreichbar: – –	
Klären der Situation und Behebung des Problems:	Mitarbeiter von	
Kann das Problem nicht in kurzer Zeit oder nur mit Fremdunterstützung behoben werden, Meldung an:	–	
Ggf. Beauftragung von:	–	
	–	

2.5.8 Weitere Szenarien

Beispieltext

Aktivität	**Adressat/Ausführender**	**Verantwortlich** Meldender Mitarbeiter
Erstmeldung an:	– wenn nicht erreichbar: – –	
Klären der Situation und Behebung des Problems:	Mitarbeiter von	
Kann das Problem nicht in kurzer Zeit oder nur mit Fremdunterstützung behoben werden, Meldung an:	–	
Ggf. Beauftragung von:	–	
	–	

3 Notfallbewältigung

In den nachfolgenden Kapiteln ist zu beschreiben, aus welchen Teilen die reaktive Notfallorganisation besteht, wie und wann sie aktiviert wird und welche Aufgaben die einzelnen Rollen haben.

3.1 Notfallstab

In diesem Kapitel sind die Aufgaben der Notfallorganisation zu beschreiben. Darüber hinaus ist die Besetzung zu beschreiben und festzulegen. Aufgrund der Wichtigkeit der Aufgabe für das Unternehmen ist es zwingend erforderlich, dass ein Mitglied der Geschäftsführung vertreten ist.

Beispieltext

Das zentrale Führungsgremium der Notfallbewältigung ist der Notfallstab. Er tritt zusammen, wenn die Geschäftsführung entschieden hat, dass es sich bei der vorliegenden Lage um einen IT-Notfall handelt.

Die Notfallbewältigung erfolgt hierbei auf Grundlage der bestehenden Notfalldokumentation.

Der Notfallstab stellt dabei eine besondere Aufbauorganisation dar, die für die Dauer der Bewältigung eines Notfalls abteilungsübergreifende Kompetenzen bündelt.

Der Notfallstab hat den Auftrag, die schnellstmögliche Wiederaufnahme des Geschäftsbetriebs zu gewährleisten und mögliche Folgeschäden auf ein Minimum zu begrenzen.
Mitglieder des Notfallstabs sind:

Rolle/Funktionsbezeichnung	Name
Mitglied der Geschäftsführung:	–
Stellvertreter:	–
Notfallbeauftragter:	–
Stellvertreter:	–
Leiter IT oder Leiter IT-Sicherheit:	–
Stellvertreter:	–
Bereichsleiter der betroffenen Organisationseinheiten:	–
	–
Weitere Mitarbeiter:	–
	–
Externe Dienstleister:	–
	–
Ggf. weitere externe Dienstleister/ Ansprechpartner:	–
	–

An dieser Stelle kann das Organigramm der reaktiven Notfallorganisation zur Verdeutlichung eingefügt werden.

3.2 Aufgaben des IT-Notfallbeauftragten

Hier sind die Aufgaben des Notfallbeauftragten zu beschreiben.

Beispieltext

Der Notfallbeauftragte ist verantwortlich für die Planung aller Maßnahmen, die bei der erfolgreichen Bewältigung eines IT-Notfalls notwendig sein könnten. Hierbei soll der Notfallbeauftragte besonders berücksichtigen, dass bei einem Ausfall der IT ggf. elektronische Medien sowie übliche Kommunikationsmittel und -wege nicht genutzt werden können.

Der Notfallbeauftragte ist dafür verantwortlich, dass der vorliegende Notfallplan aktuell ist. Gerade vor dem Hintergrund der typischerweise häufigen Veränderungen in der IT-Infrastruktur ist der Notfallbeauftragte über wesentliche Veränderungen zu unterrichten.
Der Notfallbeauftragte soll mittels geeigneter Maßnahmen dafür Sorge tragen, dass bei der Institution ein gemeinsames Verständnis darüber erreicht wird, welche Anwendungen oder Systeme für das Unternehmen kritisch sind.

Nach Meldung eines notfallrelevanten Ereignisses stellt der Notfallbeauftragte den Informationsfluss zu allen an der Durchführung der Sofortmaßnahmen beteiligten Personen sowie ggf. den Mitgliedern der Notfallorganisation sicher.
Der Notfallbeauftragte trifft zusammen mit der Geschäftsführung die Entscheidung, welche Organisationseinheiten ihren Bereichsleiter für den Notfallstab abstellen.
Der Notfallbeauftragte stellt sicher, dass im Notfall die Meldungen an externe Stellen ausgeführt werden.
Der Notfallbeauftragte ist gegenüber der Institutionsleitung berichtspflichtig. Falls zusätzlich Notfallkoordinatoren eingesetzt sind, initiiert und leitet der Notfallbeauftragte regelmäßige Gremienveranstaltungen. Verteilt arbeitende Notfallkoordinatoren werden vom 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.

Nach einer überstandenen Notfallsituation hat der Notfallbeauftragte die aus der Notfallbewältigung gewonnenen Erfahrungen anhand der Dokumentationen nachzubereiten und der Institutionsleitung zu berichten. Informationen wie z. B. aufgetretene Probleme in der Notfallbewältigung sind als Grundlage für eine Überarbeitung und Aktualisierung des IT-Notfallplans zu nutzen.
Es darf nicht vergessen werden, dass der Notfallbeauftragte einen qualifizierten Vertreter benötigt, der stets gut über den aktuellen Sachstand informiert sein sollte.

3.3 Lagezentrum

Bei einer Eskalation zu einem Notfall werden die Mitglieder des Notfallstabs umgehend informiert und treffen sich an einem vom Notfallbeauftragten festgelegten Ort, dem Lagezentrum. Diese Räumlichkeiten dienen dem Notfallstab als Arbeitsumgebung, für die besondere Anforderungen bezüglich des Standorts und der Ausstattung gelten. Insbesondere müssen Telekommunikations- und Arbeitsmittel verfügbar sein, die unabhängig von den normalerweise genutzten Systemen funktionieren.
Die Kommunikationsmittel des Notfallstabs sind so zu wählen, dass eine in Bezug auf Integrität, Verfügbarkeit, Vertraulichkeit und Verbindlichkeit sichere Kommunikation ermöglicht wird.
An dieser Stelle sind die Ausstattung, mögliche Zutrittsbeschränkungen sowie weitere Sicherheitsanforderungen des Lagezentrums zu beschreiben. Eine detaillierte Beschreibung, welche Anforderungen an die Ausstattung gestellt werden, ist dem BSI-Standard 100-4, Kapitel 7.1.3 zu entnehmen.

Beispieltext

Das Lagezentrum für IT-Notfälle befindet sich

Nach Ausrufung des Notfalls ist das Lagezentrum wie folgt vorzubereiten:

Ausstattung	Verantwortlich
Mobiliar, Arbeitsmaterialien, Präsentationsausstattung (z._B. Flipchart)	
Kommunikations-IT, z._B. analoges Telefon, autarker und definitiv nicht kompromittierter Computer	
Aktuelle Notfallpläne	
Aktuelle Pläne für die IT-Infrastruktur	
Aktuelle Netzpläne für die Strom- und Telekommunikationsversorgung	

3.4 Dokumentation im Notfallstab

An dieser Stelle ist zu beschreiben, auf welche Art und Weise der Notfallstab Informationen und Entscheidungen zu dokumentieren hat.
Werden hierzu standardisierte Formblätter und Vordrucke durch die Institution verwendet, ist darauf hinzuweisen. Die Formblätter und Vordrucke sind direkt oder in Form eines Dokumentverweises im Anhang des Notfallhandbuchs zu hinterlegen.

Beispieltext

Alle eingehenden und ausgehenden Meldungen sowie alle Entscheidungen und Maßnahmen sind schriftlich zu dokumentieren. Dazu gehören mindestens:

- Zeitpunkt der Arbeit des Notfallstabs
- Lagebild (Art, Umfang und Abläufe der Ereignisse)
- Eckpunkte aller getroffenen Entscheidungen sowie Name und Rolle der daran Beteiligten
- Beschlossene Maßnahmen, Verantwortliche für deren Umsetzung, Fertigstellungstermine und jeweiliger Umsetzungsstatus (Aufgabenüberwachung)

3.5 Meldungen an externe Stellen

Ist ein IT-Notfall eingetreten, sind je nach Situation externe Stellen zu benachrichtigen.

Beispieltext

Bei nachfolgend beschriebenen IT-Notfällen ist die Benachrichtigung von externen Institutionen entweder sinnvoll oder sogar vorgeschrieben. Die Meldung ist nicht zwingend sofort zu leisten, sondern kann nach den Erstmaßnahmen zur Bewältigung des Notfalls erfolgen.

Datenrechtsverletzung	**Dieser Text ist rechtlich nicht abgesichert. Beim Erstellen des Notfallplans ist eine Prüfung der Inhalte durch die Institution oder ggf. den externen Datenschutzbeauftragten zu leisten.** Gemäß DSGVO und BDSG ist in bestimmten Situationen nach maximal 72 Stunden die zuständige Datenschutzaufsichtsbehörde des Bundeslandes über die Datenpanne zu unterrichten.
Möglichkeit des Eintritts eines Haftpflichtanspruchs aufgrund einer Datenrechtsverletzung, einer IT-Sicherheitsverletzung oder eines Hackerangriffs	Schadenmeldung an die 24-Stunden-Soforthilfe-Hotline DE: +49 (0) 800 62 75 35 0 AT: +43 (0) 800 00 01 83 CH: +41 (0) 800 80 33 56
Inanspruchnahme von externen Rechts-, Public-Relations- oder Krisenberatern	Nur nach Absprache mit dem Versicherer über die 24-Stunden-Soforthilfe-Hotline DE: +49 (0) 800 62 75 35 0 AT: +43 (0) 800 00 01 83 CH: +41 (0) 800 80 33 56
Ggf. weiteres Ereignis	

3.6 Kommunikation und Öffentlichkeitsarbeit im Notfall

Die Kommunikation ist einer der zentralen Erfolgsfaktoren der Notfallbewältigung. Dies umfasst die Kommunikation mit verschiedenen Interessengruppen während und nach einem Notfall mit dem Ziel, weiteren Schaden zu verhindern, zu informieren und Vertrauens- und Imageverluste zu vermeiden. Hierbei kann zwischen interner und externer Kommunikation unterschieden werden.

Eine detaillierte Beschreibung, welche Anforderungen an die Kommunikation gestellt werden, ist dem BSI-Standard 100-4, Kapitel 7.3 „Krisenkommunikation“ zu entnehmen.

Beispieltext

Ein Notfall kann schnell von der Öffentlichkeit oder beteiligten Institutionen wahrgenommen und bewertet werden. Die hieraus resultierenden Auswirkungen für die Institution sind häufig schwer vorherzusehen, sodass die folgenden Vorgaben von allen Mitarbeitern der Institution zu berücksichtigen sind:

- Keine Stellungnahme gegenüber Medien, externen Personen oder Institutionen
- Mutmaßungen und Spekulationen sind zu vermeiden

Alle Anfragen zu Auskünften sind „an die verantwortliche Stelle für Kommunikation Bezeichnung einfügen weiterzuleiten.

3.7 Deeskalation

Ist der Notfall überstanden, so wird deeskaliert, die normale Linienstruktur wieder in Kraft gesetzt und werden ggf. eingeräumte Sonderbefugnisse der BAO wieder entzogen. Wie für die Eskalation sind auch für die Deeskalation Kriterien festzulegen, die eine geordnete Rückführung in den Normalbetrieb gewährleisten. Hierzu ist zu beschreiben, unter welchen Bedingungen eine Rückführung in den Normalbetrieb möglich ist, durch wen die Deeskalation erfolgt und welche Informationswege einzuhalten sind.

Beispieltext

Nur der Notfallstab ist ermächtigt, den Notbetrieb zurückzunehmen. Hierzu informiert der Notfallstab alle betroffenen Organisationseinheiten über die geplante Rückführung in den Normalbetrieb. Ob und in welchem Umfang Maßnahmen zur Reduzierung etwaiger Arbeitsrückstände umzusetzen sind, ist zentral durch den Notfallstab vorzugeben und selbstständig innerhalb der Organisationseinheiten umzusetzen. Die Leiter der Organisationseinheiten geben in regelmäßigen Abständen eine Statusmeldung an den Notfallstab ab. Erst nach vollständiger und erfolgreicher Rückführung in den Normalbetrieb löst sich der Notfallstab auf.

3.8 Analyse und Bewertung der Notfallbewältigung

An dieser Stelle ist zu beschreiben, auf welche Art und Weise die Notfallbewältigung in der Nachbereitung analysiert und bewertet wird. Eine Beschreibung, welche Anforderungen an die Analyse und Bewertung der Notfallbewältigung gestellt werden, ist dem BSI-Standard 100-4,Kapitel 7.1.7 „Analyse der Notfallbewältigung“ zu entnehmen.

Beispieltext

Nach der Rückkehr in den Normalbetrieb sind die aus der Notfallbewältigung gewonnenen Erfahrungen anhand der Dokumentationen nachzubereiten und der Institutionsleitung zu berichten. Informationen wie z. B. aufgetretene Probleme bei der Notfallbewältigung sind als Grundlage für eine Überarbeitung und Aktualisierung des Notfallmanagement-Prozesses zu nutzen. Der Notfallbeauftragte hat die zeitgerechte Umsetzung der Verbesserungsmaßnahmen zu überwachen und der Institutionsleitung regelmäßig Bericht zu erstatten.

4 Wiederanlauf und Wiederherstellung

IT-Anwendungen und IT-Systeme erfordern einen koordinierten Wiederanlauf. Beispielsweise benötigt eine Anwendung eine intakte Basisinfrastruktur (Strom, Klimatechnik, Hardware, physische Netzwerkanbindung etc.) sowie ggf. vorgelagerte Basisdienste (Virtualisierungscluster, SAN, Datenbank-Server etc.), um einen Wiederanlauf und eine Wiederherstellung zu ermöglichen.

Hier werden die Rahmenbedingungen für den Wiederanlauf und die Wiederherstellung festgelegt. Übergeordnete Wiederanlauf- und Wiederherstellungspläne sollen das Zusammenwirken der einzelnen Wiederanlauf- bzw. Wiederherstellungspläne steuern.

Beispieltext

IT-Anwendungen und IT-Systeme erfordern sowohl einen koordinierten Wiederanlauf als auch eine koordinierte Wiederherstellung. Dabei ist darauf zu achten, dass zuerst die Anwendungen und Systeme wieder in Betrieb gebracht werden, die für den Unternehmenserfolg wichtig bzw. kritisch sind; d. h. deren maximale Ausfallzeit vergleichsweise gering ist, bevor ein größerer Schaden für die Institution eintritt. Zudem wird die Reihenfolge der Wiederanlauf- und Wiederherstellungsmaßnahmen durch die Abhängigkeiten zwischen den Systemen bestimmt.

4.1 Wichtige IT-Anwendungen und IT-Systeme

Beispieltext

Für den Unternehmenserfolg wichtig bzw. kritisch sind:

Priorität	**IT-Anwendung/IT-System**	**Wird benötigt** für:	**Max. akzeptable Ausfallzeit:**

4.2 Wiederanlauf- und Wiederherstellungspläne

Sofern die Wiederanlauf- und Wiederherstellungsplanung in separaten Dokumenten beschrieben wird, sind die Verweise auf die Dokumente tabellarisch zu benennen. Soll die Wiederanlauf- und Wiederherstellungsplanung innerhalb des Notfallhandbuchs dokumentiert werden, so sind alle Kapitel aus den Dokumentvorlagen „Wiederanlaufplan“ und „Wiederherstellungsplan“ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html zu entnehmen, unterhalb dieses Kapitels einzufügen und gemäß den Ausfüllanleitungen zu Wiederanlauf- und Wiederherstellungsplanung zu befüllen.

Beispieltext

Die Informationen zu Wiederanlauf und Wiederherstellung der IT-Anwendungen und IT-Systeme befinden sich in der folgenden Tabelle:

Name der IT-Anwendung oder des IT-Systems	**Kurzbeschreibung**	**Verweis auf den Ablageort der Anleitung zum Wiederanlauf bzw. zur Wiederherstellung**

5 Anhang

5.1 Kontaktdaten der Notfallorganisation

In diesem Kapitel sind in tabellarischer Form die Kontaktdaten der zu alarmierenden Personen zu benennen.

Rolle	Name, Vorname oder Gruppennummer	Telefon dienstlich	Telefon mobil
Notfallbeauftragter			
Verantwortliches Mitglied der Geschäftsführung			
IT-Helpdesk			
Haustechnik			
Leiter IT			
Ggf. Leiter ITSicherheit			

5.2 Vertretungsregelungen

Hier sind in tabellarischer Form die Kontaktdaten der benannten Vertreter der an einem Notfall beteiligten Rollen zu benennen.

Rolle	Besetzung	Vertretung	Kontaktdaten der Vertretung
Notfallbeauftragter			

5.3 Kontaktdaten externer Dienstleister und Institutionen

In diesem Kapitel sind in tabellarischer Form die wichtigsten Rufnummern zu hinterlegen. Mindestens müssen alle Rufnummern derjenigen Personen, Organisationseinheiten oder Dienstleister genannt werden, die in diesem IT-Notfallhandbuch erwähnt werden.

Im Rahmen der Markel Cyber-Versicherung steht Ihnen die 24-Stunden-Soforthilfe-Hotline der Markel Insurance SE kostenfrei zur Verfügung. Über diese Soforthilfe-Hotline erhalten Sie Kontakt zu IT-Security-Spezialisten und IT-Forensikern als Unterstützung bei den Erstmaßnahmen und bei der Beseitigung von Schäden, die über die Cyber-Versicherung mitversichert sind. Darüber hinaus stehen Ihnen Experten zur Datenaufbereitung/-wiederherstellung, für Public-Relations-/Krisenkommunikationsmaßnahmen, Benachrichtigungs-/Call-Center-Dienste, Kreditkarten-Monitoring, juristische Beratung bei Datenrechtsverletzungen sowie weitere Maßnahmen zur Verfügung. Bitte nennen Sie bei Kontaktaufnahme die Nummer der Police Ihrer Cyber-Versicherung:

Telefonnummer der 24-Stunden-Soforthilfe-Hotline:	DE: +49 (0) 800 62 75 35 0 AT: +43 (0) 800 00 01 83 CH: +41 (0) 800 80 33 56
Nummer der Police Ihrer Cyber-Versicherung:	

Weitere Dienstleister und Institutionen:

Organisation	Ansprechpartner	Rufnummer 1	Rufnummer 2
Für Cyber-Angriffe zuständiges Dezernat Landeskriminalamt			
Bezeichnung der Datenschutzaufsichts-behörde des Bundeslandes			
Webhoster			
Kanzlei für IT-Recht			
Kommunikation/PR			
Krisenberater			
Datenschutzbeauftragter (ggf. extern)			
Telekommunikations-anbieter			
IT-Dienstleister 1:			
IT-Dienstleister 2:			
Cloud-Service-Provider			

5.4 Weitere unterstützende Pläne und Listen

In diesem Kapitel sind alle Pläne, Listen etc. zu benennen oder direkt zu hinterlegen, die für die Notfallbewältigung relevant sind.