Bundesamt
für Sicherheit in der
Informationstechnik

Notfallvorsorgekonzept

- Beispiel -

Stand: Dezember 2008

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Wichtige Hinweise zur Nutzung des Musterdokuments

In diesem Musterdokument wird beschrieben, welche Inhalte ein komplettes Notfallvorsorgekonzept enthalten sollte. Diese Anleitung unterscheidet sich aber von den übrigen Beispielen und Musterdokumenten des BSI. Während diese Dokumente relativ einfach an individuelle Gegebenheiten angepasst werden können und sofort zu mehr Sicherheit führen, ist beim Entwurf eines eigenen Notfallvorsorgekonzepts mehr Eigenarbeit nötig.

Dieses Musterdokument zum Aufbau eines Notfallvorsorgekonzepts gliedert sich in einen Hauptteil und zwei Anhänge.

Das erste Kapitel des Hauptteils führt in das Thema Notfallvorsorge ein, kann in einem individuellen Konzept stark gekürzt und sollte durch eine eigene Einleitung ergänzt werden.

Die folgenden Kapitel des Hauptteils beschreiben die Gliederung eines Notfallvorsorgekonzepts und den Ablauf der Behandlung von Sicherheitsvorfällen und Notfällen. Sie verweisen dabei immer wieder auf Dokumente im Anhang für detaillierte Darstellungen.

Anhang A beschreibt allgemein einige typische Rollen und Funktionen in einer Notfall-Organisation und muss in einem realen Konzept durch die Beschreibung der individuellen Organisationsstruktur ersetzt werden.

Anhang B gibt einen Überblick über notwendige Dokumentationen, die im Idealfall vor dem ersten Sicherheitsvorfall erstellt werden sollten. Der Kern eines jeden Notfallvorsorgekonzepts sind dabei die Notfallpläne für einzelne Schadensszenarien.

Beispiel: Was ist zu tun, wenn die Vertriebsdatenbank ausfällt? Welche Verhaltensregeln gelten, wenn durch Hochwasser das Rechenzentrum zu überfluten droht?

Da diese Szenarien sehr individuell sind, kann das BSI hier keine Vorlagen erstellen. Jede Institution muss selbst festlegen, welches Ereignis für sie einen Notfall darstellt und wie darauf zu reagieren ist.

Auch Zuständigkeiten ("Wer darf entscheiden, wann die Firmenrechner ausgeschaltet werden, um einen bösartigen Virus zu entfernen?") können nur vor Ort von jeder Institution individuell festgelegt werden.

Das Muster-Notfallvorsorgekonzept des BSI hilft jedoch, das eigene Konzept sinnvoll zu gliedern und keine wichtigen Themen zu vergessen. Es ist als roter Faden beim Schreiben eines "echten" Notfallvorsorgekonzepts zu verstehen.

Im Text selbst wird in der rechten Spalte auf Maßnahmen der IT-Grundschutzkataloge verwiesen, in denen mehr Informationen zu den im Text markierten Begriffen zu finden sind. Im wesentlichen beruht das Musterdokument auf den Bausteinen zu den Themen "Notfallvorsorge-Konzept" und "Behandlung von Sicherheitsvorfällen". Weitere Informationen und Denkanstöße finden sich in den BSI Standards.

Kommentare zum besseren Verständnis sowie Hinweise, an welchen Stellen sich eine individuelle Anpassung oder Ergänzung des Musterkonzeptes besonders empfiehlt, sind gelb hinterlegt.

Inhaltsverzeichnis

1 Einleitung: Was ist ein Notfallvorsorgekonzept?

1.1 Notfall-Definition

Der Ausfall eines IT-Systems in Folge eines Sicherheitsvorfalls kann einen großen Schaden nach sich ziehen. So kann der Ausfall eines zentralen IT-Systems zu einem Ausfall des gesamten IT-Betriebs führen. Auch der Ausfall von Komponenten der technischen Infrastruktur, beispielsweise Klimaanlage oder Stromversorgung, kann zu Störungen des IT-Betriebs führen.

Technisches Versagen muss nicht zwingend die Ursache für den Ausfall von IT-Systemen sein. Ausfälle werden oft durch menschliches Fehlverhalten (z. B. fahrlässige Zerstörung von Gerät oder Daten) oder vorsätzliche Handlungen (z. B. Diebstahl, Sabotage, Viren-Angriff) verursacht. Auch durch höhere Gewalt (wie Feuer, Blitzschlag oder Hochwasser) können hohe Schäden eintreten.

Ein Sicherheitsvorfall stellt jedoch nicht zwangsläufig einen Notfall dar. Für einen Notfall gilt die folgende Definition:

Ein Notfall tritt ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit nicht möglich ist ***und*** *sich daraus ein untragbarer Schaden ergibt.*

1.2 Zielsetzung eines Notfallvorsorgekonzepts

Um größere Schäden zu begrenzen bzw. diesen vorzusorgen, ist eine zügige und effiziente Behandlung von Sicherheitsvorfällen, die zum Ausfall von IT-Systemen führen, notwendig.

Ein Notfallvorsorgekonzept hat zum Ziel, die Geschäftstätigkeit während eines Ausfalls eines IT-Systems oder einer IT-Anwendung aufrechtzuerhalten und sicherzustellen (Business Continuity) sowie die Betriebsfähigkeit innerhalb einer tolerierbaren Zeitspanne wiederherzustellen (Business Recovery).

Dabei sind nicht nur die technischen Maßnahmen zum Wiederanlauf zu beachten. Besonders wichtig ist die Planung im Vorfeld, um Notfälle zu verhindern oder zumindest die Auswirkungen begrenzen zu können. Zur Vorbereitung gehören die Dokumentation von Verfahren und Maßnahmen sowie organisatorische Regelungen. Im Notfall muss es z. B. Verantwortliche mit klaren Kompetenzen geben. Zu einer guten Vorbereitung gehören ebenso Notfallschulungen und -übungen sowie eine stetige Pflege und Aktualisierung des Notfallvorsorgekonzeptes.

Ein Notfallvorsorgekonzept beschreibt, welche Maßnahmen zur Vorbereitung auf Notfälle unternommen werden und was im Notfall zu tun ist.

2 Verantwortliche Personen

Ein "Notfall" sollte formal durch einen Notfall-Verantwortlichen ausgerufen werden, da schnelle Entscheidungen unabhängig von Hierarchieebenen getroffen und Mitarbeiter vielleicht außerhalb der normalen Arbeitszeit verständigt werden müssen. Auch könnten Maßnahmen, die vom normalen Arbeitsablauf abweichen und Sonderberechtigungen erfordern, notwendig werden. In Notfällen müssen unter Umständen Beschränkungen und Sicherheitsvorkehrungen außer Kraft gesetzt werden, um ein Problem schneller lösen zu können.

M 6.2

In den Notfallplänen muss daher festgelegt werden, welche Aufgaben einzelne Personen im Notfall übernehmen und welche Rechte sie haben. Die beteiligten Personen und Organisationseinheiten sind dann im Notfall befugt, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen.

M 6.7, M 6.59

Anhang A enthält vertiefende Hinweise zu verschiedenen Rollen.

3 Verhalten in Notfällen

3.1 Allgemeine Regeln für alle Mitarbeiter

Folgende Verhaltensregeln gelten allgemein für alle Mitarbeiter:

- Alle Mitarbeiter haben im Vorfeld die Erstellung des Notfallfallvorsorgekonzepts (z. B. Erstellung der Dokumentationen) nach Kräften zu unterstützen. Nur durch eine gute Vorbereitung ist es möglich, im Notfall Ruhe zu bewahren und nicht durch unüberlegte Handlungen den Schaden zu vergrößern.
- Unregelmäßigkeiten, die auf einen Sicherheitsvorfall hindeuten, sind gemäß der *Alarmierungspläne* (siehe Kapitel 3.3) unverzüglich zu melden.
- Die *Handlungsanweisungen für ausgewählte Schadensereignisse* (siehe Anhang B 2) sind einzuhalten.
- Es sind die Anweisungen des Notfall-Verantwortlichen und etwaige spezielle Verhaltensregeln zu beachten.
- Alle Begleitumstände sind ungeschönt, offen und transparent zu erläutern, um damit Schäden zu mindern, schnell Lösungen zu finden und Erkenntnisse zur Verbesserung des IT-Sicherheitskonzepts zu gewinnen.
- Informationen über den Notfall dürfen nicht an unautorisierte externe Dritte weitergegeben werden.
- Nach einem Notfall ist der sichere Normalzustand wieder herzustellen und an der Aufarbeitung des Notfalls mitzuarbeiten.
- Das Notfallvorsorgekonzept ist stets aktuell zu halten und zu verbessern.

3.2 Sofortmaßnahmen

Derjenige, der einen Sicherheitsvorfall bemerkt, leitet umgehend erste Maßnahmen ein (z. B.: Alarmierung, Rechner ausschalten, Fenster schließen, ...).

Welche Verhaltensregeln bei Vorfällen gelten, muss in den *Handlungsanweisungen für ausgewählte Schadensereignisse* (siehe Anhang B 2) beschrieben werden.

3.3 Alarmierung

Die verantwortlichen Stellen, die aktiv handeln oder Verantwortung übernehmen müssen, sind zu alarmieren (z. B. Feuerwehr, Pförtner, Administrator, IT-Sicherheitsbeauftragter). Sie übernehmen dann in der Regel die weitere Untersuchung und Bewertung des Vorfalls und leiten Maßnahmen ein.

Im Vorfeld sind Alarmierungspläne zu erstellen, die die Meldewege für ausgewählte Schadensereignisse (siehe Anhang B 2.1) beschreiben. M 6.8, M 6.60

Als Anhang müssen Adress- und Telefonlisten geführt werden. Relevante Telefonnummern externer Dienstleister und Behörden dürfen nicht vergessen werden, z. B.:

- Feuerwehr
- Polizei
- Notarzt
- Wasser- und Stromversorger
- Ausweichrechenzentrum
- Telekommunikationsanbieter
- IT-Techniker
- Softwarehersteller

Bei Bedarf ist ein Ruf- oder Bereitschaftsdienst einzurichten.

Damit allen Mitarbeitern die Ansprechpartner bekannt sind werden diese Listen an alle in Schriftform verteilt sowie im Intranet bereitgestellt.

3.4 Untersuchung und Bewertung des Vorfalls

Um einen Sicherheitsvorfall untersuchen und bewerten zu können, sind in der Regel folgende Informationen notwendig: M 6.63

- betroffene IT-Komponenten (IT-Systeme und IT-Anwendungen)
- betroffene Geschäftsprozesse
- Ansprechpartner (Technik und Fachabteilung)
- Verfügbarkeitsanforderungen der IT-Komponenten
- Schutzbedarf der IT-Komponenten und der damit verarbeiteten Informationen
- möglicher Schaden: Schadensart, Schadenshöhe, Geschädigte (z. B. Kunden oder Geschäftspartner)
- mögliche Folgeschäden
- Ursache des Vorfalls (technisches Versagen, Unachtsamkeit, gezielter Angriff)
- Maßnahmen zur Behebung des Vorfalls

Um alle Informationen schnell zur Hand zu haben sind mindestens folgende Vorarbeiten nötig (siehe Anhang B 4 und B 5):

- Beschreibung und Bestand der Hard- und Software
- Schutzbedarfsfeststellung
- Zusammenstellung der Verfügbarkeitsanforderungen
- Beschreibung der Infrastruktureinrichtungen

3.5 Eskalation des Vorfalls

Unter Umständen müssen Stellen mit größerer Kompetenz und höherer Verantwortung benachrichtigt werden. Anhand einer Eskalationsstrategie ist zu entscheiden, M 6.61

- ob eine sofortige Eskalation ohne weitere Untersuchungen und Bewertungen erforderlich ist,

- ob zunächst eine genauere Untersuchung des Vorfalls erfolgen soll,
- wer intern informiert werden muss,
- welche externen Stellen informiert werden müssen.

Die *Eskalationsstrategie* sollte in einem eigenen Dokument festgehalten werden (siehe Anhang B 3).

3.6 Maßnahmen zur Problemlösung

3.6.1 Reihenfolge der Fehlerbehebung

Bei der Behebung von Schäden sind verschiedene Aspekte zu berücksichtigen, wenn unterschiedliche Vorfälle, mehrere IT-Komponenten oder verschiedene Geschäftsprozesse betroffen sind und eine Wiederanlaufreihenfolge festgelegt werden muss.

- Bedeutung einer ausgefallenen IT-Komponente oder des betroffenen Geschäftsprozesses
  Siehe Anhang B 2 (Schutzbedarfsfeststellung, insbesondere Verfügbarkeitsanforderungen).
- Bewertung unterschiedlicher Schadensarten durch die Unternehmens- oder Behördenleitung
  Entsprechende Vorgaben sollten nach Möglichkeit vorab dokumentiert werden (siehe Anhang B 1).
- Technische oder ablaufbedingte Abhängigkeiten der IT-Systeme und IT-Anwendungen voneinander.
  Es besteht die Möglichkeit, dass bestimmte Prozesse erst dann wiederhergestellt werden können, wenn andere, die als Grundlage zu sehen sind, bereits wieder funktionsfähig sind.
  Entsprechende Dokumentationen sind im Vorfeld anzufertigen (siehe Anhang B 4.4).

3.6.2 Voraussetzungen für kurze Wiederanlaufzeiten

Um im Schadensfall Probleme möglichst schnell lösen zu können, müssen rechtzeitig Vorbereitungen getroffen werden:

- Erstellung von eigenen Dokumentationen und sorgfältige Archivierung von externen Dokumenten (siehe Anhang B 2 und B 4)
- Datensicherung (siehe Kapitel 6.1)
- Verträge mit externen Dienstleistern, Herstellern und Lieferanten (siehe Kapitel 6.2)
- Ersatzbeschaffungsplan für Hardware (siehe Anhang B 4.3)

3.6.3 Notbetrieb

Nicht immer kann jedes Problem in einer tolerierbaren Zeitspanne behoben werden (Beispiel: Reparatur eines IT-Systems dauert zu lange). In diesen Fällen ist es erforderlich, die wichtigsten Geschäftsprozesse provisorisch aufrecht zu erhalten. Verschiedene Möglichkeiten bieten sich je nach Vorfall an:

- Einschränkung des IT-Betriebs
  Um bei einem eingeschränkten IT-Betrieb die geschäftskritischen Prozesse betreiben zu können, ist für IT-Anwendungen die zur Verfügung gestellte Kapazität auf das notwendige Maß zu reduzieren (siehe Anhang B 4.1). M 6.5
- manuelle Ersatzverfahren (siehe Anhang B 6.1)

- interne oder externe Ausweichmöglichkeiten (siehe Anhang B 6.2)

Die notwendigen Dokumentationen sowie Kontaktadressen von Dienstleistern, Herstellern und Lieferanten sind im Vorfeld zusammenzustellen.

3.7 Informationspolitik

Unter Umständen müssen betroffene interne und externe Stellen über den Vorfall informiert werden. Dies sind insbesondere diejenigen Stellen, die direkt durch den Sicherheitsvorfall Schäden erleiden könnten, Gegenmaßnahmen ergreifen müssen oder solche, die Informationen über Sicherheitsvorfälle aufbereiten und bei der Vorbeugung oder Behebung helfen können. In Einzelfällen kann es auch notwendig sein, die Medien zu informieren. M 6.65

Anweisungen für bestimmte Schadensszenarien mit den nötigen Kontaktdaten sind vorab zusammenzustellen.

3.8 Dokumentation

Eine Dokumentation des Notfalls ist notwendig, um für zukünftige Vorfälle zu lernen und Veränderungen an IT-Systemen und IT-Anwendungen nachvollziehen zu können. Dies ist besonders wichtig, wenn unter Zeitdruck oder mit Sonderrechten gearbeitet wurde. M 6.64

Protokoll- und Log-Dateien können im Nachhinein eine wertvolle Hilfe sein und sollten daher gesichert werden.

Bei der Dokumentation sollte auch an eine mögliche Strafverfolgung gedacht werden.

4 Nachbereitung von Notfällen

Eine Nachbereitung von Notfällen hat aus zwei Gründen zu erfolgen: M 6.66

Verbesserungspotentiale erkennen

Dazu sind z. B. folgende Fragen zu klären:

- Waren die Reaktionszeiten ausreichend?
- Hat die Alarmierung funktioniert oder gab es Probleme bei der Eskalation des Vorfalls?
- Wurde die Ursache des Vorfalls schnell gefunden und wurden die Auswirkungen richtig eingeschätzt?
- Waren alle Dokumentationen brauchbar und aktuell?
- Wenn es einen Täter gab: Was hat ihn motiviert?
- Was muss in Zukunft verbessert werden?

Wiederherstellung eines stabilen Normalzustandes

Nach einem Notfall ist dafür zu sorgen, dass möglichst schnell der sichere Normalzustand wieder erreicht wird. Zur Behebung des Notfall sind unter Umständen Anwendungen, IT-Systeme oder Konfigurationen verändert oder elektronische Abläufe durch manuelle ersetzt worden.

Es kann z. B. auch erforderlich sein, Passwörter neu zu vergeben und zu verändern. M 2.11, M 2.7

5 Revision des Notfallvorsorgekonzepts

Das Managementsystem zur Behandlung von Sicherheitsvorfällen, und damit auch das Notfallvorsorgekonzept, muss regelmäßig auf seine Aktualität und Wirksamkeit geprüft werden. Die Notfallübungen (siehe Kapitel 6.5.2) können dabei wertvolle Erkenntnisse liefern. M 6.58 M 6.12

Alle Maßnahmen müssen regelmäßig daraufhin überprüft werden, ob sie

- wirksam und effektiv sind,
- den betroffenen Mitarbeitern bekannt sind,
- unter Stress umsetzbar sind und
- in den Betriebsablauf integrierbar sind.

6 Prävention und Vorbereitung

Die folgenden Maßnahmen sollten zur Notfallvorsorge ergriffen werden.

6.1 Datensicherungsplan

Datensicherungen sind zu erstellen, um Datenverlust vorzubeugen und Ersatz-Systeme schnell in Betrieb nehmen zu können.

Mit Hilfe eines Datensicherungsplans muss ein sachverständiger Dritter in der Lage sein, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten in angemessener Zeit beschaffen und installieren zu können. Ein Datensicherungsplan muss Auskunft geben können über: M 6.13

- Datum der Datensicherung
- Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert)
- Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind
- Datenträger, auf dem die Daten gesichert wurden
- für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer)
- bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.)
- Ort der Aufbewahrung

Es ist ein Datensicherungskonzept zu erstellen und zu beachten, in dem die Datensicherung explizit geregelt wird.

6.2 Outsourcing, Verträge mit Hersteller und Lieferanten

Notfallvorsorge muss Bestandteil von Verträgen mit externen Dienstleistern sein. Außerdem kann es erforderlich sein, bei Notfällen auf die Dienste von Spezialisten zurückzugreifen.

Die wichtigsten Vorgaben sind vertraglich zu vereinbaren, z. B: M 2.253, M 6.83

- Zuständigkeiten, Ansprechpartner und Abläufe
- Datensicherung
- Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen
- regelmäßige Notfallübungen

Alle für eine Ersatzbeschaffung von IT-Systemen notwendigen Vereinbarungen mit Lieferanten (Servicezeiten, Lieferfristen etc.) sind zu treffen.

Bei der Auswahl von Software sind Support- und Serviceleistungen als Auswahlkriterium zu berücksichtigen. Bei Bedarf sind vertragliche Regelungen (Hotline, Antwortzeiten, individuelle Updates und Patches) mit den Herstellern abzuschließen.

Es ist das Sicherheitskonzept für Outsourcing zu beachten.

6.3 Versicherungsschutz

Verbleibende Restrisiken sollten möglichst unter Beachtung von Kosten-

Nutzen-Aspekten durch Versicherungen abgedeckt werden. Beispiele sind: M 6.16

- Sachversicherungen
- Feuerversicherung
- Einbruchdiebstahlversicherung
- Transportversicherung
- Datenträgerversicherung
- Elektronik-Versicherung

Die Fachverantwortlichen sind dafür verantwortlich, dass für ihre Prozesse der Abschluss von Versicherungen untersucht wird.

6.4 Technische Maßnahmen

Um zu vermeiden, dass ein Sicherheitsvorfall zum Notfall wird, müssen Sicherheitsvorfälle durch technische Maßnahmen verhindert oder möglichst frühzeitig entdeckt werden.

6.4.1 Einsatz von technischen Detektionsmaßnahmen

Es gibt eine Reihe von Sicherheitsvorfällen, die mit entsprechender technischer Unterstützung automatisiert und daher frühzeitig erkannt werden können. Zu diesem Zweck sollen Detektionsmaßnahmen installiert werden. M 6.67

Beispiele für solche technischen Detektionsmaßnahmen sind:

- Gefahrenmeldeanlage M 1.18
- Rauchmelder M 1.54
- Fernanzeige von Störungen M 1.31
- Computer-Viren-Schutzprogramme M 2.157
- Intrusion Detection und Intrusion Response Systeme M 5.71
- Kryptographische Checksummen und digitale Signaturen M 4.34

Die technischen Detektionsmaßnahmen müssen durch zusätzliche organisatorische Maßnahmen ergänzt werden (z. B. Meldewege, regelmäßige Aktualisierung und Überprüfung).

Bei der Auswahl von Detektionsmaßnahmen ist immer eine Kosten-Nutzen-Berechnung vorzulegen und die Wirksamkeit kritisch zu hinterfragen.

6.4.2 Sichere Infrastruktur

Die Infrastruktur (Gebäude und Räume) ist durch geeignete Maßnahmen zu sichern. Dazu gehören beispielsweise die Bereiche Zugangsschutz, Diebstahlschutz, Schutz vor Naturereignissen, Stromversorgung, Klimatisierung.

Durch eine unterbrechungsfreie Stromversorgung ist sicherzustellen, dass für hochverfügbare IT-Systeme ein kurzzeitiger Stromausfall keinen Schaden verursacht. M 1.28

6.5 Ausbildung und Training der Mitarbeiter

6.5.1 Notfallschulungen

Ein qualitativ hochwertiges Notfall- und Kontinuitätsmanagement greift nur dann optimal, wenn die Mitarbeiter zum einen für sicherheitsrelevante Vorfälle sensibilisiert sind und zum anderen bestmöglich für sicherheitsrelevante Vorfälle geschult werden. M 2.198 M 6.12

Sämtliche Mitarbeiter (auch nicht unmittelbar mit dem IT-Betrieb befasste Personen wie Pförtnerdienst oder Wachpersonal) werden in der Anwendung des Notfallvorsorgekonzeptes geschult. M 6.3

6.5.2 Notfallübungen

Es sind regelmäßig angekündigte und unangekündigte Übungen durchzuführen. M 6.12

Übungen sind sorgfältig zu planen, um Schäden an IT-Systemen, Daten oder sonstigem zu verhindern.

Bei einer Notfallübung sind z. B. folgende Tätigkeiten durchzuführen:

- Durchspielen der Notfallsituation im Team
- Wiedereinspielen von Datensicherungen
- Wiederanlauf nach Ausfall eines ausgewählten IT-Systems
- Durchführung einer Alarmierung
- Funktionstests von Stromaggregaten
- Durchführung von Feuerübungen

Es sollten nicht nur Schreibtischübung, sondern auch Feldübung mit Problemsimulationen sowie echte Übung (z. B. Notstromprobe) durchgeführt werden.

Die wichtigsten Ergebnisse einer Notfallübung sind zu dokumentieren und bekannt zu geben. Die Erkenntnisse aus den Übungen sollten möglichst schnell zur Verbesserung des Notfallvorsorgekonzepts genutzt werden.

A. Anhang: Verantwortliche Personen

1 Notfall-Verantwortlicher

Es sollte ein Notfall-Verantwortlicher berufen werden. M 6.2, M 2.193

Der Notfall-Verantwortliche hat folgende Aufgaben:

- Erstellung und Pflege des Notfallvorsorgekonzepts
- Bewertung von Sicherheitsvorfällen
- formale Ausrufung und Beendigung des Notfalls
- Koordination der Notfallmaßnahmen
- Dokumentation des Notfalls, Erstellung eines Abschlussberichts
- Unterrichtung der betroffenen Fachabteilungen sowie bei Bedarf der Leitungsebene.
- Zusammenstellung und Einberufung eines Notfall-Teams
- Organisation und Vorbereitung von Notfall-Schulungen und -Übungen

Hinweis: Der IT-Grundschutz empfiehlt die Berufung *eines* Notfall-Verantwortlichen. Nach der IT-Grundschutz-Philosophie muss eine Maßnahme nicht *wörtlich*, sondern sollte *ihrem Sinn nach* umgesetzt werden. Das heißt in diesem Fall: Es muss geklärt sein, **wer** einen Notfall ausrufen und die dann notwendigen, weitreichenden Maßnahmen anordnen darf. Die Entscheidung über die Anzahl der Personen, die einen Notfall ausrufen können und die Zugehörigkeit zur Hierarchieebene müssen an die individuellen Bedürfnisse angepasst werden. Es ist z. B. denkbar, einen Notfall-Verantwortlichen zu berufen, der direkt der Unternehmens- oder Behördenleitung angehört.

2 IT-Sicherheitsbeauftragter

M 6.59

Der IT-Sicherheitsbeauftragte nimmt Meldungen über Sicherheitsvorfälle entgegen und informiert bei Bedarf den Notfall-Verantwortlichen. Bei der Behebung und Aufarbeitung eines Notfalls unterstützt er die Verantwortlichen. Er überwacht auch, ob alle IT-Sicherheitsmaßnahmen nach Beendigung des Vorfalls wieder in Kraft gesetzt werden und überprüft mit den Erkenntnissen aus dem Vorfall das IT-Sicherheitskonzept auf Schwächen und Verbesserungsmöglichkeiten.

Hinweis: Die Aufgabenteilung zwischen dem Notfall-Verantwortlichen und dem IT-Sicherheitsbeauftragten muss an individuelle Bedürfnisse angepasst werden. Die Positionen "Notfall-Verantwortlicher" und "IT-Sicherheitsbeauftragter" können auch zusammengelegt werden.

3 IT-Benutzer

M 6.59

Alle Mitarbeiter haben die Notfallvorsorge zu unterstützen. Das gilt besonders für die Fachabteilungen bei der Erstellung von spezifischen Notfallplänen und Dokumentationen sowie der Zusammenarbeit mit dem Notfall-Verantwortlichen.

Im Notfall gelten für alle die allgemeinen Verhaltensregeln, die in Kapitel 3.1 des Hauptdokuments zusammengefasst sind.

4 Brandschutzbeauftragter

Es sollte ein Brandschutzbeauftragter benannt werden, der für die Einhaltung der Brandschutzvorschriften verantwortlich ist. M 1.6

A. Anhang: Verantwortliche Personen

Zu den Aufgaben des Brandschutzbeauftragten zählen u. a. Brandschutzbegehungen, die Zusammenarbeit mit der Feuerwehr, Aufstellung der Brandschutzordnung, die Kontrolle und Wartungsüberwachung der Brandmelde- und Löschvorrichtungen und die Durchführung von Übungen. M 2.15

Der Brandschutzbeauftragte und der IT-Sicherheitsbeauftragte arbeiten eng zusammen und sorgen dafür, dass bei den Brandschutzmaßnahmen die besonderen Belange der Informationssicherheit berücksichtigt werden. (Negativbeispiel: Brandlöschung durch Sprinkleranlagen verursacht Wasserschäden an Hardware).

5 Weitere Rollen

M 6.59

Unternehmens- oder Behördenleitung

Die Leitung trifft abschließende Entscheidung zur Durchführung von Maßnahmen. Sie schaltet die Polizei und Strafverfolgungsbehörden ein, wenn der Verdacht auf kriminelle Handlungen besteht.

Administratoren

Administratoren haben eine große Verantwortung. Sie überwachen ihre IT-Systeme und Anwendungen und sind die ersten Ansprechpartner von IT-Benutzern bei Problemen und Fragen. Sie werden daher oftmals die ersten sein, die erkennen, dass eine Unregelmäßigkeit sicherheitsrelevant ist. Sie müssen dann verantwortungsbewusst entscheiden, ob sie das Problem selbst beheben können oder ob sie den Vorfall eskalieren.

Pressestelle

In Notfällen sollte die Öffentlichkeit ausschließlich durch die Pressestelle informiert werden. Die Pressestelle muss Informationen über den Notfall zusammen mit den technischen Experten aufbereiten und mit der Leitung vor der Weitergabe abstimmen.

Justitiar, Datenschutzbeauftragter, Betriebs- oder Personalrat

Diese Positionen sind heranzuziehen, sofern ein Notfall juristische, datenschutzrechtliche oder mitbestimmungspflichtige Aspekte hat.

Ersthelfer

Es sollten qualifizierte Ersthelfer benannt werden, um bei Erkrankungen oder Verletzungen schnell Hilfe leisten zu können.

6 Sicherheitsvorfall-Team

Ein Sicherheitsvorfall-Team empfiehlt sich für größere Institutionen mit vielen Hierarchieebenen und vielen Schnittstellen (Leitung, Fachabteilungen, IT-Abteilung, Revision etc.). M 6.59

Bei einem Notfall unterstützt das Sicherheitsvorfall-Team den Notfall-Verantwortlichen. Das Sicherheitsvorfall-Team ist befugt, die übertragenen Aufgaben eigenverantwortlich durchzuführen.

Zu einem Sicherheitsvorfall-Team können je nach Ausmaß und Art des Notfalls folgende Personenkreise gehören:

- Behörden oder Unternehmensleitung
- IT-Sicherheitsbeauftragter
- IT-Verantwortlicher

A. Anhang: Verantwortliche Personen

- Administrator
- Pressestelle
- Datenschutzbeauftragter
- Justitiar
- Personalrat oder Betriebsrat
- Fachabteilungen
- die Bereiche Beschaffung, Haustechnik, Organisation, Personal
- Brandschutzbeauftragter
- ...

Je nach Bedarf wird das Sicherheitsvorfall-Team vom Notfall-Verantwortlichen zusammengestellt und einberufen.

B. Anhang: Dokumente

1 Vorgaben zur Priorisierung von Sicherheitsvorfällen

Ein Sicherheitsvorfall hat in der Regel unterschiedliche Schäden zur Folge (Beispiel: Der Vorfall bedeutet einen Verstoß gegen Gesetze, hat finanzielle Auswirkungen und bewirkt einen Imageschaden.)

Wenn möglich, sollte die Unternehmens- oder Behördenleitung Prioritäten für die Problembeseitigung vor dem ersten Vorfall festlegen. M 6.62
Beispiel: Hat ein mittlerer finanzieller Schaden eine höhere Priorität als ein hoher Imageschaden?

Diese Prioritäten haben Einfluss auf die Reihenfolge, in der die Probleme angegangen werden und der Wiederanlauf geschehen soll.

2 Handlungsanweisungen für ausgewählte Schadensereignisse

2.1 Schadensszenarien und Handlungspläne

Bei Sicherheitsvorfällen und in Notfällen ist es entscheidend, dass alle Mitarbeiter wissen, was zu tun ist. Aus diesem Grund sind für die wichtigsten Schadensereignisse Handlungsanweisungen und Verhaltensregeln aufzustellen.

Die Fachverantwortlichen müssen entscheiden, für welche Geschäftsprozesse, Abläufe und Szenarien derartige Handlungspläne sinnvoll und notwendig sind. Beispiele sind: M 6.9, M 6.60

Schäden durch höhere Gewalt, die Auswirkungen auf die Verfügbarkeit der Informationsverarbeitung haben:

- Brand, Explosion
- Stromausfall
- Hochwasser
- Hardware-Ausfall aufgrund technischer Defekte
- Ausfall der Datenübertragungseinrichtungen wie DFÜ
- Virenbefall
- Vandalismus, Sabotage, Einbruch
- Rechenzentrum nicht zugänglich (Unfall, Streik, Bombendrohung etc.)
- ...

IT-Sicherheitsvorfälle, die zu Notfällen werden können:

- Ausfall einzelner IT-Systeme
- Ausfall einzelner Anwendungen
- Ausfall eines Netzes
- ...

2.2 Inhalt der Dokumentation

Für jedes Szenario sollten folgende Aspekte beschrieben werden (Verweise beziehen sich auf das Hauptdokument):

- **Sofortmaßnahmen** (siehe Kapitel 3.2)
  Wie muss derjenige, der einen Vorfall bemerkt, umgehend reagieren?
- **Alarmierungsplan** (siehe Kapitel 3.3) M 6.8
  Welche verantwortlichen Stellen müssen zuerst benachrichtigt werden?

B. Anhang: Dokumente

- **Maßnahmen zur Schadensbegrenzung**
- **Maßnahmen zur Behebung des Vorfalls**
- **Informationspolitik** (siehe Kapitel 3.7)
  Welche internen und externen Stellen sind zusätzlich zu informieren?

3 Eskalationsstrategie

Die Meldung über einen Sicherheitsvorfall oder eine darauf hindeutende Unregelmäßigkeit muss zunächst dahingehend geprüft werden, welches Ausmaß und Bedeutung der Vorfall bzw. die Unregelmäßigkeit hat, um dann entsprechende Maßnahmen zu ergreifen. Innerhalb einer Eskalationsstrategie werden Personen, Zeitpunkte und Medien der Eskalation definiert.

M 6.63
M 6.61

Entscheidungshilfe für Eskalation

Es ist für Sicherheitsvorfälle und Notfallszenarien festzulegen, in welchen Fällen aufgrund besonders großer Gefahren eine sofortige Eskalation ohne weitere Untersuchungen und Bewertungen erforderlich ist.

Anschließend ist für die restlichen Fälle vorzugeben, wann eine Eskalation stattzufinden hat. Gründe dafür können z. B sein:

- (Vermutete) Schadenshöhe übertrifft den Verantwortungsbereich.
- Kosten und Ressourcen für die erforderlichen Maßnahmen übertreffen den Kompetenzbereich.
- Komplexität des Sicherheitsvorfalls übersteigt Kompetenz- bzw. Zuständigkeitsbereich.

Eskalationswege

Es ist zu definieren, wer an wen eine Meldung weitergibt. Dabei sind sowohl die regulären Eskalationswege als auch der Vertretungsfall zu berücksichtigen. Ein solcher Eskalationswegeplan ist vorfallsspezifisch – sinnvoller weise graphisch – zu erstellen.

M 6.60

Die notwendigen Adress- und Telefonlisten sind zu führen.

Art und Weise der Eskalation

Es sollten zum einen zeitliche Vorgaben gemacht werden, zum anderen die Art der Benachrichtigung festgeschrieben werden (telefonisch, Formular, E-Mail etc.). In zeitkritischen Fällen sollte die Eskalation persönlich oder per Telefon erfolgen.

4 Dokumentation der Informationstechnik

4.1 Beschreibung und Bestand der Hard- und Software

Planung, Steuerung, Kontrolle und Notfallvorsorge des IT-Einsatzes basieren auf einer aktuellen Dokumentation der vorhandenen Geschäftsprozesse, IT-Anwendungen und IT-Systeme. Wer nach IT-Grundschutz vorgegangen ist, sollte in der IT-Strukturanalyse bereits einen großen Teil der benötigten Informationen finden.

BSI-Standard 100-2

Oberstes Ziel muss sein, anhand einer guten Dokumentation die wichtigsten Geschäftsprozesse und ihre Abhängigkeit von IT-Anwendungen und IT-Systemen nachvollziehen zu können.

Bei einem Netzbetrieb ist die physikalische Netzstruktur und die logische

Netzkonfiguration zu dokumentieren.

Es ist zu erfassen, welche IT-Systeme betrieben werden und mit welcher Hard- und Software diese ausgestattet sind. Ein Bestandsverzeichnis der Systemsoftware sowie der zu dem IT-System gehörenden Systemdaten ist zu führen. Dazu gehört auch die Dokumentation der Systemkonfiguration. M 2.25

Die Dokumentation muss auch die wichtigsten IT-Anwendungen beschreiben und ihre Abhängigkeit von den IT-Systemen darstellen. Wichtig ist dabei auch, die minimalen Kapazitätsanforderungen von IT-Anwendungen zu erfassen. M 6.4

Alle Dokumentationen müssen für die jeweilige Zielgruppe verständlich sein und regelmäßig aktualisiert werden. Sie sind so aufzubewahren, dass sie im Bedarfsfall jederzeit verfügbar sind, aber trotzdem nur zuständigen Personen zugänglich sind.

Es ist zu prüfen, welche Dokumentation für die IT-Prozesse und IT-Anwendungen notwendig ist. Unter Umständen ist es unerlässlich, auch die Abhängigkeiten der IT-Anwendungen untereinander zu dokumentieren, um bei Problemen schnell alle Zusammenhänge überblicken zu können.

4.2 Schutzbedarf und Verfügbarkeitsanforderungen

Es ist festzulegen, welche Geschäftsprozesse von hoher Relevanz für die Geschäftstätigkeit sind und daher ein Verlust oder die Nicht-Verfügbarkeit einen hoher Schaden bedeutet.

Der Schutzbedarf der wichtigsten IT-Anwendungen (einschließlich der verarbeiteten Informationen) und IT-Systeme ist zu bestimmen. Dabei sind insbesondere die Verfügbarkeitsanforderungen festzulegen. M 6.1

4.3 Ersatzbeschaffungsplan

Wenn die Reparatur eines ausgefallenen IT-Systems nicht möglich ist oder zu lange dauert, kann eine Ersatzbeschaffung notwendig werden. Zur Vorbereitung ist ein Ersatzbeschaffungsplan mit folgenden Angaben zu erstellen: M 6.14

- Bezeichnung der IT-Komponente
- Hersteller
- Lieferant
- Dauer der Re-Installation

Ersatzbeschaffungspläne haben neben der Wiederherstellung der Verfügbarkeit des IT-Systems auch die Fortentwicklung der Informationstechnik zu berücksichtigen. Dies erfordert eine regelmäßige Überarbeitung des Ersatzbeschaffungsplans. Der Ersatzbeschaffungsplan ist der Dokumentation der IT-Systeme beizulegen.

4.4 Wiederanlaufreihenfolge

Technische oder ablaufbedingte Abhängigkeiten der IT-Systeme und IT-Anwendungen sowie deren Wichtigkeit beeinflussen die Wiederanlaufreihenfolge nach einem Ausfall eines IT-Systems oder dem Abbruch einer Anwendung. Entsprechende Zusammenhänge sind dokumentieren.

5 Beschreibung der Infrastruktureinrichtungen

Baupläne, Fluchtwegpläne, Feuerwehrlaufkarten etc. müssen dokumentiert werden. M 1.57

B. Anhang: Dokumente

Darüber hinaus sind alle gebäudeweiten Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung etc. und die Verkabelung von IT-Systemen zu dokumentieren. M 1.11 M 5.4

6 Ersatzverfahren und Ausweichmöglichkeiten

6.1 Manuelle Ersatzverfahren

Manuelle Ersatzverfahren für IT-Prozesse sind zeit- und arbeitsaufwendig, können aber kurzzeitig helfen, den Ausfall von IT-Anwendungen oder IT-Systemen zu kompensieren. Alle Fachverantwortlichen sollten für ihren Verantwortungsbereich manuelle Ersatzverfahren für den Notfall vorbereiten. Die erforderlichen Hilfsmittel (Faxgerät, Formulare, Papierlisten, Mikrofiche etc.) sind bereitzuhalten.

6.2 Ausweichmöglichkeiten

Angaben zu Ausweichmöglichkeiten sollten der Dokumentation der IT-Systeme beigefügt werden. Das Ausweichen auf alternative Rechenzentren, IT-Systeme, Arbeitsplätze etc. sollte in Notfallübungen ausreichend geprobt werden.

6.2.1 Interne Ausweichmöglichkeiten

Alle Fachverantwortlichen sollten prüfen, ob bei Problemen mit den standardmäßig genutzten IT-Systemen ein Ausweichen auf andere IT-Systeme möglich ist (z. B. Ausweichen auf den Entwicklungsrechner, wenn der Produktionsrechner ausfällt). Bei der Untersuchung von Ausweichmöglichkeiten ist insbesondere auf die technischen Anforderungen an das Ausweich-IT-System zu achten. Kompatibilität und ausreichende Kapazitätsreserven des Ausweich-IT-Systems sind Grundvoraussetzung für dessen Benutzung. M 6.6 M 6.4

6.2.2 Externe Ausweichmöglichkeiten

Externe Ausweichmöglichkeiten sind dann heranzuziehen, wenn mit internen Ausweichmöglichkeiten die Verfügbarkeitsanforderungen nicht mehr oder nicht wirtschaftlich erfüllt werden können. Ausweichmöglichkeiten für nicht IT-spezifische Komponenten sind auch zu berücksichtigen. Beispielsweise im Bereich der Infrastruktur sind Ausweichmöglichkeiten für Serverräume in Betracht zu ziehen.

Ausweicharbeitsplätze, -Räume, -Rechenzentren etc. sind so vorzubereiten, dass im Notfall die Wechselzeit tolerierbar ist.

6.2.3 Ausweichlösungen für DFÜ-Versorgung

Aufgrund der oftmals hohen Verfügbarkeitsanforderungen sind für die DFÜ-Verbindungen Ausweichlösungen bereitzuhalten. Ausweichmöglichkeiten sind beispielsweise: M 6.10

- Ersatz der Datenübertragung durch Austausch von Datenträgern oder Druckerzeugnissen per Kurier
- Datenübertragung über andere DFÜ-Einrichtungen
- Einsatz mobiler Kommunikationseinrichtungen

Der Notfallplan für den DFÜ-Ausfall beinhaltet die Handlungsanweisungen, die bei Ausfall von DFÜ-Einrichtungen durchzuführen sind.