



DER.4 Notfallmanagement

1. Beschreibung

1.1. Einleitung

In Notfällen müssen Institutionen weiter auf Informationen zugreifen können, um einen Geschäftsprozess, ein IT-System oder eine Fachaufgabe wiederherstellen zu können. Um die Informationssicherheit auch in einem Notfall aufrechterhalten zu können, sollten deshalb entsprechende Prozesse geplant, etabliert und überprüft werden.

Nur wenn geplant und organisiert vorgegangen wird, ist eine optimale Notfallvorsorge und Notfallbewältigung möglich. Ein professioneller Prozess zum Notfallmanagement reduziert die Auswirkungen eines Notfalls und sichert somit den Betrieb und Fortbestand der Institution. Es sind geeignete Maßnahmen zu identifizieren und umzusetzen, durch die zeitkritischen Geschäftsprozesse und Fachaufgaben zum einen robuster und ausfallsicherer werden. Zum anderen sollten diese Maßnahmen ermöglichen, einen Notfall schnell und zielgerichtet zu bewältigen.

Die Aufrechterhaltung der Informationssicherheit im Notfall ist in ein übergreifendes Notfallmanagement, idealerweise in ein Notfallmanagementsystem, einzubinden. Das Notfallmanagement hat jedoch einen eigenen Prozessverantwortlichen, den Notfallbeauftragten oder die Notfallbeauftragte, der oder die sich mit dem oder der ISB abstimmt.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Anforderungen zu beschreiben, um die Informationssicherheit in Institutionen selbst in kritischen Situationen zu gewährleisten. Dazu sind die entsprechenden Maßnahmen in ein ganzheitliches Notfallmanagement einzubetten. Zudem sind alle Aspekte zu betrachten, die erforderlich sind, um die Informationssicherheit auch bei Schadensereignissen oder Notfällen aufrechterhalten zu können. Dies reicht von der Planung bis zur Überprüfung aller Prozesse.

1.3. Abgrenzung und Modellierung

Der Baustein DER.4 *Notfallmanagement* ist immer für den gesamten Informationsverbund einmal anzuwenden.

Tritt ein Schadensereignis ein, müssen die richtigen Informationen vollständig und korrekt zur Verfügung stehen. Im vorliegenden Baustein werden weder Kriterien noch Prozesse erläutert, anhand derer die Verantwortlichen entscheiden können, ob ein Notfall vorliegt oder nicht. Die Entscheidung

darüber wird getroffen, während der Sicherheitsvorfall behandelt wird (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

Krisen werden im Rahmen eines eigenen Krisenmanagements betrachtet und in diesem Baustein nur als Schnittstelle behandelt, z. B. im Rahmen der weiteren Eskalation von Notfällen. Weiterführende Informationen zu den einzelnen Phasen des Notfallmanagements sowie der Abgrenzung des Notfallmanagements zum Krisenmanagement sind im BSI-Standard 100-4 „Notfallmanagement“ enthalten.

2. Gefährdungslage

Da IT-Grundsicherheits-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein DER.4 *Notfallmanagement* von besonderer Bedeutung.

2.1. Personalausfall

Fällt Personal aus, kann das schnell bedeuten, dass eine Institution ihre Fachaufgaben und Geschäftsprozesse nicht mehr ausführen kann. Die Gründe für einen Personalausfall können vielfältig sein. Durch Keime in der Kantine oder einen Streik können beispielsweise viele Mitarbeitende gleichzeitig ausfallen. Auch der Tod eines Mitarbeitenden kann zu Ausfällen oder Beeinträchtigungen von wichtigen Geschäftsprozessen oder Fachaufgaben führen. Zudem könnten relevante Informationen zum Wiederanlauf des Geschäftsprozesses oder der IT-Systeme nicht mehr zugänglich sein. Oft verfügen einzelne Personen über spezifisches Fachwissen (Kopfmonopole), sodass ein Schaden auch dann eintreten kann, wenn der Personalausfall zahlenmäßig nur sehr gering ist.

2.2. Ausfall von IT-Systemen

Fallen Komponenten eines IT-Systems aus, z. B. durch defekte Hardware oder einen Stromausfall, kann der gesamte IT-Betrieb gestört werden. Dadurch ist die Verfügbarkeit der jeweiligen Informationen und damit auch des jeweiligen Geschäftsprozesses gefährdet. Zudem können wichtige Informationen, die für Wiederanlaufmaßnahmen benötigt werden, nicht zur Verfügung stehen.

2.3. Ausfall eines Weitverkehrsnetzes (WAN)

Die Ursachen für den Ausfall eines Weitverkehrsnetzes (Wide Area Network, WAN) können vielfältig sein. Daher ist es möglich, dass sich ein Netzausfall lediglich auf einzelne Benutzende, einen Anbietenden oder eine bestimmte Region auswirkt. Häufig stören solche Ausfälle nur kurz und betreffen dann nur die Geschäftsprozesse und Fachaufgaben, die eine entsprechend hohe Verfügbarkeit des WAN benötigen. Es gibt aber auch immer wieder längere Ausfälle, die massive Probleme in der Kommunikation und Erreichbarkeit nach sich ziehen können.

2.4. Ausfall eines Gebäudes

Gebäude können unvorhergesehen unbenutzbar werden, z. B. weil sie durch Feuer, Sturm, Hochwasser, Erdbeben oder eine Explosion teilweise oder vollständig zerstört wurden. Ein Gebäude kann aber auch ausfallen, weil die Polizei oder die Feuerwehr das Umfeld sperrt und das Gebäude nicht mehr betreten werden kann oder verlassen werden muss, etwa weil Strom, Wasser, Abwasser, Heizung oder Klimatisierung über einen gewissen Zeitraum nicht mehr funktionieren.

2.5. Ausfall einer Lieferung oder Dienstleistung

Sind Institutionen von Dienstleistungen abhängig, kann dies schnell zu Unterbrechungen der eigenen betrieblichen Kontinuität führen, wenn die dienstleistende oder liefernde Institution teilweise oder vollständig ausfällt. Wird beispielsweise zur Produktion die Lieferung eines bestimmten Werkstoffs benötigt und diese Lieferung fällt aus, so ist möglicherweise die gesamte Produktion gefährdet. Aber auch der Ausfall eines extern bereitgestellten Dienstes, wie z. B. einer Cloud oder auch E-Mail, kann den eigenen Betrieb sehr stark einschränken, bzw. sogar komplett unterbrechen. Dies gefährdet insbesondere kritische Geschäftsprozesse und Fachaufgaben.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.4 *Notfallmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Notfallbeauftragte
Weitere Zuständigkeiten	Informationssicherheitsbeauftragte (ISB), Vorgesetzte, Institutionsleitung, Personalabteilung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

DER.4.A1 Erstellung eines Notfallhandbuchs (S)

Es SOLLTE ein Notfallhandbuch erstellt werden, in dem die wichtigsten Informationen zu

- Rollen,
- Sofortmaßnahmen,
- Alarmierung und Eskalation sowie
- Kommunikations-, grundsätzlichen Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungsplänen

enthalten sind. Zuständigkeiten und Befugnisse SOLLTEN zugewiesen, kommuniziert und im Notfallhandbuch festgehalten werden. Es SOLLTE sichergestellt sein, dass im Notfall entsprechend geschultes Personal zur Verfügung steht. Es SOLLTE regelmäßig durch Tests und Übungen überprüft werden, ob die im Notfallhandbuch beschriebenen Maßnahmen auch wie vorgesehen funktionieren.

Es SOLLTE regelmäßig geprüft werden, ob das Notfallhandbuch noch aktuell ist. Gegebenenfalls SOLLTE es aktualisiert werden. Es SOLLTE auch im Notfall zugänglich sein. Das Notfallhandbuch SOLLTE um Verhaltensregeln für spezielle Fälle ergänzt werden, z. B. Brand. Die Regeln SOLLTEN allen Mitarbeitenden bekanntgegeben werden.

DER.4.A2 Integration von Notfallmanagement und Informationssicherheitsmanagement (S) [Informationssicherheitsbeauftragte (ISB)]

Die Prozesse im Sicherheitsmanagement SOLLTEN mit dem Notfallmanagement abgestimmt werden (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

DER.4.A3 Festlegung des Geltungsbereichs und der Notfallmanagementstrategie (H) [Institutionsleitung]

Der Geltungsbereich für das Notfallmanagementsystem SOLLTE eindeutig festgelegt werden. Die Institutionsleitung SOLLTE eine Notfallmanagementstrategie festlegen, welche die angestrebten Ziele und das Risikoakzeptanzniveau darlegen.

DER.4.A4 Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Institutionsleitung (H) [Institutionsleitung]

Die Institutionsleitung SOLLTE eine Leitlinie zum Notfallmanagement verabschieden. Diese SOLLTE die wesentlichen Eckpunkte des Notfallmanagements enthalten. Die Leitlinie zum Notfallmanagement SOLLTE regelmäßig überprüft und gegebenenfalls überarbeitet werden. Sie SOLLTE allen Mitarbeitenden bekanntgegeben werden.

DER.4.A5 Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement (H) [Institutionsleitung]

Die Rollen für das Notfallmanagement SOLLTEN für die Gegebenheiten der Institution angemessen festgelegt werden. Dies SOLLTE mit den Aufgaben, Pflichten und Kompetenzen der Rollen schriftlich dokumentiert werden. Es SOLLTEN für alle Rollen im Notfallmanagement qualifizierte Mitarbeitende benannt werden. Die Organisationsstruktur im Notfallmanagement SOLLTE regelmäßig darauf überprüft werden, ob sie praxistauglich, effektiv und effizient ist.

DER.4.A6 Bereitstellung angemessener Ressourcen für das Notfallmanagement (H) [Institutionsleitung]

Die finanziellen, technischen und personellen Ressourcen für die angestrebten Ziele des Notfallmanagements SOLLTEN angemessen sein. Der oder die Notfallbeauftragte bzw. das Notfallmanagement-Team SOLLTE über genügend Zeit für die Aufgaben im Notfallmanagement verfügen.

DER.4.A7 Erstellung eines Notfallkonzepts (H) [Institutionsleitung]

Alle kritischen Geschäftsprozesse und Ressourcen SOLLTEN identifiziert werden, beispielsweise mit einer Business-Impact-Analyse (BIA). Es SOLLTEN die wichtigsten relevanten Risiken für die kritischen Geschäftsprozesse und Fachaufgaben sowie deren Ressourcen identifiziert werden. Für jedes identifizierte Risiko SOLLTE entschieden werden, welche Risikostrategien zur Risikobehandlung eingesetzt werden sollen. Es SOLLTEN Kontinuitätsstrategien entwickelt werden, die einen

Wiederanlauf und eine Wiederherstellung der kritischen Geschäftsprozesse in der geforderten Zeit ermöglichen. Es SOLLTE ein Notfallkonzept erstellt werden. Es SOLLTEN solche Notfallpläne und Maßnahmen entwickelt und implementiert werden, die eine effektive Notfallbewältigung und eine schnelle Wiederaufnahme der kritischen Geschäftsprozesse ermöglichen. Im Notfallkonzept SOLLTE die Informationssicherheit berücksichtigt und entsprechende Sicherheitskonzepte für die Notfalllösungen entwickelt werden.

DER.4.A8 Integration der Mitarbeitenden in den Notfallmanagement-Prozess (H) [Vorgesetzte, Personalabteilung]

Alle Mitarbeitenden SOLLTEN regelmäßig für das Thema Notfallmanagement sensibilisiert werden. Zum Notfallmanagement SOLLTE es ein Schulungs- und Sensibilisierungskonzept geben. Die Mitarbeitenden im Notfallmanagement-Team SOLLTEN regelmäßig geschult werden, um die benötigten Kompetenzen aufzubauen.

DER.4.A9 Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse (H) [Institutionsleitung]

Es SOLLTE sichergestellt werden, dass Aspekte des Notfallmanagements in allen Geschäftsprozessen und Fachaufgaben der Institution berücksichtigt werden. Die Prozesse, Vorgaben und Verantwortlichkeiten im Notfallmanagement SOLLTEN mit dem Risikomanagement und Krisenmanagement abgestimmt werden.

DER.4.A10 Tests und Notfallübungen (H) [Institutionsleitung]

Alle wesentlichen Sofortmaßnahmen und Notfallpläne SOLLTEN in angemessener Weise regelmäßig und anlassbezogen getestet und geübt werden. Der zeitliche Rahmen und die fachliche Abdeckung aller Übungen SOLLTEN übergreifend in einem Übungsplan dokumentiert werden. Im Notfallmanagement SOLLTEN ausreichend Ressourcen für die Planung, Konzeption, Durchführung und Auswertung der Tests und Übungen bereitgestellt werden.

DER.4.A11 ENTFALLEN (H)

Diese Anforderung ist entfallen.

DER.4.A12 Dokumentation im Notfallmanagement-Prozess (H)

Der Ablauf des Notfallmanagement-Prozesses, die Arbeitsergebnisse der einzelnen Phasen und wichtige Entscheidungen SOLLTEN dokumentiert werden. Ein festgelegtes Verfahren SOLLTE sicherstellen, dass diese Dokumente regelmäßig aktualisiert werden. Darüber hinaus SOLLTE der Zugriff auf die Dokumentation auf autorisierte Personen beschränkt werden.

DER.4.A13 Überprüfung und Steuerung des Notfallmanagement-Systems (H) [Institutionsleitung]

Die Institutionsleitung SOLLTE sich regelmäßig anhand von Managementberichten über den Stand des Notfallmanagements informieren. Sie SOLLTE so das Notfallmanagement-System regelmäßig überprüfen, bewerten und gegebenenfalls korrigieren.

DER.4.A14 Regelmäßige Überprüfung und Verbesserung der Notfallmaßnahmen (H) [Institutionsleitung]

Alle Notfallmaßnahmen SOLLTEN regelmäßig oder bei größeren Änderungen daraufhin überprüft werden, ob sie noch eingehalten und korrekt umgesetzt werden. Es SOLLTE geprüft werden, ob sie sich noch dazu eignen, die definierten Ziele zu erreichen.

Dabei SOLLTE untersucht werden, ob technische Maßnahmen korrekt implementiert und konfiguriert wurden und ob organisatorische Maßnahmen effektiv und effizient umgesetzt sind. Bei Abweichungen SOLLTEN die Ursachen für die Mängel ermittelt und Verbesserungsmaßnahmen veranlasst werden. Diese Ergebnisübersicht SOLLTE von der Institutionsleitung freigegeben werden. Es SOLLTE zudem

ein Prozess etabliert werden, der steuert und überwacht, ob und wie die Verbesserungsmaßnahmen umgesetzt werden. Verzögerungen SOLLTEN frühzeitig an die Institutionsleitung gemeldet werden.

Es SOLLTE von der Institutionsleitung festgelegt sein, wie die Überprüfungen koordiniert werden. Die Überprüfungen SOLLTEN so geplant werden, dass kein relevanter Teil ausgelassen wird. Insbesondere SOLLTEN die im Bereich der Revision, der IT, des Sicherheitsmanagements, des Informationssicherheitsmanagements und des Notfallmanagements durchgeführten Überprüfungen miteinander koordiniert werden. Dazu SOLLTE geregelt werden, welche Maßnahmen wann und von wem überprüft werden.

DER.4.A15 Bewertung der Leistungsfähigkeit des Notfallmanagementsystems (H) [Institutionsleitung]

Es SOLLTE regelmäßig bewertet werden, wie leistungsfähig und effektiv das Notfallmanagement-System ist. Als Grundlage SOLLTEN Mess- und Bewertungskriterien wie z. B. Leistungskennzahlen definiert werden. Diese Messgrößen SOLLTEN regelmäßig ermittelt und mit geeigneten vorangegangenen Werten, mindestens aber mit den Vorjahreswerten, verglichen werden. Weichen die Werte negativ ab, SOLLTEN die Ursachen ermittelt und Verbesserungsmaßnahmen definiert werden. Die Ergebnisse der Bewertung SOLLTEN an die Leitung berichtet werden.

Die Leitung SOLLTE entscheiden, mit welchen Maßnahmen das Notfallmanagement weiterentwickelt werden soll. Alle Entscheidungen der Institutionsleitung SOLLTEN dokumentiert und die bisherigen Aufzeichnungen aktualisiert werden.

DER.4.A16 Notfallvorsorge- und Notfallreaktionsplanung für ausgelagerte Komponenten (H) [Institutionsleitung]

Bei der Notfallvorsorge- und Notfallreaktionsplanung für ausgelagerte Komponenten SOLLTE regelmäßig das Notfallmanagement der liefernden oder dienstleistenden Institution in den unterzeichneten Verträgen geprüft werden. Auch SOLLTEN die Abläufe in Notfalltests und -übungen mit der liefernden oder bereitstellenden Institution abgestimmt und, wenn angemessen, gemeinsam durchgeführt werden.

Die Ergebnisse und Auswertungen SOLLTEN regelmäßig zwischen der Institutionsleitung und den liefernden Institutionen oder Dienstleistenden ausgetauscht werden. In den Auswertungen SOLLTEN auch eventuelle Verbesserungsmaßnahmen enthalten sein.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology - Security techniques - Information security management systems - Requirements“ im Anhang A17 „Information security aspects of business continuity management“ Vorgaben für die Sicherstellung der Informationssicherheit im Notfall.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 22301:2012 „Societal security - Business continuity management systems - Requirements“ ein Rahmenwerk für ein Business Continuity Management (BCM), in das die Anforderungen aus der oben genannten Norm ISO/IEC 27001:2013 beispielsweise integriert werden können.

Der BSI-Standard 100-4 „Notfallmanagement“ beschreibt, wie ein BCM etabliert, aufrechterhalten und kontinuierlich verbessert werden kann.

Das vom BSI veröffentlichte Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4 (UMRA) beinhaltet weitere Hilfsmittel, um die Etablierung eines BCMSs zu erleichtern.

Zusätzlich bietet der Webkurs „Notfallmanagement“ nach dem BSI-Standard 100-4 eine Einführung in das Thema.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in der Kategorie BC - Business Continuity - Vorgaben zur Business Continuity. Es fordert dort unter anderem auch, dass die Kontinuitätsstrategie mit der Informationssicherheitsstrategie abgestimmt sein soll.

Das National Institute of Standards and Technology (NIST) stellt in seiner Special Publication 800-34, Rev. 1, „Contingency Planning Guide for Federal Information Systems“, einen Leitfaden zur Erstellung einer Kontinuitätsplanung von (bundesstaatlichen) Informationssystemen zur Verfügung, der auch die Informationssicherheit berücksichtigt. Zusätzlich liefert dieses Dokument auch Informationen über Zusammenhänge zwischen einer solchen Kontinuitätsplanung von Informationssystemen und anderen Arten von sicherheits- und notfallmanagementbezogenen Kontinuitätsplänen, z. B. einem Business Continuity Plan.