Der neue BSI-Standard BSI 100-4 „Notfallmanagement“

In Ergänzung zu den BSI-Standards 100-1 bis 100-3 [1,2,3] wird das Thema Notfallvorsorge und Notfallbehandlung demnächst in einem neuen BSI-Standard 100-4 behandelt. Die Informationen, die bei der Erstellung eines IT-Sicherheitskonzepts zusammengestellt werden, können in eine Notfallvorsorge-Konzeption mit einfließen. Ebenso ist es nützlich, beispielsweise gewonnene Ergebnisse aus einer Business-Impact-Analyse (BIA) in die Sicherheitskonzeption mit einfließen zu lassen.

Von Robert Kallwies, HiSolutions AG und Angelika Jaschob, BSI.

Die Informationssicherheit ist integraler Bestandteil aller Geschäftsprozesse und hat einen wesentlichen Einfluss auf die Qualität, Effizienz und Wirtschaftlichkeit der Aufgabenerfüllung einer Institution. Der Umgang mit Informationssicherheit berührt viele Bereiche eines Unternehmens, zum Beispiel die IT-Infrastruktur, Personal, physische Umgebungen, IT-Systeme, Anwendungen et cetera. Zudem sind gesetzliche Anforderungen und internationale Normen, wie zum Beispiel ISO 27001, einzuhalten.

Institutionen, sowohl Behörden als auch Wirtschaftsunternehmen, sind hochgradig abhängig vom ordnungsgemäßen Funktionieren der Versorgungsnetze. Dazu gehören heutzutage nicht nur die Wasser- und Energienetze, sondern auch die Informations- und Kommunikationsnetze. Die Informations- und Kommunikationstechnik entwickelt sich rasant – jede neue Technik umfasst auch immer andere Sicherheitsrisiken. Um diesen angemessen begegnen zu können, müssen frühzeitig geeignete Sicherheitsmaßnahmen konzipiert werden. Aber auch die Wiederherstellung kritischer Geschäftsprozesse nach einem Notfall (Krise) sind für die Institutionen immer wichtiger.

Zur stabilen Ausgestaltung von Unternehmensprozessen muss ein Notfallmanagement alle potenziellen Ursachen für eine Störung des Betriebs betrachten. Eine Institution, die über mehrere verteilte Standorte mit redundanten und vergleichbaren Aufgaben und Techniken verfügt, ist gut aufgestellt – dieser Zustand ist jedoch eher selten anzutreffen. Durch die immer stärkere Globalisierung und Zentralisierung von Aufgaben, Geschäftsprozessen und Standorten steigt die Abhängigkeit von einzelnen zentralisierten und spezialisierten Standorten. Daher ist eine Einführung eines Notfallmanagement-Prozesses von großer Bedeutung.

Regularien, wie zum Beispiel die „Mindestanforderungen an das Risikomanagement“ (MaRisk) im Bankenbereich, fordern weit mehr als die Fokussierung auf den ausfallsicheren Betrieb der IT. Vielmehr besteht die Forderung für alle kritischen Geschäftsprozesse eine Notfallvorsorge zu treffen.

IT-Grundschutz

Das Grundschutzhandbuch des BSI war bis Ende 2005 stark auf IT-Sicherheit fokussiert. Auf dieser Ebene wurden Maßnahmen und Gefährdungen auf einem hohen Detaillierungsgrad, das heißt konkrete Maßnahmenvorschläge für IT-Komponenten, beschrieben. Mit der Synchronisation des IT-Grundschutzhandbuchs mit dem Standard ISO 27001 „Information Security Management“ erfolgte ein Paradigmenwechsel mit dem Ziel einer ganzheitlichen prozessbezogenen Betrachtung der IT-Sicherheit.

Zu den herausfordernden Aufgaben für IT-Sicherheitsverantwortliche gehört es, den Überblick über die abzusichernden Geschäftsprozesse und die zugehörige IT zu bewahren und angemessene Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Mit dem IT-Grundschutz bietet das BSI hierfür eine einfache Methode an. Mit der Kombination aus der IT-Grundschutz-Vorgehensweise im BSI-Standard 100-2 [2] und den IT-Grundschutz-Katalogen [4] stellt das BSI sowohl eine Sammlung von IT-Sicherheitsmaßnahmen als auch eine entsprechende Methodik zur Auswahl und Anpassung geeigneter Maßnahmen zur Verfügung.

Der Grundschutzbaustein 1.3 „Notfallvorsorge-Konzept“ der IT-Grundschutz-Kataloge, der bis heute die Empfehlungen für ein Notfallmanagement in Unternehmen darstellt, ist bisher jedoch ausschließlich technisch fokussiert. Eine ausreichende Betrachtung eines iterativen Prozessregelkreises erfolgt bisher nicht. Daher wurde es erforderlich, diese Lücke zu schließen und für den Bereich Notfallmanagement eine angemessene Vorgabe zu entwickeln. Der neue Standard BSI 100-4 „Notfallmanagement“ wird die eigenverantwortliche Notfallvorsorge und Notfallbehandlung der Institutionen unterstützten und wird sich in die IT-Grundschutzmethodik [2]

und die Risikoanalyse auf Basis von IT-Grundschutz [3] integrieren.

Normen und Standards

Weltweit existieren verschiedenste Standards zur Implementierung eines Notfallmanagements. Mit dem im November letzten Jahres veröffentlichen British Standard BS 25999 „Business continuity management – Part 1: Code of practice“ [5] steht im europäischen Raum ein Standard zur Verfügung, der das ganzheitliche Business-Continuity-Management (BCM) behandelt. Der BS 25999 beschreibt auf abstrakter Ebene die Etablierung eines BCM-Prozesses. Hier im deutschsprachigen Raum mangelt es jedoch an Standards und Leitfäden zum Aufbau und Umsetzung eines umfassenden Notfallmanagements.

Die Inhalte des BS 25999 sind der Ausgangspunkt für die Neugestaltung des Notfallmanagements nach IT-Grundschutz. Der neue Standard BSI 100-4 wird jedoch nicht nur eine abstrakte Vorgehensweise wie der BS 25999-1 beschreiben. Er wird – wo es möglich und sinnvoll ist – auch konkrete Hinweise zur Umsetzung geben.

Weitere relevante Standards, die sich mit Notfallmanagement beschäftigen, sind ITIL (Service Continuity, [7]), die Public Available Specification 77 [8] und NIST 800-34 [9]. Es wurde versucht, die Stärken der bereits bestehenden Standards aufzunehmen und Synergieeffekte zu nutzen. Insbesondere wurde die vollständige Kompatibilität mit dem Standard 25999-2 [6] erreicht und nachgewiesen.

Inhalt des BSI-Standards 100-4

Das Notfallmanagement bietet eine Hilfestellung zur Vorbereitung und Bewältigung von Schadensereignissen in einer Institution, aufbauend auf dem IT-Sicherheitsprozess. Für die Gestaltung des Notfallmanagements ist ein systematisches Vorgehen erforderlich. Im Standard BSI 100-4 werden Wege und Methoden für das generelle Vorgehen, aber auch für die Lösung spezieller Probleme aufgezeigt. Die nachstehende Vorgehensweise, zum Aufbau und Betreiben eines Notfallmanagements, besteht aus folgenden Phasen:

- Planung und Konzeption der Notfallvorsorge,
- Erstellung eines Notfallhandbuchs zur Notfallbewältigung,
- Etablierung und Pflege einer Notfallmanagement-Kultur,
- Planung und Durchführung von Übungen und Tests,
- permanente Aufrechterhaltung des Notfallmanagements.

Einige dieser Phasen können auch parallel durchgeführt werden, zum Beispiel sollten Maßnahmen zur Schulung und Sensibilisierung zu Notfallmanagement-Aspekten während des gesamten Prozesses angelegt werden.

Planung und Konzeption zur Notfallvorsorge

Eine Leitlinie (Policy) zum Notfallmanagement, welche von der Unternehmensleitung initiiert und freigegeben wird, ist zur Einführung zu erstellen. Als weitere Basisarbeit sind im Rahmen der Schaffung der organisatorischen Voraussetzungen für das Notfallmanagement Rollenbeschreibungen zu erstellen und Verantwortliche für das Notfallmanagement zu ernennen. Ein Mitglied der Geschäftsführung sollte für die Etablierung und Aufrechterhaltung des Notfallmanagements verantwortlich sein.

Basis für alle weiteren Aktivitäten zum Notfallmanagement ist eine Business-Impact-Analyse (BIA). Diese geht weit über eine Schutzbedarfsfeststellung des BSI hinaus. Das Ziel einer BIA ist die Identifizierung der kritischen Geschäftsprozesse und zugehöriger Ressourcen (Personal, Anwendungen, Daten usw.). Ein besonderes Augenmerk gilt der Ermittlung von so genannten „Single Points of Failure“, also Ressourcen, bei deren Ausfall ein Geschäftsprozess nicht mehr ausgeführt werden kann. Innerhalb der BIA können auch Mindestanforderungen an einen potenziellen Notbetrieb mit erhoben werden.

Einer der wichtigsten Punkte bei der BIA ist die Ermittlung der maximal tolerierbaren Ausfallzeit aufgrund der entstehenden Schäden, die über eine Ausfallzeitachse monetär beziffert werden können. Es können jedoch auch Faktoren wie vertragliche Anforderungen oder zu erwartender Imageschaden bewertet werden. Die maximal tolerierbare Ausfallzeit dient später bei der Auswahl der Notfallvorsorgestrategie als Kerngröße. Hat beispielsweise ein Zahlungsverkehrsprozess einer Bank eine maximal tolerierbare Ausfallzeit von 15 Minuten, so müssen alle beteiligten Ressourcen – vor allem die IT-Komponenten – redundant ausgelegt sein, damit diese Anforderungen eingehalten werden können.

Im Anschluss an die BIA folgt eine Risikoanalyse, in der ermittelt wird, welche Risiken auf die als kritisch eingestuften Ressourcen wirken. Die Risikoanalyse umfasst die Erhebung von Schwachstellen und Bedrohungen. Den Risiken muss mit Notfallvorsorgestrategien und -maßnahmen begegnet werden. In welchem Umfang Maßnahmen gewählt werden, hängt im Wesentlichen von der Risikobereitschaft eines Unternehmens ab. Zur Umsetzung der Strategien werden konkrete Maßnahmen definiert, in einem Notfallvorsorgekonzept beschrieben und entsprechend umgesetzt.

Erstellung eines Notfallhandbuchs zur Notfallbewältigung

Zur Unterstützung einer raschen Notfallbewältigung ist ein

Notfallhandbuch zu erstellen. Hier wird der BSI 100-4 ein Beispiel vorgeben, wie ein Notfallhandbuch zu strukturieren ist und welche Mindestinhalte zu beschreiben sind. Nachfolgend werden beispielhaft Kerninhalte dargestellt:

_____ Krisenmanagement: Welche Aufgaben hat ein Krisenstab in der Notfallbewältigung?
_____ Alarmierungsplan und Meldewege: Welches Mitglied der Notfallteams kann über welche Medien (Telefon, SMS, E-Mail, Kurier) alarmiert werden?
_____ Konkrete Aufgaben für einzelne Personen/Funktionen im Notfall: Welche Aufgaben haben die Notfallteams?
_____ Wiederanlauf: Welche Maßnahmen müssen umgesetzt werden, um in den Notbetrieb zu gelangen (z. B. Inbetriebnahme eines Alternativstandorts)?
_____ Notbetrieb: Wie wird der Notbetrieb der kritischen Prozesse sichergestellt?
_____ Wiederherstellung: Welche Maßnahmen müssen umgesetzt werden, um wieder in den Normalbetrieb übergehen zu können (z. B. Renovierung eines Gebäudes nach einem großflächigen Wasserschaden)?
_____ Rückkehr in den Normalbetrieb: Ab welchem Zeitpunkt kann mit welchen Schritten in den Normalbetrieb zurückgekehrt werden?

Etablierung und Pflege einer Notfallmanagement-Kultur

Das Notfallmanagement sollte wie andere unternehmensübergreifende Themen, beispielsweise Arbeitssicherheit oder IT-Sicherheit, in der Unternehmenskultur fest verankert werden. Im Standard werden Maßnahmen zur Umsetzung aufgezeigt, wie beispielsweise Schulung und Sensibilisierung der Mitarbeiter.

Planung und Durchführung von Übungen und Tests

Zur Sicherstellung der Wirksamkeit der entwickelten Maßnahmen und Verfahren zur Notfallbewältigung sollten Übungen durchgeführt werden. Das Üben der Abläufe und Verfahren schult auch die Mitglieder der Notfallteams. Technische Vorsorgemaßnahmen werden im Rahmen von Tests auf Funktion und Wirksamkeit verifiziert. Der BSI 100-4 zeigt auf, wie Übungspläne und -konzepte aufgebaut sein sollten. Die verschiedenen Testarten und deren inhaltliche Ausgestaltung werden ebenfalls beschrieben.

Permanente Aufrechterhaltung des Notfallmanagements

Zur Aufrechterhaltung des Notfallmanagements gehören sowohl die regelmäßige Aktualisierung der Dokumente als auch die Überprüfung und Pflege von Notfallvorsorgemaßnahmen. Zusätzlich sollte eine regelmäßige Bewertung der Angemessenheit des Notfallmanagements erfolgen, um Verbesserungspotenzial zu erkennen und umsetzen zu können. Auch für diese Punkte zeigt der Standard Möglichkeiten der Gestaltung auf.

Fazit

Mit dem neuen BSI-Standard 100-4 werden die sich aus der klassischen IT-Grundschutz-Vorgehensweise ergebenden Aussagen zum Thema Verfügbarkeit konkretisiert und differenziert. Bei vollständiger Umsetzung dieses Standards und des korrespondierenden Bausteins in den IT-Grundschutz-Katalogen kann jede Institution ein effizientes Notfallmanagement etablieren. Der Entwurf des BSI-Standards 100-4 wird derzeit mit externen Anwendern diskutiert; seine Veröffentlichung soll im Sommer erfolgen. ■

Literatur

[1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.0, Dezember 2005, www.bsi.bund.de/literat/bsi_standard/standard_1001.pdf

[2] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 1.0, Dezember 2005, www.bsi.bund.de/literat/bsi_standard/standard_1002.pdf

[3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.0, Dezember 2005, www.bsi.bund.de/literat/bsi_standard/standard_1003.pdf

[4] BSI, IT-Grundschutz-Kataloge, Standardsicherheitsmaßnahmen, Loseblattsammlung, Schriftenreihe Band 3, Bundesanzeiger-Verlag, ISBN 978-3-88784-915-3, online auf www.bsi.bund.de/gshb/

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

[6] British Standards Institute, BS 25999-2, Business continuity management, Part 2: Specification, www.thebci.org/standards.htm

[7] IT Infrastructure Library, Service Management – ITIL (IT Infrastructure Library), www.ogc.gov.uk/guidance_itil.asp

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

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