Bundesamt
für Sicherheit in der
Informationstechnik

Notfall-management

BSI-Standard 100-4 zur Business Continuity

PRAXISWISSEN PROFESSIONALS

PRAXISWISSEN PROFESSIONALS PDF

Bundesanzeiger Verlag

Vorwort

Aufgrund der zunehmenden Komplexität von technischen Informationssystemen sowie der verstärkten Automatisierung von Geschäftsprozessen können Katastrophen wie Hochwasser oder flächendeckende Stromausfälle, Pandemien, Brände, aber auch Virenbefall oder Hackerangriffe zu einer existenziellen Gefährdung von Unternehmen und Behörden führen. Selbst kurzfristige Unterbrechungen wichtiger Geschäftsprozesse können erhebliche Auswirkungen haben und große Schäden verursachen. Um die Überlebensfähigkeit von Unternehmen und Behörden zu erhöhen, fordern gesetzliche Vorgaben wie Basel II, Solvency II, Sarbanes-Oxley-Act oder KonTraG die Etablierung eines Notfallmanagements und die Erstellung von Notfallkonzepten.

Nur die Planung und Umsetzung eines Notfallmanagements kann dazu beitragen, die Risiken für Geschäftsunterbrechungen zu minimieren. Damit wird zugleich die Voraussetzung für eine erfolgreiche und koordinierte Bewältigung von Notfällen und Krisen geschaffen. Es gilt, die Auswirkungen von Szenarien mit hohem Schadenspotenzial zu begrenzen, den Geschäftsbetrieb im Schadensfall schnell wieder herzustellen und wirtschaftliche Schäden wie auch Imageverluste zu minimieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschäftigt sich seit langem mit dem Thema Notfallmanagement. Seit der ersten Ausgabe der IT-Grundschutz-Kataloge gibt es einen Baustein zur Notfallvorsorge. Darauf aufbauend wurde jetzt der BSI-Standard zur Business Continuity erstellt, mit dem das BSI einen wichtigen Beitrag zur Sensibilisierung und fachlichen Unterstützung von Behörden und Unternehmen leistet. Er beschreibt bewährte Herangehensweisen zum Aufbau eines Notfallmanagement-Prozesses, gibt wertvolle Hilfestellung und dient der Vereinheitlichung von Fachbegriffen. Durch die ganzheitliche Betrachtungsweise können die Empfehlungen relativ einfach an die individuellen Gegebenheiten von Unternehmen und Behörden angepasst werden.

Bonn, im Dezember 2008

Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Inhaltsverzeichnis

Notfallmanagement: BSI-Standard 100-4 zur Business Continuity

Version 1.0
Stand: November 2008

Kontakt:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat IT-Sicherheitsmanagement und IT-Grundschutz
E-Mail: grundschutz@bsi.bund.de
Internet: www.bsi.bund.de/grundschutz

1 Einleitung

1.1 Versionshistorie

Stand	Version	Verfasser
November 2008	1.0	BSI

1.2 Zielsetzung

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

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

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

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

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

1.3 Adressatenkreis

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

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

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

1.4 Anwendungsweise

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

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

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

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

1.5 Literaturverzeichnis

[BMIKI] Bundesministerium des Innern (BMI), Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden, Dez. 2007

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2 Notfallmanagement und IT-Grundschutz

2.1 Einordnung in die BSI-Standards

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

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

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

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

2.2 Begriffe

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

Störung

Eine Störung ist eine Situation, in der Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die dadurch entstehenden Schäden sind als gering einzustufen. Ein „geringer" Schaden ist ein Schaden, welcher im Verhältnis zum Gesamtjahresergebnis eines Unternehmens bzw. zum Haushaltsvolumen einer Behörde zu vernachlässigen ist oder die Aufgabenerfüllung nur unwesentlich beeinträchtigt. Störungen werden durch die im allgemeinen Tagesgeschäft integrierte Störungsbehebung beseitigt. Störungen können sich jedoch zu einem Notfall ausweiten und sind deshalb genau zu beobachten, sorgfältig zu dokumentieren und zeitnah zu beheben. Dies ist jedoch nicht Teil des Notfallmanagements, sondern Aufgabe des Störungsmanagements.

Notfall

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

Krise

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

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

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

Katastrophe

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

stellt sich eine Katastrophe als Krise dar und wird intern durch die Notfallbewältigung der Institution in Zusammenarbeit mit den externen Hilfsorganisationen bewältigt.

2.3 Weitere Standards für Notfallmanagement

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

BS 25999-1/BS 25999-2

Der im November 2006 vom British Standards Institute veröffentlichte BS 25999-1 „Business Continuity Management – Part 1: Code of Practice" beschreibt den Aufbau eines Management-Systems für das Notfallmanagement [BS259991]. Dazu zählt unter anderem die Organisationsstruktur, die Umsetzung eines Business Continuity Management Prozesses auf Basis von Good Practice Vorgaben und die Konzeption organisatorischer Maßnahmen. Die detaillierten Arbeitsschritte oder konkrete Maßnahmen für ein Notfallmanagement werden nicht beschrieben. Hierfür wird auf weitere Standards wie ISO 27001, ISO 20000 oder PAS77 verwiesen.

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

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

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

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

Good Practice Guidelines (GPG)

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

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

Die BCI GPG 2008 sind in sechs Sektionen eingeteilt:

- Sektion 1: BCM Policy & Programme Management (Entwicklen der BCM-Vorgaben und Prozess-Management),

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

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

ISO/PAS 22399

Die Vornorm ISO/PAS 22399 „Societal security – Guideline for incident preparedness and operational continuity management" wurde 2007 veröffentlicht [ISO22399]. Diese Vornorm „Sicherheit und Schutz des Gemeinwesens – Leitfaden für Planung, Vorbereitung und operationelle Kontinuität" beschreibt in der bekannten generischen Art von ISO-Normen auf 31 Seiten den Prozess und die Prinzipien für „Incident Preparedness and Operational Continuity Management" (IPOCM). Der IPOCM-Lifecycle gliedert sich in die Phasen:

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

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

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

ISO 27001/ISO 27002

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

Bei der ISO/IEC 27002 (bisher ISO/IEC 17799) „Information technology – Code of practice for information security management" [ISO27002] handelt es sich um eine Sammlung von Erfahrungen, Verfahren und Methoden aus der Praxis. Ihr Ziel ist es, ein Rahmenwerk für das Informationssicherheitsmanagement zu definieren. Die Norm befasst sich daher

hauptsächlich mit den erforderlichen Schritten, um ein funktionierendes Sicherheitsmanagement aufzubauen und in der Organisation zu verankern. Die entsprechenden Sicherheitsempfehlungen werden kurz auf den circa 100 Seiten angerissen. Mit dem Thema Business Continuity Management (BCM) beschäftigt sich Kapitel 14 des ISO/IEC 27002. Die fünf Seiten umfassenden Empfehlungen zu BCM im Rahmen des Sicherheitsmanagements sind sehr generisch gehalten und beschreiben auf Management-Ebene die wesentlichen Prozess-Schritte.

NIST SP 800-34

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

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

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

- Entwickeln einer Leitlinie,
- Durchführen einer Business Impact Analyse,
- Definieren von präventiven Maßnahmen (Notfallvorsorge),
- Entwickeln von Wiederherstellungsstrategien,
- Entwickeln von IT-Notfallplänen,
- Schulen, Üben und Testen von IT-Notfallplänen und
- Aktualisieren der IT-Notfallpläne.

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

PAS 77/BS 25777

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

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

ISO/IEC 24762

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

ITIL

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

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

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

- Initiierung des Prozesses: Festlegung der Richtlinien (Policy) und des Umfangs/Geltungsbereichs/IT-Verbunds (Scopes),
- Erfordernisse und Strategie: Business Impact Analysis (BIA), Risikoanalyse und Kontinuitätsstrategie,
- Implementierung: Entwicklung von Kontinuitätsplänen, Wiederherstellungsplänen und Teststrategien,
- Operatives Management: Schulung und Sensibilisierung, Revisionen, Tests und Änderungsmanagement (Change Management).

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

ISO/IEC 20000

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

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

Das neue Werk „Notfallmanagement - BSI-Standard zur Business Continuity" enthält den BSI-Standard 100-4, den ersten deutschen Standard zum „Notfallmanagement". Der Standard ergänzt die Empfehlungen zur IT-Grundschutz-Vorgehensweise.

Mit dem BSI-Standard 100-4 wird ein systematischer Weg aufgezeigt, ein Notfallmanagement aufzubauen, um auf Notfälle und Krisen adäquat vorbereitet zu sein und effizient reagieren zu können. Ziel eines Notfallmanagements ist es, die Ausfallsicherheit zu erhöhen und die wichtigen Geschäftsprozesse in einem Notfall schnell wieder aufnehmen zu können, um den Schaden für die Behörde oder das Unternehmen zu minimieren.

IHRE VORTEILE

- Sie erhalten eine Übersicht über den gesamten Notfallmanagement-Prozess sowie konkrete Hinweise zur Notfallvorsorge.
- Praktische Hilfestellung durch Empfehlungen zur Erstellung eines Notfallhandbuches zur Notfallbewältigung und zur Durchführung von Übungen und Tests.
- Praxistipps: Wie kann das Notfallmanagement permanent aufrecht erhalten werden?

PROFESSIONALS

PRAXISWISSEN

ISBN 978-3-89817-693-4

9 783898 176934

www.bundesanzeiger-verlag.de