

BS 25999 – eine britische Norm auch für Deutschland

Der Weg zum funktionierenden Business Continuity Management

Der Standard BS 25999 wurde in den Jahren 2006 und 2007 von der British Standards (BS) Institution in zwei Teildokumenten veröffentlicht. Der geplante korrespondierende deutsche Standard 100-4 „Notfall Management“ des Bundesamts für Sicherheit in der Informationstechnik, der sich derzeit in der Abstimmungsphase befindet, soll zum BS 25999 vollständig kompatibel werden. Daher lohnt sich ein genauer Blick auf das Original.



Von Tobias Timmler (l.) und Lothar Goecke, Hamburg

Es fällt auf, dass der British Standard nur in geringem Maße auf die Realisierung von technischen und organisatorischen Maßnahmen eingeht, die zu einer angemessenen Business Continuity Management (BCM) Strategie gehören. Dies betrifft unter anderem die IT-Umgebung des Unternehmens. Durch die wenig ausführliche Behandlung der IT lässt sich die fehlende Abgrenzung von BCM gegenüber dem IT-Sicherheitsmanagement erklären, nicht jedoch die fehlende Abgrenzung zu den Themen Störungs- und Krisenmanagement. Davon aber einmal abgesehen stellt der BS 25999 eine in sich geschlossene Methode dar, die aus der Praxis kommt. So bietet er eine gute Möglichkeit, das eigene BCM-Projekt auf den Prüfstand zu stellen oder es von Anfang an in die richtige Richtung zu lenken.

Der BS 25999

Mit seiner Hilfe werden potentielle Gefahren für ein Unternehmen und deren mögliche Auswirkungen identifiziert und bewertet. Er hat weiterhin die Aufgabe, die Widerstandsfähigkeit des Unternehmens gegenüber Störfällen und

Betriebsunterbrechungen durch die Fähigkeit zu wirksamer Gegenreaktion zu erhöhen. Ziel aller diesbezüglichen Maßnahmen ist es, die Belange wichtiger Interessengruppen, etwa von Anteilseignern, zu wahren sowie den Ruf des Unternehmens, die Marken und die wertschöpfenden Tätigkeiten angemessen zu schützen. Es ist aber vorher gut zu überlegen, welche Maßnahmen und Reaktionen sinnvoll sind – denn bezüglich der Wertschöpfungskette sind die einzelnen Aktivitäten unterschiedlich kritisch und daher die Investitionen in ihre Absicherung unterschiedlich sinnvoll. Um das gesteckte Ziel, eine angemessene Geschäftskontinuität, erreichen zu können, fordert der BS 25999, einen BCM-Lebenszyklus im Unternehmen zu etablieren. Dieser ist das zentrale Element der Norm.

Das Unternehmen verstehen

Der Einstieg in den BCM-Prozess beginnt damit, das Unternehmen zu analysieren und zu verstehen. Zu diesem Zweck bedient sich der BS 25999 der Business Impact Analyse (BIA). Hier geht es darum, zunächst alle geschäftskritischen Prozesse sowie deren gegenseitige Abhängigkeiten zu ermitteln und darüber hinaus auch deren maximale tolerierbare Ausfalldauer zu bestimmen. Was ist aber ein geschäftskritischer Prozess und wie lässt sich die maximale tolerierbare Ausfalldauer ermitteln? Die Antwort darauf folgt aus der Schadensbetrachtung, also der Analyse des Schadens, der für das Unternehmen entsteht, wenn ein Geschäftsprozess ausfällt. Die Schadenshöhe wird dabei

auf einen Zeitstrahl projiziert, denn sie steigt in den meisten Fällen mit der Ausfalldauer. Wenn dann noch festgelegt wird, welche Schadenshöhe für das Unternehmen höchstens akzeptabel ist, lässt sich daraus die maximale tolerierbare Ausfalldauer ableiten. Nach der Feststellung der geschäftskritischen Prozesse werden weitere Informationen ermittelt:

- Welche Aktivitäten sind in welchem Ausmaß im Rahmen eines temporären Notbetriebs durchzuführen?
- Welche Ressourcen werden hierfür benötigt (Personal, EDV-Equipment, Telefon etc.)?
- Bis wann muss die Rückkehr zum Normalbetrieb spätestens erfolgt sein?

Bei der Beantwortung dieser Fragen sind die Prozessverantwortlichen gefragt. Die erzielten Ergebnisse bilden die Basis, um später Maßnahmen für einen möglichen Notfall festlegen zu können. Im Anschluss an die BIA wird eine Risikoanalyse (auch als „Risk-Assessment“ bezeichnet) gefordert. Darin wird untersucht,

- welche Bedrohungen Unternehmensressourcen beeinträchtigen können, die in Folge zur Beeinträchtigung geschäftskritischer Prozesse führen,
- welche Schwachstellen bestehen, über die Bedrohungen sich auswirken können,
- wie hoch der mögliche Schaden bei Eintritt einer Bedrohung ist,
- und wie wahrscheinlich der Eintritt einer solchen Bedrohung ist. ▶

Aus Schaden und Wahrscheinlichkeit in Bezug auf die einzelnen Bedrohungen und Ressourcen errechnen sich die Risiken, denen das Unternehmen ausgesetzt ist. Nun wird anhand zuvor festgelegter Kriterien festgestellt, welche Risiken tolerierbar sind und wo Handlungsbedarf besteht:

- Was sind die kritischen Kernprozesse?
- Wie greifen diese Prozesse ineinander?
- Welche Organisationseinheiten sind involviert?
- Welche EDV-Anwendungen werden hierfür benötigt?

Diese Fragen können heute viele Unternehmen nicht vollständig beantworten. Häufige Gründe sind, dass Quartalszahlen im Vordergrund stehen, zu wenig Personal vorhanden ist oder der Profit-Druck so hoch ist, dass für die notwendigen Analysearbeiten keine Zeit bleibt und kein Budget zur Verfügung steht.

BCM Strategie festlegen

Nun geht es darum, Verfügbarkeitsstrategien zu entwickeln. Diese dienen der Reduzierung von Ausfallrisiken, der Verkürzung der Ausfallzeiten und der Wiederaufnahme der Prozesse nach einem Notfall, mit dem Ziel den Schaden zu begrenzen, der durch eine Unterbrechung entsteht. Die kritischen Arbeitsabläufe sind zu dokumentieren, um so das Fachwissen der Mitarbeiter des Unternehmens möglichst einfach weitergeben zu können. Insbesondere sind „Single Points of Know How“ zu vermeiden. Eventuell ist es sogar sinnvoll, auf einen Standort zentralisierte Kerngeschäftsprozesse präventiv auf mehrere Orte zu verteilen, damit der Verlust eines Standortes nicht zu einer vollständigen Unterbrechung führt.

Für Gebäude, in denen geschäftskritische Prozesse abgewickelt werden, sind Ausweichmöglichkeiten zu entwickeln. Diese können etwa Ausweicharbeitsplätze in anderen Gebäuden oder Heim-Arbeitsplätze mit Remote Access sein. Für die IT-Landschaft sind Strategien wie zum Beispiel standortübergreifende Hochverfügbarkeitslösungen, tägliche ausgelagerte Datensicherungen und Ausweichrechenzentren an entfernten Standorten zu etablieren. Da

ein Rechenzentrum wenig nutzbringend ist, wenn es nicht mit der Außenwelt kommunizieren kann, ist eine separate Anbindung des Ausweichrechenzentrums an andere Unternehmensstandorte, zu Geschäftspartnern und an das Internet notwendig.

Auch weitere Informationen, die nicht in der IT gespeichert sind, müssen betrachtet werden. Hierzu gehören unter anderem Verträge und Papierunterlagen, die in Aktenordnern vorgehalten werden. Solche Dokumente sollten entweder kopiert und ausgelagert oder als elektronische Kopien in einem Dokumenten-Management-System vorgehalten werden.

Werden für geschäftskritische Prozesse bestimmte Betriebsmittel und Einrichtungen benötigt, so müssen auch hierfür Notfall-Strategien entwickelt werden. Diese können die Aufteilung von Lägern und Produktionseinrichtungen auf mehrere Standorte sein oder sich in Notfalllieferabkommen manifestieren. Schließlich muss auch an die Kontakte des Unternehmens mit der Außenwelt gedacht werden. Kunden, Lieferanten, Geschäftspartner, Medien, Kapitaleigner wollen alle in einem Notfall ausführlich über den Stand der Dinge informiert werden. Erhalten sie die gewünschten Informationen nicht, ziehen sie ihre Schlüsse aufgrund von Gerüchten und Halbwahrheiten. Solche Resultate sind leider nur selten im Interesse des Unternehmens.

BCM anwenden

In einem weiteren Schritt werden Pläne entwickelt, die greifen sollen, wenn eine Geschäftsunterbrechung trotz aller Vorsorge eintritt. Es wird dabei zwischen folgenden Planarten unterschieden:

- Ein Incident-Management-Plan (IMP) dient dazu, die erste akute Phase eines Vorfalles zu regeln.
- Ein Business-Continuity-Plan (BCP) beschreibt, wie die Aktivitäten des Unternehmens anschließend wiederhergestellt bzw. aufrecht erhalten werden.

Typische Inhalte von Incident-Management-Plänen sind etwa die Beschreibung der Aktivitäten und Verantwortlichkeiten bei Evakuierungen und bei

der Ersthilfe, Regelungen für die Kommunikation mit Medien, Geschäftspartnern und Behörden, die Festlegung von Stabszentralen sowie alle notwendigen Kontaktdaten. In Business-Continuity-Plänen für die Fachbereiche werden sowohl die Prozeduren zur Geschäftsfortführung, der Notbetrieb an einem Ausweichstandort und die Wiederaufnahme des Normalbetriebs beschrieben. Ebenso sind Pläne für die IT und die weitere Infrastruktur zu erstellen, die durch eine möglichst genaue Beschreibung einen reibungslosen und anforderungsgerechten Wiederanlauf ermöglichen. Über all dem steht ein übergeordneter Wiederanlaufplan, der die Durchführung einzelner (Teil-)Pläne steuert.

BCM üben und verbessern

Alle Vorsorgemaßnahmen und Pläne müssen überprüft und geübt werden. Dies dient einerseits der Erkenntnis, ob alle Mechanismen so funktionieren, wie sie geplant wurden. Andererseits werden auch die betroffenen Mitarbeiter für das Thema BCM sensibilisiert und in der Anwendung der Pläne geschult, was für einen reibungslosen Ablauf im Ernstfall unumgänglich ist. Die Übungen sollen realitätsnah sein und sich an die vorher erarbeiteten Szenarien halten, sollten jedoch nicht so stark ausgeweitet werden, dass sie selbst eine Störung des Unternehmensbetriebs verursachen. Wichtig sind folgende Erkenntnisse, die sich aus den Übungen ergeben:

- Ist die Vorsorge ausreichend?
- Ist ein Wiederanlauf in der vorgesehenen Zeit möglich?
- Wie vollständig und verständlich sind die Pläne?

Der BS 25999 sieht die BCM-Kultur insgesamt nicht als einen einzelnen Punkt im BCM-Zyklus. Vielmehr umfasst sie den gesamten Prozess und begleitet ihn während all seiner einzelnen Phasen.

Über unsere Autoren:

Lothar Goecke ist Geschäftsführer des Beratungsunternehmens consequa GmbH. Seine Arbeitsschwerpunkte sind Organisationsentwicklung, Rechenzentrumsorganisation, Systempflege und Bürokommunikation. Tobias Timmler ist Berater bei der consequa GmbH. Seine Arbeitsschwerpunkte sind IT-Continuity, Konzeption von Backup-Rechzentren, IT-Sicherheit, Business Continuity, Krisenmanagement und Notfallplanung. Kontakt: www.consequa.de