INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Business Continuity Management (BCM)

Ist es wirklich nötig, dass immer zuerst etwas passieren muss? Ein BCM hilft die kritischen Prozesse zu kennen sowie Strategien und Notfallpläne zur Begegnung möglicher Zwischenfälle zu erarbeiten.

Dieser INFONEWS geht auf den Inhalt, das Vorgehen und erweiterte Möglichkeiten für die IT ein und beantwortet folgende Fragen:

- Zahlt sich ein BCM aus?
- Welche Schritte sind für die Einführung eines BCMs nötig?
- Welche Möglichkeiten hat die IT?

Inhaltsverzeichnis

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Einleitung

Sagt Ihnen der Namen swisspor etwas? Dann sind Sie entweder in der Baubranche tätig (die Firma swisspor stellt Produkte zum Dämmen Dichten und Schützen von Bauten her) oder Sie mögen sich an den verheerenden Brand vom Frühjahr 2007 in Steinhausen erinnern. Aber wissen Sie auch, ob es diese Firma heute überhaupt noch gibt?

Nach dem Wiederaufbau des niedergebrannten Gebäudes meinte der Patron der Swisspor-Gruppe in einem Interview:

Früher waren Investitionen in die Sicherheit ein notwendiges Übel, die man wegen den Versicherungen und den gesetzlichen Vorschriften tätigen musste. Beim Neuaufbau habe ich in die Sicherheit wesentlich mehr investiert, als überhaupt vorgeschrieben wäre.[1]

Ist es wirklich nötig, dass immer zuerst etwas passieren muss, bevor der Mensch die nötige Sensibilität, für teils einfache vorbeugende Massnahmen erlangt? Eigentlich sollten wir als intelligente Spezies in der Lage sein, aus Fehlern und Erfahrungen anderer zu lernen. Noch immer ist aber eine der effizientesten Methoden etwas zu lernen, wenn es greifbar ist und erlebt werden kann. Menschen, welche sich regelmässig in einem Umfeld mit überdurchschnittlicher Sicherheitssensibilität bewegen, entwickeln häufig selbst einen routinierteren Bezug zum Umgang mit Risiken als andere. Nicht alle Menschen, welche in der Geschäftsleitung einer Firma sind, mussten schon mit ausserordentlichen Krisen umgehen (und das ist auch gut so). Umso schwieriger ist es entsprechend, wenn ein IT-Leiter oder ein Sicherheitsverantwortlicher (der in einem Umfeld mit überdurchschnittlicher Sicherheitssensibilität zuhause ist) die Geschäftsleitung davon überzeugen möchte, ein BCM (Business Continuity Management) einzuführen. Einfacher wird es, wenn dies gesetzlich vorgeschrieben wäre…

[1] Zitat von Bernhard Alpstaeg (Patron der Swisspor-Gruppe), in einem Interview mit der Zeitschrift „Intelligent bauen“ (August 2009)

1.1 Zahlt sich ein BCM überhaupt aus?

Die Frage, ob sich ein BCM überhaupt auszahlt, kann nicht pauschal beantwortet werden. Werden die Investitionen als Beispiel über einen Zeithorizont von zehn Jahren betrachtet und die betroffene Unternehmung muss sich nie mit einem Notfall oder einer schweren Krise auseinandersetzen, könnte man davon ausgehen, dass sich die Investition in den Aufbau und den Betrieb eines BCMs nicht gelohnt haben. Anders sieht es natürlich aus, wenn eine Krise erfolgreich gemeistert wurde und sich die erstellten Notfallpläne bewährt haben. Eine gewisse Ähnlichkeit mit dem Abschliessen einer Versicherung ist nicht von der Hand zu weisen.

Auf keinen Fall darf an dieser Stelle aber vergessen werden, dass der aktive Betrieb eines BCMs viele Vorteile bringt, welche nur schwer messbar, aber klar vorhanden sind, auch wenn das Unternehmen von einer schweren Krise verschont bleibt. Zwei wichtige Faktoren seien an dieser Stelle kurz erwähnt. Durch die Identifikation der kritischen Prozesse und der ständigen Frage, was ist wirklich zwingend notwendig, hat ein Unternehmen die Chance den Kern der Firma besser kennenzulernen. Nicht selten erlaubt dies, die Effizienz von Kernprozessen weiter zu steigern. Des Weiteren können alleine durch die Sensibilität über die Jahre die Kernprozesse für einen allfälligen

Notfall optimiert und vorbereitet werden, ohne dass in jedem Fall hohe Kosten entstehen.

Ein Beispiel dazu: Die IT eines Dienstleistungsbetriebs hat durch das BCM die Geschäftsleitung sensibilisiert, dass der Betrieb der IT der kritischste Prozess ist. Bei der Planung zur Expansion der Firma konnte bei der Suche nach einem zweiten Standort die IT-Leitung von Anfang an einbezogen werden, so dass ein zweites Rechenzentrum mit verhältnismässig geringem Aufwand an einem zweckmässigen Standort aufgebaut werden konnte. Ohne diesen Input wäre am bestehenden Gebäude ein Anbau realisiert worden.

Ob sich ein BCM auszahlt, hängt entsprechend einerseits davon ab, wie konsequent proaktive Massnahmen für eine verbesserte Situation in einem Krisenfall gesucht und umgesetzt werden. Möglich ist das aber nur, wenn die kritischen Prozesse und Abläufe bekannt sind. Genau diese Identifikation ist ein wichtiger Bestandteil eines BCMs. Andererseits darf nicht erwartet werden, dass die nötigen Investitionen sich direkt auszahlen. Im Falle einer grossen Krise hingegen ist die Vorbereitung auf die Krise entscheidend, ob und wie ein Unternehmen nach der Krise noch existiert.

2 BCM

2.1 Ziel eines BCM

Der British Standard 25999 definiert BCM in seiner deutschen Übersetzung wie folgt:

BCM = Holistischer Managementprozess zur Kennzeichnung potentieller Bedrohungen auf die Geschäftstätigkeiten und zur Bereitstellung eines Rahmens zur Schaffung einer entsprechenden Widerstandsfähigkeit der Organisation mit der Fähigkeit zu einer wirksamen Antwort zum Schutz der Interessen ihrer bedeutendsten Teilhaber sowie ihres Rufes, ihrer Marke und wertschöpfenden Aktivitäten.

Diese Definition ist sehr treffend. Denn wie im Kapitel 2.4 beschrieben wird, geht es beim BCM nicht um die ersten Massnahmen nach einem Ereignis, wie zum Beispiel die Evakuation eines Gebäudes, sondern ausschliesslich um einen möglichst schmerzfreien resp. schmerzarmen Weiterbetrieb der „normalen" Geschäftstätigkeiten, nach Eintreten eines Ereignisses.

2.2 Gesetzliche Grundlagen

In der Schweiz gibt es von diversen Stellen Empfehlungen zum Betrieb eines BCMs. Als Beispiel seien die Bakom-Richtlinien 2009 für Telekomanbieter, die BCM-Empfehlungen des VSE (Verein schweizerischer Energie-Produzenten) oder die BCM Richtlinien der SBVg (Schweizerische Bankier Vereinigung) 2007 genannt. Eine generelle Pflicht zum Betrieb eines BCM gibt es nicht. Einzelne Unternehmen unterliegen aber speziellen Gesetzen aufgrund ihrer Tätigkeit (z.B. Störfallverordnung). Für solche Unternehmen können z.T. verbindliche Vorgaben zur Vorbereitung auf mögliche Krisen gelten.

2.3 Standards

Ein bekannter und bewährter Standard für den Betrieb eines BCM ist der British Standard BS 25999. Unternehmen können sich nach diesem Standard (BS 25999-2) zertifizieren lassen. Voraussichtlich ab Ende des Jahres 2011 wird zudem der ISO-Standard 22301 erscheinen. Auch dieser ist für die Zertifizierung vorgesehen. Im BCM-

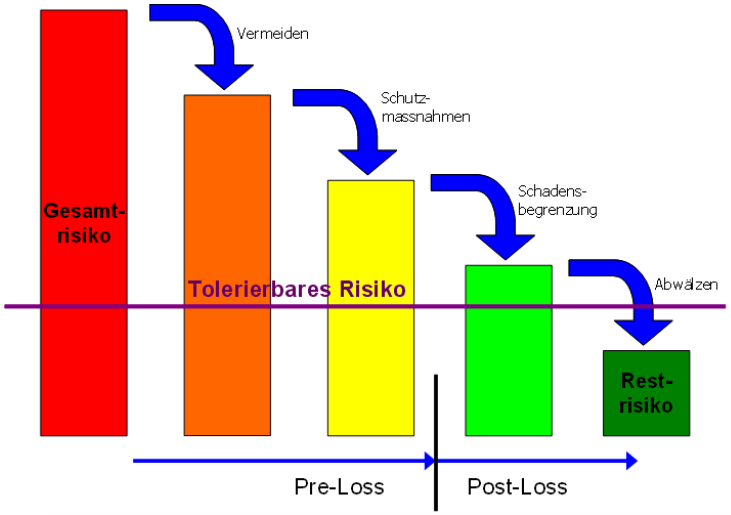
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Umfeld ist der BSI 100-4-Standard ebenfalls bewährt (BSI: Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de). Einige Schweizer Banken arbeiten nach diesem, in BCM-Kreisen als soliden geltenden Standard. Der BSI-Standard orientiert sich am British Standard 25999 und baut auf der Methodik des BSI-Standards 100-2 (IT-Grundschutz-Vorgehensweise) auf.

2.4 Abgrenzung Krisen- und Risikomanagement

Die drei Bereiche Risiko-Management, Krisenmanagement und Business Continuity Management sind zwar miteinander verbunden, dürfen aber nicht verwechselt werden. An dieser Stelle sei darum eine Abgrenzung der verschiedenen Themen untereinander gegeben.



Das **Risikomanagement** spielt sich vor möglichen Ereignissen ab. Es geht darum, Risiken zu identifizieren und mittels Eintrittswahrscheinlichkeit und Auswirkung zu bewerten und in einem nächsten Schritt Risiken zu bewältigen.

Ein Risikomanagement findet grundsätzlich unabhängig von tatsächlichen Ereignissen statt, wird aber von solchen geprägt (insbesondere die Eintrittswahrscheinlichkeit). Unmittelbar nach einem Ereignis (Brand, Verseuchung, Wasserflut, Mitarbeiter-Ausfall usw.) kommt das Notfall- oder Krisenmanagement zum Zug.

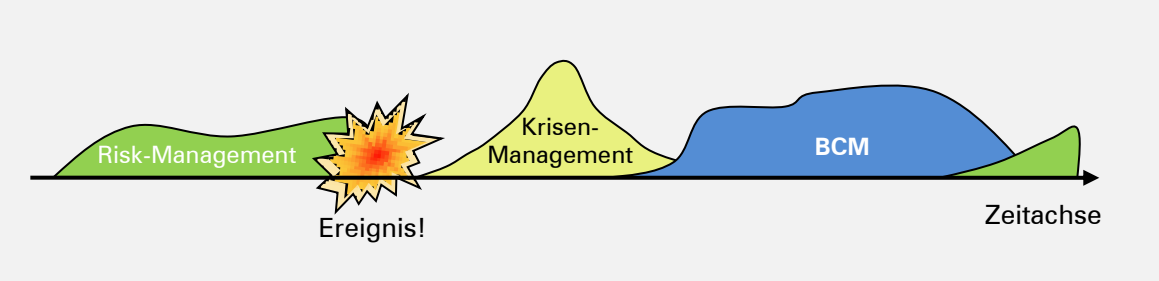
Das **Krisenmanagement** ist unabhängig von Unternehmensprozessen und das Ziel besteht darin, Menschen zu retten (z.B. Gebäude-Evakuation in der Schadensbegrenzung (Umwelt / Sachwerte) Aber auch die Betreuung von Mitarbeitern und gegebenenfalls Angehörigen von Verletzten oder verstorbenen Mitarbeitern und den Medien sind klassische Aufgaben des Krisenmanagements. In dieser Phase sind insbesondere bei Ereignissen höherer Gewalt, Rettungsorganisationen wie Feuerwehr, Sanität und Polizei involviert.

Das Resultat aus dem **BCM** (die Notfallpläne / Business Continuity Pläne) kommen erst nach (resp. während) des Krisenmanagements zum Zug und haben den Zweck die kritischen Prozesse der Unternehmung weiter zu betreiben oder rasch wieder aufzunehmen.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



Ein weiterer grosser und entscheidender Unterschied zwischen Risikomanagement und BCM besteht weiter darin, dass beim BCM mögliche Ereignisse / Gefahren nicht nach der Eintrittswahrscheinlichkeit beurteilt werden. Dieser Faktor wird beim BCM bewusst ausser Acht gelassen.

Wichtiger Hinweis:
Im BCM wird eine weitere Vereinfachung vorgenommen, welche gewöhnungsbedürftig ist, aber unbedingt eingehalten werden muss. Beim Risikomanagement ist das Ereignis, welches zu einem Ausfall eines Prozesses führt, das zu bearbeitende Element. Beim BCM spielt die Ursache keine Rolle. Betrachtet werden nur die Auswirkungen. Ein Beispiel: Ob das Produktionsgebäude aufgrund eines Brandes, einer Überschwemmung einer Kontamination oder einer Beschlagnahmung durch die Behörden ausgefallen ist, wird nicht unterschieden. Das „BCM-Problem“ in diesem Fall heisst: Ausfall des Produktionsgebäudes.

2.5 Klassisches Vorgehen

Das klassische Vorgehen für die Einführung und den Betrieb eines BCMs gemäss BS 25999 (und BSI 100-4) sieht wie folgt aus und nennt sich Lebenszyklus:

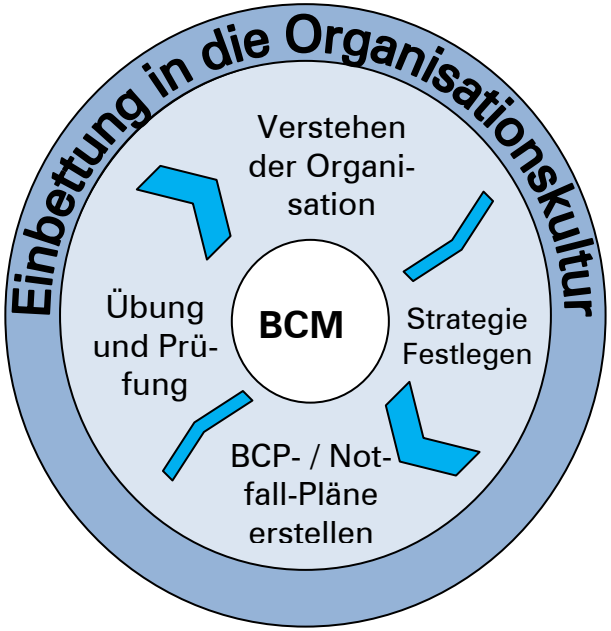
- (Begriff Definitionen)
- Umfassendes Verstehen (Transparenz) der eigenen Organisation (üblicherweise durch die Durchführung einer Business Impact Analyse BIA)
- Entwickeln einer BCM-Strategie
- Entwickeln und implementieren von Reaktionsmassnahmen und BC-Notfallplänen
- Durchführen von BCM-Übungen, Überprüfungen und Weiterentwickeln der BC-Notfallpläne und Massnahmen (Dieser letzte Schritt muss in einen Prozess geführt werden)

Die folgende grafische Darstellung wird im Standard BS 25999 verwendet und als Lebenszyklus des betrieblichen Kontinuitätsmanagements bezeichnet.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



2.5.1 Definitionen

In keinem Standard zum Thema BCM kann beim Vorgehensmodell als erstes der Titel Definitionen gefunden werden. Die Erfahrung zeigt aber, dass der Zeitpunkt kommt, an dem hitzige Diskussionen entstehen, welche sich auf Missverständnisse der Begriffe zurückführen lassen. Grundsätzlich ist es sinnvoll gebräuchliche Begriffe zu verwenden. Wichtiger ist aber, dass diese kurz erklärt werden. Einige, welche auch für dieses Dokument wichtig sind, werden nachfolgend definiert:

Begriff Abkürzung	Erklärung
MTPD	Maximum Tolerable Period of Disruption – Maximal tolerierbare Ausfallzeit. Dieser Wert stellt den Zeitpunkt dar, ab welchem der betroffene Prozess wieder aufgenommen werden muss (Not- oder Normalbetrieb). Wird der MTPD überschritten, ist der Fortbestand der Unternehmung gefährdet. Der Wert ist durch Umstände gegeben und kann durch Massnahmen beeinflusst, nicht aber frei gewählt werden.
MTA	Maximum Tolerable time in Alternative – Maximal tolerierte Zeit, in welcher ein Notbetrieb gefahren wird.
Notfall	Situation, welche für das Unternehmen kritisch ist, gegebenenfalls auch weitreichende Katastrophe.
RTO	Recovery Time Objective – Zielsetzung der Wiederaufnahme, resp. Wiederanlaufzeit (z.B. Notbetrieb 60%). Dieser Wert kann grundsätzlich selbst definiert werden. Wichtig: RTO < MTPD
RPO	Recovery Point Objective – Zeitspanne mit Datenverlust (Zeit zwischen letzter Sicherung und Ereignis.
BIA	Business Impact Analysis – Instrument zur Identifikation der kritischen Prozesse
OCM	alternativer Begriff für BCM (o=Operational), wird häufig bei Verwaltungen verwendet

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2.5.2 Verstehen der Organisation

Das Ziel und Endprodukt dieses Schrittes ist die Identifikation der kritischen Prozesse. Kritische Prozesse sind solche mit grossem Einfluss auf andere Prozesse und einer hohen Wichtigkeit. Um diese Prozesse zu identifizieren wird üblicherweise eine BIA (Business Impact Analyse) erstellt. Mit einer BIA werden Prozesse mit hohem Einfluss auf andere Prozesse und auch Abhängigkeiten von Prozessen untereinander erfasst. Als Hilfsmittel dienen dabei eine Einfluss- und eine Abhängigkeitsmatrix. Wichtig ist, dass die Matrizen als Hilfsmittel gesehen werden und bei der Auswertung der gesunde Menschenverstand nicht zu kurz kommt. Nicht umsonst wird der Schritt als „Verstehen der Organisation" bezeichnet. Beim Ausfüllen der Matrizen stellt sich oft die Frage, ob der Einfluss hoch oder sehr hoch ist. Deshalb ist auch hier die Definition der Werte vor dem Abfüllen der Werte sehr wichtig. Mit der Einflussmatrix wird ein numerischer Wert ermittelt (BIA-Score). Dazu wird der jeweilige Einfluss der verschiedenen Geschäftsprozesse auf unterschiedliche Einflusskategorien (z.B. Finanzen oder Reputation) ermittelt und schliesslich pro Prozess addiert.

2.5.2.1 Einflussmatrix (vereinfachtes Modell)

Durch die Abhängigkeitsmatrix werden zwei Werte ermittelt. Dazu werden die Abhängigkeiten der Prozesse untereinander bewertet und ebenfalls addiert. Als Resultat ist ersichtlich, welche Prozesse von vielen anderen Prozessen abhängig sind und welche Prozesse wichtig für andere Prozesse sind. Mit dem jeweiligen Ranking wird zudem eine Reihenfolge ermittelt.

Einflussmatrix	Einflusskategorie						
Prozess	Finanzen	Kunden	Reputation (Ruf)	Unternehmenssteuerung	Personensicherheit	MTPD (in Tagen)	Impact-Score (Summe der einzelnen Werte)
Produktion	5	4	3	2	3	1	17
Lager	2	3	1	1	1	3	8
Verkauf	4	4	4	1	1	2	14
Technischer Dienst	1	1	1	2	2	1	7
IT	2	3	4	5	2	1	16

1 = sehr geringer Einfluss
5 = sehr hoher Einfluss

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2.5.2.2 Abhängigkeitsmatrix (vereinfachtes Modell)

Abhängigkeitsmatrix	Prozess						
Prozess	Produktion	Lager	Verkauf	Technischer	IT	Dependency-Score	Dependency-Rank
Produktion		2	4	3	5	14	1
Lager	3		2	2	4	11	2
Verkauf	2	2		1	4	9	3
Technischer Dienst	1	1	1		3	6	4
IT	1	1	1	1		4	5
Importance-Score	7	6	8	7	16		
Importance-Rank	3	4	2	3	1		

1 = sehr geringe Abhängigkeit
5 = sehr hohe Abhängigkeit

Aus dieser Kurz-Analyse (als Beispiel zu verstehen) geht hervor, dass die IT, die Produktion und der Verkauf sehr wichtig und von der IT sehr viele Prozesse stark abhängig sind. Zu den kritischen Prozessen gehören die IT, die Produktion und der Verkauf. Wichtig ist auch die alleinige Betrachtung der MTPD-Werten Da die drei Prozesse mit dem tiefsten Wert dem Resultat aus den beiden Matrizen entsprechen, scheint die Definition der kritischen Prozesse nicht falsch zu sein.

Wie bereits erwähnt, dürfen diese Analysen nie „blind" durchgeführt werden. Die BIA hilft beim Verstehen der Organisation, bringt den Durchführenden, bei korrekter Ausführung, sicherlich auf den richtigen Weg und kann ihn unterstützten. Die Resultate müssen aber immer mit einem gesunden Misstrauen hinterfragt werden. Plausibilitätskontrollen helfen dabei, Sicherheit zu gewinnen. Die nächsten Schritte konzentrieren sich immer auf die kritischen Prozesse.

2.5.3 Festlegung der BCM-Strategie

Nach der Identifizierung der kritischen Prozesse muss eine BCM-Strategie festgelegt werden. In der Praxis wird dieser Schritt zum Teil mit dem Erstellen der Notfallpläne vermischt. Diese Variante ist meist nicht ideal und wird nicht empfohlen. Es ist durchaus möglich, dass bei der Erstellung der Pläne (siehe nächstes Kapitel) weitere Fragen auftauchen, welche geklärt werden müssen. Die Grundstrategie muss aber zuerst festgelegt werden.

Doch was muss in dieser Strategie festgelegt werden?

Als Beispiel wird auf den kritischen Prozess Produktion eingegangen. Die Strategie für diesen Prozess kann in die Richtung gehen, dass das Lager vergrössert wird, um längere Ausfälle abzufangen. Die Strategie kann auch vorsehen, die Produktion auf mehrere Standorte zu verteilen, so dass mittels Schichtbetrieb, selbst bei einem Ausfall des Gebäudes, nur ein geringer Ausfall des Prozesses zu erwarten ist. Eine andere Strategie könnte die Zusammenarbeit mit Mitbewerbern vorsehen.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Die folgende Liste ist nicht abschliessend, gibt aber einen Überblick über mögliche Strategien:

- Ausweichstandorte
- Replikation / Redundanz
- Reserve / Standby-Anlagen
- Arbeiten an Dritte vergeben
- Vorbereitung von Wiederbeschaffung (z.B. in der IT)
- Versicherungen
- Nichts tun (z.B. für nicht kritische Prozesse)

2.5.4 BC-Notfallpläne erstellen

Gemäss BS 25999-2 muss eine Organisation ihre definierte Strategie zur Entwicklung und Verwirklichung angemessener Pläne und Vorkehrungen verwenden, um die Kontinuität ihrer entscheidenden Aktivitäten (Anmerkung: kritischen Prozesse) sowie das Management eines Zwischenfalls zu gewährleisten.

Für die Erstellung der BC-Notfallpläne müssen die Prozessverantwortlichen stark involviert werden. Dies weil Know-how-Träger an dieser Stelle enorm wichtig sind. Grundsätzlich sind Gestaltung und Inhalt den Gegebenheiten anzupassen. Es empfiehlt sich aber eine allgemeine Struktur für alle Pläne zu verwenden. Üblicherweise wird pro kritischem Prozess ein BC-Notfallplan erstellt.

Folgende Punkte sind dabei wichtig:

- Versions- und Revisionskontrolle
- Einleitung
- Definitionen (Begriff Definitionen) u.U. als Anhang
- Notfalldefinition
- Anleitung und Anweisung zur konsequenter Journalführung über alle Aufgaben
- Definition von Sofortmassnahmen
- Medienkontakte und Medien-Strategie
- Adressen und Telefonnummern von internen Mitarbeitern und externen Kontakten
- Verantwortlichkeiten und Zuständigkeiten in einem Notfall
- Alarmierung (von Mitarbeitern und Externen)
- Treffpunkt (Sammelpunkt) bei einem Notfall
- Vorgabe der Kommunikationskanäle
- Taktischer Führungsrhythmus
- Ausweichstandorte (falls vorhanden)
- Ablage von Notfallplan und ergänzenden Dokumenten
- Definition des Notfallequipments
- Prozess zur Deeskalation (wann ist der Notfall beendet, was geschieht dann)
- Organisatorisches (Review Notfallplan)
- Notfallübungen (unter Umständen nicht pro Notfallplan)

Hinweis:
BC-Notfallpläne müssen möglichst kurz, einfach zu verstehen und klar formuliert sein. Die Verwendung von Grafiken zur Darstellung von Abläufen und die Verwendung von einheitlichen, leicht lesbaren Tabellen sind langen Texten vorzuziehen.

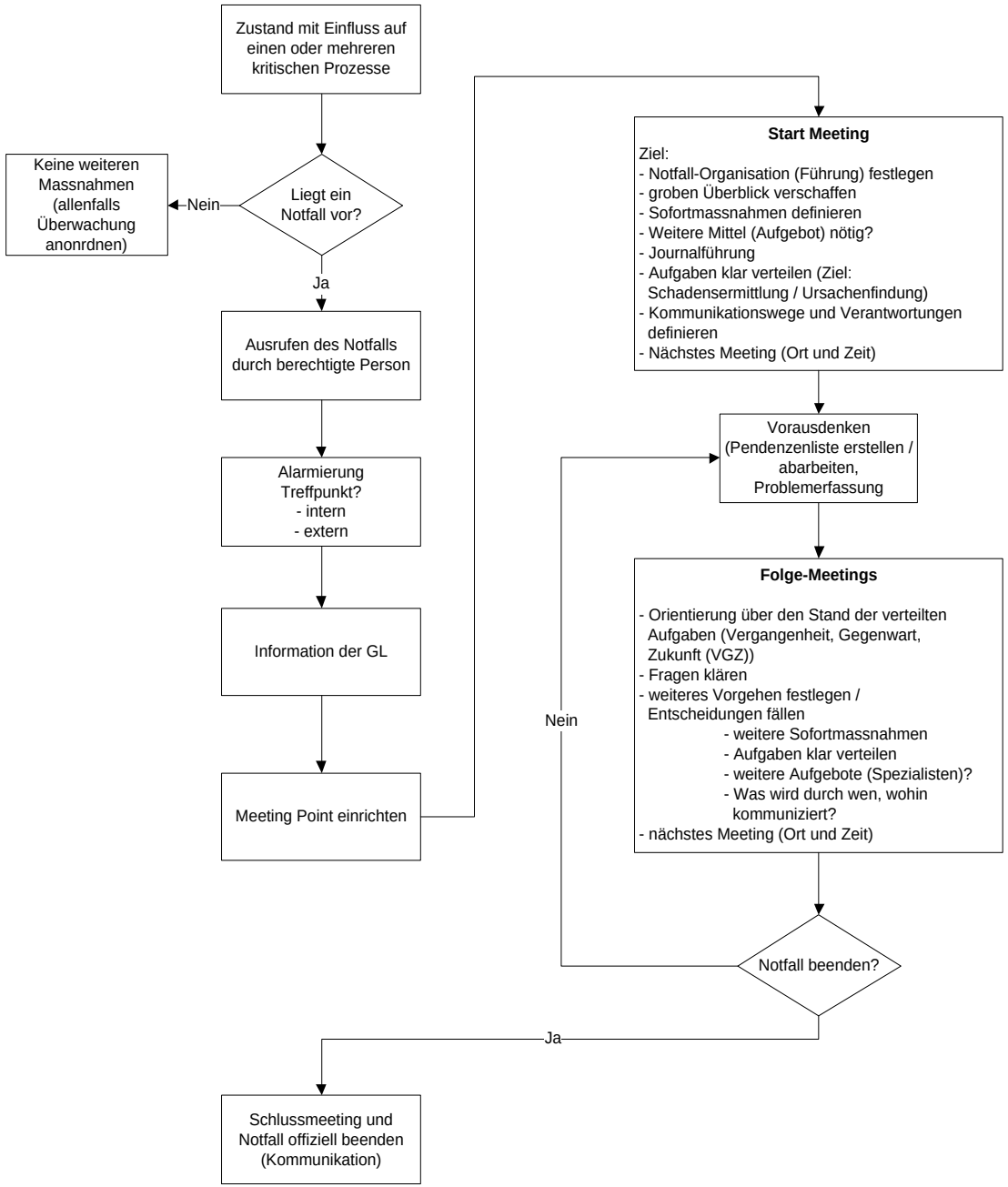
2.5.4.1 Notfallprozess

Die Definition eines Notfallprozesses regelt die ersten Schritte, sobald ein Notfall ausgerufen wird. Dieser muss einfach und verständlich gehalten werden. Im Folgenden ist ein Beispiel für einen BC-Notfallplan des IT-Prozesses. Grundsätzlich kann dieser Notfallprozess auch auf andere Bereiche projiziert werden.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21



goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2.5.5 Aufrechterhaltung und Prüfung

Nach der Erstellung der Pläne sind einige Manager der Meinung, ist das BCM-Projekt abgeschlossen. BCM ist aber kein Projekt, sondern ein Prozess. Um solche Missverständnisse zu vermeiden, sollte der Begriff BCP (Business Continuity Planning) auch nur mit Vorsicht und stattdessen besser der Begriff BCM (Business Continuity Management) verwendet werden. Die Wichtigkeit zur Durchführung von Übungen kann leicht begründet werden. Oder haben Sie schon einmal eine Feuerwehr-Organisation gesehen, welche ein Löschfahrzeug gekauft, an einem runden Tisch ein theoretisches Vorgehen ausgearbeitet und anschliessend auf den ersten Einsatz gewartet hat?

Nur durch die regelmässige Übung der in den Plänen definierten Abläufen können diese trainiert (Erfahrungen durch die Mitarbeiter gesammelt), Stolpersteine entdeckt und dokumentiert und die Sicherheit, dass der Plan wunschgemäss funktioniert, erlangt werden. Regelmässige Übungen mit den entsprechenden Nacharbeiten (Überarbeitung und Verbesserung der Pläne) erfüllen bereits einen grossen Teil des Aufrechterhaltungsprozesses. Wird ein BCM eingeführt sowie mit dem Erstellen der Pläne abgeschlossen und dadurch nie geübt, überprüft oder gepflegt, war das BCM tatsächlich nichts mehr als eine Investition ohne grossen Nutzen. Dies muss durch Schliessen des BCM-Llifecycles unbedingt verhindert werden. Damit dieser Prozess funktioniert, müssen klare Verantwortlichkeiten geschaffen werden. Die Aufgaben dieser Verantwortlichen müssen kontrolliert werden.

Mögliche Zyklen:

- Mind. jährliche Durchführung von Übungen inkl. Nachbearbeitung (zu Beginn häufiger)
- Mind. alle 3 Jahre: Durchführung Prüfung des BCMs, inkl. Durchführen einer BIA

Wichtig für die Durchführung von Übungen ist der Grundsatz klein und einfach zu beginnen. Es wird sich in den meisten Fällen als kontraproduktiv erweisen, als allererstes eine Grossübung mit Ausfall aller Prozesse und komplizierten Gegebenheiten zu organisieren. Mit grosser Wahrscheinlichkeit wird vieles nicht annähernd so funktionieren, wie gewünscht und am Schluss herrscht Frustration, anstelle von Motivation und Genugtuung unter den Beteiligten. Ein Notfall ist immer eine aussergewöhnliche Stress-Situation. Jeder Mensch reagiert anders unter Stress. Reaktionen können häufig nicht vorausgeahnt werden und als ruhige Personen geltende Menschen können plötzlich nicht mehr klar denken und richten nur noch (mehr) Chaos an. Die betroffenen Mitarbeiter müssen darum langsam an das Thema geführt werden. Als erstes darf durchaus eine rein applikatorische Übung mit einzelnen Elementen gemacht werden, welche es dann zu steigern gilt. Kann zu einem späteren Zeitpunkt dann auch eine etwas komplexere Notfallübung erfolgreich gemeistert werden, wird das Team dadurch stark motiviert.

Enorm wichtig ist die Nachbearbeitung jeder Übung. Nach der offiziellen Beendigung muss als erstes darauf geachtet werden, dass die wichtigen Bedürfnisse der involvierten Mitarbeiter und externen Stellen berücksichtigt werden können (Essen, Trinken, allenfalls Schlaf, Familie usw.). Höchstens drei Arbeitstage nach Beendigung der Übung muss ein erstes Debriefing mit den Prozessinhabern stattfinden. Inhalte dieser Debriefings sind:

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

- Dank aussprechen
- Alle Anwesenden auf denselben Wissensstand bringen
- Über aktuellen Stand informieren
- Termin für einen Workshop definieren (falls nicht vor der Übung geplant), um die Erkenntnisse aus der Übung sowie Massnahmenanpassungen zu definieren (höchstens eine Woche später)

Hinweis:
Die durchgeführten Übungen müssen mit den wichtigsten Erkenntnissen protokolliert werden

3 Die Möglichkeiten der IT

3.1 Praxis

Wie bereits in der Einleitung erwähnt, bewegt sich die IT in einem sicherheitssensibilisierten Umfeld. Immer wieder taucht darum bei der IT (sei es aus Eigeninitiative oder aufgrund eines Audits) die Frage nach einem Notfallmanagement (BCM) auf. Wie aus den vorangehenden Kapiteln ersichtlich, handelt es sich beim BCM aber nicht um die Aufgabe einer Abteilung, sondern um eine firmenweite Aufgabe, welche von der Geschäftsführung her unterstützt und geführt werden sollte. Nicht immer stösst die IT mit dem Vorstoss zur Einführung eines BCM auf Verständnis. Die Betrachtungsweise, dass die Notfallplanung ausschliesslich Aufgabe der IT sei und diese darum den Auftrag erhält einen Notfallplan zu erstellen, ist in der Praxis ebenfalls anzutreffen.

Fakt ist, dass beim Beispiel für die BIA in Kapitel 2.5.2 der Betrieb der IT als einer der kritischsten Prozesse resultiert, ist kein Zufall. Ebenfalls kein Zufall ist die Tatsache, dass viele Standards zum Thema Notfallplanung IT-fokussiert sind. In den meisten Unternehmungen ist der reibungslose Betrieb der IT eine wichtige Grundvoraussetzung, damit die Kernprozesse überhaupt funktionieren und Umsatz generiert werden kann.

3.2 IT als Vorreiter

Bekommt die IT, ohne dass ein BCM eingeführt wird, den Auftrag Notfallpläne zu erstellen, ist dies durchaus realisierbar, auch wenn der Nutzen für die Unternehmung, im Gegensatz zu einem firmenweiten BCM, nicht optimal ist. Möglich ist dies auch, wenn die IT-Leitung auf die Einführung eines BCMs drängt, die Geschäftsleitung aber keine Unterstützung gewährt.

3.2.1 Verstehen der Organisation

Daher muss in diesem Fall der Ablauf etwas angepasst werden. Insbesondere die BIA muss differenziert durchgeführt werden. Falsch wäre es, diese einfach auszulassen. Der Notfallplan wird in einem solchen Fall nur für den Prozess IT-Betrieb erstellt. Erarbeitet werden müssen im Minimum folgende Punkte:

- Welcher Unternehmensprozess hat welchen MTPD
- Welcher Unternehmensprozess hat welche Abhängigkeit und Wichtigkeit
- Welcher wichtige Prozess hat welche Abhängigkeit von welchen IT-Mitteln

Das Ziel dieses ersten Schrittes ist es herauszufinden, welcher Prozess von welchen IT-Mitteln abhängig ist und wie lange dieser ausfallen darf, bevor das Unternehmen ernsthaft gefährdet wird. Für die Erfassung dieser Werte

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

können einfache Formulare erstellt und durch die Prozesseigner ausgefüllt werden. Wichtig bei der Erstellung der Formulare ist, dass wirklich nur die wesentlichen Aspekte erfragt werden, ansonsten ist die Unterstützung der Prozesseigner meist nicht gegeben. Häufig reicht die Erfassung von Prozessname, Prozesseigner, MTPD und eine Ankreuzliste für die benötigten IT-Mittel. Die Idee und Funktion des MTPD muss dabei gut erklärt werden. Zeigen Plausibilitätskontrollen Unregelmässigkeiten, muss der MTPD-Wert nochmals nachgefragt und erklärt werden.

Eine weitere Aufgabe der IT in diesem Zusammenhang ist die Abhängigkeit der einzelnen IT-Elemente untereinander aufzuzeigen (Dieser Schritt muss auch beim normalen Ablauf spätestens bei der Erstellung der Notfallpläne getätigt werden). Mit diesen Informationen kann anschliessend eine Wiederherstellungsreihenfolge definiert werden. Wichtig ist, dass die Grunddienste (Netzwerk, Internet, AD, DHCP, DNS, Rechenzentrum usw.) nicht vergessen gehen.

3.2.2 Weitere Schritte

Alle weiteren Schritte entsprechen wieder mehr oder weniger dem klassischen Vorgehen. Die Strategie wird jedoch nur für die IT festgelegt und natürlich werden auch nur Notfallpläne für die IT definiert. Bei der Festlegung der Strategie wird nicht selten festgestellt, dass umfassende (Investitionsträchtige) Strategien für die Einhaltung der von den Prozesseignern festgelegten MTPD-Werten nötig sind. Es lohnt sich an dieser Stelle zuerst nochmals nachzufragen (persönlich, nicht per E-Mail) und den Prozesseignern zu erklären, was durch ihre Definition ausgelöst wird. Es ist teilweise erstaunlich, wie lange ein Prozess dann plötzlich ausfallen darf.

Die Resultate aus dem „IT-BCM“ sollten unbedingt der Geschäftsleitung präsentiert werden. Durch den zusätzlichen Einbezug dieser in die Durchführung von Übungen (diese sollten nicht „heimlich“ durchgeführt werden), kann unter Umständen ein Umdenken angeregt werden.

3.2.3 Fazit

Das klassische Vorgehen beim BCM ist sicherlich effektiver, als wenn die IT im Alleingang die Notfallplanung übernehmen muss. Manchmal ist es jedoch nötig, dass die IT den Anfang macht. Die BC-Notfallpläne können nie perfekt sein und müssen sich entwickeln. Da die IT stark in den BCM-Prozess involviert ist, kann es nicht falsch sein, wenn die IT die Vorreiter-Rolle übernimmt. Die Erfahrung zeigt, dass die Geschäftsleitung meist positiv vom Resultat überrascht ist und nicht selten, über kurz oder lang, die Einführung eines BCMs folgt. Diese unternehmensweite Einführung kann wiederum von den Erfahrungen der IT profitieren.

4 Quellen

Swisspor:
www.swisspor-gruppe.com/images/content/pressespiegel/intelligentbauen_07_08_2009.pdf

http://www.swisspor-gruppe.com/index.php?page=1390

BSI Standard 100-4 Notfallmanagement:
https://www.bsi.bund.de/cln_156/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html