# BCM – auf den Notfall vorbereitet

**Im Kapitel 17 dreht sich alles um das Kontinuitätsmanagement (Business Continuity Management). Vorbereitungen auf einen möglichen Notfall werden getroffen, um die negativen Folgen einzugrenzen und ein Überleben des Unternehmens sicherzustellen. Die Norm verlangt, dass die Informationssicherheit auch in einer Krisensituation gewährleistet bleibt.**

Eine Krise oder Katastrophe kann schnell eintreten. Passiert dies ein Unternehmen unvorbereitet, kann die Existenz gefährdet sein. Dies können beispielsweise ein länger andauernder Ausfall der Hauptinfrastruktur, ein erfolgreicher Hackerangriff oder der Ausfall von wichtigen Mitarbeitenden sein und das Unternehmen vor eine grosse Herausforderung stellen. Tritt ein solches Ereignis ein, gilt es vorzubereitet sein und nicht in wilde Hektik auszubrechen. Auch gewohnte Regeln und Abläufe dürfen nicht einfach über den Haufen geworfen oder die Informationssicherheit vernachlässigt werden. Die Norm verlangt in A.17.1.2 klar: «Die Organisation sollte Prozesse, Verfahren und Massnahmen festlegen, dokumentieren, umsetzen und aufrechterhalten, um das erforderliche Niveau an Informationssicherheit in einer widrigen Situation aufrechterhalten zu können.»

In einem ersten Schritt geht es darum, die Ereignisse und mögliche Auswirkungen zu erfassen. Dies geschieht klassisch als BIA (Business Impact Analyse). Die wichtigen Prozesse werden erfasst und bewertet. Wie lange darf ein Prozess maximal ausfallen? Welcher Datenverlust kann maximal verkraftet werden. Gleichzeitig kann überlegt werden, wie gross der Schaden zum Beispiel nach 1, 2, 4, 8, 24, 48 und 72 Std. ist. Anschliessend werden die im jeweiligen Prozess genutzten Ressourcen (Menschen, Gebäude, Maschinen, IT-Infrastruktur, Lieferanten usw.) verknüpft. Die Ressourcen erben damit die definierten Anforderungen. Da oft die gleiche Ressource in verschiedenen Prozessen genutzt wird, zum Beispiel das Active Directory, der E-Mail-Server oder das CRM, definiert die kleinste Anforderung, wie die Ressource ausgelegt werden muss. Gleichzeitig gibt dies einen Indiz, in welcher Reihenfolge Ressourcen wieder zur Verfügung stehen müssen.

Ein kleiner Hinweis am Rande: Beim BCM, im Unterschied zur einer Risiko-Analyse, spielt die genaue 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 nicht mehr verfügbar ist, wird nicht unterschieden. Das «BCM-Problem» in diesem Fall heisst: Ausfall des Produktionsgebäudes.

## 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 nicht ideal und sollte klar getrennt werden. Es ist durchaus möglich, dass bei der Erstellung der Pläne weitere Fragen auftauchen, welche geklärt werden müssen. Die Grundstrategie gilt es aber zuerst festzulegen.

Bild: Archiv

Eine Krise oder Katastrophe kann die Existenz eines Unternehmens gefährden.

Inhaltlich schauen wir den kritischen Prozess «Produktion» an. Die Strategie für diesen Prozess kann in die Richtung gehen, dass das Lager vergrössert wird, um längere Produktionsausfälle abzufangen. Die Strategie kann auch vorsehen, die Produktion auf mehrere Standorte zu verteilen, sodass mittels Schichtbetrieb, selbst bei einem Ausfall des Gebäudes, nur ein geringer Ausfall des Prozesses zu erwarten ist. Eine Alternative könnte auch die Zusammenarbeit mit Mitbewerbern vorsehen.

Erst jetzt werden konkrete Notfallpläne erarbeitet. Erfahrungsgemäss lohnt es sich hier Schritt-für-Schritt-Anleitungen inkl. Checklisten zu schreiben. Der Mensch arbeitet unter enormem Druck einfach anders und wichtige Elemente können in der Hektik vergessen gehen. Für jeden Plan gibt es einen oder mehrere Verantwortliche (inklusive Stellvertreterregelung). Diese Personen müssen über genügend Befugnisse, Erfahrung und Kompetenz verfügen. Weitere Punkte, die es zu regeln gilt, sind:

- Definition des Krisenteams (wer, welche Rolle, Aufgaben und Verantwortlichkeiten usw.)
- Das Support-Team (zum Beispiel organisieren Trinken und Essen, informieren Personen, klären Dinge ab usw.)
- Definition der Einsatzzentrale (Intern, Extern, notwendige Ausrüstung, Schnittstellen usw.)
- Definition, wer und wie kommuniziert
- Umgang mit Behörden (zum Beispiel im Falle von Datenschutzverletzung mit der entsprechenden Aufsichtsbehörde)
- Mögliche Evakuierung (wann wird diese ausgelöst, wo trifft man sich, wie ist das Verhalten dort usw.)
- Definition der notwendigen Ressourcen (Menschen, Orte, Maschinen, ICT-Mittel usw.)
- Kontakt mit Lieferanten und Partnern

Papier (egal ob ausgedruckt oder elektronisch) ist dabei willig. Veränderungen gehören bei jedem Unternehmen dazu. Stetiger Wandel begleitet nicht nur die IT. Dies gilt es in den Plänen zu berücksichtigen. Mindestens jährlich und bei grösseren Veränderungen sind diese zu überarbeiten und an die neue Situation anzupassen.

Ebenfalls gilt es, die Pläne auch durchzuspielen. Aus langjähriger Audit-Tätigkeit weiss ich, dass selten eine Übung auf Anhieb klappt. Darum fordert die Norm unter A.17.1.3: «Die Organisation sollte in regelmässigen Abständen die festgelegten und umgesetzten Massnahmen zur Aufrechterhaltung der Informationssicherheit überprüfen um sicherzustellen, dass diese gültig und in widrigen Situationen wirksam sind.» Damit können die Prozesse, Verfahren und Massnahmen auf Herz und Nieren untersucht werden. Involvierte Personen merken damit auch, dass sie einen entsprechenden Beitrag leisten können oder müssen. Auch dies ist bereits vorgekommen, dass in der Checkliste erwähnte Personen gar nichts von ihrer Aufgabe wussten.

## Redundanz

Je nach Ergebnissen der Business Impact Analyse müssen Systeme redundant betrieben werden. Dies verlangt auch die Massnahme A.17.2.1 «Informationsverarbeitende Einrichtungen sollten mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen realisiert werden.» Gerade für kritische Systeme ist dies eine wichtige Grundvoraussetzung. Zum Beispiel der zentrale Dienst Active Directory (AD) gilt es redundant auszulegen. Ohne AD läuft in einem Windows-Netzwerk nichts mehr. Doch das AD sollte nicht im gleichen Serverraum auf der gleichen Hardware betrieben werden, sondern gehört an einen zweiten Standort, dies kann auch in einem anderen Brandabschnitt sein.

Bereitet sich ein Unternehmen auf eine mögliche Krise vor, kann diese schneller unter Kontrolle gebracht und eine grössere Katastrophe verhindert werden. Dazu gehört im ersten Schritt eine umfassende Impact Analyse und daraus abgeleitet eine BCM-Strategie. Als Ergebnis leiten sich genaue Checklisten ab, die helfen, strategisch vorzugehen und nichts zu vergessen. Somit kann das Überleben des eigenen Unternehmens auch in einer Krise sichergestellt werden.

**INFOS | KONTAKT**

**goSecurity GmbH**
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch