Link: http://www.computerwoche.de/a/print/noimages/2546356

Notfallmanagement in der IT

Business Continuity Management - Sind Sie auf den Ernstfall vorbereitet?

Datum: 16.10.2013
Autor(en): Stanislav Wittmann

Stunden, Minuten, ja sogar Sekunden entscheiden über Erfolg oder Versagen von Unternehmen. Um Ausfälle zu kompensieren, investieren diese zunehmend ins Notfallmanagement, auch Business Continuity Management (BCM) genannt.

Eine BCM-Strategie verfolgt zwei Ziele: Zum einen sollen kritische Geschäftsprozesse im Falle einer Störung nicht beeinträchtigt werden, zum anderen soll im Fall einer Unterbrechung deren rechtzeitige Wiederaufnahme sichergestellt sein. Um beide Aufgaben erfüllen zu können, müssen Unternehmen eine gewisse Vorarbeit leisten. Ein erster Schritt ist die Identifizierung von kritischen Geschäftsprozessen: Welche Geräte besitzen die am geringsten tolerierbare Ausfallzeit? Welche Daten dürfen niemals verfälscht werden? Diese Fragen müssen in einer **Risikoanalyse**[1] geklärt sein.

Kritische Geschäftsprozesse aufzuspüren, ist aber nur die halbe Miete. Denn ohne Unterstützung der Geschäftsleitung wird es schwer, ein BCM aufzubauen. Es braucht Zeit, Geld und eventuell auch neues Personal. Ein uneinsichtiges Management lässt sich vielleicht mit den Haftungsrisiken überzeugen, die es im Schadensfall eingeht. Sicherheitsbeauftragte, die weitere Argumente brauchen, können auch eine Business Impact Analyse (BIA) vornehmen. Dabei spielen sie potenzielle Schadensszenarien im Unternehmen durch, um die Bedeutung einer Notfallvorsorge zu unterstreichen. Die kritischen Prozesse, die Schäden verursachen könnten, sollten bereits im Rahmen der Risikoanalyse bekannt sein.

Plan-Do-Check-Act

Ohnehin ist eine BIA sinnvoll, um zielgerichtet Lösungen für ein BCM zu finden. Reicht das zur Überzeugung des Managements immer noch nicht, hilft vielleicht das Argument, dass eine (Re-)Zertifizierung nach ISO 27001 scheitern kann. Denn der **Demingkreis**[2] (Plan-Do-Check-Act-Zyklus) im Sinne des kontinuierlichen Verbesserungsprozesses ist auch beim BCM ein Muss.

Ist das Management überzeugt, geht es an die Einrichtung eines BCM. Hilfestellungen dazu finden sich beispielsweise in den Dokumentation der ISO 2700+-Reihe. So führt der Anhang A14 der ISO 27001 Anforderungen für ein BCM auf. Konkreter ist die ISO 27002, in der der Leitfaden für ein **ISMS**[3] (Information Security Management System) samt BCM deutlicher beschrieben ist. Kostenfreie Informationen zum Thema Notfallmanagement stellt auch das **Bundesamt für Sicherheits- und Informationstechnik (BSI)**[4] bereit, unter anderem im **Grundschutzkatalog 100-4**[5].

"Derzeit sind zudem verschiedene Normen für BCM in der Entwicklungsphase", so Ernst Döbbeling, Professor für Security Engineering an der Hochschule Furtwangen und Vorsitzender des betreffenden DIN-Spiegelausschusses. Die Entwicklung spreche dafür, dass das Thema in Zukunft eine größere Relevanz erhalten werde. Zumal nicht mehr nur Großunternehmen, sondern zunehmend auch Mittelständler von der Sinnhaftigkeit des BCM überzeugt seien.

Bleibt die Frage: Wie sieht ein funktionierendes Business-Continuity-Management aus? Im Folgenden werden dafür einige Beispielszenarien aufgezeigt, die besonders der IT-Abteilung im Unternehmen als Checkliste dienen können - gemäß der Frage "Sind Sie auf den Ernstfall vorbereitet?"

Serverräume

Wo eine IT-Abteilung existiert, ist ein Serverraum nicht weit weg. Selbst wenige Minuten Serverausfall können hier fatal sein. Um Ausfällen vorzubeugen oder sie zu kompensieren, gibt es verschiedene Möglichkeiten. Eine zweite Räumlichkeit, also einen redundanten Serverraum aufzustellen, ist eine Option - aber nicht gerade die günstigste. Denkbar ist eine Betriebsausfallversicherung, doch auch diese bezahlt nur den monetären Schaden. Kunden und Folgeaufträge bleiben vom Versicherungsschutz unberührt. Doch ein BCM lässt sich auch in der Planungsphase von Serverräumen, speziell im Bereich des Brandschutzes, mit einbeziehen. Der vorbeugende Brandschutz - bestehend aus baulichem, technischem und organisatorischem Brandschutz - muss eine lückenlose Kette der Sicherheit bilden. Schon die Wahl des Löschverfahrens/Löschmediums ist entscheidend. Falsche Löschwerkzeuge können Nutzer in ihrer Arbeit einschränken, unter Umständen gar zerstörerische Folgen nach sich ziehen.

"Um bei der Konzeptionierung von IT-Sicherheit erfolgreich zu sein, muss interdisziplinär und fachübergreifend gearbeitet werden", fordert Andreas Koch, Lehrbeauftragter für technischen Brandschutz an der **Hochschule Esslingen**[6]. Wer für seine Serverräume beispielsweise geeignete Löschsysteme suche, habe diverse Kriterien zu beachten. Zum einen sei vorher festzustellen, wie empfindlich die Technik auf Temperaturschwankungen, Feuchtigkeit oder auch Schalleinflüsse reagiere, so Koch. Zum anderen spielten bauliche Voraussetzungen eine Rolle - wie beispielsweise die Dichtigkeit und Druckbeständigkeit des Raumes. Des Weiteren seien organisatorische Randbedingungen zu beachten: Bestimmten Personengruppen, die für den IT-Betrieb verantwortlich sind, könnten die Serverräume dauerhaft zugänglich sein. Koch resümiert: "Der Brandschutzexperte sollte Teil des IT-Sicherheitsteams sein. Er besitzt neben dem baulichen und organisatorischen Brandschutz auch fundierte Kenntnisse im technischen Brandschutz."

Systeme

Oberstes Ziel einer BCM-Strategie ist es, kritische Systeme angemessen und vertretbar zu schützen. Neben Servern dürfen dabei andere wichtige Systeme nicht fehlen. Zu nennen sind hier wichtige Steuerungselemente für Fertigungen oder andere Clients. Eine transparente Risikobetrachtung ist das A und O. Die Verantwortlichen müssen sich fragen, wie kritisch das jeweilige System ist und ob ein gezieltes Notfallmanagement hier überhaupt sinnvoll ist. Schließlich können es sich viele Unternehmen finanziell nicht leisten, eine redundante Kommunikationsverbindung aufzustellen oder diese zu versichern. Das ist aber auch gar nicht nötig - ein BCM taugt nicht für alle Systeme.

Anwendungen

Auf Clients laufen Anwendungen. Das ist zum einen Software zur Steuerung von Anlagen, zum anderen welche, die im Rahmen der alltäglichen Geschäftsabwicklung benötigt wird - wie E-Mail-Clients. Um die Integrität der Daten zu wahren und sich vor Verlusten zu schützen, hilft die regelmäßige Datensicherung. Der **BSI-Grundschutzkatalog**[7] gibt dazu Hilfestellungen.

Immer im Blick haben müssen IT-Verantwortliche das Maximumprinzip, die ganzheitliche Betrachtung von Räumen, den darin enthaltenen Systemen und Anwendungen. Der maximalste Schutzbedarf ist ausschlaggebend für alle darunter liegenden Faktoren. Auch dazu sind **weitergehende BSI-Informationen verfügbar**[8].

Personal

Vergessen wir aber nicht den Dauerpatienten Mensch - sowohl das interne als auch das externe Personal. Unternehmen sollten zumindest darauf vorbereitet sein, dass die wichtigsten Mitarbeiter ausfallen oder das Unternehmen Richtung Konkurrenz verlassen. Eine Möglichkeit ist, andere Mitarbeiter rechtzeitig mit deren Know-how zu schulen, was allerdings zeitaufwändig ist und den laufenden Betrieb einschränken kann. Besser ist es, auf externe Personaldienstleister zurückzugreifen. Jedoch kann auch das zum Risiko werden. Thorsten Hoth, langjähriger Unternehmer in der Sicherheitsbranche, kennt die Gefahr aufgrund des herrschenden Niedriglohn-Niveaus und einer lediglich vorausgesetzten Ein-Tages-Prüfung seitens der IHK gut: "In dem meisten Fällen bieten unsere Sicherheitsfirmen nur Statisten, die unmotiviert und oft übernächtigt sind." Diese helfen in wirklichen Notsituationen kaum weiter. Deshalb sei es wichtig, nicht nur auf den Faktor Personalkosten zu schauen: "Statt dem billigsten Anbieter den Zuschlag zu erteilen, sollte man den günstigen wählen. Denn günstig heißt hier, das beste Preis-Leistungsverhältnis zu nehmen", rät Hoth. Nur so stellten Unternehmen wirklich sicher, dass bei Personalausfall professioneller Ersatz vorhanden sei und die Sicherheit nicht zusätzlich leide.

Vorsätzliche Handlungen

Hacker, Einbrecher, **Social Engineers**[9] und auch Insider mit falschen Absichten können IT-Abteilungen enorme Kopfschmerzen bereiten. Deshalb müssen sie ebenfalls Teil einer BCM-Strategie sein. Im ISO-Standard 27001 ist im Appendix A 13 der Punkt "Umgang mit Informationssicherheitsvorfällen" aufgeführt, der derartige Risiken behandelt. Weil kaum ein Unternehmen von vorsätzlichen Handlungen unberührt bleibt, sind deren Kategorisierung und die Aufstellung geeigneter Gegenmaßnahmen so wichtig. Nehmen etwa die Hacker-Angriffe von außen zu, müssen die Mitarbeiter entsprechend darauf geschult sein. Reicht das nicht aus, lässt sich das Problem vielleicht mit einer Aufstockung des Personals beheben (siehe auch Punkt "Personal").

Höhere Gewalt

In der IT-Abteilung fällt der Strom aus. Und das Unternehmen ist nicht darauf vorbereitet. Der GAU. Nicht so, wenn Notstromaggregate oder zumindest eine Betriebsausfallversicherung vorhanden sind. Was ist bei Brand, Hochwasser oder gar Erdbeben? Hoffentlich befindet sich der Serverraum nicht im Keller. Falls doch, welche Maßnahmen wurden gegen Hochwasserschäden getroffen?

Sicherlich sind solche Szenarien eher die Ausnahme als die Regel. Und doch sollten sie in der BCM-Planung enthalten sein. Entscheidend ist die Frage nach der Risikoakzeptanz. Wie mobil ist die IT-Abteilung und sind entsprechende redundante Räumlichkeiten vorhanden? Die zeitliche Umsetzung solcher Maßnahmen gehört natürlich auch in die Planung mit hinein.

Regelmäßiges Testen des BCM

Ein BCM soll nicht nur auf Papier stehen, sondern auch in der Realität funktionieren. Regelmäßige Prüfungen sind daher ein Muss. Zu prüfen sind vor allem Funktionalität und Effektivität der Maßnahmen. Aber auch der Stand der Technik ist mit zu beachten. Schließlich dreht sich die Welt und mit ihr die Entwicklung der Sicherheitstechnik. Und gerade im IT-Bereich kann es schnell passieren, dass man den Anschluss verliert.

Es ist nicht verkehrt, derartige Tests durch externe Spezialisten wie Auditoren oder Penetrationstester vornehmen zu lassen - sie werfen noch einmal einen anderen Blick auf mögliche Risiken.

Fazit

"Die Informationstechnologie hat sich in den vergangenen Jahren rasant entwickelt. In komplexen Prozessen und Strukturen, die sich heutzutage meist auf computergestützten Systemen abstützen und in ein ISMS eingebettet sein sollten, fällt es nicht immer leicht, alle Schwachstellen frühzeitig zu erkennen", erläutert Andreas Teuscher, Chief Information Security Officer bei der **SICK AG**[10], ISO 27001 Lead-Auditor und Vorstand des **ISACA Germany Chapter**[11].

Genau darum geht es beim BCM: Das Restrisiko so weit wie möglich reduzieren und mögliche Schäden transparent machen. Aber genau das ist auch das größte Hindernis im Notfallmanagement: Wer nicht ehrlich zu sich selbst ist, verliert. Teuscher stellt klar: "Ein risikoorientierteres BCM bildet eine Art zweiten Verteidigungsring und hilft die Lücken in einer ach zu optimistischen Risikoanalyse zu schließen. Grundvoraussetzung ist jedoch, dass sich eine BCM auf das Wesentliche beschränkt, Routinen etabliert und alle Wiederanlaufszenarien getestet worden sind".

Oberstes Ziel des Business-Continuity-Managements ist es, gar nicht erst greifen zu müssen. Um das zu erreichen, gilt es, alle Sicherheitsvorfälle genau zu untersuchen und auch zu protokollieren. Erst dadurch lassen sich wirksame Gegenmaßnahmen entwickeln.

BCM ist ein komplexes Thema und keine unabhängige, für sich alleinstehende Säule. Nur eingebunden in die Gesamtstrategie des Unternehmens hält es, was es verspricht. Neben einem seriösen Risiko-Management braucht es dafür vor allem eine Geschäftsleitung, die selbst hinter dem BCM steht, auch wenn dessen Nutzen nicht unbedingt direkt sichtbar ist. Dazu abschließend ein Vergleich: Jahrhunderte lang waren in Europa nur **weiße Schwäne**[12] bekannt und daraus folgte die (induktive) Schlussfolgerung, dass alle Schwäne weiß seien. Die Existenz schwarzer Schwäne wurde ausgeschlossen - bis diese These mit der Entdeckung Australiens widerlegt wurde. Die Frage an Sie als Unternehmen lautet: Sind Sie auf die schwarzen Schwäne vorbereitet? (sh)

Links im Artikel:

[1] **http://de.wikipedia.org/wiki/Risikoanalyse**
[2] **http://de.wikipedia.org/wiki/Demingkreis**
[3] **http://www.computerwoche.de/a/zertifiziertes-isms%2C2538518**
[4] **https://www.bsi.bund.de/**
[5] **https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile**
[6] **http://www.hs-esslingen.de/de/**
[7] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m06/m06026.html**
[8] **https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile**
[9] **http://www.computerwoche.de/a/wie-sich-mitarbeiter-vor-social-engineering-schuetzen%2C2540578**
[10] **http://www.sick.com/de/de-de/home/Seiten/Homepage1.aspx**
[11] **http://www.isaca.de/**
[12] **http://www.risiko-manager.com/index.php?id=58&no_cache=1&tx_ttnews%5btt_news%5d=16595&cHash=b33e89ea254fb18d322084b68f6c2ac1**
