Business Continuity Management: Wie abhängig sind Geschäftsprozesse von der IT?

Für grosse wie kleine Unternehmen heisst dies ganz klar, dass die IT-Sicherheit weit über den täglichen Backup hinausgeht. Für die komplexe Thematik drängt sich eine umfassende Betrachtungsweise auf. Technische Risiken sind genauso ernst zu nehmen wie menschliches Versagen, höhere Gewalt oder gar kriminelle Handlungen wie Diebstahl und Hacking.

Wolfgang Sidler

Sobald ein Unternehmen Daten erfasst oder Informationen speichert, muss auch die Frage der Sicherheit geklärt werden – unabhängig von Art und Grösse der Organisation. Und mit steigenden Investitionen in Netzwerktechnologien steigt der Bedarf an Sicherheitsmassnahmen weiter. Diesbezügliche Kosteneinsparungen werden allzu schnell durch Ausfallzeiten, Datenwiederherstellung oder sogar Wirtschaftsspionage wieder eingebüsst. Die «Disaster Recovery Studie» von der Firma Veritas, welche im Oktober 2004 veröffentlicht worden ist, zeigt auf wie Schweizer Unternehmen trotz Notfallplan nicht optimal auf eine Katastrophe im Rechenzentrum vorbereitet sind.

95 % der befragten IT-Manager in der Schweiz gaben an, dass sie ohne Disaster Recovery-Plan Katastrophen und Ausfällen schlicht ausgeliefert wären. Als die beiden grössten Bedrohungen wurde mit 86 und 80 % Hard- und Software-Fehler sowie Viren und Hacker-Angriffe genannt, gefolgt von Naturkatastrophen mit 78 %. Ausfälle aufgrund unabsichtlichem oder bösartigem Verhalten von Mitarbeitern stuften 64 % der Befragten als bedrohlich ein. 58 % der befragten Unternehmen erachten Krieg und Terrorismus als eine grosse Bedrohung.

45 % der befragten Schweizer Unternehmen mussten ihren Notfallplan in den vergangenen zwölf Monaten in die Praxis umsetzen. Erschreckend ist, dass lediglich bei 4 % der Befragten monatliche Tests stattfinden. Ebenso überprüfen wenige Unternehmen ihre Pläne auf einer monatlichen Basis. Ein jährlicher Test erfolgt immerhin bei 46 % der Befragten, während die jährliche Überprüfung bei 40 % liegt. Einfache Backupsysteme sind in 90 % der befragten Unternehmen im Einsatz. 56 % sichern ihre Daten an einem zweiten Standort, während 48 % ein eigentliches Disaster Recovery-Team gebildet haben.

Gefahren lauern überall

Die Bedrohungen, denen Informationen ausgesetzt sind, haben vielseitigen Ursprung:

- Höhere Gewalt: Feuer, Blitz, Sturm, Überschwemmung, Personalabgänge, Krankheiten
- Technisches Versagen: Netzwerkausfall, Ausfall Disk-Systeme, mangelnde Kompatibilität, Software-Fehler
- Menschliches Versagen: Fehlmanipulation, fehlende Sensibilisierung, Übermüdung
- Vorsätzliche Handlungen: Hacking, Diebstahl, Spionage, Erpressung, Missbrauch von Daten, Viren

Gerade auch die Sensibilisierung der Geschäftsleitung und sämtlichen Mitarbeitenden auf die oben genannten Risikofaktoren ist von grosser Bedeutung.

Vertrauen ist gut – Kontrolle ist besser

Die Weiterentwicklung der Informationstechnik (IT) wird zu einem erheblich erweiterten Einsatz informationstechnischer Systeme führen. Dadurch wächst die Abhängigkeit von Verwaltung und KMU zunehmend von dem einwandfreien Funktionieren und der uneingeschränkten Verfügbarkeit informationstechnischer Systeme. Gleichzeitig ist mit der Zunahme von Bedrohungen zu rechnen, die die Vertraulichkeit, Verfügbarkeit und Integrität der Daten (IT-Sicherheit) gefährden. Vertrauenswürdige und sichere Geschäftsprozesse sind jedoch entscheidende Erfolgsfaktoren:

- Welche kritischen Abläufe bestimmen den Geschäftserfolg?
- Welche Informationen benötigen man heute und in Zukunft unbedingt für die Geschäftsabläufe?
- Welche relevanten Risiken bestehen für unternehmenskritische Informationen?
- Welche Sicherheitsziele setzt man sich für die kritischen Informationen im Unternehmen?

Die Verfügbarkeit stellt eine eminent wichtige Komponente der Informationssicherheit dar, kann doch der Verlust von Daten bzw. der Ausfall von Transaktionssystemen enormen materiellen und immateriellen Schaden bedeuten. Im Sinne eines Business Continuity Managements (BCM) sind daher Vorkehrungen zu treffen, die in erster Linie darauf abzielen, Systemkonfigurationen zu vermeiden, bei denen der Ausfall einer Komponente zum Ausfall des Gesamtsystems führt.

Business Continuity Management (BCM) und Disaster Recovery Planning (DRP)

BCM ist eigentlich nichts Neues – aber wurde seit dem 11. September wieder aktuell – abgesehen von der modischen Anglisierung des Begriffs. Früher benutzten wir die Begriffe wie Krisenmanagement oder Notfallplanung. Ereignis- und Krisenmanagement sowie Business Availability (Verfügbarkeit) Business Continuity (Geschäftsfortführung) und Business Recovery (Wiederanlauf) ist für viele Unternehmen zu einer realen Herausforderung geworden.

Doch die Anforderungen an BCM haben sich mit den Unternehmen verändert. Die Firmen sind heute viel stärker auf elektronische Geschäftsprozesse angewiesen, die rund um die Uhr funktionieren müssen. Betriebsunterbrüche führen daher potenziell zu höheren Schäden. Nicht nur das betriebliche, sondern auch das sich verändernde regulatorische Umfeld tragen zu den gesteigerten Anforderungen an das BCM bei. Unternehmensweites Risikomanagement und Corporate Governance stehen derzeit weltweit im Brennpunkt von Regulatoren und Gesetzgebern (Basel II, Sarbens-Oxley-Act etc.).

BCM ist keine reine IT-Angelegenheit mehr. Dabei kommt der Schnittstelle zwischen IT und dem Business eine zentrale Rolle zu. Business-Anforderungen müssen bis ins Detail mit einer Business Impact-Analyse identifiziert und bewertet werden.

So schlägt BCI (www.thebci.org) einen sechsstufigen Plan (Life Cycle) vor:

1. Geschäftsprozess-Analyse: Welche Prozesse könnten in welcher Form betroffen sein? Wie müsste ein Notfallbetrieb aussehen (Wiederanlauf oder unterbruchslos)? Die Durchführung einer Business Impact-Analyse und einer Risikoanalyse stellt einen wesentlichen Teil dieses Schritts dar.
2. Entwicklung der BCM-Strategie: Evaluation und Selektion von entsprechenden Handlungsoptionen, z. B. interne Vorkehrungen, Übertragung des Notfallbetriebs an einen externen Dienstleister, Entscheid über die geforderte Ausfallzeit (keine, 1 Stunde, 8 Stunden)
3. Umsetzung der Massnahmen auf Geschäftsprozess- und IT-Ebene. Dazu zählen z. B. die Erarbeitung eines Notfallhandbuches und Bildung eines Krisenstabs.
4. Verankerung einer BCM-Kultur im Sinne einer Qualitätsmassnahme.
5. Durchführen von Notfallübungen, schrittweise Verbesserung der getroffenen Massnahmen.
6. Etablierung eines permanenten Programm-Managements zur kontinuierlichen Verbesserung der BCM-Massnahmen. Das BCM-Programm wird Teil des Risk Managements des Unternehmens.

Damit Business Continuity Management ein Erfolg wird, müssen einige Voraussetzungen erfüllt werden:

- Unterstützung durch die Unternehmensführung: Oftmals fehlen der Geschäftsleitung und den Geschäftsverantwortlichen das Verständnis dafür, dass BCM nicht eine Aufgabe ist, die delegiert werden kann. BCM ist nur dann erfolgreich, wenn es von der gesamten Geschäftsleitung mitgetragen und als Aufgabe aller Geschäftseinheiten verstanden wird. Es genügt nicht mehr, diese Aufgabe an die IT zu delegieren, zumal die Auswirkungen einer Katastrophe das ganze Unternehmen betreffen.

- Taktgeber ist das «Business»: Um die relevanten Risiken überhaupt identifizieren und bewerten zu können, braucht es spezifische Kenntnisse der Geschäftsabläufe (Prozesse). Es ist daher zwingend notwendig, für die Business Impact-Analyse des Schadenspotenzials und der internen und externen Abhängigkeiten die betroffenen Geschäftseinheiten frühzeitig zu involvieren. So entstehen Business Recovery-Strategien, welche auf die Anforderungen der Geschäftseinheiten abgestimmt sind. Der IT als interner Dienstleistungserbringer kommt in vielen Fällen die Hauptlast in der Umsetzung von Vorsorgemassnahmen (Disaster Recovery-Plänen) zu.
- Priosisierung: Der Schlüssel zu einem erfolgreichen BCM liegt darin, zwischen unternehmenskritischen und -unkritischen Geschäftsprozessen zu unterscheiden. Die Fokussierung auf unternehmenskritische Prozesse erleichtert die Identifikation derjenigen Ressourcen – und da gehören IT-Dienstleistungen dazu –, welche nach einer Katastrophe unbedingt wieder bereit gestellt werden müssen.
- Integraler Ansatz: BCM muss prozess- und bereichsübergreifend koordiniert werden. Es nützt nichts, wenn die Verkaufsabteilung nach kurzer Zeit wieder Bestellungen entgegennehmen kann, diese aber nicht abgewickelt werden können, weil die Lagerbewirtschaftung noch nicht operativ ist. Eine saubere Analyse der Schnittstellen und Abhängigkeiten hilft, die Anforderungen und Fähigkeiten von Leistungsbezügern und Leistungserbringern transparent zu machen. Dies fördert zudem die direkte Kommunikation zwischen Business und IT.
- BCM als Prozess: In Zeiten, in denen Organisations-Strukturen bereits wieder falsch sind, kaum sind sie publiziert, veralten BCM-Pläne sehr schnell. Deshalb ist es notwendig, die BCM-Pläne periodisch einer Prüfung zu unterziehen und anzupassen. Die BCM-Pläne müssen regelmässig getestet und die betroffenen Mitarbeiter und Krisenstäbe geschult werden.

Fazit

Security- und Risk-Management wird für zahlreiche Unternehmen immer mehr zu einem kritischen Erfolgsfaktor. Daraus abgeleitet wird die Operationalisierung der Informationssicherung – und damit die Sicherheits (BCM)-Kultur – durch die Geschäftsleitung bestimmt und auf der obersten Führungsebene verankert. Mithilfe der Business Impact-Analyse werden die unternehmenskritischen Prozesse (Kernprozesse) und die hierfür notwendigen Organisationseinheiten, IT- und Gebäudeinfrastrukturen identifiziert und zueinander in Beziehung gesetzt. Die Entscheidung über die tragbaren Restrisiken und die daraus abgeleiteten Szenarien ist durch die Risikopolitik der Unternehmung sowie durch Kosten-Nutzen-Überlegungen bestimmt und durch den Verwaltungsrat oder die Geschäftsleitung zu treffen.

Tritt trotz der präventiven Massnahmen ein Schadensfall ein, sind in erster Priorität Menschenleben zu schützen, zweitens die Datenbestände, die für die Weiterführung der Geschäftstätigkeit immer wichtiger werden. ■