ILLUSTRATIONEN: CW/THÜ

Unternehmen, die in Sachen Business Continuity Management knausern, nehmen enorme materielle und immaterielle Schäden in Kauf.

Vorsorgen für den Ernstfall

IT-Sicherheit geht weit über den täglichen Backup hinaus. Technische Risiken sind genauso ernst zu nehmen wie menschliches Versagen, höhere Gewalt oder gar kriminelle Handlungen. **VON 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 letzte Disaster-Recovery-Studie von Veritas zeigt auf, dass Schweizer Unternehmen trotz Notfallplan nicht optimal auf eine Katastrophe im Rechenzentrum vorbereitet sind. 95 Prozent 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 wurden mit 86 und 80 Prozent Hard- und Software-Fehler sowie Viren und Hacker-Angriffe genannt, gefolgt von Naturkatastrophen mit 78 Prozent. Ausfälle aufgrund unabsichtlichem oder bösartigem verhalten von Mitarbeitern stuften 64 Prozent der Befragten als bedrohlich ein. 58 Prozent der befragten Unternemen erachten Krieg und Terrorismus als eine grosse Bedrohung.

45 Prozent der Firmen mussten ihren Notfallplan in den vergangenen zwölf Monaten in die Praxis umsetzen. Erschreckend ist, dass lediglich bei 4 Prozent der Befrag-

ten monatliche Tests stattfinden. Ebenso wenige Unternehmen überprüfen ihre Pläne auf einer monatlichen Basis. Ein jährlicher Test erfolgt immerhin bei 46 Prozent der Befragten, während die jährliche Überprüfung bei 40 Prozent liegt.

Wachsende Abhängigkeit

Die Weiterentwicklung der Informationstechnik 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 gefährden. Vertrauenswürdige und sichere Geschäftsprozesse sind jedoch entscheidende Erfolgsfaktoren.

> Security- und Risk-Management wird für Unternehmen immer mehr zu einem kritischen Erfolgsfaktor.

Die Verfügbarkeit stellt eine eminent wichtige Komponente der Informationssicherheit dar, kann doch der Verlust von Daten beziehungsweise 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.

BCM ist eigentlich nichts Neues – abgesehen von der modischen Anglisierung des Begriffs. Früher benutzte man 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, Sarbanes-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.

Zahlreiche Voraussetzungen

Damit Business Continuity Management ein Erfolg wird, müssen einige Voraussetzungen erfüllt werden: Oftmals fehlen der Geschäftsleitung und den Geschäftsverantwortlichen das Verständnis dafür, dass BCM nicht eine Aufgabe ist, welche 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. 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.

Der Schlüssel zu einem erfolgreichen BCM liegt ausserdem darin, zwischen unternehmenskritischen und -unkritischen Geschäftsprozessen zu unterscheiden. Die Fokussierung auf unternehmenskritische Prozesse erleichtert die Identifikation derjenigen Ressourcen – und da gehören IT-Dienstleistungen dazu – die nach einer Katastrophe unbedingt wieder bereitgestellt werden müssen.

Im Weiteren muss BCM 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.

Und schliesslich gilt es, BCM als Prozess zu verstehen. 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 Sicherheitskultur – durch die Geschäftsleitung bestimmt und auf der obersten Führungsebene verankert. Mithilfe der Business-Impact-Analyse werden die unternehmenskritischen Prozesse 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. ■

WEITERE INFORMATIONEN

Das BCI-Phasenmodell

Das Business Continuity Institute (BCI) empfiehlt in Sachen BCM einen sechsstufigen Plan:

1. Geschäftsprozess-Analyse: Welche Prozesse könnten in welcher Form betroffen sein? Wie müsste en Notfallbetrieb aussehen?
2. Entwicklung der BCM-Strategie: Evaluation und Selektion von entsprechenden Handlungsoptionen.
3. Umsetzung der Massnahmen auf Geschäftsprozess-Ebene und IT-Ebene.
4. Verankerung einer BCM-Kultur im Sinne einer Qualitätsmassnahme.
5. Durchführen von Notfallübungen.
6. Etablierung eines permanenten Programm-Managements zur kontinuierlichen Verbesserung der BCM-Massnahmen.

* Wolfgang Sidler ist eidg. Wirtschaftsinformatiker und Mitautor des «Sicherheitshandbuches für die Praxis». www.sihb.ch