Reale Risiken – realistische Sicherheitsmassnahmen

Business Continuity

Von Justin Clark

Niemand kann vorhersehen, was die Zukunft bringt. Aber Unternehmen können bestimmte Massnahmen ergreifen, um sicherzustellen, dass sie für jedes zukünftige Ereignis angemessen vorbereitet sind.

Im Falle einer Katastrophe zeigen sich schnell die Unterschiede zwischen Unternehmen, die über ausgereifte Pläne zur Fortsetzung des Geschäftsbetriebes verfügen, und solchen, bei denen dies nicht der Fall ist. Gut vorbereitete Unternehmen ziehen schnell in neue Räume um, stellen ihre Daten wieder her und arbeiten weiter. Den anderen bleibt nicht viel anderes übrig, als ihren Betrieb stillzulegen oder einzuschränken, bis eine Lösung gefunden wird. Die Verzögerungen können kostspielig sein und schlimmstenfalls die Existenz des Unternehmens selbst gefährden. In einem ernüchternden Report berichtete beispielsweise die britische Handelskammer, dass 80 Prozent der Unternehmen, die durch ein kritisches Ereignis betroffen waren, nicht wieder eröffneten und innerhalb von 18 Monaten den Geschäftsbetrieb einstellen mussten [1].

Feststellen, was passieren könnte ...

Voraus planen

Warum versäumen es dann aber manche Unternehmen, ausreichend in so genannte «Business Continuity»-Massnahmen zu investieren oder geeignete Notfallpläne zu entwickeln? Das Problem ist, dass die Vorteile erst dann richtig erkennbar werden, wenn etwas passiert. Unternehmen sind heute jedoch mehr Risiken ausgesetzt als je zuvor – nicht nur grossen Katastrophen wie Überschwemmungen, Orkanen und Attentaten von Terroristen, sondern auch «alltäglichen» Gefahren wie Stromausfällen, Verkehrsunfällen, Erkrankungen des Personals und Softwareviren.

So schätzte beispielsweise Ende 2004 die Analystenfirma Computer Economics, dass die Computerwürmer Netsky und Sasser Schäden von zirka 6,25 Milliarden US-Dollar angerichtet haben und Hunderte von Organisationen weltweit infizierten, unter anderem die britische Küstenwache, den Flughafen Heathrow und die Europäische Kommission [2]. Selbst ein einziger Bedienfehler kann zu erheblichen Datenverlusten führen und grosse Probleme verursachen. Was muss also getan werden, um das Risiko effektiv zu managen und einen unterbrechungsfreien Geschäftsbetrieb sicherzustellen?

Die richtigen Fragen stellen

Es gibt dafür drei Erfolgsregeln. Die erste lautet, dass man das eigene Geschäft kennen muss. Dies mag einfach klingen, aber man benötigt eine gründliche Kenntnis der Organisation von oben nach unten. Hierbei sind die Perspektiven aller Beteiligten zu berücksichtigen – die der Aktionäre ebenso wie die der Kunden und Mitarbeiter. Die Ansichten müssen ausgewogen, exakt, vollständig und aktuell sein. Ist dies nicht der Fall, so werden auch die Entscheidungen, welche Schritte für die Fortführung des Geschäftsbetriebs erforderlich sind, fehlerhaft sein.

Ohne externe Hilfe können sich Firmenangehörige damit schwer tun, eine ausreichend detaillierte und exakte Darstellung zu liefern. Wenn man in einem Unternehmen arbeitet, kennt man die gewohnten Abläufe und kann leicht etwas übersehen, was für einen externen Experten ganz offensichtlich ist. Oft zeigt sich, dass hausinterne Teams nicht so viele Fra-

Archivbild

Das Risiko ständig im Auge behalten

Justin Clark, Business Continuity Consultant,
BT Global Services, pp A5P BT Centre,
81 Newgate Street, London EC1A 7AJ,
Tel. +44 (0)1473 607 326, justin.clark@bt.com

gen stellen, wie sie sollten, und eher Annahmen auf der Basis ihrer Erfahrung treffen.

Um ein Unternehmen so kostengünstig wie möglich abzusichern, sind detaillierte Kenntnisse der Zielsetzungen, Prioritäten und Tätigkeiten dieses Unternehmens erforderlich. Anschliessend müssen alle Risiken betrachtet werden – nicht nur Katastrophen, sondern auch alltägliche Vorkommnisse, die sich nachteilig auf Bereiche der Geschäftstätigkeit auswirken können. Natürlich muss man die Folgen eines Ausfalls von IT- und Kommunikationssystemen berücksichtigen, aber dies ist nur der Anfang. Auch Risiken wie Bedienfehler, der mögliche Ausfall eines wichtigen Lieferanten usw. müssen hier einbezogen werden.

Hier zeigt sich der Vorteil externer Berater. Diese werden eine Menge einfacher Fragen zu grundlegenden Dingen stellen und damit gründlich feststellen, was passiert und was passieren kann. Sie werden ihre Befunde auch in einer konzentrierten Weise präsentieren, was eine ausgewogene Analyse der Risiken ermöglicht.

Vom Risiko zum ROI

Die zweite Regel lautet, dass der Zusammenhang zwischen Kosten und Nutzen bekannt sein muss. Dabei ist die Kostenseite direkt einsichtig – der Zeitaufwand zur Ausarbeitung und Einführung von Business-Continuity-Plänen, die Redundanz zum Verlagern von Geschäftstätigkeiten bei Ausfall eines Bereiches oder die zusätzlichen IT-Einrichtungen für die Datensicherung und für den Schutz gegen den Ausfall einzelner Komponenten. Wenn man jedoch bedenkt, dass diese Investitionen erfolgen, um das Unternehmen gegen einen möglicherweise niemals eintretenden Ernstfall zu schützen, wie kann der Nutzen ermittelt werden?

Mit gründlichen Kenntnissen von der Funktionsweise eines Unternehmens sowie einer umfassenden Analyse der möglichen Konsequenzen lassen sich die Kosten vorhersagen, die sich aus einem Zwischenfall ergeben könnten, vor und nach der Aufstellung eines Notfallplans und mit den notwendigen Infrastruktur-Investitionen. Hierdurch lassen sich mehrere Investitionsmöglichkeiten unter dem Gesichtspunkt beurteilen, wie sie dazu beitragen können, das finanzielle Gesamtrisiko des Unternehmens zu verringern.

Die dazu erforderliche detaillierte Analyse kann noch einen weiteren nützlichen Nebeneffekt haben. So lassen sich beispielsweise Abläufe identifizieren, deren Effektivität noch optimiert werden kann.

Eignungsnachweis

Die dritte Erfolgregel ist der Test. Eine jüngere Umfrage des CSO-Magazine lieferte ein beunruhigendes Ergebnis: Die überwältigende Mehrheit der Unternehmen in den USA (93 Prozent) verfügte zwar über irgendeine Form von Business-Continuity-Plan, aber nur in 37 Prozent der Unternehmen wurde dieser auch in einer realistischen Situation getestet [3].

Hier sei nur das Beispiel eines bedeutenden Unternehmens erwähnt. Dieses verfügte über einen Business-Continuity-Plan, der von mehreren technischen Fachleuten und vom Vorstand genehmigt wurde, der es aber erforderlich machte, 3000 Mitarbeiter aus dem Geschäftsviertel in den Londoner Docklands innerhalb von 30 Minuten in ein Notfallzentrum im Norden Londons zu verlegen. Dies bedeutet, dass eine Strecke von gut 17 km mitten durch eine der belebtesten Wirtschaftsmetropolen Europas in weniger als einer halben Stunde zurückgelegt werden sollte.

In diesem Fall war es klar, dass der Plan im Ernstfall nicht funktionieren würde. In den meisten Fällen sind die Schwachstellen jedoch weniger offensichtlich, weswegen der Business-Continuity-Plan jedes Unternehmens in regelmässigen Abständen auf seine Tauglichkeit überprüft werden muss. Wie es auch bei den Rettungsdiensten üblich ist, müssen Ereignisse simuliert werden, und es ist nachzuweisen, dass man im konkreten Fall richtig darauf reagieren kann. Es hat keinen Zweck, einfach anzunehmen, dass man die Daten aus der Datensicherung regenerieren kann oder dass ein Call-Center in Asien für eines in Europa einspringen kann – man muss es konkret nachweisen können.

BCI – Best Practices

Das in England ansässige Business Continuity Institute (BCI) wurde 1994 gegründet. Es hat mehr als 1650 Mitglieder in 45 Ländern. Das BCI zertifiziert seine Mitglieder in zehn Kernkompetenzen, über die ein BCM-Spezialist verfügen sollte, um das Business-Continuity-Management vollständig und professionell umsetzen zu können. BCI hat Richtlinien für sinnvolle Verfahrensweisen herausgegeben, die eine gute Grundlage für jeden Business-Continuity-Plan darstellen. In Grossbritannien beruht hierauf die Spezifikation PAS56 des British Standards Institution – dies ist ein erster Schritt zu einem formalen Standard für das Business-Continuity-Management von Unternehmen.

Info: www.thebci.org

Wo liegt der Nutzen, wenn der Ernstfall nie eintritt?

Prüfung auf Herz und Nieren

Ebenso wichtig ist es, dass die Mitarbeiter wissen, wie sie sich im Falle eines Falles verhalten müssen. In den Unternehmen wird gewöhnlich die Evakuierung des Gebäudes im Brandfall trainiert. Warum sollte man also nicht auch das Verhalten der Mitarbeiter in anderen – möglicherweise sogar wahrscheinlicheren – Notsituationen testen?

Die Statistiken legen nahe, dass ein grösserer Schaden im Unternehmen eher durch einen ungeschickten Klempner als durch einen terroristischen Anschlag verursacht wird. Meistens sind es die scheinbar einfachen Dinge, gegen die wir uns alle absichern müssen. Dies erfordert geschulte Fachleute, die das Risiko ständig im Auge behalten, die jeden Stein umdrehen und die Best-Practice-Verfahren anwenden. Und um ganz sicher zu gehen, dass sie ihre Arbeit gut gemacht haben, und dass alle wissen, was von ihnen erwartet wird, muss man testen, testen und nochmals testen. Es ist eine mühsame Arbeit, die aber über den Fortbestand eines Unternehmens entscheiden kann. ■

Literatur

[1] The Guardian, Controlling the risk – cheaply, 2003

[2] www.computing.co.uk/computing/analysis/2075989/despatches-frontline-war-against-pc-viruses

[3] CSO-Magazine, Business Continuity Survey, 2005