VOM IT INCIDENT ZUM DESASTER, … ZUR PLEITE?

Bewusst vorbeugen

AXEL SITT*

VORFÄLLE WIE DEEPWATER HORIZON ZEIGEN DIE DYNAMIK, DIE EIN «KLEINES EVENT» AUFNEHMEN KANN, WENN ES SCHLECHT GEMANAGT IST UND IN DER FOLGE AUSSER KONTROLLE GERÄT. DIES GILT NICHT NUR FÜR TECHNISCHE RISIKEN, SONDERN AUCH UND SPEZIELL FÜR IT-RISIKEN.

Unternehmen jeder Grösse, speziell Banken, sind auf ihre Informationstechnologie angewiesen. IT ist inzwischen ein elementarer Bestandteil ihres Geschäftsmodells. Da die Verfügbarkeit von Daten für Unternehmen von enormer Wichtigkeit ist, muss auch ein Disaster-Recovery-Plan als essentiell erachtet werden. Während die Finanzinstitute versuchen, neue Technologien zu ihrem Vorteil zu nutzen, müssen sie sich zunehmend auch mit deren Auswirkungen auf die Sicherheit auseinandersetzen.

Gemäss der von Ernst & Young durchgeführten «13th Annual Global Information Security Survey» haben Banken weltweit ihre Ausgaben im Bereich Sicherheit erhöht. Trotzdem sind sie noch weit davon entfernt, den Sicherheitsanforderungen der neuen Zeit gerecht zu werden. 60 Prozent der 1600 befragten Führungskräfte aus 56 verschiedenen Ländern sagten, sie nähmen ein erhöhtes Sicherheitsrisiko durch Social Networks und persönliche Mobilkommunikation wahr. Aufgrund des Mangels an Kontrolle dieser Technologien gibt es keine hundertprozentigen Sicherheitsgarantien mehr. Interessanterweise taucht hier ein Desaster-Fall in den Bedenken nicht mal auf. Nur zu gerne gehen wir davon aus, dass alles stabil läuft und das auch so bleibt.

Ausgelöst durch Fusionen, Kostensenkungsdruck und Fokussierung auf Kernkompetenzen ist ein weiteres hohes Gefahrenpotenzial entstanden: der Trend zum Outsourcing von Sicherheitsleistungen. Ohne Zweifel kann ein professionelles und bedürfnisgerechtes Outsourcing auch für Banken eine wichtige Rolle einnehmen. Es ist jedoch ein Trugschluss zu glauben, dass man mit dem Outsourcing auch das Systemrisiko outsourcen könnte. Risiken lassen sich nicht «outsourcen»! Zwar können diese durch Versicherungsverträge oder durch operative Regelungs- und Kontrollmassnahmen abgefedert werden, aber wenn ein System ausfällt, hat dies immer auch erhebliche Konsequenzen auf das Geschäft eines Unternehmens.

Vor diesem Hintergrund ist ein technisch orientiertes Disaster-Recovery-Konzept kombiniert mit einem funktionierenden Unternehmens-Krisenmanagement im Rahmen eines gezielten Risikomanagements je länger je wichtiger. Was passiert, wenn in Ihrem Unternehmen die IT ausfällt?

- Werden Sie Daten verlieren?
- Entsteht aus dem Verlust evtl. ein Haftungsrisiko?
- Sind Sie ausreichend auf diese Situation vorbereitet?
- Wie lange darf es dauern, bis nach einer Katastrophe alle Prozesse wieder laufen?
- Ab welcher Unterbruchszeit muss der Betrieb ausgesetzt werden?
- Und was kostet das?

Die Schlüsselbegriffe sind hier Recovery Point Objectives (=RPO), Recovery Time Objectives (=RTO) und Maximum Tolerable Outage Time (= MTO). Die Praxis zeigt, dass die damit verbundenen Fragestellungen in diversen IT-Umgebungen überhaupt nie detailliert angeschaut worden sind oder unter Umständen die Perspektive nicht stimmte.

Startpunkt ist eine sogenannte Business-Impact-Analyse (=BIA). Diese sollte gestützt sein durch, oder kombiniert werden mit einer Risikoanalyse. Der Unterschied liegt in der Vorgehensweise. Liegen die Resultate der BIA vor, geht es daran zu ermitteln, inwieweit die realexistierende IT-Landschaft diesen Erfordernissen gerecht werden kann. Mit entsprechenden Erfahrungen kann man in Form eines Quick-Checks relativ schnell ermitteln, wie anfällig evtl. eine IT-Landschaft für einen Desaster-Fall sein kann.

Nicht selten kommen dabei Erkenntnisse zu Tage, die auf strukturelle Schwächen in der Organisation, der Dokumentation oder den Prozessen der jeweiligen IT-Abteilung zurückzuführen sind. Man könnte auch sagen, ein funktionierendes Desaster Management ist durchaus als Gradmesser für die Qualität der IT zu interpretieren. In einem Desaster-Fall geht man davon aus, dass grössere Teile der IT-Infrastruktur oder der IT-Applikationen nicht mehr vorhanden ist oder nicht mehr zeitgerecht oder leistungsgerecht arbeiten. Das heisst, die Beteiligten müssen davon ausgehen, dass mindestens

- Daten verloren gegangen sind
- Hardware komplett ersetzt oder neu aufgesetzt werden muss
- Netzwerkstrukturen nicht mehr vorhanden sind oder nicht mehr ordentlich funktionieren
- User nicht mehr arbeiten können
- Geschäftsvorfälle nicht abgewickelt werden können
- Kunden die eine oder andere Auswirkung zu spüren bekommen

Als Folge müssen Back-up-Konzepte detailliert untersucht werden nach Intervallen, Vollständigkeit, technischer Lösung, Reproduzierbarkeit und weiteren Aspekten. Es reicht nicht aus, mit einem Stan-

dard-Back-up-Approach zu arbeiten. Dieser wird mit hoher Wahrscheinlichkeit in Einzelfällen dem Bedarf nicht gerecht.

Zur erfolgreichen Bereitstellung einer Disaster-Recovery-Planung gilt es folgende Punkte zu beachten:

- IT-Disaster-Recovery-Planung ist eine vielseitige Herausforderung: Es gilt Szenarien zu analysieren und Optionen abzuwägen. Deshalb ist eine solide Datenbasis ein Muss. Wer nicht auf Knopfdruck sagen kann, welche Applikationen betroffen sind, wenn bestimmte Server oder Netzelemente ausfallen, wird evtl. schon durch Change-Management oder Updating/Patching heikle Momente zu spüren bekommen.
- Monitoring: Nach der Einführung eines Disaster-Recovery-Plans muss die erarbeitete Datenbasis kontinuierlich gepflegt und überwacht werden.
- Den Recovery-Plan testen: Was der Recovery-Plan zu leisten vermag, kann nur durch regelmässige Tests herausgefunden werden. Beim Testing sind aber klare Strukturen und Anforderungen zu beachten. Andernfalls besteht die Gefahr, dass die Tests Scheinsicherheit schaffen.
- Das Back-up-Konzept muss gut durchdacht, gepflegt und getestet werden. Um einen physischen Totalverlust zu vermeiden ist eine externe Sicherung zu gewährleisten, die sicher ist und zugleich nicht den gleichen Point of Failure haben darf.
- Einrichtung zusätzlicher Server erwägen für alle kritischen Daten/zur Sicherstellung einer alternativen Zugriffsmöglichkeit. Je nach Kritikalität verschiedener Systeme, Daten und Zugriffsmöglichkeiten ist über ein Redundanz-Konzept nachzudenken.

Die Liste könnte noch eine Weile fortgesetzt werden. Neben diesen mehrheitlich technischen Fragestellungen werden dann aber diverse organisatorische Fragestellungen gerne übersehen. Dazu zählen zum Beispiel:

- Koordinierte Ferienpläne von Technikern und Schlüsselpersonen in der IT
- Aufbau alternativer Kompetenzen bei Engpässen
- Verfügbarkeit von kompetentem Personal im Notfall
- Notfall-Strukturen (Alarmierung, Eskalation, Krisenmanagement)

Ein Disaster-Management-Konzept muss auch das Unmögliche vorhersehen.

- Geeignete und vorbereitete Kommunikation
- Einhaltung von Security-, Compliance- und IKS-Erfordernissen im Disaster-Fall
- Management der sekundär betroffenen Ressourcen. Damit sind die Unternehmensteile gemeint, die entweder als Folge eines Vorfalls nicht arbeiten können oder diejenigen, die evtl. alternativ tätig sein könnten.
- Vorausschauendes Business Management der Folgen eines Incident/Disaster

Wer heutzutage davon ausgeht, dass ein IT Incident auch ein reiner IT Incident bleibt, der könnte sich schnell in einer Situation wiederfinden wie die BP-Verantwortlichen, die anfangs offensichtlich auch nur von einem technischen Versagen ausgegangen sind.

Gemessen an den Kosten, die ein Disaster-Fall potenziell hat, sind die Präventionskosten verschwindend gering. Diese Aussage hält auch dem fatalistischen Schwarz-Weiss-Ansatz stand, «Man könne ja sowieso nichts tun». Dies ist eine reine Schutzbehauptung, die in 99 von 100 Fällen nicht stimmt.

Dr. Axel Sitt ist Geschäftsführer der comratio Technology & Consulting GmbH mit Sitz in Zürich.