Kapitel 9

Disaster Recovery: Wenn Albträume wahr werden

Die Hersteller von Speicherausrüstung und Backup-Software werden nicht müde zu betonen, dass die so genannten Ereignisse vom 11. September 2001 in Sachen Recovery und Katastrophenvorsorge einen wahren Bewusstseinsschub bewirkt hätten. IT-Leitern, Netzwerkadministratoren und sogar CEOs oder Geschäftsführern sei schlagartig klar geworden, dass nach dieser realen Katastrophe dringender Handlungsbedarf bestehe. Doch auf die Frage, was denn inzwischen getan worden sei und ob das neue Bewusstsein auch zu neuen Umsätzen geführt habe, geben die Hersteller keine Antwort. Und die Anwender schweigen. So wie immer.

Über Disaster und Recovery spricht man nicht. Nach wie vor gilt es als geschäftsschädigend, den erlittenen Schaden publik werden zu lassen und so Schwachstellen in den Sicherungssystemen offen zu legen. Success Storys auf diesem Felde sind denn auch eher selten. Das hat sich auch nach jenem berühmten Datum kaum geändert. Dell und andere Hersteller können zwar stolz jede Menge Schreiben vorweisen, in denen sich New Yorker Kunden nach dem 11. September 2001 überschwänglich über die schnellen Ersatzteillieferungen bei Rechnern und Speichergeräten und sonstige unbürokratische Hilfe bedankten. Doch diese Katastrophe kennzeichnete nicht den Alltag von Computer-Downtime. Deshalb kann bezweifelt werden, ob es mit dem besagten Bewusstseinsschub allzu weit her ist.

Die Analystenzunft bemächtigte sich jedenfalls sofort des Themas. Ihr Befund lautete: In Katastrophenzeiten ist besonders ein funktionierendes Kommunikationssystem gefragt, um notwendige Kontakte mit Außenstellen oder Serviceunternehmen und Reparaturen in der beschädigten IT-Infrastruktur einleiten zu können. Die IDC-Analysten sahen in ihrem ersten Report vom Herbst 2001 „How Will the World Trade Center Disaster Affect the Disaster Recovery Market?“ Nine Eleven, wie die Anschläge von New York und Washington in Amerika genannt werden, als gute Chance, dem Markt für Disaster Recovery auf die Beine zu helfen und den Kunden eine Always-on-Infrastruktur zu verschaffen. Dazu zählen sie Outsourcing-, ASP- (Application Service Providing) und High-Availability-Dienstleistungen. Auch eine Reihe von Backup-Anbietern und Servicefirmen nutzte die Gunst der Stunde und legte ihre alten Recovery-Konzepte neu auf.

Aus Schaden wird man ...

Doch ob die Kunden selbst nach den Ereignissen vom September 2001 bereit sind, auf externe Rechenzentren mit derartigen Angeboten zu setzen und dafür eventuell die Kontrolle über businesskritische Applikationen und Daten aus der Hand zu geben, bezweifelte IDC schon damals. Dem ASP-Konzept hat der Anschlag nicht geholfen. Dazu war das Geschäftsmodell selbst zu desaströs – nach einhelliger Meinung aller Kritiker, die es hinterher immer ganz genau wissen. Und Outsourcing als neuer Geschäftszweig konnte auch nicht in dem erwarteten Maß profitieren: In diesem Bereich gibt es nach wie vor übliche Konjunkturen, die eher mit der Standardisierung von IT und tatsächlichen Kostenvorteilen im Einzelfall als mit Katastrophen zu tun haben.

Zumindest bei Speicherherstellern und Anbietern von Recovery- oder Business-Continui-

ty-Dienstleistungen galt schon immer, dass die Zahlen über den Schaden nach einer Katastrophe nicht hoch genug sein können: Darin sind sich vor allem die Hersteller einig. Allzu gerne verweisen sie auf Branchen wie den Bankensektor, in dem eine Bank praktisch bankrott sei, wenn nur für ein paar Stunden die Geldautomaten oder die Buchungscomputer ausfielen. So verteilte Sun vor einigen Jahren Zahlen, wie sie dramatischer nicht sein konnten. Unter der Überschrift „Ausfallzeit kann sehr teuer sein" wurden die durchschnittlichen Kosten pro Stunde Downtime wie folgt angegeben:

Geldautomaten	25.000 Mark
Flugreservierung	160.000 Mark
Pay TV	270.000 Mark
Kreditkarten-Institut	4,7 Millionen Mark
Börsenhändler	11,7 Millionen Mark

Die Liste könnte beliebig verlängert werden, hört allerdings gerne bei den Branchen auf, wo die Umsätze aller Gewerbe zusammenfließen und so schön viel Geld bewegt wird. Schließlich kommt man gerade hier auf die marketingmäßig gewünschten horrenden Ausfälle beziehungsweise Verluste. Und die lassen sich erfreulicherweise durch eine einfache Division ermitteln: durchschnittlicher Jahresumsatz der Branche dividiert durch 8.760. Schon die einfache persönliche Erfahrung spricht dagegen, dass diese Rechnung korrekt sein kann. Viele Menschen sind zum Beispiel das Warten und Schlangestehen gewohnt – nicht nur in Großbritannien. Und ob der Ausfall eines Börsensystems den Finanzhändler nicht doch vor einer Fehlentscheidung bewahrt hätte, wird man uns wahrscheinlich nie mitteilen. In diese gängige Schadensberichterstattung fällt auch ein Spruch aus den Zeiten der New Economy: „Die Konkurrenz ist nur einen Mausklick entfernt." Derartige Weisheiten sind zwar nicht mehr ganz so häufig zu hören, sind aber genauso falsch wie die obigen Verlustrechnungen. Wer wechselt schon permanent und ohne ersichtlichen Grund von Anbieter zu Anbieter. Da bestehen im realen Leben jede Menge gewachsener Beziehungen – und sei es nur die Vorliebe für bestimmte Produkte. Zufriedene Kunden bleiben ihrem Bankhaus wohl auch dann treu, wenn Bankautomaten und IT einmal mehr als 24 Stunden ausfallen.

Die Kirche im Dorf ließ auf seine Art der New Yorker Analyst Jonathan Spira von der Basex Group, der in einem Interview im Februar 2002 zu Protokoll gab: „Viele Firmen waren wochenlang damit beschäftigt, überhaupt festzustellen, was sie im Detail verloren hatten. Das sind Extrakosten, und der normale Arbeitsprozess ist teilweise unterbrochen. Im Unterschied zu Computerdateien ist es bei analogen Daten häufig sehr schwierig, im Nachhinein zu definieren, wo sie sich zuletzt befanden. Dieser Aspekt wird gerne unterschätzt. Hinzu kommt eine gewisse Wahrscheinlichkeit, dass digitale Daten mehr als einmal vorhanden sind – bei analogen Informationen ist das gewöhnlich nicht der Fall. Kopien gibt es kaum, außer bei Formularen." Spira schätzt, dass beim Anschlag auf das World Trade Center mehr als 50 Prozent der Datenverluste aus dem nicht digitalen Bereich stammten.

Der Prozess des Data Recovering muss – so Spira – stärker berücksichtigen, ob im Katastrophenfall tatsächlich alle Planungsmaßnahmen umgesetzt werden können: Es nützt nichts, auf den Transport von Tapes aus dem Ausweichrechenzentrum oder sicheren Lager weit weg per Flugzeug zu setzen, wenn tagelang die Flughäfen geschlossen sind. Zeitverzögerungen bei alternativen Trans-

Checkliste Disaster Recovery

Unternehmen, die ein Projekt für Disaster Recovery planen, sollten folgende Fragen beachten:

1. **Wie lange kann das Unternehmen ohne Onlinezugang zu den Daten arbeiten? Wie hoch werden Verluste pro Stunde einer „Downtime" sein?**
2. **Bis zu welchem Zeitpunkt müssen die Daten wieder komplett zur Verfügung stehen?**
3. **Bis zur letzten Transaktion, also ohne jeden Zeitverlust?**
4. **Kann eine kleine Zahl von Aktionen verloren gehen?**
5. **Bis zur letzten Nacht, zur letzten Woche et cetera?**
6. **Wie hoch werden die Kosten geschätzt, um verloren gegangene Daten wiederherzustellen?**
7. **Wie wahrscheinlich ist eine Katastrophe? Gegen welche Art von Katastrophe gilt es sich primär zu schützen?**
8. **Wie ist die bestehende IT-Infrastruktur beschaffen? Gibt es mehr als ein Rechenzentrum oder auswärtige Speichersysteme? Wie groß sind die Entfernungen?**
9. **Wie steht es mit der Energieversorgung und den Bandbreiten?**
10. **Welches Budget kann für das Disaster-Recovery-Projekt veranschlagt werden?**

Quelle: Gartner Group

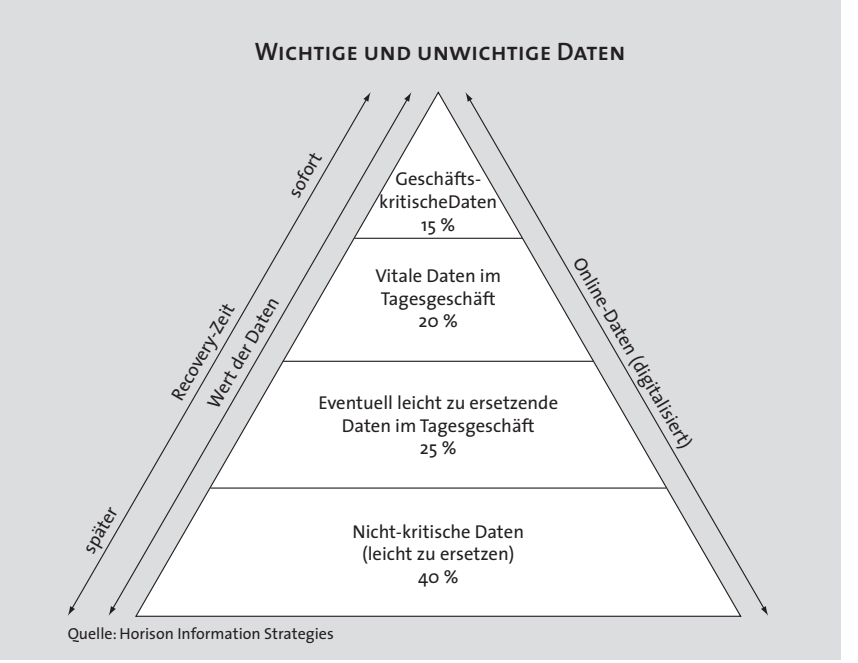
portwegen müssten ebenfalls rechtzeitig bedacht werden. Und nicht zu vergessen: Wie zuverlässig sind Internet, Telefonfestnetz und mobile Verbindungen? So funktionierten während und nach dem Zusammensturz der Türme in New York gerade die neueren Technologien wie Internet, Mobiltelefonie oder die permanente Weiterleitung von E-Mails über das drahtlose Netz des Anbieters Research in Motion (RIM) mit seinen in den USA gerade im Businessbereich weit verbreiteten Blackberry-Geräten. Zur Erinnerung: Die Gründung des Internet als eines dezentralen Informationssystems ging auf eine Initiative des amerikanischen Verteidigungsministeriums zurück (Arpanet).

Wie Peter Kraemer, IT-Direktor der Commerzbank und zuständig für das Disaster Recovery, einräumt, geraten selbst die sichersten Bunker und die besten Planspiele schnell zur Makulatur, wenn der Ernstfall eintritt. Katastrophenübungen seien zwar notwendig, würden aber aus Kostengründen nur am Wochenende durchexerziert – und nicht, wie eigentlich erforderlich, an einem normalen Arbeitstag mit allen seinen realen Bedingungen. Und Analyst Josh Krischer von der Gartner Group bilanziert: „Um wirklich konstante Datenverfügbarkeit zu garantieren, muss Redundanz auf allen Ebenen gegeben sein. Doch selbst die besten Storage-Subsysteme sind nicht gefeit gegen Katastrophen wie Feuer, Wassereinbruch, Erdbeben oder Sabotage."

Business Continuity, Disaster Recovery oder Business as usual?

Fachleute unterscheiden landläufig den „einfachen" Prozess von Disaster Recovery als Datenwiederherstellung beziehungsweise Wiederaufbau der IT-Infrastruktur und das „übergeordnete" Verfahren von Business Continuity, das möglichst alle Aspekte der Datensicherung, Ernstfallvermeidung und Rekonstruktion einschließt. Damit versuchen sie, eine Art Ordnung oder zumindest ein Ordnungsschema in die Katastrophenabwehr zu bringen. Die „Begriffsklärung" sieht dann häufig so aus:

- Disaster Recovery „macht einen Betriebsablauf oder ein ganzes Unternehmen nach einem Disaster innerhalb einer definierten Zeitspanne wieder verfügbar; die maximale Zeitspanne richtet sich nach Parametern wie Ausfallkosten, Einnahmeverlusten, vertraglichen Bedingungen, gesetzlichen Regelungen" (NetworkWorld 11/2002).
- Business Continuity ist ein „Prozess, der die Wahrscheinlichkeit reduziert, dass eine Gefahr für das Unternehmen, vorwiegend im Bereich der Datenhaltung, besteht; hält Schäden gering und stellt Recovery-Prozeduren bereit" (a.a.O.).



Untersuchungen über die Bedeutung von Daten für die Unternehmen zeigen, dass nur ein kleiner Teil wirklich geschäftskritisch ist. Disaster Recovery muss speziell diese Daten im Auge haben.

Genau besehen handelt es sich dabei um all das, was ein gewöhnlicher Prozess von Datensicherung zumindest in einem größeren Unternehmen als Standard vorsieht: redundante Hardware, Clustering, High Availability, Load Balancing, RAID-Systeme (Plattenarrays), Backup-Prozeduren, Ausweichrechenzentren oder Remote Copy. Anders gesagt: Business Continuity und der von diesem Standpunkt aus untergeordnete Prozess des Disaster Recovery sollten zu den Selbstverständlichkeiten gehören, für die moderne Unternehmen auch bereit sind, Geld auszugeben. Die Wirklichkeit sieht allerdings ganz anders aus, nur eine Minderheit dürfte tatsächlich die nötigen Mittel zur Verfügung stellen. Da nur wenige darüber sprechen möchten, ergeben sich bei den Unternehmen höchstwahrscheinlich riesige Differenzen zwischen dem, was sie planen, wirklich durchführen und dann auch bezahlen.

Ketzerisch ausgedrückt bedeutet dies: Wer sein Backup und Recovery ordentlich plant, der kann sich Extraausgaben für Disaster Recovery und Business Continuity sparen – so scheinen auf jeden Fall viele Anwender zu denken. Ob zu Recht, das hängt auch von der Überzeugungskraft der Hersteller und der Spezialanbieter mit ihren Programmen für Disaster Recovery ab. Und natürlich von den Preisen.

Es liegt aber auch an der funktionierenden Infrastruktur im Unternehmen. Wenn im Alltag LAN und SAN, Server, Leitungen oder Speichergeräte ohne Komplikationen zusammenarbeiten und das Management endlich den (Ideal-) Zustand eines hohen Automatisierungsgrades und „selbstheilender Mechanismen" à la IBMs Eliza-Projekt erreicht haben, könnten angenehmere Zeiten für Administratoren heranbrechen. Einen wirksamen Schutz gegen Katastrophen wird es aber auch dann nur bedingt geben. Wer das als Befürwortung einer Laisser-faire-Haltung interpretieren sollte, liegt mit Sicherheit falsch. Ein kleines Beispiel: Das unterirdische Rechenzentrum der Lufthansa Systems in Kelsterbach bei Frankfurt mag dem Besucher überdimensioniert und eher wie ein kriegstauglicher Bunker erscheinen, funktional ist es dennoch: Die Firmen, die hier Teile ihrer IT-Infrastruktur untergebracht, vielleicht sogar einen kompletten Outsourcing-Vertrag abgeschlossen haben, können ruhig schlafen. Allerdings nur so lange, bis der ganz große Knall kommen sollte. Kraemer von der Commerzbank relativiert die Bedeutung eines derartigen Aufwands: „Irgendwo endet das Katastrophenszenario. Was nützt es, wenn die Bank nach der Explosion eines Kernkraftwerks noch voll funktionsfähig ist? Dann geht doch in einem so dicht besiedelten Gebiet wie dem Frankfurter Raum gar nichts mehr." Es komme darauf an, bei aller Katastrophenplanung gesunden Menschenverstand zu beweisen. Zwar seien mit Remote-Copy-Lösungen auch Ausweich-Rechenzentren am anderen Ende der Welt realisierbar. „Doch irgendwo ist Schluss", resümiert Kraemer. „Mir reichen die paar Dutzend Kilometer zu unserem sekundären Standort." Und für die viel gescholtene Ausgabenpolitik einer IT-Abteilung könnte so ein Standpunkt durchaus nützlich sein.

Katastrophe ist nicht gleich Katastrophe. Vernünftige Planung für Disaster Recovery lässt sich nicht von der Panikmache einiger Anbieter und Experten einschüchtern.