

MONITOR | Ausgabe 2/2007 - Strategien

**Kostenrechnung****Keine Kaffeesudleserei: IT-Ausfall richtig kalkulieren**

Um sich dagegen zu wappnen, benötigen Unternehmen ein systematisch organisiertes Betriebskonzept. Wie aber lassen sich die Kosten möglichst genau berechnen? Experten warnen vor allzu einfachen Methoden, wie abgehobenen mathematischen oder "esoterisch" geprägten Modellen.

*Lothar Lochmaier*

Eine führende britische Forschungsuniversität erlitt einen katastrophalen Datenverlust, nachdem in der Informatikfakultät ausgerechnet an einem Wochenende in den Morgenstunden ein Feuer ausgebrochen war, berichtet Kroll Ontrack, Experte für die Datenwiederherstellung, in seinen zehn kuriosesten Fällen des vergangenen Jahres.

Die Folge des Vorfalls bestand darin, dass Qualm und Löschwasser die meisten IT-Gerätschaften beschädigten. Immerhin konnten die Experten dreißig PCs noch retten und Daten mit einem Volumen von mehr als einem Terabyte rekonstruieren. Manchmal haben Unternehmen Glück, so dass die große Katastrophe ausbleibt. Doch sollten Firmenlenker sich nicht darauf verlassen. Denn oftmals sind es nur kleine Nachlässigkeiten, die einen rasanten Schneeballeffekt in der IT auslösen.

Was würde etwa passieren, wenn nicht nur Server, Festnetzanschlüsse oder die E-Mail-Kommunikation ausfielen, sondern auch die IP-Telefonie (VoIP). Mobile Business-Lösungen sowie zahlreiche externe Speichermedien erhöhen die Gefahr, Schädlinge ins Unternehmen einzuschleppen. Passiert das Unerwartete trotzdem und sind IT-Prozesse plötzlich "offline", so liefert eine "Betriebsstörung" nützliche Anregungen für eine gründliche Revision der Prozesslandschaft.

Fest steht, dass ein klar umrissenes Prozedere für den Notfall die Zeit bis zum erfolgreichen "Wiedereintritt" in den Markt verkürzt. Aber: Ungefähr 80 Prozent der Masse eines Eisbergs liegt unterhalb der Wasseroberfläche, weshalb es vielen Unternehmen schwer fällt, die für sie relevanten Risiken konkret einzuschätzen. Mathematische Modelle eignen sich nur bedingt, und haben sich in der Praxis häufig als eine Art "Kaffeesudleserei" erwiesen.

Es macht nämlich schon einen großen Unterschied, ob es sich um den systembedingten Ausfall bei einer Flugreservierung oder einem Online-Broker handelt, oder aber bei einem Unternehmen, das weit weniger kritische Prozesse im Internet betreuen muss. Eine grundlegend falsche Annahme ist es, Sicherheitsmaßnahmen als Maßnahmen für mehr Umsatz zu betrachten. Auch wenn IT-Sicherheit vielfach als "Business

BACK

**INSERTATE**


**HOST-PROFIS**


domain

alle

noch frei?

---

  
Computertraining  
and Services



Enabler" dargestellt wird, so werden die Maßnahmen doch in erster Linie zur Kostenreduktion ergriffen.

## **Allzu simple Berechnung als Stolperstein**

Häufig erweisen sich deshalb allzu simpel gestrickte Berechnungen des Security-Return-on-Invests (ROI) als Stolperstein. Man kommt nicht umhin anzuerkennen, dass der Blick in die Zukunft immer auf der Basis einer Prognose erfolgt, um den ROI abzuschätzen. Je differenzierter sich die Entscheider im Unternehmen mit den Ausfallszenarien und deren Abhängigkeiten auseinander setzen, sowie mit der Erforschung der Zusammenhänge und Ursachen beschäftigen, umso genauer fällt die Prognose im Laufe der Zeit aus.

Kurzum: Ein einfaches Produkt aus Eintrittswahrscheinlichkeit mal Schadenshöhe ist Kaffeesudleserei. Experten sehen hier erhebliche Handlungsdefizite bei den Unternehmen. Oftmals wird die Bedeutung der IT-Systeme überschätzt, ohne konkrete Berechnungen, einfach auf Basis des Bauchgefühls. Nicht selten führt auch die Eskalation von kleineren Ausfällen oder Unterbrechungen an den Vorstand zu dem allgemeinen Verständnis, dass ein Ausfall nicht akzeptabel ist.

Konkret drückt sich diese ‚falsche‘ Annahme durch zu kurze Wiederherstellungszeiten (Recovery Time Objective) aus. Jede Verkleinerung der RTO führt jedoch zu einem unproportional hohen Anstieg der Kosten für Ersatzsysteme. Dies wiederum führt zu erheblichen Fehlinvestitionen, die an anderer Stelle fehlen. Der Grat zwischen über- und unterdimensionierter Prävention ist schmal.

Ein zentraler ‚Fehler‘ ist die Entkopplung von Business und IT: Letztere läuft Gefahr, die Anforderungen in aller Regel vollkommen überhöht abzubilden. Die Folge: Ein sehr aufwändiges und detailreiches Disaster-Recovery-Konzept, das aufgrund seiner hohen Kosten vom Business abgelehnt wird. Oftmals starten die Unternehmen daraufhin einen meist nicht sehr erfolgreichen zweiten Anlauf mit erniedrigten Anforderungen.

Externe Dienstleister versuchen dem entgegen zu wirken, indem sie deutlich machen, was der Kunde von einer Security ROI-Betrachtung erwarten kann und welche Ansätze nur eine Scheinsicherheit vermitteln. Falls die dann abgeschätzten Kosten aber weiterhin vom Business nicht mitgetragen werden, sind alle Beteiligten so frustriert, so dass die Übung gleich zu Beginn wieder einschläft.

Das Projekt eines umfassenden Konzepts für die IT-Notfallvorsorge verstaubt infolgedessen in den Aktenschränken. Die IT hat sich zwar alle Mühe gegeben und viel Zeit investiert, und der Businesspart anscheinend seine Aufgabe erfüllt. Nur die Ergebnisse fehlen. Diese Blockierung ist dann nur noch schwer aufzuheben, es wird keine oder zumindest nur ein suboptimale Lösung ausgewählt.

## **"Falsche" Annahmen vermeiden**

Um diesem allgemeinen strategischen Dilemma zu entkommen, müssen die Unternehmen sich über einige grundlegende Aspekte Klarheit verschaffen. Zunächst einmal gilt es "falsche" Annahmen zu vermeiden. Häufig fehlen adäquate Strukturen zur Erfassung von bezifferbaren Kosten. Beispielsweise ist kein "Cost Code" zur Erfassung von Reparaturaufwänden vorhanden, so dass die "Reparaturaufwände" in "Produktionsaufwände" hinein gerechnet sind.

Hinzu kommt der Hemmschuh, dass Abhängigkeiten zwischen Sicherheitsereignissen sowie die zeitliche und örtliche Ungleichverteilung von Sicherheitsereignissen nicht berücksichtigt werden. Folglich wird die Unsicherheit von Schätzungen nicht als Parameter integriert (Cost of Residual Uncertainty). Es wird versucht, Erfahrungen anderer Unternehmen auf das Eigene zu übertragen, wo dies nicht möglich ist. Und

schließlich wird die Existenzbedrohung eines IT-Ausfalls bei sehr bedrohlichen, aber unwahrscheinlichen Ereignissen, gleich gänzlich außer Acht gelassen.

### "Recovery Time Objective"

Deshalb gilt es die richtigen Fragen zu adressieren, beim konzeptionellen Ansatz einer internen Bewertung. Wie lange darf das betreffende System ausfallen, wie lange dauert der Wiederanlauf? Bei der "Recovery Time Objective" handelt es sich um die Zeit, die vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der EDV-Systeme vergehen darf. Der Zeitraum reicht hier von "null Minuten" (Systeme müssen sofort verfügbar sein), bis zu mehreren Tagen oder Wochen, je nachdem wie relevant die Systeme für das Funktionieren der Geschäftsprozesse sind.

Danach beginnt die Ermittlung des individuellen unternehmerischen Risikos. Wie konsistent ist der Datenbestand, wie hoch ist der Datenverlust, der in Kauf genommen werden kann? Dabei handelt es sich um die möglichst präzise Ermittlung des Zeitpunkts, wann und wie oft etwa die Datensicherung auf den unterschiedlichen Ebenen erfolgen soll, das heißt, wie viele Daten bzw. Transaktionen zwischen den einzelnen Sicherungen verloren gehen können. Neben diesen eher grundsätzlichen Fragestellungen hilft eine klare Vision der einzelnen Kostenblöcke, die sich in bezifferbare, schätzbare und nicht-bezifferbare Kosten untergliedern lassen.

---

## IT-Ausfälle richtig kalkulieren

**Was ist Disaster Recovery (DR)?** Disaster Recovery bezeichnet Maßnahmen, die nach einem Unglücksfall in der Informationstechnologie eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur sowie Hardware. Umfassender als Disaster Recovery ist der Begriff Business Continuity, der nicht die Wiederherstellung, sondern das kontinuierliche Funktionieren des Betriebs in den Vordergrund stellt.

**Was beinhaltet das Konzept?** Das jeweilige Konzept stellt sicher, dass die Notfallrisiken für die Geschäftstätigkeit identifiziert und bewertet sind, dass entsprechende Vorsorge- und Notfallmaßnahmen organisiert sind und der Wiederanlauf der Prozesse in Notfallsituationen gezielt gesteuert werden kann.

**Wie geht das Unternehmen am besten vor?** Disaster Recovery (DR) ist Teil eines systematischen Risikomanagements. Zu den Regeln für ein Vorgehen im Notfall gehören die technische Absicherung (Disaster Recovery Plan), aber auch die Klärung der Verantwortlichkeiten für die Fortführung kritischer Unternehmensprozesse und die Gestaltung der Wiederanlaufphase - Business Continuity beziehungsweise Recovery Plan. Auch die regelmäßige Erprobung des Ernstfalls sollte routinemäßig durchgespielt werden, um häufig auftretende Pannen abzustellen. Zudem sensibilisieren Übungen die Mitarbeiter für die Risiken.

## Checkliste - Kosten

**"Bezifferbare" Kosten:** Reparatur von Schäden einschließlich Personalaufwendungen

- Vertragsstrafen z.B. bei Just-In-Time oder Just-In-Sequence, Lieferverpflichtungen, Bußgelder
- Zukünftig: Höhere Kreditkosten (Basel II) bei unzureichender Risikovorsorge. Für den Großteil der klein- und mittelständischen Wirtschaft ist damit zu rechnen, dass Kredite teurer werden.
- Bezifferbar bedeutet aber nicht, dass diese Kosten in den Unternehmen immer bekannt sind.

**"Schätzbare" Kosten:** Umsatzverlust durch mangelnde Verfügbarkeit.

- Konkreter Verlust von Kunden bei Imageschäden
- Kompensation von Minderleistung, z. B. Zukauf externer Ressourcen

**"Nicht bezifferbare" Kosten:** Verlust von Marktanteilen durch Imageschäden

- Verlust von Intellektuellem unternehmerischen Kapital
- Mangelnde Produktivität oder Mitarbeiterverlust durch Demotivation
- Mangelnde Produktivität durch Sicherheitsereignisse
- Kontrollverluste wie höhere Vorsorge oder niedrigere Produktivität

---

## Links

<http://roc.cs.berkeley.edu/projects/downtime> - hier gibt es Infos zum Recovery Oriented Computing Project (ROC) der Universität Berkeley/Stanford

[http://roc.cs.berkeley.edu/papers/Cost\\_Downtime\\_LISA.pdf](http://roc.cs.berkeley.edu/papers/Cost_Downtime_LISA.pdf) - A simple way to estimate the cost of downtime - Ein einfacher Weg die Kosten eines IT-Ausfalls zu schätzen

Um ausschließlich vitale IT-Risiken genauer zu erfassen bzw. zu messen, hat die Universität Berkeley/Stanford das Programm Recovery Computing (ROC) ins Leben gerufen. Auf der Website können sich Unternehmen mit einem "Downtime-Rechner" einen ersten einfachen

Überblick über ihre Überlebenslage verschaffen und hochrechnen, was passiert, wenn sie mehrere Stunden oder Tage "offline" sind.

---



**Ausgabe 2/2007 als Acrobat PDF!**

[PDF hier gratis downloaden](#)

**Die Druckausgabe des MONITOR im Abonnement?**  
Nur € 33,20 für 14 Ausgaben & IT-Business in Österreich.

[Mehr Information](#)

**[umantis Nachfolgeplanung](#)**

Ende gut, Anfang gut. Mit Software einfach besser planen.

**[Bloß keine Strategien](#)**

Falls doch: Es gibt Experten für Potenziale, Ziele und Strategien

MONITOR | Ausgabe 2/2007 - Strategien

**BACK**