



## **Effiziente Business Continuity dank professioneller IT-Notfallplanung**

Das vielgefürchtete Szenario ist eingetreten: Die IT-Systeme sowie die gesamte  
5 IT-Infrastruktur versagen ihre Dienste. Was ist zu tun? Gibt es  
Ausweichmöglichkeiten? Wie und wann ist die IT-Funktionalität wieder  
vollständig hergestellt? Diese Fragen beschäftigen Unternehmen und ihre  
Geschäftsführer, wenn der Notfall bereits eingetreten ist. Die Planung und  
Prävention sollte aber viel früher ansetzen. Die gesamte Geschäftstätigkeit eines  
10 jeden Unternehmens ist heute mehr denn je von einer IT-Hochverfügbarkeit  
abhängig. Deshalb sollten effiziente Sicherheitskonzepte und Notfallstrategien zu  
Standard-Maßnahmen in den Betrieben gehören und nicht erst nach einer  
Katastrophe entwickelt werden. Was zudem unterschätzt wird: verstärkte  
gesetzliche Sicherheitsrichtlinien, wie KonTraG oder Basel II, fordern die  
15 Umsetzung eines umfangreichen Sicherheitskonzepts. In diesem Zusammenhang  
sind ein individuell abgestimmtes und effizientes IT-Sicherheitssystem sowie ein  
genau definiertes Krisenmanagement Pflicht. Dabei geht es nicht nur um die  
logische und technische Sicherheit der IT. Im Sinne eines ganzheitlichen  
Sicherheitsmanagements muss auch die physikalische Komponente  
20 berücksichtigt werden, um Totalausfälle grundsätzlich zu verhindern. Von  
Relevanz ist neben einer raschen Wiederherstellung des Betriebsablaufs die  
Reduzierung von Ausfallzeiten auf ein Minimum. Um Business Continuity im  
Notfall zu sichern, sollten IT-Notfallpläne strategisch entwickelt und umgesetzt  
werden.

25

### **In nur 3 Schritten zu einer erfolgreichen IT-Notfallplanung**

Basis für die IT-Notfallplanung ist eine Business Impact Analyse (BIA) und eine  
Risikoanalyse. Mittels dieser werden Korrelationen einzelner  
Unternehmensbereiche aufgedeckt sowie Konsequenzen bei Prozessausfällen

30 aufgeführt. Die Entwicklung geeigneter Konzepte sowie die fachkundige Implementierung festgelegter Sicherheitslösungen bilden die weiteren Stationen einer erfolgreichen IT-Notfallplanung.

Die BIA eruiert die Empfindlichkeiten wichtiger IT-Prozesse. Die Gefahrenanalyse knüpft daran an und erfasst die bestehenden physikalischen Risikofaktoren und  
35 fragt, welche Konsequenzen eine IT-Beeinträchtigung für das Unternehmen haben kann bzw. welche Schutzziele sich daraus ableiten lassen. Ferner müssen während der Analyse folgende Fragen beantwortet werden: Wer wird im Notfall informiert? Welche Personen sitzen im Krisenmanagement und welche Funktionen übernehmen sie dort? Wie werden die unternehmenskritischen  
40 Geschäftsfunktionen fortgeführt? Informationen über Umfang möglicher Schäden, einzelne Risikoarten (höhere Gewalt: Feuer, Überschwemmung; technisches Versagen: Netzwerkausfall; menschliches Versagen: fehlende Sensibilisierung; vorsätzliches Handeln: Spionage) sowie deren Eintrittswahrscheinlichkeit (unrealistische Fälle, Problemfälle, kritische Fälle)  
45 vervollständigen die Analyse und klären den Handlungsbedarf. Die daraus gewonnenen Daten definieren den Soll-Zustand für die Notfallplanung und den maximal tolerierbaren Datenverlust nach zuletzt erfolgter Sicherung.

Es folgt in einem zweiten Schritt die Disaster-Recovery-Strategie (DRS). Diese bestimmt die Vorkehrungen die zur Rekonstruktion der Datenbestände nach  
50 einem Katastrophenfall nötig sind und die zu einer Wiederaufnahme der Geschäftstätigkeit innerhalb kürzester Zeit beitragen. Aus den definierten Soll- und Mindestanforderungen für die Aufrechterhaltung des Geschäftsbetriebs, resultieren Wiederanlaufzeiten, die sog. Recovery Points Objective, und Wiederanlaufdauer, auch Recovery Time Objective genannt, die auf einen  
55 minimalen Wert reduziert sein müssen. Damit dies gewährleistet ist, sind eventuelle bauliche, technische oder organisatorische Modifikationen von Relevanz. Back-up-Konzepte, Stagesysteme, Hard- und Software-Lösungen sowie eine unterbrechungsfreie Stromversorgung (USV) müssen ebenfalls berücksichtigt werden. Darüber hinaus zählt zu den obligatorischen

60 Vorkehrungen einer erfolgreichen Business Continuity die Datensicherung. Ob  
Bänder, Ausweichräume, Server-Cluster oder räumlich getrennte Rechenzentren  
nötig sind, orientiert sich an dem Verfügbarkeitsanspruch der geschäftskritischen  
Daten der einzelnen Unternehmen. In diesem Zusammenhag sollten die  
Sicherheitskategorien überprüft und gegebenenfalls Zugriffregelungen  
65 implementiert werden. Abschließend wird der Umfang der Service-Levels in  
Absprache mit dem Kunden definiert.

Die Planung und Umsetzung der Strategie in einem dritten Schritt geht mit der  
Optimierung der bisherigen IT-Infrastruktur einher. Dabei ist eine gut  
organisierte Projektkoordination wichtig, damit Sanierung, Umbau und/oder  
70 Auslagerung von IT-Komponenten zügig und erfolgreich durchgeführt werden  
können.

Im optimalen Fall sollten die entwickelten Strategien in einem Notfallhandbuch  
zusammengefasst werden, damit Alarm- und Ablaufpläne für das beteiligte  
Personal jederzeit verfügbar sind und Handlungsanweisungen im Notfall  
75 umgesetzt werden können. Kontinuierliche Notfallübungen runden einen  
professionellen Notfallplan ab und sichern damit den reibungslosen Ablauf im  
Ernstfall.

### **Höchste Ansprüche an die Planungs-Spezialisten**

80 Erfolgreiches Business Continuity zeigt sich, wenn detaillierte Risiko-Analyse,  
Planungsprozesse für die Aufrechterhaltung der Geschäftaktivität und  
Implementierung nahtlos ineinander greifen. Kompetente Spezialisten sind  
gefragt, die interdisziplinär die Zusammenhänge von Planung, Durchführung und  
Dokumentation erkennen. Für die ganzheitliche Sicherheitslösung und –  
85 Umsetzung steht in der Regel nur ein Ansprechpartner zur Verfügung. Dabei wird  
branchenunabhängig ein individuelles IT-Konzept entwickelt, welches den  
gesetzlichen Anforderungen nicht nur gerecht wird, sondern auch mittelfristig  
absehbare Änderungen berücksichtigt.