

# Notfallvorsorge ist mehr als Backup

› Im Katastrophenfall benötigen Unternehmen und Mitarbeiter klare Angaben über Verantwortlichkeiten und Prozesse.

von Gerrit-Leonhard Stein 02.02.2011



Foto: Gina Sanders/Fotolia.com

Die Büroflächen stehen in Flammen, die Produktionssysteme sind zerstört und Daten nicht mehr zugänglich. Sind dann auch noch die verantwortlichen Führungskräfte nicht erreichbar, sollten **Mitarbeiter**<sub>1</sub> zumindest die notwendigen Maßnahmen und Verantwortlichkeiten kennen. Doch selten werden diese Dinge im Vorfeld geklärt. Häufig gibt es technische Backup-Konzepte, die organisatorische Vorsorge kommt indes zu kurz.

## » Das Management Commitment

Die organisatorischen Fragen zu klären, ist nicht vornehmliche Aufgabe der **IT**<sub>2</sub>-Abteilung. Ihr obliegen die klassischen IT-Recovery-Konzepte (Backup-Strategien). Die Verantwortung für die übergreifende Ausrichtung liegt bei der Unternehmensführung. Grundlage für eine erfolgreiche Vorsorgeplanung sind zwei Aspekte:

1. Das Bewusstsein des **Managements**<sub>3</sub> für den Bedarf einer entsprechenden Planung.
2. Das Commitment des Managements für die notwendigen Maßnahmen.

Die Vorsorgeplanung und ihre regelmäßige Überprüfung ist Teil des Risiko-Managements und damit Bestandteil der **Compliance**<sub>4</sub>-Anforderungen. Sowohl das Aktienrecht, als auch das GmbH-Gesetz verlangen von der Unternehmensleitung, sich mit Krisen- und Notfallsituationen zu beschäftigen. In den Mindestanforderungen an das Risiko-Management (MaRisk) wird die Vorsorgeplanung für Notfälle gefordert (siehe auch "Rechtliche Rahmenbedingungen").

Leider mangelt es dennoch vielerorts am notwendigen Risikobewusstsein. Unternehmenslenker und **CIOs**<sub>5</sub> wähnen sich in Sicherheit, weil sie die Aufgaben in die Fachbereiche delegiert haben. Doch das entbindet sie nicht von der Verantwortung.

## » Vorsorge braucht Vorgaben

Jede Vorsorgeplanung benötigt klare Ziele etwa zur gewünschten Wiederherstellungszeit und Notfallverfügbarkeit. Am Anfang steht daher die Antwort auf die Frage, welchen Ausfall sich ein Unternehmen leisten kann. Daraus lässt sich ableiten, welche Prozesse zu welchem Zeitpunkt wieder verfügbar sein müssen und welche beziehungsweise wie viele Notfallarbeitsplätze bis zur Wiederherstellung benötigt werden. Aus diesen Zielvorgaben ergeben sich die notwendigen Vorsorgekosten. Nicht zuletzt dies ist ein wesentlicher Punkt, weshalb die Planungen zwingend eine Management-Entscheidung benötigen.

### Rechtliche Rahmenbedingungen

Die gesetzlichen Anforderungen an das Risiko-Management und die Kontrollsysteme sind in den vergangenen Jahren gestiegen. Folgende Gesetze sind relevant:

- Bundesdatenschutzgesetz (BDSG): Personenbezogene Daten müssen gegen Zerstörung und Verlust geschützt werden.
- Aktiengesetz (AktG): Allgemeinen betrieblichen Risiken sollten im Rahmen eine Risiko-Managements erfasst und bewertet werden.
- Gesetz zur Transparenz und Kontrolle im Unternehmensbereich (KonTraG): Zur Kontrolle und Transparenz im Unternehmen ist ein Frühwarnsystem erforderlich. Das Gesetz verlangt ein umfangreiches Sicherheitskonzept.
- Sabanes-Oxley Act (SOX): Alle für die Finanzergebnisse relevanten internen Prozesse müssen durch Wirtschaftsprüfer durchleuchtet werden.
- Basel II: Unternehmensbezogenen Daten müssen gesichert werden. Außerdem muss ein ausreichendes Notfallkonzeptes vorhanden sein.
- EuroSOX, Richtlinie 2006/43/EG: Es sind Planungen für den langfristigen Erhalt des Betriebs sowie ein Notfallkonzept erforderlich.
- Mindestanforderungen an das Risiko-Management (MaRisk) für Kreditinstitute und Versicherungen: Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) verlangt ein Risiko-Management.
- IDW PS 951: Das Institut der Wirtschaftsprüfer (IDW) hat einen Prüfungsstandard zur Bewertung der Angemessenheit (Typ A) und Wirksamkeit (Typ B) von Kontroll- und Risiko-Managementsystemen auf Basis des amerikanischen Prüfungsstandard SAS 70 definiert.
- Gesetz zur Modernisierung des Bilanzrechts (BilMoG): Die Weiterentwicklung der HGB-Regelungen zu Ansatz-, Ausweis- und Bewertungswahlrechte enthalten auch zusätzliche Anforderungen an das interne Kontroll- und Risiko-Managementsystem.

### » Die 5 W-Fragen

Für die Vorsorgeplanung sind die so genannten 5 W-Fragen hilfreich:

Elemente des Vorsorgeplanung



**Die Vorsorgeplanung muss detaillierte Angaben zu Aufgaben, Verantwortung und Prozessen machen, sollte die Informationen aber möglichste einfach darstellen, damit sie im K-Fall verwendet werden können.**

Foto: Helbling Management Consulting

**Was muss getan werden?** Kernstück der Vorsorgeplanung ist es, die notwendigen Maßnahmen und

Aufgaben festzulegen. Dazu zählen die Erstmaßnahmen, die unmittelbar nach Vorfall etwa die Informations- und Eskalationskontakte nennen und Notfallprozesse beschreiben. Anschließend sind die Aufgaben zur Notfallbewältigung wichtig. Dazu zählen etwa Wiederanlaufpläne, Wiederbeschaffungsprozeduren, der Transport von **Mitarbeitern**<sub>6</sub> und Güter sowie die Beschaffung von notwendigen Hilfs- und Finanzmitteln. Die erforderlichen Aufgaben sollten in leicht zu vermittelnde Arbeitspakete unterteilt werden, die sich am Unfallort sowie am späteren, temporären Geschäfts- und Produktionsort einfach anwenden lassen.

Ein besonderes Augenmerk sollte den Kommunikationsplänen gelten, denn sowohl der interne und externe Kommunikationsfluss muss reibungslos funktionieren. Daher sollten die Planer im Vorfeld für wesentliche Unternehmensaspekte ermitteln, welche Informationen zu welchem Zeitpunkt an Mitarbeiter, Kunden, Lieferanten und Medien kommuniziert werden müssen.

Unberücksichtigt bleibt häufig, den zerstörten Bereich zu sichern und abzuwickeln. Denn nicht minder wichtig, als die Betrieb möglichst schnell wieder anlaufen zu lassen, ist es Dokumenten und Ordnern sowie Datenträger auf **PCs**<sub>7</sub> und **Servern**<sub>8</sub> einzusammeln. Alle Maßnahmen müssen zudem in vertragliche Vereinbarungen mit Dienstleistern eingebunden werden, der im Bedarfsfall Notfallarbeitsplätze und Stand-by-Rechenzentren zur Verfügung stellt.

Muster Checklisten in der Notfallplanung



**Im Bedarfsfall helfen Checklisten, die anfallenden Aufgaben verlässlich abuarbeiten.**

Foto: Helbling Management Consulting

**Wer kann etwas tun?** Die Planer müssen definieren, wer im Notfall für welche Rollen und Aufgaben geeignet und vorgesehen ist. Dabei sollten sie bei der Verteilung der Zuständigkeiten davon ausgehen, dass die im Produktionsbetrieb verantwortlichen Personen nicht verfügbar sind. Auf Basis von unterschiedlichen K-Fall-Szenarien sollten Funktionen und Rollen mit entsprechenden Verantwortlichkeiten definiert, jedoch keinen Personen zugeordnet werden. Hier steckt viel Diskussionspotenzial, denn Bestandteil einer Vorsorgeplanung ist unter anderem, festzulegen, wer die Notfallprozesse freigeben darf. Das geschieht oft abseits der gewohnten Genehmigungsabläufe. Manch ein Vorgesetzter muss hier über seinen Schatten springen und den Mitarbeitern vertrauen.

Gefordert sind entscheidungswillige **Manager**<sub>9</sub>, gute Kommunikatoren, Organisationstalente sowie struktur- und aufgabenorientierte Mitarbeiter. Organisatorisch löst man diese Herausforderung, indem man Teams und Teamrollen je Aufgabengebiet (sachliche und örtliche zusammenhängende Aufgaben) definiert, die durch ein zentrales K-Fall-**Management**<sub>10</sub>-Team koordiniert und gesteuert werden. Eine Verantwortungsmatrix unterstützt die Zusammenarbeit. Das schafft Sicherheit und vermeidet zeitraubende Diskussionen über die Kompetenzen.

**Wie muss etwas getan werden?** Erläuterungen und Checklisten helfen den Verantwortlichen, ihre Aufgaben im K-Fall zu erledigen. Komplexe Handbücher liest im Notfall sowieso keiner, besser sind einfache Übersichten, Schaubilder und strukturierte Formulare als PDF-, Excel- und Word-Datei sowie in gedruckter Form.

**Wann muss etwas getan werden?** Für jede Aktivität ist der Zeitpunkt festzulegen, außerdem sollte die sinnvolle Reihenfolge der Arbeit geklärt werden. Das ist keine leichte Aufgabe, denn in der Konzeption des Ablaufs müssen die Planer berücksichtigen, dass viele Prozesse zur Bewältigung der Katastrophe parallel betrieben werden müssen.

**Wo muss etwas getan werden?** Da manche Aufgaben notwendigerweise an einem bestimmten Ort erledigt werden müssen, sollte der Arbeitsort jedes Teams ebenfalls definiert - und soweit möglich - vorbereitet sein.

Das gilt etwa für Sammelplätze, Notfallarbeitsplätze, Ausweichproduktionsstätten und Backup-Rechenzentren<sup>11</sup>.

## » Dokumentation ... aber richtig!

Sind Vorsorgepläne erstellt und Verantwortlichkeiten festgelegt, ist eine K-Fall-sichere Dokumentation erforderlich. Es nützt in der Regel nichts, wenn die Maßnahmenpläne auf den Firmen-Servern gespeichert werden oder in den Schränken des designierten Krisen-Managers<sup>12</sup> liegen. Sind Büro- und IT<sup>13</sup>-Räume von einem Vorfall betroffen, haben die Einsatzkräfte keinen Zugriff auf wichtige Informationen.

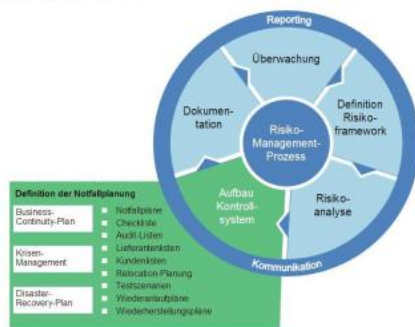
Für die Dokumentation der kritischen Planungsinformationen bieten sich verschlüsselte Container auf Firmen-Notebooks<sup>14</sup> an. Überlegenswert ist auch die Auslagerung an einen Sicherheitsdienst, der rund um die Uhr besetzt ist, oder die Ablage in einen zugänglichen Safe bei einem Partnerunternehmen. Grundsätzlich sollten Aktivierungspläne lokal und schnell verfügbar vorgehalten werden, so dass im Katastrophenfall die wesentlichen ersten Maßnahmen beispielsweise auch vom Pförtner angestoßen werden können.

Die Art der erforderlichen Daten variiert je Unternehmen. Zur Auswahl stehen folgende wichtigen Informationen:

- Kontaktdaten wichtiger Partner, Lieferanten, Kunden und Mitarbeiter<sup>15</sup>;
- Management<sup>16</sup>-Informationen und Handlungsanweisungen für den Geschäftsbetrieb;
- Aktivierungsplanung der Fachbereiche, Recovery-Checklisten für Produktions- und IT-Bereiche;
- Vollmachten;
- Zugang zu Finanzmitteln und
- Versicherungsinformationen.

## » Nach der Planung kommt der Test

Die Notfallvorsorge ist Teil des Kontrollsystems im Rahmen des Risikomanagement-Prozesses



**Die Vorsorgeplanung muss ständig überprüft und aktualisiert werden. Sie muss sich in den Prozess für das Risiko-Management einfügen.**

Foto: Helbling Management Consulting

Nicht jeder Ablauf und jede Regel funktioniert in der Praxis wie sie in der Theorie erdacht wurde. Aus diesem Grund müssen die vorbereiteten Maßnahmen regelmäßig überprüft werden. Jährliche K-Fall-Übungen zeigen, ob die Hilfsmittel zur Katastrophenbewältigung praxisgerecht sind, und ob der Betrieb in der geplanten Zeitspanne wieder aufgenommen werden kann.

Veränderungen in der Organisation, den Unternehmensprozessen und der technischen Infrastruktur erfordern eine regelmäßige Überprüfung der Vorsorgeplanung. Ein wesentliches Element, eine praxistaugliche Vorsorgeplanung sicherzustellen, ist ein kontinuierlichen Verbesserungsprozesses der K-Fall-Vorsorge.

## » Das Management ist in der Pflicht

Vorsorgeplanung ist kein alleiniges IT-Thema. Eine detaillierte Planung sowie ausreichende Dokumentation von Maßnahmen sind über alle Unternehmensbereiche erforderlich. Zusätzlich muss ein kontinuierlicher Verbesserungsprozess sowie eine regelmäßige Überprüfung der Planung in Hinblick auf organisatorische, prozessuale und technologische Veränderungen etabliert und sichergestellt werden. Die Verantwortung für eine Vorsorgeplanung liegt daher bei der Geschäftsführung. Zwingende Voraussetzung für ein funktionierendes K-Fall-Konzept sind daher Vorgaben durch das Management und ein Commitment der Entscheider. (jha)

### **IT Operations Day - Achtung: Die Digital Natives kommen!**

Digital Natives verkörpern alles, was das effizienz-getriebene IT-Management als Herausforderung, wenn nicht als Bedrohung empfindet. Im bevorstehenden „War of Talents“ werden alle Unternehmen gezwungen sein, in immer stärkeren Maße mit Digital Natives zu agieren – als Mitarbeiter, Freelancer, Influencer oder in welcher Rolle auch immer. Um so notwendiger ist es daher, dass vor allen Dingen auch IT-Verantwortliche die Zusammenarbeit mit den Digital Natives lernen!

Social Networks, Cloud Computing, Mobility – Was IT-Manager und Digital Natives voneinander lernen können: [IT Operations Day am 12. Mai 2011 in Berlin](http://www.idgevents.de/konferenzen/418/it_operations_dayachtung_die_digital_natives_kommen.html)<sup>17</sup>

- 1 <http://www.computerwoche.de/schwerpunkt/m/Mitarbeiter.html>
- 2 <http://www.computerwoche.de/schwerpunkt/i/IT.html>
- 3 <http://www.computerwoche.de/management/>
- 4 <http://www.computerwoche.de/management/compliance-recht/>
- 5 <http://www.computerwoche.de/schwerpunkt/c/CIO.html>
- 6 <http://www.computerwoche.de/schwerpunkt/m/Mitarbeiter.html>
- 7 <http://www.computerwoche.de/schwerpunkt/p/PC.html>
- 8 <http://www.computerwoche.de/schwerpunkt/s/Server.html>
- 9 <http://www.computerwoche.de/schwerpunkt/m/Manager.html>
- 10 <http://www.computerwoche.de/management/>
- 11 <http://www.computerwoche.de/schwerpunkt/r/Rechenzentrum.html>
- 12 <http://www.computerwoche.de/schwerpunkt/m/Manager.html>
- 13 <http://www.computerwoche.de/schwerpunkt/i/IT.html>
- 14 <http://www.computerwoche.de/schwerpunkt/n/Notebook.html>
- 15 <http://www.computerwoche.de/schwerpunkt/m/Mitarbeiter.html>
- 16 <http://www.computerwoche.de/management/>
- 17 [http://cw.idgevents.de/konferenzen/418/it\\_operations\\_dayachtung\\_die\\_digital\\_natives\\_kommen.html](http://cw.idgevents.de/konferenzen/418/it_operations_dayachtung_die_digital_natives_kommen.html)

IDG Business Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Business Media GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in Computerwoche unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von Computerwoche aus gelinkt wird, übernimmt die IDG Business Media GmbH keine Verantwortung.