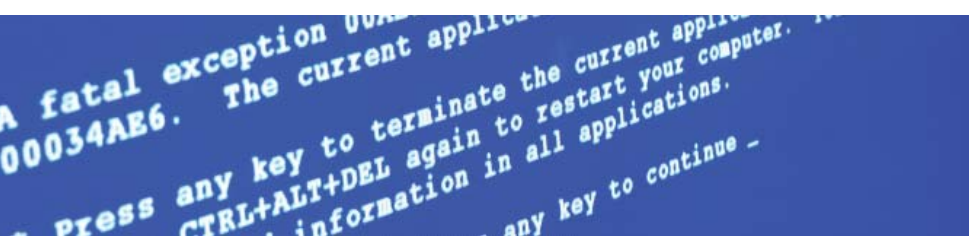


# Ontrack® Data Recovery



## Whitepaper Disaster Recovery

# Inhaltsverzeichnis

---

<b>Bedrohungspotenzial einschätzen und bewerten</b>	<b>3</b>
Prüfen Sie Ihr Bedrohungspotenzial	4
Fallbeispiel: Controllerfehler	4
Fallbeispiel: Bedienerfehler	5
<b>Sicherheitskonzept erstellen und umsetzen</b>	<b>10</b>
Business Continuity	10
Leitfaden für die Planung	13
Bedrohungen und Gefahren für Daten	15
Datenrettung als Bestandteil des Disaster-Recovery-Plans	16
<b>Vorbeugung statt Katastrophe</b>	
<b>Backup</b>	<b>17</b>
<b>RAID – Ersatz für Backup?</b>	<b>16</b>
Backup und Verfügbarkeit	10
<b>Datenrettung als Bestandteil des Notfallplans</b>	<b>24</b>
Wann brauchen Sie einen Datenrettungsspezialisten?	24
Worauf kommt es bei der Auswahl eines Datenretters an?	25
Maßnahmen im Schadensfall	26
<b>Expertentipps für den Notfall</b>	
Praktisch und schnell: Online-Datenrettung	27
Datenrettungstipps für Server	28
<b>Zusammenfassung</b>	
<b>Anhang</b>	<b>29</b>
Zuverlässigkeitskriterien	29

## Disaster Recovery

Dieses Whitepaper beschäftigt sich mit einer der größten Gefahren für Unternehmen: dem immensen Anstieg der elektronisch gespeicherten Daten und den Risiken, die durch Datenverlust entstehen können.

Kaum ein Unternehmen ist sich des Wertes seiner Daten bewusst. Erst, wenn der Ernstfall - ein unvorhergesehener Datenverlust eingetreten ist - wird darüber nachgedacht!

Umfragen haben ergeben, dass nahezu 90% aller Daten digital erstellt werden und nur ein Bruchteil davon jemals ausgedruckt wird. Was aber, wenn genau diese Daten nicht mehr verfügbar sind?

Unternehmen hängen heute in weit größerem Umfang von ihren Daten ab, als noch vor einigen Jahren. War zunächst die Lagerung der Aktenberge das einzige Problem im Zusammenhang mit den Unternehmensdaten, müssen sich die Firmen heute nicht nur der Datenflut mit ihrem immer weiter ansteigenden Hunger nach Speicherplatz auseinandersetzen, sondern auch mit der sicheren „Lagerung“ dieser Daten. Unternehmensprozesse und nicht zuletzt gesetzliche Auflagen erfordern ein beständiges Vorhalten wichtiger Unternehmensdaten - von der Produktionsstatistik über Kundendaten bis zur Geschäftskorrespondenz in der E-Mail. Vom Logistiker über produzierende Unternehmen, Forschung oder Dienstleistung verlässt sich nahezu jedes Unternehmen auf eine beständig funktionierende IT-Infrastruktur - sei es in Form von Produktionsdaten und Entwürfen, Warenwirtschaftslösungen oder der aktuelle Buchhaltungs- und Kundendaten.

„Data Mining“ und „Data Warehousing“ lassen die Datenmengen immer weiter anwachsen und damit auch die Anforderungen an die Verfügbarkeit. Die zunehmende Vernetzung und Internationalisierung stellt zudem wachsende Anforderungen an die Ausfallsicherheit der Informationssysteme - bis hin zu Modellen, die eine Verfügbarkeit der Daten und Systeme rund um die Uhr an 365 Tagen im Jahr verlangen.

Sind diese Daten plötzlich nicht mehr verfügbar, kommen auf das Unternehmen nicht nur die Kosten des Betriebsstillstandes zu, sondern es kann aufgrund des Verlustes wichtiger Produktions- und Kundendaten sogar in relativ kurzer Zeit handlungsunfähig werden.

### **Ausfälle? So etwas kann mir nicht passieren. Oder doch?**

- Rechenzentren verzeichnen im Schnitt einen jährlichen Datenzuwachs von 50 - 80%.
- Bei 50,7% aller Unternehmen fällt der Server bis zu zwei Mal im Jahr aus, bei knapp 11% noch häufiger.
- 6% aller PCs (ca. 1.065 Mio.) erlebten 2005 mindestens einen Fall von Datenverlust.
- 20% aller Laptops erleben in den ersten drei Jahren einen Hardwareausfall mit Datenverlust.
- 2 von 5 Unternehmen, deren Systeme längere Zeit nicht verfügbar sind, melden innerhalb von fünf Jahren Konkurs an.
- 56% der Ursachen für Datenverluste entstehen durch Hardwareprobleme, 26% durch Benutzerfehler.
- 69% der deutschen IT-Entscheider haben keinen Plan für „Disaster Recovery“ und „Business Continuity“.

Laut einem Bericht der *International Data Corporation (IDC)* wurden allein im Jahr 2004 rund 177,5 Millionen PCs neu angeschafft - für 2005 wird nochmals mit einer um 10% höheren Zahl gerechnet. Das Datenvolumen der im Jahr 2005 ausgelieferten Festplatten beträgt vermutlich gut 15 Millionen Terabyte. Der Nachrichtenverkehr machte im gleichen Jahr ein Volumen von geschätzten 19,7 Billionen E-Mails aus. Der durchschnittliche E-Mail-Nutzer verschickt und empfängt damit ein Datenvolumen von gut und gerne 4,6 MB pro Tag. Für Unternehmen mit 5.000 Mitarbeitern bedeutet allein der E-Mail-Verkehr eine Datenmenge von 800 MB pro Mitarbeiter.

Die IT-Storage-Infrastruktur ist heute, zusammen mit einem Konzept zur Rücksicherung und Wiederherstellung unternehmenskritischer Daten, ein maßgeblicher Erfolgsfaktor für Unternehmen.

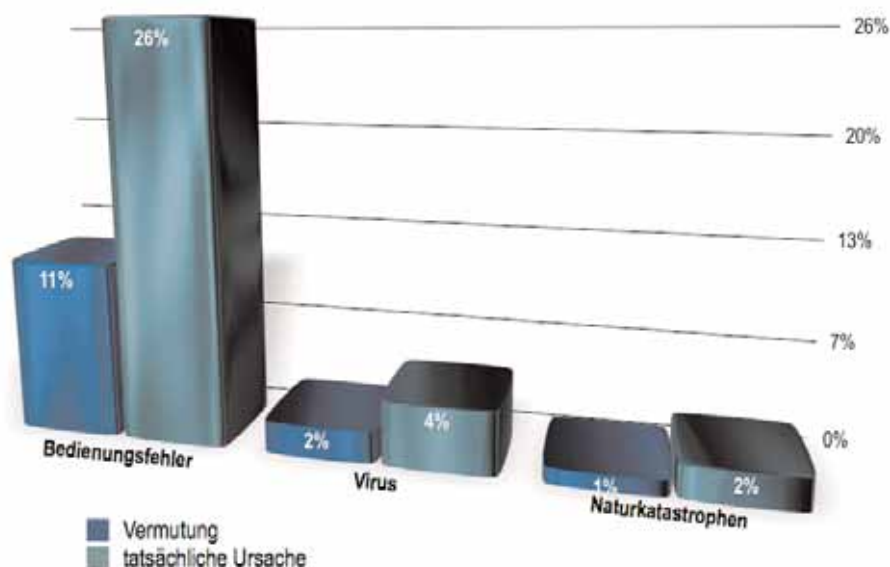
Der Begriff „Disaster Recovery“ (Notfallwiederherstellung) bezeichnet Maßnahmen, die nach einem Unglücksfall in der Informationstechnologie eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur und Hardware. Umfassender als „Disaster Recovery“ ist der Begriff „Business Continuity“, der nicht die Wiederherstellung, sondern die Prozesskontinuität in den Vordergrund stellt.

## Bedrohungspotenzial einschätzen und bewerten

Daten sind heute Dreh- und Angelpunkt für unternehmerische Entscheidungen und stellen einen der wichtigsten Produktionsfaktoren für Unternehmen dar. Die Nichtverfügbarkeit von Daten oder Informationssystemen beeinträchtigt stark den Prozess der betrieblichen Leistungserstellung und –verwertung oder macht ihn sogar ganz unmöglich. Ein Ausfall der Systeme oder der Verlust der Daten kann im schlimmsten Fall die Existenz eines Unternehmens bedrohen. Eine hohe Zuverlässigkeit und Verfügbarkeit der Daten ist daher, unabhängig davon, ob es sich um kleine oder große Unternehmen handelt, von elementarer Bedeutung.

Dabei hat der Ausfall einer wichtigen Business-Anwendung weit größere Folgen als nur die unmittelbare Nichtverfügbarkeit des jeweiligen Dienstes. Neben den direkten Folgen, wie etwa akuter Umsatzeinbußen durch den Stillstand von Produktion oder Verkauf kommen noch zusätzliche Aspekte hinzu. Dazu gehören beispielsweise die Arbeitszeit, die zum Aufsetzen eines neuen Systems notwendig ist oder der Vertrauensverlust bei Kunden und Partnern. Gehen Daten bei einem Ausfall ganz verloren, kann es in der Folge zudem Probleme mit dem Gesetzgeber oder dem Finanzamt geben.

### Vermutete Gründe für Datenverluste



Trotz aller Warnungen sind bis heute viele Firmen nicht ausreichend auf Katastrophen vorbereitet. Dabei muss man nicht nur an extreme Fälle wie etwa die Terroranschläge des 11. September denken. Tatsächlich gibt es weit mehr Ursachen für Systemausfälle - beispielsweise Fehlbedienung, Computerviren, Stürme und Hochwasser, Diebstahl und Sabotage, Brände, Stromausfälle sowie Fehler und Versagen von Soft- oder Hardware. Pannen treten oft völlig unerwartet auf. Bei dem Versuch, die Kapazität eines Fileservers für einige hundert Anwender zu erweitern, schloss Neil Smith, IT-Manager bei einem Healthcare-Unternehmen, einen Satz von 14 Laufwerken an seinen RAID-Controller an. Dabei ging die RAID-Konfiguration verloren – und mit ihr 400.000 Dateien mit zusammen ca. 250 GB.

Beim Versuch eines Rebuild stellte das IT-Team am nächsten Morgen fest, dass die ursprüngliche RAID-Konfiguration überschrieben wurde. Die Daten waren nicht mehr zu erreichen. Durch eine Remote-Datenrettung konnten schließlich 99% der Daten wiederhergestellt werden.

## Prüfen Sie Ihr Bedrohungspotenzial

- Wie wichtig sind die einzelnen Daten/Dateien?
- Wie lange kann Ihr Unternehmen ohne seine Daten weiterarbeiten?
- Was ist der Wert der verlorenen Daten?
- Wie hoch wären die Verluste bei einem Totalausfall des System?

## Fallbeispiel: Controllerfehler

### System:

Novell Netware 6.x

### Problem:

Bei einem SAN mit 10 voneinander abhängigen RAID-5-Verbänden stieg einer der zehn RAID-Verbände aus nicht nachvollziehbarem Grund aus. Alle Festplatten im SAN waren physikalisch einwandfrei. Das Backup wurde vor dem Zurückspielen auf einem alternativen Server getestet und es stellte sich heraus, dass mehrere Stunden an wichtigen Kundentransaktionen verloren gegangen waren.

Die Platten des RAID-Verbunds konnten zur Diagnose nicht ins Kroll Ontrack-Labor eingeschendet werden, da sich die verlorenen Daten physikalisch auf mehrere RAID-Systeme im SAN verteilen.

Die einzige Lösung, um die Transaktionen wiederherzustellen, war die „Kroll Ontrack Remote Datenrettung“. Die Spezialisten von Kroll Ontrack konnten die Bearbeitung vom Labor aus starten und das SAN blieb physikalisch unverändert im Serverraum.

Nach wenigen Stunden gaben die Datenrettungsingenieure einen ersten Zwischenstand. Durch das logisch verloren gegangene RAID sind die Strukturen des Dateisystems im SAN beschädigt worden. Mit Hilfe der Kroll Ontrack-Werkzeuge konnten die Dateistrukturen erfolgreich wiederhergestellt werden.

Die Daten wurden gescannt und es wurde eine Dateiliste erstellt. Die Daten wurden nach Beauftragung der Wiederherstellung auf ein separat bereitgestelltes Volume kopiert. Innerhalb von wenigen Stunden wurden alle verloren geglaubten Transaktionen wiederhergestellt.

## Fallbeispiel: Bedienerfehler

### System:

Windows 2003 Server

### Problem:

Ein RAID System mit 5 Festplatten im RAID-Level 5 meldet über den RAID-Controller die Platte Nummer 2 als defekt. Die Platten sind jedoch nicht ausreichend beschriftet und es wird versehentlich von der falschen Seite eine Platte - aus dem Schubfach 4 - gezogen und ausgetauscht.

Nach dem Austausch wird versucht, ein Rebuild zu fahren. Dieser führte nicht zum Erfolg, da sich weiterhin die defekte Festplatte im System befand und zusätzlich eine weitere, welche keine Paritätsinformationen liefern konnte. Danach wurden mehrere Platten in anderer Reihenfolge eingesetzt, bis schließlich versehentlich über die vier intakten Festplatten eine Neuinitialisierung des RAID-Level-5-Verbandes durchgeführt wurde.

Somit war eine Wiederherstellung über die Parity-Informationen des RAID-Level-5-Verbandes nicht mehr möglich. Zusätzlich wurden viele Datenbereiche in regelmäßigen Abständen überschrieben.

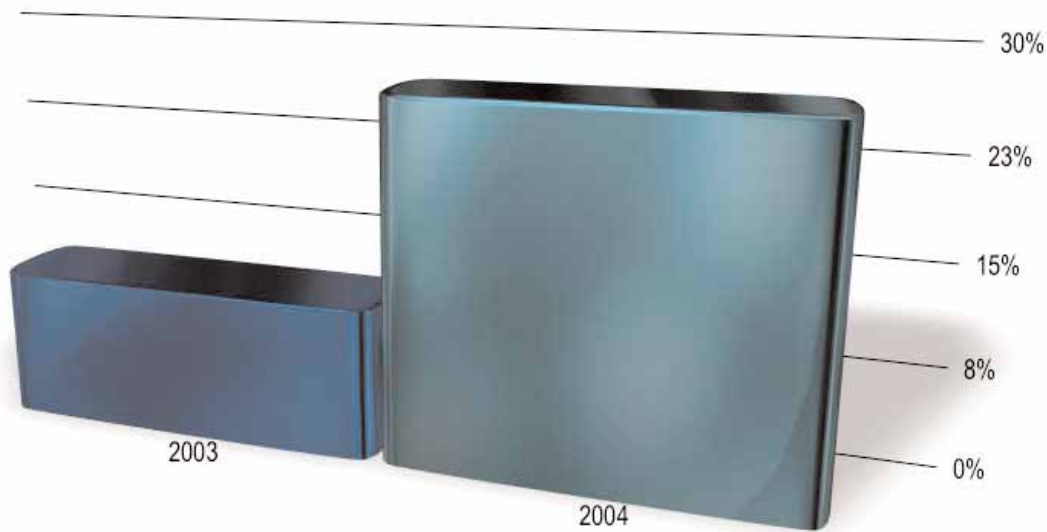
Benötigt wurden viele kleine Dateien von einem Fileserver.

Die Festplatten wurden mit einem SCSI-Controller an ein bootfähiges Microsoft-Windows-System angehängt. Die schwer wiegend beschädigte RAID-Struktur wurde mit Werkzeugen von Kroll Ontrack diagnostiziert. Nach einer abgeschlossenen Neuinitialisierung mit zwei fehlenden Platten blieb in den meisten Fällen nur eine Signatursuche, um an die Dateien zu kommen. Das Kroll Ontrack-Tool bestimmt die Dateiart dann über die Signatur.

Es konnten tausende von doc-, xls-, pdf-, und jpg-Dateien funktionstüchtig wiederhergestellt werden. Die Dateien wurden nach beauftragter Datenwiederherstellung von den Anwendern manuell gesichtet und neu benannt.

Es gibt also Gründe genug für Unternehmen, sich mit Strategien für Datensicherheit, Ausfallsschutz und Katastrophenplanung zu befassen. Dabei sind sich deutsche IT-Entscheider der wirtschaftlichen Folgeschäden größerer Ausfälle bewusst: 70 Prozent befürchten Produktivitätseinbußen, 31 Prozent rechnen mit verschlechterten Kundenbeziehungen und 30 Prozent mit Umsatz- und Gewinnverlusten. Entsprechend nimmt der Disaster-Recovery-Plan einen immer höheren Stellenwert im Unternehmen ein.

Obwohl der Entscheidungsfindungsprozess in 60 Prozent der Fälle in der Verantwortung eines IT-Managers liegt, ist die Geschäftsleitung im Vergleich zum Vorjahr mehr als doppelt so häufig involviert.



Quelle: Symantec

## Geschäftsleitung verantwortlich für Disaster Recovery

Fällt beispielsweise bei einem RAID-Level-5-System eine Festplatte aus, sollte im Normalfall kein anderes Laufwerk in seiner Funktion betroffen sein. In der Realität kommt es jedoch auch bei RAID-Systemen mit Paritycode immer wieder zu größeren Problemen. Trotz modernster Speichertechnologie kann sich innerhalb kürzester Zeit ein Disaster anbahnen. Mit der Komplexität des Systems erhöht sich auch die Zahl der potenziellen Fehlermöglichkeiten.

### RAID-Szenario

**3:00 Uhr.** Das Bereitschafts-Handy klingelt. Das könnte alles Mögliche bedeuten: Feuer, Einbruch, Ausfall der Klimaanlage im Serverraum oder möglicherweise sogar ein Server-Crash.

**3:25 Uhr.** Der IT-Techniker kommt vor Ort an und verschafft sich einen ersten Überblick über die Situation. Kein Brand, keine Anzeichen eines Diebstahls, die Temperatur im Serverraum liegt bei 18°C. Ein schneller Blick auf die Server zeigt den Login-Bildschirm. Nach dem Testen von zwei oder drei Maschinen, wird klar, dass es irgendwann ein Stromproblem gegeben haben muss. Die USV-Einheiten (Unterbrechungsfreie Stromversorgung) bestätigen einen Strom-Ausfall, außerdem zeigen alle drei großen Batterie-Einheiten Ausfälle an.

**3:40 Uhr.** Der IT-Techniker ruft sofort den verantwortlichen Techniker und den Abteilungsleiter an und informiert sie über die Situation. Bevor die beiden sich auf den Weg machen, bekommt der IT-Techniker vor Ort noch die Anweisung, die Überprüfung der Applikations-Server vorzunehmen. Einer dieser Server verwaltet die Kunden-Datenbank inkl. aller Abwicklungen sowie Gehälter und das Buchhaltungs-System. Der zweite Server wird als E-Mail-Server der Firma verwendet.

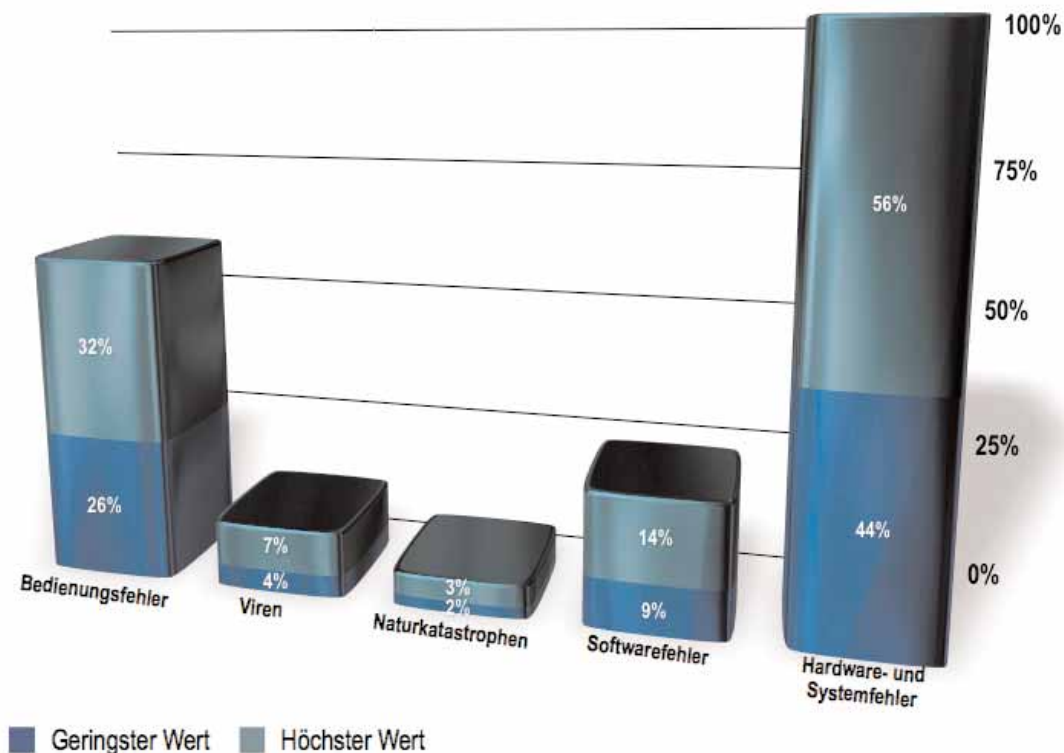
**3:55 Uhr.** Der IT-Techniker stellt fest, dass das Backup des RAID-Verbundes des Firmen-Daten-Servers nicht wieder online geht. Der E-Mail-Server war wieder hochgefahren, jedoch erscheint eine Fehlermeldung beim Start der E-Mail-Applikation. Der Techniker realisiert, dass der E-Mail-Server während der Ausfallzeit inkrementelle Backups ausgeführt hat. Er entscheidet, dass er dieses Problem dem verantwortlichen Techniker aufzeigen wird, sobald dieser eingetroffen ist.

**4:00 Uhr.** Der Abteilungsleiter und der verantwortliche Techniker kommen an. Der Techniker beginnt sofort, am E-Mail-Server zu arbeiten. Der IT-Mitarbeiter ist mit dem fehlgeschlagenen RAID-Verbund beschäftigt. Die Management-Console zeigt, dass der Festplattenverbund einen Fehler hat. Der Controller kann nur drei der 10 Platten erkennen. Nach einem kompletten Stromausfall und einem Neustart der Server und der Festplatten, zeigt die Management-Console, dass die Platten wieder online sind, dennoch hat der Verbund einen "Ausfall" registriert.

**4:30 Uhr.** Der IT-Techniker ruft den technischen Support des RAID-Verbund-Herstellers an. Die Auswahlmöglichkeiten in der Firmware sind ihm unklar und der IT-Techniker möchte wissen, ob der Festplattenverbund wiederhergestellt wird, wenn die Platten wieder online sind. Der Support bestätigt dies, jedoch besteht die Möglichkeit, dass die Daten auf dem Speicherplatz möglicherweise korrupt sind. Der Support erkundigt sich nach der Aktualität des letzten Backups. Der IT-Techniker antwortet, dass das Backup schon eine Woche alt sei und dass ein Zurückgreifen darauf unter keinen Umständen akzeptabel sei. Eine ganze Woche mit der Wiedereingabe der Daten zu verlieren sei untragbar. Der Techniker hadert mit der Entscheidung, welche Möglichkeit die Beste sei.

Auch komplexe redundante Systeme können ausfallen – denn mit der Komplexität des Systems erhöht sich auch die Zahl der potenziellen Fehlermöglichkeiten. Hier kann ein Fehler zu katastrophalen Folgen für die Datensicherheit führen. Andererseits wird gerade bei RAID-Systemen die Datensicherung oft vernachlässigt, da diese Systeme ja als "fehlertolerant" gekauft wurden. Neben „echten“ technischen Problemen muss hier auch immer der Faktor Mensch mit in Betracht gezogen werden. Ein Fehler innerhalb eines komplexen Systems kann da schon der Auslöser größerer Folgeschäden sein.

## Gründe für Datenverluste

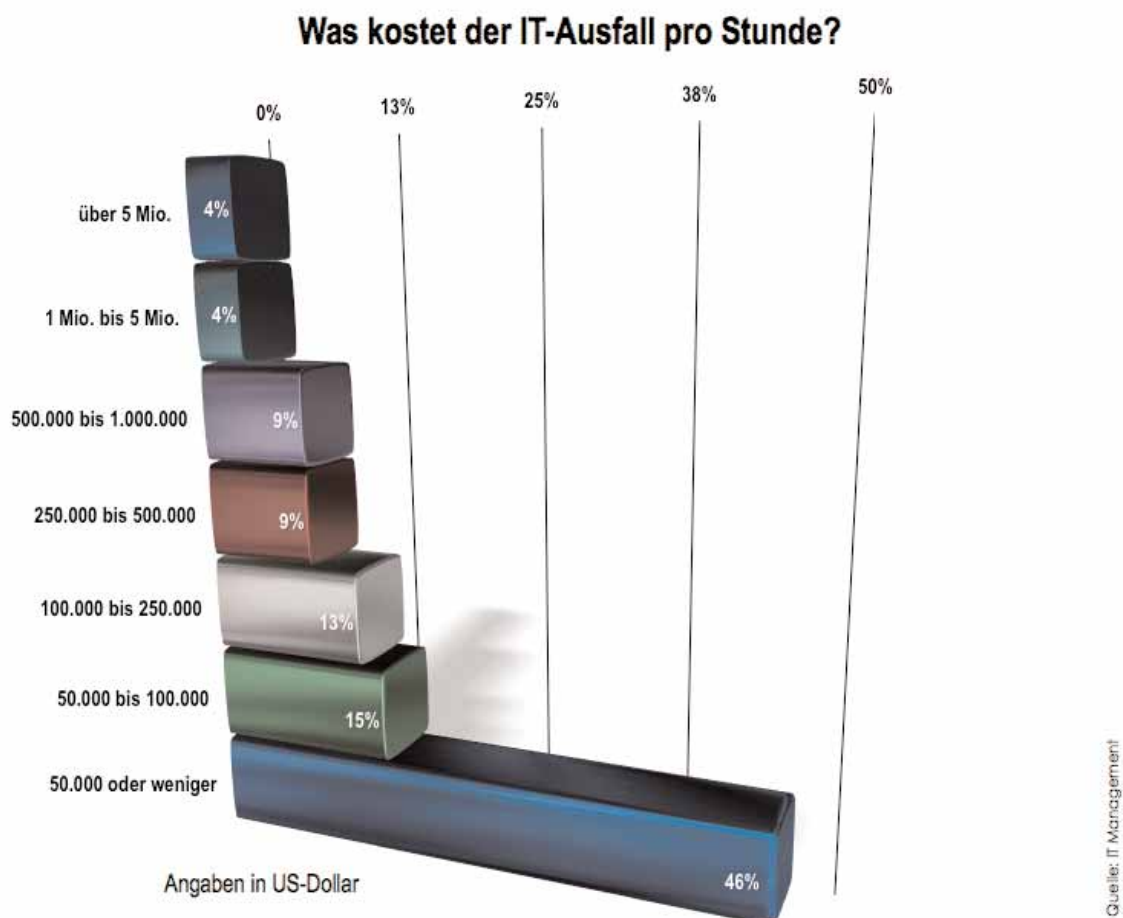


Hardwareprobleme in einem Array sind durchaus möglich. Es können beispielsweise mehrere Festplatten gleichzeitig ausfallen. Das klingt zunächst nicht sehr wahrscheinlich, ist aber möglich, wenn beispielsweise die benutzten Festplatten aus derselben Produktionslinie stammen und möglicherweise so über dieselbe Anfälligkeit für einen bestimmten Fehler verfügen.

Die Verfügbarkeit von Daten und Applikationen wird meist in erster Linie an der eingesetzten Hardware festgemacht. Eine oft unterschätzte, aber ebenso wichtige Komponente ist jedoch die Wiederherstellbarkeit der Software selbst. Die hier auftretenden Probleme können häufig auch mit einer Hochverfügbarkeitslösung nicht behoben werden.

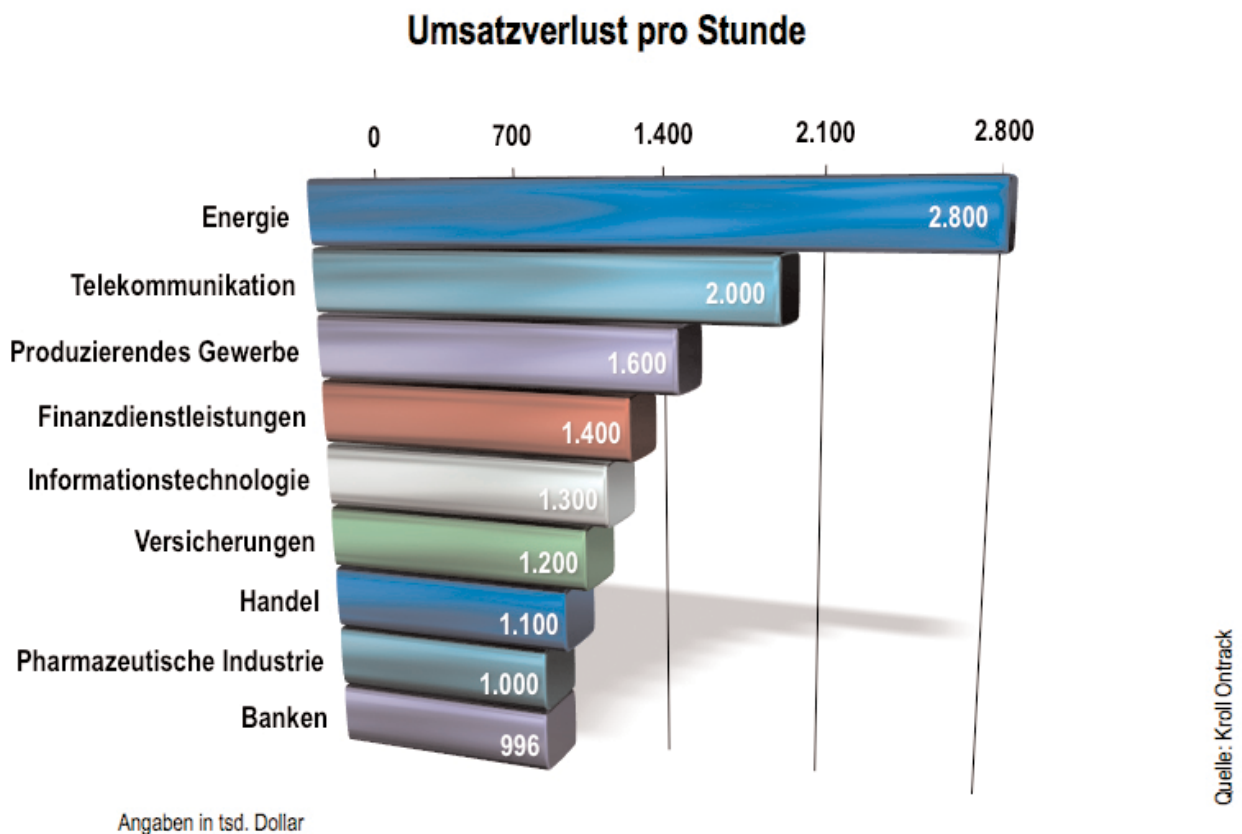
### Kosten von Verlust und Ausfall

Schon ein kurzzeitiger Ausfall oder gar der totale Verlust von Daten kann immense Kosten zur Folge haben. Bei Ausfall des Buchungssystems einer Fluggesellschaft fallen laut Contingency Planning Research/Datamation Kosten von rund 108.000 Dollar pro Stunde an, bei Ausfall einer Anwendung für Kreditkartentransaktionen wird bereits eine Summe von 3.160.000 Dollar und Wertpapierhändler müssen beim Ausfall ihrer Infrastruktur mit Einbußen von fast 8 Millionen Dollar pro Stunde Downtime rechnen.



Die Kosten setzen sich zusammen aus den Kosten für entgangene Geschäfte, Kosten für entgangene Arbeitsproduktivität, Kosten für Imageverlust und Kosten für die Wiederherstellung verlorener Daten. Jeder Tag, an dem das System stillsteht, erhöht die Kosten um ein Vielfaches. Die Folgekosten eines Ausfalls sind damit um ein vielfaches höher als die eigentlichen Kosten der Schäden der Hardware, die zum Ausfall geführt haben.

Laut einer aktuellen Umfrage von Symantec fallen bei 50,7 Prozent aller Unternehmen die Server bis zu zwei Mal im Jahr aus. Bei 11 Prozent der Unternehmen ist ein solcher Ausfall sogar noch häufiger pro Jahr zu beklagen. Zur eigentlichen Ausfallzeit der Server addiert sich die Zeit, die eine IT-Abteilung benötigt, um das System wieder herzustellen. Dazu gehören Reparaturen, der Ersatz von Hardware, die Neuinstallation von Betriebssystemen und entsprechenden Servicepacks, Systemneustarts und die eigentliche Wiederherstellung der Daten vom Backup Medium. 37,7 Prozent aller Befragten wenden mehr als 4 Stunden auf die Wiederherstellung des Systems auf, 15,7 Prozent davon mehr als 8 Stunden und weitere 9,4 Prozent können den tatsächlichen Aufwand nicht quantifizieren. Verluste sind die Folge: 30,7 Prozent der Befragten beziffern ihre Verluste im Hinblick auf Produktivität und Umsatz mit bis zu 10.000 Euro. Auf der anderen Seite konnten trotz erlaubter Schätzwerte 48 Prozent der Befragten Verluste zwar vermuten, aber nicht in Zahlen angeben.



Kaum zu kalkulieren, aber nicht minder beeinflussend sind auch die negativen Auswirkungen auf das Image des Unternehmens in der Öffentlichkeit sowie der langfristige Einfluss auf Geschäftsbilanzen und Aktienkurs.

Einer Studie der Universität von Texas zufolge nehmen die kritischen Auswirkungen eines Schadenfalles zu, je länger er die Datenkommunikation unterbindet. Es wird angenommen, dass über 85% der Unternehmen komplett von ihren Informationssystemen abhängen und sie rund 40% ihrer täglichen Einnahmen im Schadensfall verlieren würden.

## Sicherheitskonzept erstellen und umsetzen

Beim Begriff „Disaster“ denkt man unwillkürlich zunächst an GAUs, an die „größten anzunehmenden Unfälle“, wie beispielsweise Naturkatastrophen, militärische Konflikte oder Terrorismus. Es gibt aber weit mehr Möglichkeiten einer ernsthaften Bedrohung für die Unternehmensinfrastruktur. An den tatsächlichen Schadensfällen haben echte Katastrophen sogar nur einen sehr geringen Anteil. Meist entstehen die Schäden durch das Zusammenspiel sich addierender kleiner Fehler, Kopflosigkeit und schlechter Planung bzw. Vorbereitung auf den Notfall. Das Augenmerk bei Überlegungen zur „Disaster Recovery“ darf daher nicht nur auf einer Handvoll „echter“ (und eher unwahrscheinlicher) Katastrophen liegen, sondern muss vielmehr auch die nahe liegenden Fehler und Schwachstellen berücksichtigen.

## Business Continuity

Neben dem Wiederherstellen des Datenbestandes (Recovery) spielen im Schadensfall auch der Bestand und die Arbeitsfähigkeit des betroffenen Unternehmens (Continuity) eine maßgebliche Rolle bei der Planung eines Krisenfalles.

Es dürfen nicht nur technische Aspekte berücksichtigt werden, sondern es muss unter anderem auch analysiert werden, welche geschäftlichen Aspekte besonders zu berücksichtigen sind, welche Daten wichtiger oder schützenswerter sind als andere, welche Mitarbeiter im Krisenfall benötigt werden und wie diese geschult sein müssen.

Business-Continuity-Pläne sind genau das, wonach sie sich anhören: Pläne zur Sicherung eines kontinuierlichen, reibungslosen Geschäftsbetriebs im Fall einer Störung oder Katastrophe. Sie beschreiben die notwendigen Abläufe und Vorgehensweisen, um die wesentlichen Betriebsfunktionen im Krisenfall aufrecht zu erhalten.

Die sieben Todsünden der Business-Continuity-Planung
Planung nur für „Worst case“-Szenarien
Planung nur für die wahrscheinlichsten Katastrophen
Unzureichendes oder fehlendes Testen
Geringes oder gar kein Commitment des Managements
Keiner fühlt sich zuständig
Fokus bei der Planung auf Schadensbegrenzung anstatt auf die Vermeidung von Schäden
Auswahl eines zu kleinen Tool-Spektrums, um den Plan auszuführen

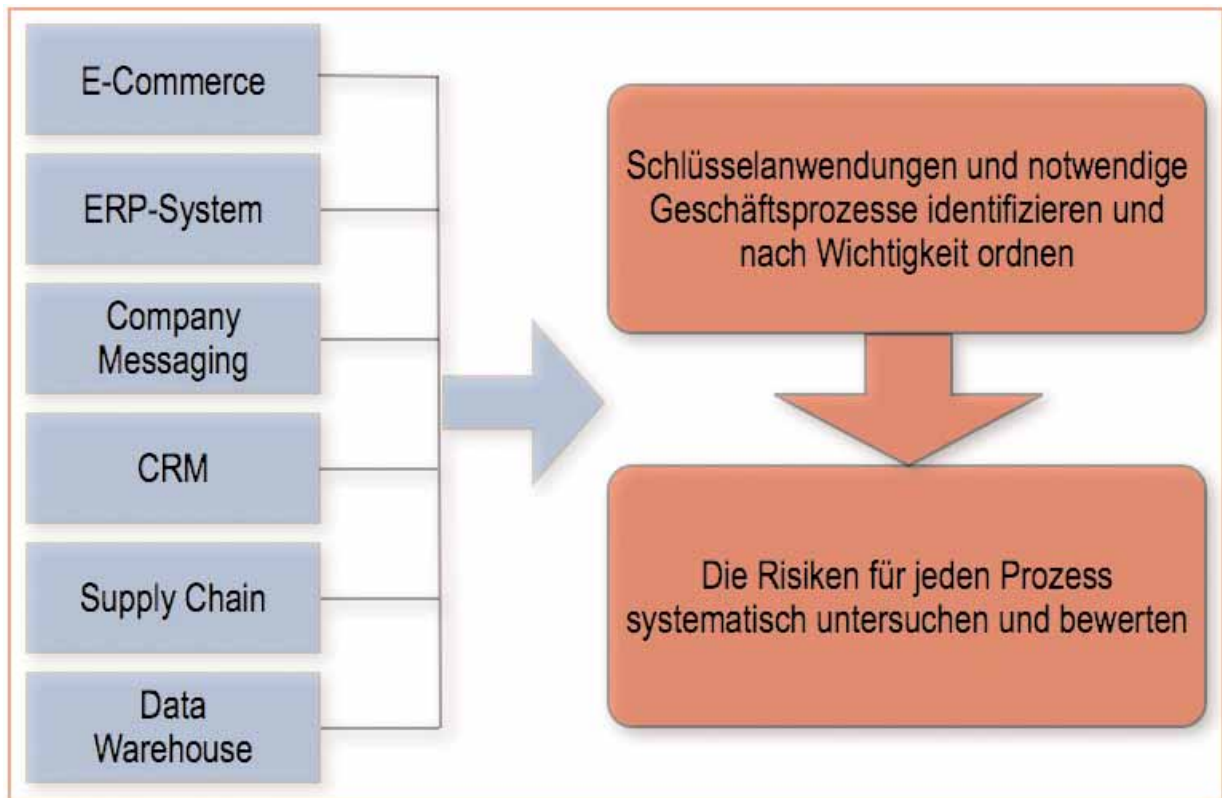
Quelle: Legato

Zur Festlegung dieser Prozesse ist zunächst eine Risikoanalyse notwendig, bei der die Gefahren für die IT-Struktur des Unternehmens identifiziert und nach der Schwere ihrer Auswirkungen bewertet werden. Diese Risikoanalyse sollte alle Faktoren mit einbeziehen – etwa auch die Verlässlichkeit des „Internet Service Providers“, die Möglichkeit interner Sabotage, das Platzen eines Wasserrohres im Serverraum oder die Überlegung, wie der Geschäftsbetrieb fortgesetzt werden kann, falls die Geschäftsräume beschädigt oder zerstört werden.

Mit Hilfe der Risikoanalyse wird ein sogenanntes Risiko-Inventar erstellt, in dem die bewerteten Gefahren ihrer Wichtigkeit entsprechend aufgelistet werden. Das Risiko-

Inventar bildet dabei auch die Beziehungen verschiedener Prozesse und Anwendungen ab und ist umso wirkungsvoller, je genauer die Wichtigkeit der einzelnen Risiken bewertet wird. Im Idealfall werden möglichst viele Mitarbeiter eingebunden, um die für ihre Abteilung wichtigen Schlüsselprozesse zu identifizieren. Betroffene Abteilungen können beispielsweise der Kundenservice, die Rechtsabteilung oder die Buchhaltung sein.

Zur genauen Ermittlung notwendiger Geschäftsprozesse und ihrer Wichtigkeit sollten die Mitarbeiter, die spezielle Geräte oder Anwendungen bedienen, gezielt nach der Nutzung befragt werden. Beispielsweise kann hier gefragt werden, wie der jeweilige Mitarbeiter an seinem Arbeitsplatz mit einem Ausfall von 24, 48 oder 72 Stunden zu Recht käme und welche Probleme oder welchen Kostenaufwand für das Unternehmen er an seinem Arbeitsplatz durch einen solchen Ausfall erwartet.



### **Risiken & Bedrohungen identifizieren**

#### **Aufgaben innerhalb der Risikoanalyse sind u. a.:**

- Entwicklung eines Kriterienkataloges für Risiken
- Identifizierung der wichtigsten Business-Prozesse
- Identifizierung von Systemen und Informationen, die von den wichtigen Business-Prozessen benötigt werden
- Identifizierung wichtiger Daten und Aufzeichnungen
- Ermittlung der Auswirkung auf die Kosten
- Festlegung von Wiederherstellungszeiträumen
- Identifizierung von möglichen Bedrohungen

Nachdem die priorisierte Liste der Risiken erstellt wurde, bewertet das Unternehmen, mit welcher Wahrscheinlichkeit der jeweilige Schadensfall eintreten kann und welche Kosten aufgewendet werden müssen, um das Risiko einzudämmen. So lässt sich relativ sicher abwägen, ob die Kosten für die Schutzmaßnahmen wirtschaftlich vertretbar sind.

So sind beispielsweise die Folgekosten des Ausfalls eines „Enterprise Resource Planning Systems“ naturgemäß wesentlich höher, als der Ausfall eines Abteilungsservers. Entsprechend lohnt sich hier auch ein höherer Aufwand zur Sicherstellung der Verfügbarkeit.

Bei den Kosten wird zwischen den einmaligen Kosten und den laufenden Kosten, die durch die Nutzung der Schutzmaßnahmen entstehen, unterschieden. Mit wachsendem Aufwand der Schutzmaßnahmen steigen hier auch die Kosten, die durch Ausfall der Arbeitszeit, der durch die Bedienung der Schutzmaßnahmen entsteht, an.

Im Rahmen der Risikoanalyse werden so verschiedene Kriterien festgelegt, beispielsweise für die mindestens notwendige Hardwarekonfiguration oder die Anzahl der Mitarbeiter, die im Notfall gebraucht werden, um die Krise zu bewältigen.

Um eine Krisensituation erfolgreich durchstehen zu können, müssen sich die Verantwortlichen über die verschiedenen Charakteristiken einer Krise einstellen:

- Überraschung
- Nicht genügend oder ungenaue Informationen
- Eskalation der Ereignisse
- Kontrollverlust
- Intensive neugierige Beobachtung von Außen
- Belagerungsgefühl
- Panik, Kurzschlusshandlungen
- Kurzfristiges Denken

Um Sicherheit zu gewährleisten, müssen alle denkbaren Widrigkeiten ausgeschaltet werden. Eine Lücke im Schutz kann einen Großteil der aufgewendeten Mühe wieder zunichtemachen. Deshalb muss ein möglichst vollständiges Bild der Gesamtkonzeption entworfen werden und alle Aspekte durch systematisches Vorgehen erfasst und abgedeckt werden. Der Schutzbedarf muss den Schutzmöglichkeiten gegenübergestellt werden.

## Die bewerteten Schäden werden nach ihrer Schwere in so genannten Wiederanlaufklassen erfasst:

### **Klasse 1:** überlebenswichtig (essenziell)

Prozess oder Anwendung ist grundlegender Bestandteil der Unternehmens-Wertschöpfung. Sein Ausfall hat Auswirkungen auf Umsatz oder Sicherheit.

### **Klasse 2:** sehr wichtig (kritisch)

Prozess oder Anwendung ist Bestandteil der Unternehmens-Wertschöpfung. Sein Ausfall hat sofortige Auswirkungen auf Umsatz oder Sicherheit. Der Ablauf des Geschäftsprozesses ist gestört.

### **Klasse 3:** wichtig (vital)

Prozess oder Anwendung kann kurzzeitig über Ausweichlösung betrieben werden und verursacht kalkulierbaren Schaden.

### **Klasse 4:** nicht wichtig

Prozess oder Anwendung kann verschoben werden. Ausfall verursacht keine großen Verluste.

### **Klasse 5:** unwichtig

Prozess oder Anwendung kann über längere Zeit verschoben werden. Ausfall verursacht keine nennenswerten Verluste.

Auf dieser Basis kann das Unternehmen seinen Business-Continuity-Plan erstellen. Ein solcher Plan besteht aus zwei Teilen: Präventionsmaßnahmen und Kontingenzstrategien. Die Präventionsmaßnahmen sollen negative Auswirkungen der ermittelten Risiken verhindern, während die Kontingenzmaßnahmen die Auswirkungen eingetretener Risiken möglichst gering halten sollen. Die Verwendung festgelegter Pläne sorgt dafür, eine Systematik einzuhalten, die dazu beiträgt, im entscheidenden Moment kein wesentliches Element zu vergessen.

## Leitfaden für die Planung

- Stellen Sie ein Team zusammen. Wichtig sind die Zusage und Unterstützung der Firmenleitung, ein funktionsübergreifender Lenkungsausschuss sowie ein Kernarbeitsteam.
- Analysieren Sie Ihr Unternehmen. Identifizieren Sie seine Ziele, seine Leistungen, Prozesse und Ressourcen sowie die Risiken, denen es ausgesetzt ist, die möglichen Auswirkungen dieser Risiken und die Institutionen (z. B. Technologieanbieter), an die Sie sich zur Risikoverringerung wenden.
- Definieren Sie eine Strategie für Disaster-Recovery und Business-Continuity für das gesamte Unternehmen, seine Geschäftsprozesse und Ressourcen. Lösen Sie anschließend die Frage der Finanzierung.
- Entwickeln Sie einen detaillierten Plan. Definieren Sie seinen Umfang und dokumentieren Sie die Anforderungen ausführlich.
- Implementieren Sie Ihren Plan. Zu den erforderlichen Schritten gehören die Sicherstellung der unternehmensweiten Unterstützung, die Entwicklung der Implementierungsdokumentation, die Zuweisung von Funktionen und Verantwortungen, die Schulung der Mitarbeiter sowie das Testen der implementierten Komponenten.
- Verwalten Sie Ihren Plan. Sie benötigen einen Prozess für das Change-Management sowie eine Möglichkeit, das Leistungsverhalten zu überwachen und Benchmark-Tests für neue Anwendungen, Produkte und Prozesse durchzuführen.

DRBC-Leitfaden (Disaster-Recovery/Business-Continuity) des Georgia Institute of Technology

Wenn diese Pläne aufgestellt wurden, müssen sie getestet werden. Dies kann beispielsweise durch Simulationen geschehen, mit denen man ein identifiziertes Risiko mit allen Auswirkungen durchspielt.

Derartige Simulationen können dabei helfen, Lücken in der Planung zu identifizieren. Beispielsweise ist es für eine erfolgreiche Rücksicherung von Anwendungen und Daten wichtig, die Systemkonfigurationen dokumentiert und archiviert vorliegen zu haben, um Folgeschäden zu vermeiden. Unternehmen, die auf eine schnelle Reaktivierung ihrer Daten angewiesen sind, sollten über entsprechende Data-Recovery-Prozeduren verfügen.

Diese Prozeduren müssen regelmäßig mit den Mitarbeitern trainiert werden, um im Ernstfall bekannt und akzeptiert zu sein. Ein einmal erstelltes Sicherungskonzept muss laufend an geänderte oder neue Arbeitsabläufe und Anwendungen sowie an sich ändernde technische Gegebenheiten angepasst werden.

## Bedrohungen und Gefahren für Daten

Daten in Informationssystemen sind einer Vielzahl von Bedrohungen und Gefahren ausgesetzt. Die Ursachen für den Verlust von Daten sind vielfältig, die Hauptursache stellen allerdings Fehlbedienungen dar. Katastrophen sind eher selten der Grund für Datenverlust.

## Sicherheitsmaßnahmen gegen Schäden durch

### **unbeabsichtigte Handlungen durch Unwissenheit oder mangelnde Sorgfalt, wie Bedien- und Programmfehler**

- Anlegen von Backups
- Vergabe von Zugriffsrechten
- Schulung der Mitarbeiter
- Zugangskontrolle

### **Ausfall und Störungen von Hardwarekomponenten oder Stromausfall**

- Hardwareredundanzen
- Unterbrechungsfreie Stromversorgung

### **Terrorakte oder Computerviren zum Zwecke der Schädigung oder persönlichen Bereicherung**

- Zugangsberechtigungen
- Firewall-Systeme
- Virens Scanner
- Überwachungseinrichtungen

### **Feuer, Wasser oder Blitzschlag**

- Anlegen von Backups
- Feuermelder
- Notstromversorgung

Insgesamt ist ein Wechsel der Prioritäten notwendig: War bisher die Bewältigung der stark ansteigenden Datenmengen wichtig, stehen nun Fragen nach sicheren Backup-Möglichkeiten und der Gewährleistung unterbrechungsfreier Geschäftsabläufe (Business Continuity) im Vordergrund. Spezifische Verfahren zur Datensicherung sowie ein Maßnahmenplan für die Datenwiederherstellung müssen damit unverzichtbarer Bestandteil der IT-Strategie von Unternehmen sein.

Die Frage nach dem Zeitfenster der Datenwiederherstellung ist ebenso unternehmenskritisch geworden wie die Frage nach dem Backup. Die Herausforderung heißt heute, ungeheure Datenmengen, bestehend aus wichtigen Daten wie beispielsweise Kundendatenbanken oder Planungsunterlagen, möglichst schnell wiederherstellen zu können, dazu noch mit möglichst aktuellen Daten. Immer schneller gelten Daten als nicht mehr relevant und die Ansprüche an zeitnahe und sichere Backups steigen ebenso wie die Forderung nach immer kürzeren Wiederherstellungszeiten.

Allen Fortschritten der Speichertechnologie zum Trotz sind weniger als ein Viertel aller Backups erfolgreich. Einer der Gründe dafür: In der Mehrzahl der Unternehmen ist die Speicherarchitektur ein ständiges Patchwork. Zu verschiedenen Zeiten werden, je nach aktuellem Bedarf, neue Komponenten unterschiedlichster Bauart hinzugefügt. Diese komplexen Speicherumgebungen bieten ihrerseits Anlass für mögliche, unvorhersehbare Backup-Probleme. Mögliche Fehlerquellen können beispielsweise überalterte und nicht mehr lesbare Magnetbänder sein. Ebenso kann eine Backup-Software, die nicht mehr in der neuen Systemumgebung läuft, aber notwendig ist, um alte Backups wieder einzuspielen, Probleme verursachen. Schließlich können auch die Backup-Prozesse selbst fehlerhaft sein, wenn etwa die Prozeduren nicht an eine neue Infrastruktur angepasst wurden. So kann die Backup-Software beim Zurückspielen der Daten versagen und so für fehlende oder korrupte Dateien sorgen. Es genügt daher nicht, der Backup-Logdatei zu glauben, dass tatsächlich ein Backup erfolgreich auf ein Band geschrieben wurde. Im Fehlerfall kann beispielsweise nur ein Verzeichnis, nicht aber die ganze Platte gesichert worden sein. Bänder können durch Magnet einfluss unlesbar geworden sein oder ein Tape wurde zerrissen, ohne dass dies bemerkt wurde. Die installierte Backup-Software kann so eingerichtet worden sein, dass die Daten verschlüsselt gespeichert werden. Leider ist der verantwortliche Administrator nicht mehr im Unternehmen und das Passwort ist nicht bekannt.

Entscheidend dabei ist das Zeitfenster zwischen Entdeckung, Bewertung der Gefahr und dem Ergreifen von Gegenmaßnahmen. Automatisierte Lösungen zum Beispiel für das Verteilen von Patches sind eine Möglichkeit, schnell Maßnahmen ergreifen zu können und Ressourcen zu schonen. Eine weitere Möglichkeit ist die regelbasierte Erhöhung von Backupfrequenzen, um Ausfällen bei einer Attacke vorzubeugen.

Spezifische Verfahren zur Datensicherung sowie ein Maßnahmenplan für die Datenwiederherstellung sind unverzichtbar und müssen an die jeweiligen Unternehmenserfordernisse angepasst werden. Um beispielsweise im Falle eines stattgefundenen Virengriffs eine planvolle und effektive Systemwiederherstellung zu gewährleisten, sollte ein Unternehmen über Art und Stellenwert seiner Ressourcen genau Bescheid wissen und zulässige Ausfallzeiten definieren.

## Checkliste Disaster-Recovery-Plan

- Wie wichtig sind die einzelnen Daten/Dateien?
- Wie lange kann das Unternehmen ohne seine Daten weiterarbeiten?
- Was ist der Wert der verlorenen Daten?
- Wie hoch wären die Verluste bei einem Totalausfall des Systems?
- Welche Ressourcen (Rechner, Speichereinheiten etc.) müssen wann und wo zur Verfügung stehen?
- Wie aktuell müssen die Datenbestände sein?
- Könnte eine kleinere Anzahl an Daten/Aktionen verloren gehen, ohne Auswirkungen zu hinterlassen? Welche Daten müssen sofort verfügbar sein, um das System neu zu starten?
- Gibt es Daten, auf die im ersten Schritt der Recovery verzichtet werden kann? Welche?
- Wie hoch gestalten sich die Kosten, verlorene Daten wieder herzustellen?
- Sind Notrufnummern im Unternehmen gut leserlich angebracht und im Schadensfall für jeden zu finden?
- Ist das zuständige Data-Recovery-Team kompetent, auf dem aktuellsten Wissenstand und mit genügend Mitgliedern ausgestattet?
- Gegen welche Art von Katastrophe gilt es, sich primär zu schützen?
- Wie ist die IT-Infrastruktur des Unternehmens beschaffen? Existieren sekundäre Rechenzentren? Gibt es ausgelagerte gesicherte Daten (Storage-Provider)?
- Wie steht es um Zweitstromversorgung oder Bandbreiten-Zuverlässigkeit im Katastrophenfall?
- Wurde die Datensicherung bei einem Serviceprovider abgewickelt? Wie schnell kann dieser im Notfall reagieren?
- Wurden regelmäßige Tests des Disaster Recovery durchgeführt? Waren die Tests an die jeweils im Unternehmen bestehende Situation (Daten/Infrastruktur etc.) angepasst und nicht statisch?
- Welches Budget muss veranschlagt werden, um einen Recovery-Plan vernünftig zu planen und umzusetzen?
- Welche Art der Datensicherung und des Disaster Recovery sind für das Unternehmen wirklich sinnvoll?

## Datenrettung als Bestandteil des Disaster-Recovery-Plans

Die Erstellung eines Disaster-Recovery-Plans ist ein anspruchsvoller Prozess. Während der Planungsphase konzentrieren sich die meisten Anwender zunächst auf handfeste und greifbare Gefahren wie Feuer, Einbruch oder Naturkatastrophen. Aber auch andere Formen von Datenverlusten und die entsprechenden Datenrettungsschritte sollten Eingang in den Disaster-Recovery-Plan finden. Nachfolgend einige Vorschläge:

### Dokumentation

Eine regelmäßige Überprüfung und ggf. Überarbeitung der Notfallprozeduren, beispielsweise auf vierteljährlicher Basis, ist ein wichtiger Bestandteil der Schadensverhinderung. Die entscheidenden Mitarbeiter sollten mit allen technischen Belangen der primären Business- oder Nachrichtensysteme vertraut sein. Eine ausführliche Dokumentation der Konfigurationen und Softwareeinstellungen sollte im Serverraum verfügbar sein. Für jeden Rechner sollte eine Administrationsdokumentation vorliegen.

### Microsoft Exchange Server Redundanz

Verfügt beispielsweise ein Unternehmen, das einen Microsoft-Exchange-Server betreibt, über einen zweiten „Restore Server“, über den die Serverinformationen bei einem Systemausfall wiederhergestellt werden können? Alle aktuellen Versionen des Exchange-Servers nutzen Log-Dateien, um Nachrichtentransaktionen aufzuzeichnen, bevor sie an die Datenbank übermittelt werden. Während „Circular Logging“ dabei hilft, Speicherplatz einzusparen, ist ein kompletter Satz der Log-Dateien im Notfall wichtig und notwendig. Mit ihm werden während eines Datenausfalles die Nutzerdaten der über ein Restore eingespielten Datenbank auf den neuesten Stand gebracht.

### Archivierte Daten auf Bändern

Der Disaster-Recovery-Plan sollte eine externe Lagerung von Backup-Bändern oder anderen Medien vorsehen. Backup-Bänder erfordern zusätzliche Prüfungsschritte in dem Plan. Bänder sollten in regelmäßigen Abständen geprüft werden. Der Austausch der Bänder sollte regelmäßig erfolgen und die Lebensdauer der Bänder berücksichtigen, um die Gefahr des Ausfalls durch Bandfehler zu minimieren.

### RAID-Systeme

Auch RAID-Speichersysteme, SAN- und NAS-Systeme sollten in den Disaster-Recovery-Plan mit aufgenommen werden. Diese Speichersysteme verfügen über Redundanzarchitekturen, um Fehler und Ausfälle zu verhindern. Durch diese Mechanismen kann leicht ein falsches Sicherheitsgefühl entstehen.

*So hatte beispielsweise ein Kunde etwa 40 TB Speicherplatz über 20 Server verteilt. Diese Systeme waren hardwareseitig als RAID 1+0 konfiguriert. Das Problem begann in einem Server, als ein Laufwerk für einen Moment offline ging. Die Controller-Karte schaltete zur gespiegelten Kopie der Platte um, so wie es der Redundanzprozess vorsah. Dann schaltete sich das erste Laufwerk wieder online. Die Controller-Karte schaltete zum ersten Laufwerk zurück. Plötzlich lagen aus Laufwerks- und Dateisystem-Perspektive inkonsistente Daten vor. Nach einem Herunterfahren und Neustarten des Systems führte die Hardware des Speichersystems einen Reset durch. Das automatische Laufwerks-Reparaturprogramm startete und führte Korrekturen durch. So wurde die Integrität des Dateisystems noch weiter beschädigt und wichtige Daten waren plötzlich nicht mehr vorhanden. Da diese Daten umgehend benötigt wurden, war hier die „Remote Data Recovery“ (RDR) das effektivste Hilfsmittel für den Kunden.*

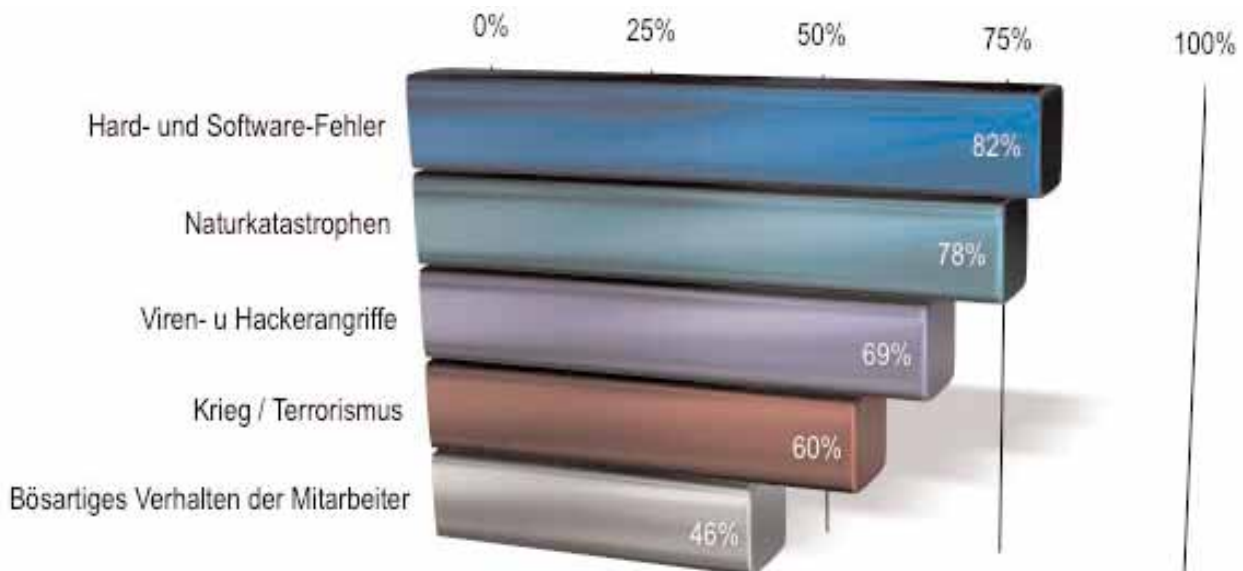
Dieser Kunde verarbeitete eine große Menge an Daten, die in drei Arbeitsschichten pro Tag generiert wurden. Eine so große Menge sich ändernder Daten täglich zu archivieren, war nicht möglich. Der Kunde musste darauf vertrauen, dass seine Speicherkonfiguration durch die Datenspiegelung absolut sicher war.

Eine solche Konfiguration hilft gegen zahlreiche Laufwerksfehler. In diesem Fall jedoch ist das Laufwerk nicht ausgefallen, sondern nur für einige Zeit offline gegangen. Als das Laufwerk wieder aktiv wurde, lagen Inkonsistenzen im Dateisystem vor. Die Daten waren schließlich nicht mehr zugänglich, als die automatischen Laufwerksreparaturen durchgeführt wurden. Nach einer Nacht konnte sämtliche Daten von den RDR-Ingenieuren wiederhergestellt werden.

Datendisaster können auf einzelnen Schäden beruhen, wie etwa dem Ausfall einer Festplatte. Ebenso häufig können Sie aber auch durch eine Kombination kleinerer Ausfälle entstehen. Die spezielle Erfahrung von Kroll Ontrack und das Verstehen der verschiedenen Umstände und Zusammenhänge unterscheidet Kroll Ontrack von vielen anderen Datenrettungsanbietern. In Zeiten, in denen der durchgängige Geschäftsbetrieb (Business Continuity) zum kritischen Faktor geworden ist, ist es wichtig, auf Schadensfälle und Katastrophen vorbereitet zu sein. Kroll Ontrack ergänzt den Disaster-Recovery-Plan um 20 Jahre Erfahrung, weltweite Niederlassungen, Reinräume, hoch spezialisierte Ingenieure und 24-Stunden-Support und -Service.

## Vorbeugung statt Katastrophe

95 Prozent der befragten IT-Manager in Deutschland gaben an, dass sie ohne Disaster-Recovery-Plan Katastrophen und Ausfällen schlicht ausgeliefert wären. Als die beiden größten Bedrohungen wurden mit 82 und 78 Prozent Hard- und Softwarefehler sowie Naturkatastrophen (z. B. Brand, Hochwasser) genannt, gefolgt von Viren und Hackerangriffen mit 69 Prozent sowie Krieg und Terrorismus mit 60 Prozent. Nicht alle Bedrohungen kommen von außen: Ausfälle aufgrund unabsichtlichen oder böswilligen Verhaltens von Mitarbeitern stuften 46 Prozent der Befragten als bedrohlich ein.



## Die größten Bedrohungen in der Einschätzung deutscher IT-Entscheider

Dass diese Bedrohungen keine graue Theorie sind, zeigt sich darin, dass 45 Prozent der befragten deutschen Unternehmen ihren Notfallplan in den vergangenen zwölf Monaten in die Praxis umsetzen mussten. Der häufigste Grund waren mit 26 Prozent Hardware- oder Softwarestörungen, gefolgt von Viren und Hackerangriffen (17 Prozent). 14 Prozent nannten Naturkatastrophen wie Brand oder Hochwasser als Ursache. Mit 7 Prozent war unabsichtliches oder böswartiges Verhalten von Mitarbeitern ein weiterer Auslöser.

**Laut der Disaster-Recovery-Studie 2003 überarbeiten 23 Prozent der Befragten den Plan seltener als einmal im Jahr – 2004 stieg diese Zahl auf 40 Prozent.**

## **Bei der Beurteilung einer Disaster-Recovery-Lösung sind folgende Punkte zu beachten:**

1. Wie lange darf ein System ausfallen, wie lange dauert der Wiederanlauf (Recovery Time Objective)? 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 kann hier von 0 Minuten (Systeme müssen sofort verfügbar sein) bis zu mehreren Tagen (in Einzelfällen Wochen) betragen.

2. Wie konsistent ist der Datenbestand, wie viel Datenverlust kann in Kauf genommen werden (Recovery Point Objective)? Bei dem „Recovery Point Objective“ (RPO) handelt es sich um den Zeitpunkt, wann (wie oft) die Datensicherung erfolgen soll, d. h., wie viel Daten/Transaktionen können zwischen den einzelnen Sicherungen verloren gehen. Ein optimaler RPO wird als „transaktionsgenau“ bezeichnet.

## **Organisatorische Maßnahmen**

Um Datensicherheit zu gewährleisten, sind neben technischen auch organisatorische Maßnahmen notwendig. Neben der klaren Festlegung von Verantwortlichkeiten ist eine Zutritts- und Zugriffskontrolle und regelmäßige Anfertigung von Backups dazu notwendig.

### **Zutrittskontrolle**

Unter Zutrittskontrollen versteht man bauliche und technische Maßnahmen, mit denen der Zugang zu Gebäuden und Räumen geregelt wird. Es soll sichergestellt werden, dass nur berechtigte Personen Zutritt zu Bereichen in Unternehmen haben, in denen mit wertvollen Daten gearbeitet wird, um diese vor versehentlicher oder willkürlicher Manipulation oder Zerstörung zu sichern.

Eine Möglichkeit ist es sensitive Bereiche so anzulegen, dass diese nur über Zugangskontrolleinrichtungen betreten werden können. Als Zugangskontrollmittel kommen dabei in Betracht:

- Schlüssel
- Lesesysteme für Chip- oder Magnetkarten
- Eingabegerät für Zahlencode
- Klingel mit Öffnung durch Mitarbeiter
- Biometrische Kontrollsysteme

Automatische Personenschleusen müssen so angelegt sein, dass sie bei erfolgreicher Legitimierung nur je eine Person in den geschützten Bereich lassen. Dem Nutzer können so entsprechend seiner Aufgabenbereiche Zutrittsrechte zu den jeweiligen Bereichen eingeräumt werden. Dies sollte im Rahmen der betrieblichen Notwendigkeiten möglichst restriktiv erfolgen. Bei Ausscheiden von Mitarbeitern sind die Zutrittsmittel unbedingt zurückzuverlangen.

Der Trend zu dezentraler Datenverarbeitung kommt hier erschwerend hinzu, sodass sich solche Maßnahmen nur für besonders kritische Bereiche, wie Rechenzentren lohnen.

Die Zugriffskontrolle soll den unbefugten Zugriff auf Rechnersysteme, Daten und Programme verhindern. Damit steht die Zugriffskontrolle in enger Verbindung mit der Zutrittskontrolle. Dabei müssen jedem Nutzer je nach Aufgabenbereich bestimmte Nutzerprofile zugeordnet werden. Auf diese Weise können auch Datenverluste durch Fehlbedienungen vermieden werden, indem beispielsweise nur bestimmte Nutzer die entsprechenden Rechte besitzen. Eine zentrale Verwaltung aller Nutzerrechte erleichtert die Freigabe oder den Entzug einzelner Dienste.

### **In den Zugriffsrechten wird geregelt,**

- wer welche Computersysteme nutzen darf,
- wer welche Daten lesen, löschen oder verändern darf
- wer welche Programme ändern und starten darf.

Hinter jeder Loginkennung sollte ein bestimmtes Nutzerprofil mit entsprechenden Zugriffsrechten stehen, an den jeweiligen individuellen Aufgabenbereich des Nutzers angepasst. Die Berechtigungen der Nutzer in den verschiedenen Anwendungssystemen sollte an zentraler Stelle erstellt und hinterlegt werden. Durch eingeschränkte Rechte wird das Risiko vermindert, Daten durch Fehlbedienungen oder versehentliches Löschen zu verlieren. In einigen Systemen ist es möglich, den einzelnen Nutzprofilen personalisierte Menüs zuzuordnen.

Um Zugang zu einem System oder einer Anwendung zu erhalten, hat sich die Kombination aus eindeutiger Benutzererkennung in Verbindung mit einem Passwort zur Identifizierung bewährt. Wenn der Zugang über ein externes Netz erfolgt, sollte mit entsprechenden Verschlüsselungstechniken für Sicherheit gesorgt werden.

Die Eingabe von falschen Passwörtern sollte auf eine bestimmte Anzahl an Fehlversuchen begrenzt werden, um automatisierte Einbruchsversuche zu verhindern. Bei der Auswahl der Passwörter ist darauf zu achten, dass diese sich nicht von Unbefugten erschließen lassen, wie beispielsweise Namen von Familienangehörigen. Die Passwörter dürfen Dritten nicht zugänglich gemacht werden. Um die Sicherungsfunktion dauerhaft gewährleisten zu können, müssen Passwörter regelmäßig geändert werden. Eine automatische Passwortalterung ist hier hilfreich, hierbei wird der Benutzer vom System nach einer definierten Zeitspanne aufgefordert, das Passwort zu ändern.

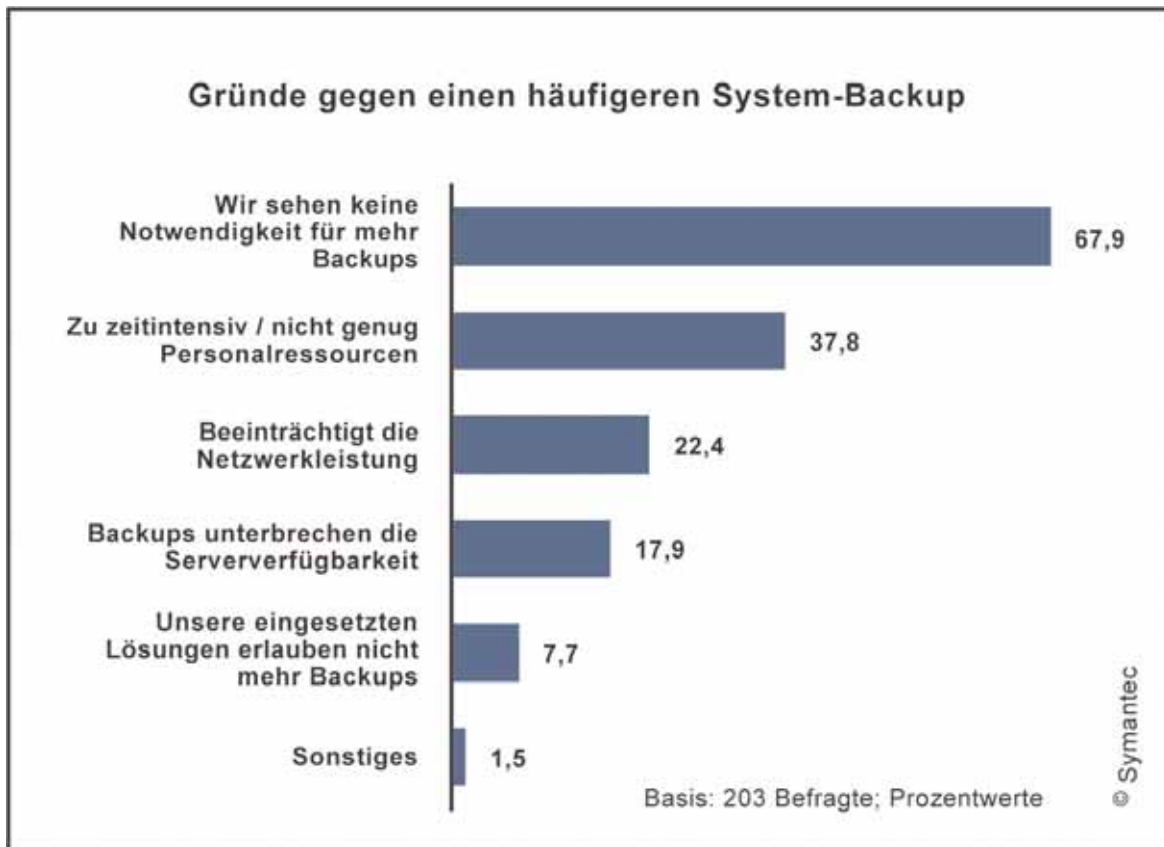
Der Schutz und die Gewährleistung der Verfügbarkeit von Daten stellt eine komplexe Aufgabe dar. Bei der Erstellung eines Konzeptes zur Datensicherung ist auf die individuellen Gegebenheiten in einem Unternehmen Rücksicht zu nehmen. Der Weg zu hochverfügbaren Systemen ist aufwendig und in der Regel sehr teuer. Letztlich kommt es darauf an, wie teuer der Ausfall für ein Unternehmen kommt. Bei unternehmenskritischen Daten und Systemen lohnt sich auch noch eine kostspielige Verbesserung der Verfügbarkeit auf der dritten Nachkommastelle.

Neben technischen und organisatorischen Maßnahmen ist eine schnelle Reaktion des Herstellers wichtig, um bei Problemfällen die Lieferung mit Ersatzteilen zu garantieren. Verfügbarkeit und Datensicherheit erfordern auch eine permanente Wartung und Pflege der Informationssysteme, möglichst über Wartungsverträge.

Das schwächste Glied in der Kette eines Informationssystems bestimmt die Verfügbarkeit und Datensicherheit, erst das Zusammenspiel und die Anpassung aller Komponenten ermöglichen wirklich hochverfügbare Dienste.

## Backup

Backups gehören heute in fast jedem Unternehmen zum IT-Alltag. Und zunächst klingen die Umfrageergebnisse dazu auch sehr viel versprechend: Rund 98,5 Prozent der Unternehmen berücksichtigen bei den internen Backuproutinen ihre Fileserver, Applikationsserver und Webserver. Doch schon um die Sicherung der im Unternehmen befindlichen Desktop-PCs und Notebooks ist es schlecht bestellt. 74,9 Prozent der Unternehmen sichern die auf den Arbeitsplätzen befindlichen Daten nicht, 83,3 Prozent sehen keine Notwendigkeit, die Notebooks in die Datensicherung mit einzubeziehen. Auch das Systembackup bietet bei näherem Hinsehen kaum die Gewähr für einen aktuellen Datenbestand: 42,4 Prozent der Unternehmen führen nur einmal pro Woche oder noch seltener regelmäßige System-sicherungen durch. Nur 15,8 Prozent sichern ihre Daten ständig oder mehrmals täglich.



Im Ernstfall gehen für die Mehrzahl der Unternehmen wertvolle Daten verloren, weil sie zu selten oder, wie im Falle des Datenbestandes auf den Arbeitsplatzrechnern, überhaupt nicht gesichert werden.

Im Dezember 2004 wurden von research+consulting IT-Verantwortliche aus Unternehmen und öffentlichen Einrichtungen in Deutschland befragt.

Spezifische Verfahren zur Datensicherung sowie ein Maßnahmenplan für die Datenwiederherstellung sind unverzichtbar und müssen an die jeweiligen Unternehmenserfordernisse angepasst werden. Um beispielsweise im Falle eines stattgefundenen Virengriffs eine planvolle und effektive Systemwiederherstellung zu gewährleisten, sollte ein Unternehmen über Art und Stellenwert seiner Ressourcen genau Bescheid wissen und zulässige Ausfallzeiten definieren.

## Tape- und Festplattensicherung

Für das Backup werden in den meisten Unternehmen nach wie vor Magnetbänder eingesetzt. Magnetbänder haben prinzipiell den Vorteil, dass für die Speicherung einer Informationseinheit mehr Fläche zur Verfügung steht, sodass die Daten magnetisch und mechanisch weniger gefährdet sind als auf einer Festplatte. Die Schreib-Lese-Methode unterscheidet sich nicht grundsätzlich, ist aber bei Magnetbändern insgesamt robuster. Trotzdem sind natürlich auch Magnetbänder – gleich welchen Typs (Streamerkassetten, Minikassetten, DAT etc.) – empfindlich gegenüber magnetischen, mechanischen und thermischen Einflüssen.

Als optische Medien werden – besonders im Bereich Datensicherung und mobile Daten – zunehmend auch CD-ROMs, DVDs oder magnetooptische Träger (MOs) eingesetzt. Diese sind zwar unempfindlich gegenüber externem Magnetismus, aber vor Datenverlust durch mechanische Beschädigung oder Hitze nicht gefeit.

Um Daten wirklich aktuell sichern zu können, reicht für Unternehmen mit dem heute üblichen hohen Datenaufkommen und der zunehmenden Wichtigkeit tagesaktueller Datenbestände eine einfache Bandsicherung nicht mehr aus. Wenn es um hochverfügbare Systeme geht, müssen heute Festplattentechnologien genutzt werden, beispielsweise da, wo sensible Finanzdaten ständige oder zumindest mehrmals tägliche Sicherung erfordern.

Im Zuge der Konsolidierung von Speicherkapazitäten stellen viele Unternehmen fest, dass sie mit klassischen Fileservern, die im lokalen Netzwerk (LAN) ihre Festplatten oder Bandlaufwerke als „Direct Attached Storage“ (DAS) zur Verfügung stellen, an ihre Grenzen stoßen. Die an einem Server lokal verfügbaren DAS-Kapazitäten erfordern aufgrund ihrer dezentralen Struktur eine zeit- und kostenintensive Verwaltung. Abhilfe bieten hier Speicherlösungen. Die Daten können zentral verwaltet werden und stehen dem gesamten Unternehmen schnell und sicher zur Verfügung. Derartige zentral administrierbare Infrastrukturen sind u. a. auf der Basis von SAN (Storage Area Network) und NAS (Network Attached Storage) möglich.

### RAID

Die Datenspeicherung kann auch verteilt stattfinden – z. B. auf mehreren Festplattensystemen an verschiedenen Orten oder in einem eigenen oder angemieteten Data-Center. Zum Einsatz kommen dabei meist ‚RAID-Systeme‘, die aus einer beinahe beliebig ausbaubaren Anzahl einzelner Festplattensysteme bestehen und entsprechend große Datenmengen speichern können. RAID-Systeme oder auch Disk-Arrays bestehen prinzipiell aus nichts anderem als einer Menge an softwaretechnisch verbundenen Festplatten. Der Unterschied zwischen mehreren in einem Rechner eingebauten Festplatten und einem RAID-System liegt nur darin, dass ein RAID-System mit einer eigenen Hard- und Software ausgestattet ist, die den Gesamtspeicher von außen als Einheit bzw. wie ein einzelnes logisches Laufwerk erscheinen lässt und durch automatisiertes Spiegeln und Verteilen von Daten für eine Redundanz der Informationen sorgt.

### Cluster

Durch die redundante Auslegung kritischer Komponenten lassen sich Verfügbarkeiten von 99% erreichen. Mit dem Einsatz von Clustern können Verfügbarkeiten von 99,99% erreicht werden, dies entspricht einer durchschnittlichen Ausfallzeit von knapp 53 Minuten pro Jahr. Unter einem Cluster versteht man den Zusammenschluss mehrerer unabhängiger Rechner, die sich dem Nutzer als ein System präsentieren, um eine Aufgabe zu lösen.

Bei Clustern wird die Ausfallsicherheit dadurch hergestellt, dass dieselben Instanzen auf mindestens zwei unterschiedlichen Systemen laufen. Wenn ein Knoten ausfällt, können die Dienste automatisch von einem anderen Knoten übernommen werden. Dabei wird entweder die Anwendung auf einem anderen Server neu gestartet oder es erfolgt eine Übernahme im laufenden Betrieb, ohne dass der Anwender etwas davon merkt. Dazu müssen die Prozesse exakt zwischen den Rechnern abgestimmt werden, um im Fehlerfall jederzeit eine aktuelle Kopie des Prozesses vorliegen zu haben.

Für die Realisierung eines Clusters stehen zwei Modelle zur Verfügung, das Shared-Storage- und das Shared-Nothing-Modell.

Beim Shared-Storage-Modell hat jeder Knoten zu jeder Zeit Zugriff auf alle verfügbaren Ressourcen, die Datenkonsistenz wird durch Verwaltungssoftware des Clusters gewährleistet.

Beim Shared-Nothing-Modell greift jeder Knoten exklusiv auf einen Teil der Ressourcen zu. Erst bei Ausfall eines Knotens übernimmt er Ressourcen des anderen Knotens und hält so die Konsistenz der Daten aufrecht.

In einem Cluster müssen alle Netzwerkkomponenten und Verbindungen redundant ausgelegt sein, um ein hochverfügbares Netzwerk zu garantieren. Redundante Verbindungen bieten gleichzeitig den Vorteil eines höheren Datendurchsatzes, was die Antwortzeiten des Systems senkt. Durch die redundante Auslegung des Clusters können einzelne Rechner im laufenden Betrieb vom Netz genommen werden, ohne dass der Gesamtverbund ausfällt. So bleiben geplante Ausfallzeiten (beispielsweise zu Wartungszeiten) ohne Auswirkung auf die Systemverfügbarkeit. Um höchste Sicherheit zu gewährleisten, kann man Cluster für unternehmenskritische Bereiche auch geografisch trennen.

## Fehlertolerante Systeme

Noch höhere Verfügbarkeiten von 99,999% können nur mit proprietären Hard- und Softwarelösungen erzielt werden. Bei solchen Systemen sind die Prozessoren, der Arbeitsspeicher und andere kritische Komponenten doppelt oder mehrfach vorhanden. Alle Komponenten arbeiten ständig parallel, sodass sich der Ausfall einer Komponente nicht auf den laufenden Betrieb auswirkt. Im Störfall wird die schadhafte Komponente isoliert und kann während des laufenden Betriebs ausgetauscht werden. Aufgrund der proprietären Komponenten sind auf fehlertoleranten Systemen jedoch nicht alle Anwendungen lauffähig.

## RAID – Ersatz für Backup?

Der Einsatz eines RAID-Systems stellt keinen Ersatz für ein Backup dar, eine regelmäßige Datensicherung auf externe Speichermedien bleibt unerlässlich, um Gefahren wie Virenbefall, vorsätzlicher Manipulation oder versehentlicher Löschung von Dateien vorzubeugen. Diese Fehler duplizieren sich ebenfalls auf die gespiegelten Laufwerke.

Für ein Backup sollte nur ein System mit Wechselmedien zum Einsatz kommen, um die gesicherten Daten abseits der Rechner aufzubewahren. Als Medien stehen Magnetbänder, Wechselplatten, optische Medien und magnetooptische Platten zur Auswahl, wobei sich in großen Netzwerken Magnetbänder, welche die größte Speicherkapazität aufweisen, etabliert haben. In einem Netzwerk kann sowohl dezentral von einzelnen Servern, als auch vom gesamten Netzwerk mit sämtlichen angeschlossenen Servern ein Backup erstellt werden. Ein dezentrales Backup belastet das Netzwerk erheblich weniger.

Die Daten, die nach dem letzten Backup erstellt worden sind, sind im Verlustfall verloren. Deshalb muss ein akzeptabler maximaler Datenverlust definiert werden. Dieser bezeichnet den Datenzustand, zu dem nach einem Fehlerfall eine sichere Rückkehr möglich ist. Dabei kann es sich um eine Datenmenge oder einen Zeitpunkt handeln. Je häufiger das Backup durchgeführt wird, desto geringer ist im Fehlerfall der Datenverlust.

Geöffnete Dateien können unter Umständen nur in einem inkonsistenten Zustand gespeichert werden, insbesondere während laufender Transaktionen. Deshalb muss sichergestellt werden, dass nur abgeschlossene Transaktionen gesichert werden. Blockierte Dateien müssen in einem zweiten Anlauf gesichert werden. Aus diesem Grund ist es ratsam, die Sicherungsläufe nachts und am Wochenende durchzuführen. Auf ein Medium darf aus Sicherheitsgründen nur immer eine Backup-Schicht gespielt werden. Nach dem Backup sollten die Backup-Medien geprüft und an einem anderen Ort möglichst in einem feuersicheren Safe verwahrt werden.

Auf eine Datenkompression der Backup-Medien sollte bei wertvollen Daten verzichtet werden, da selbst einzelne Bitfehler dazu führen können, dass der komplette Datensatz nicht mehr rekonstruierbar ist.

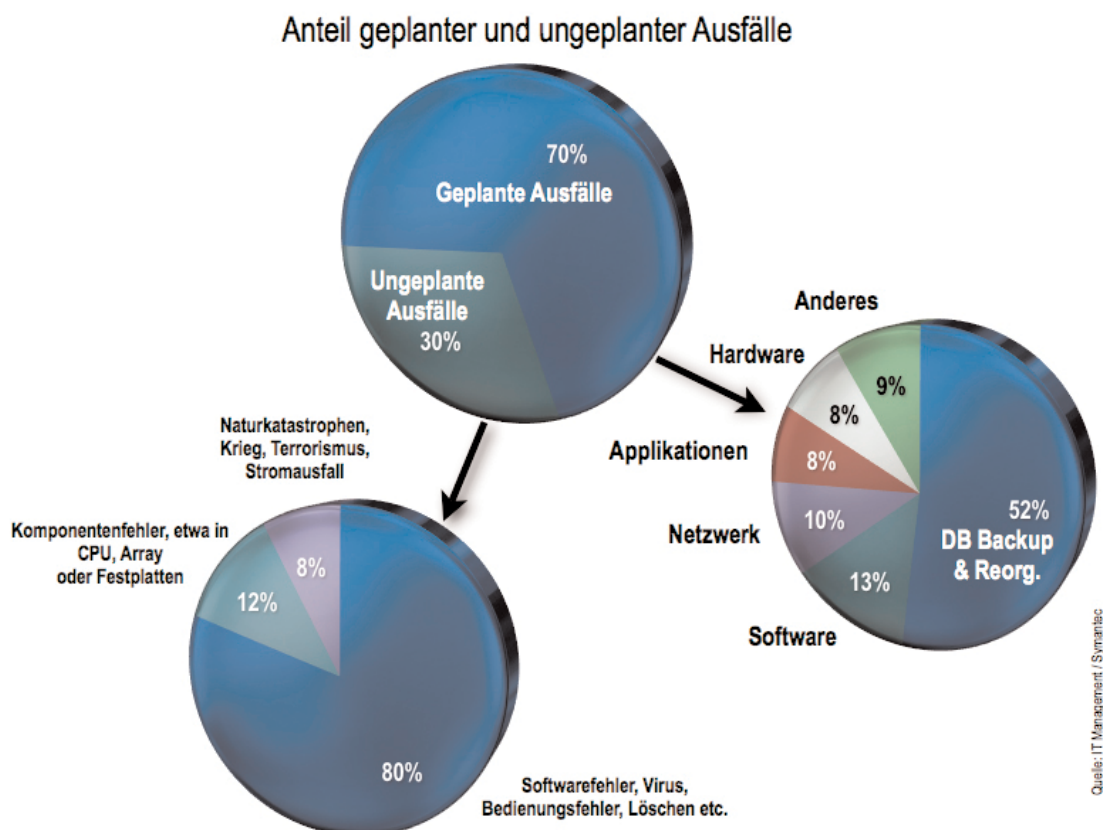
Die zur Wiederherstellung zerstörter Daten zur Verfügung stehende Zeit wird durch die Verfügbarkeitsanforderungen des Systems bestimmt. Bei 99,9% Verfügbarkeit bedeutet dies, dass ein System im ganzen Jahr nur insgesamt 8,8 Stunden außer

Betrieb sein darf und somit nur wenig Zeit zur Rekonstruktion bei Datenverlusten zur Verfügung steht.

Da auch bei der Datensicherung noch Fehler auftreten können und Sicherungsmedien unlesbar sein können, sollten Sicherungen von früheren Zeitpunkten noch eine Zeit lang aufbewahrt werden. Ein Verfahren dazu stellt das Generationenprinzip dar, das auf drei verschiedenen Sicherungsmedien basiert. Dazu werden an den ersten drei Tagen die Daten auf jeweils ein Medium gesichert und aufbewahrt. Am vierten Tag wird dann die älteste Sicherungsgeneration wieder überspielt und fortan immer die älteste Generation. Auf diese Art stehen immer zwei Ersatzgenerationen zur Verfügung, wenn die Wiederherstellung von der jüngsten Sicherungsgeneration nicht möglich sein sollte. Durch Verwendung von mehr als drei Sicherungsgenerationen kann die Sicherheit weiter erhöht werden.

## Backup und Verfügbarkeit

Datensicherungen sind der Hauptgrund für geplante Ausfallzeiten. Oft sind die zu sichernden Datenmengen zu groß und benötigen dementsprechend große Backup-Zeitfenster, welche den laufenden Geschäftsbetrieb in nicht unerheblichem Maße beeinflussen. Daten sind oft über viele Server, die über ein Netzwerk miteinander verbunden sind, verteilt. Bei der Durchführung eines Backups kommt es aufgrund der zu übertragenden Datenmengen zu einer großen Netzbelastung, die zu langen Antwortzeiten oder gar zur Nichtverfügbarkeit der Systeme führen kann. Datensicherungsmethoden müssen deshalb an den Verfügbarkeitsanspruch angepasst sein.



Die IT-Verantwortlichen in größeren Unternehmen fühlen sich meist gut geschützt. Sie setzen auf hochwertige RAID-, NAS- oder SAN-Systeme. Was soll da schon schief gehen? Die Verfügbarkeit der wichtigen kaufmännischen und produktionstechnischen Daten ist rund um die Uhr gewährleistet. Durch ihre redundante Architektur vermitteln diese Systeme leicht ein trügerisches Sicherheitsgefühl. Auf kapazitätsstarken RAID-Festplatten-Verbänden finden sich Buchhaltungsdaten, Planungsdaten, Konzepte oder Budgets, aber auch Schriftwechsel mit Kunden sowie Angebote und Rechnungen.

Umso überraschender und schmerzhafter schlägt dann ein Ausfall zu. Zeit bedeutet in diesem Falle auch Geld, da mehrere Abteilungen ihr Tagesgeschäft nicht mehr oder nur eingeschränkt fortsetzen können. Ein im informationstechnischen Sinne stillstehendes Unternehmen verursacht massive Kosten, ohne in dieser Zeit auch nur einen Euro einzubringen. Auch die Wiederherstellung der Daten kann in komplexen Strukturen auf unerwartete Widerstände stoßen. Sei es, dass der RAID-Controller fehlerhaft arbeitet und ein Laufwerk nach dem anderen als beschädigt meldet, oder dass sich herausstellt, dass das letzte vollständige Backup eine Woche zurückliegt und die wichtigsten aktuellen Transaktionen, Vertrags- und Produktionsdaten noch nicht enthalten sind. Häufig führen gerade unter Zeitdruck durchgeführte Wiederherstellungsversuche in der Folge zu noch weitaus größeren Beschädigungen am Datenbestand. Das schnelle Eingreifen von Datenrettungsexperten ist bei schwer wiegenden Fehlern der richtige Weg, um geschäftskritische Daten wiederherzustellen. Ebenso wichtig ist das richtige Verhalten im Ernstfall, um die Chancen auf eine erfolgreiche Datenrettung zu erhöhen.

## **Datenrettung als Bestandteil des Notfallplans**

Häufig nehmen die von Datenverlust Betroffenen an, dass ihre Daten unwiederbringlich verloren sind. Ein guter Datenretter ist jedoch in vielen Fällen in der Lage, die wertvollen Daten ganz oder zu einem großen Teil wiederherzustellen. In vielen dieser Fälle müssen die betroffenen Medien noch nicht einmal im Labor wiederhergestellt werden, sondern können, dann, wenn es sich nicht um einen Hardwareschaden handelt, sogar mittels Ferndatenrettung wieder „zum Leben erweckt“ werden.

Professionelle Datenretter können heute auch die Daten von RAID-, NAS- oder SAN-Systemen wiederherstellen. Häufig kann dies sogar innerhalb weniger Stunden mittels Ferndatenrettung (RDR – "Remote Data Recovery") geschehen, ohne dass auch nur eine Festplatte ausgebaut werden muss.

Die einzige und beste Prophylaxe gegen Datenverlust ist natürlich ein konsequent durchgeführtes Backup! Doch nicht immer kann diese Vorbeugungsmaßnahme in einem Unternehmen optimal umgesetzt werden. Auch hier kann Hardware ausfallen, Bänder können unsachgemäß gelagert sein oder es gibt unvorhergesehene Probleme beim Zurückschreiben der Daten. Mit den modernen Methoden der Datenrettung lassen sich jedoch auch Daten, die nicht aus einem Backup restauriert werden können, wiederherstellen.

Die Aufgaben der Datenrettung liegen in der Wiederherstellung von gelöschten bzw. beschädigten Daten auf einem Datenträger wie zum Beispiel einer Festplatte oder einem Bandlaufwerk. Die Schäden können dabei nicht nur durch beschädigte Datenstrukturen hervorgerufen werden, sondern auch durch elektronisch oder mechanisch defekte Speichermedien. Diese können so weit beschädigt sein, dass die Daten nicht mehr ohne weitergehende technische Maßnahmen gelesen werden können. Mit der genauen Kenntnis des Betriebssystems, der vorhandenen Netzstruktur und der für diesen Fall geeigneten Werkzeuge zur Datenrettung kann durch einen professionellen Eingriff oft eine rasche und erfolgreiche Datenwiederherstellung eingeleitet werden.

## **Wann brauchen Sie einen Datenrettungsspezialisten?**

Nahezu alle Daten lassen sich im Schadensfalle wiederherstellen. Doch wann benötigen Sie eigentlich einen Datenrettungsspezialisten? Unzuverlässiges Backupsystem – Ohne ein getestetes und zuverlässiges Backupsystem kann jede Form von Datenverlust zu erheblichen Verlusten und zu einer massiven Beeinträchtigung der Unternehmenstätigkeit führen.

**Fehler bei Backup- und Restore-Vorgängen** – Sowohl Backup als auch Restore können durch unlesbare Bänder, Datenkorruption oder falsche Backupprozeduren in ihrer Funktion eingeschränkt werden. Selbst, wenn das Backup korrekt durchgeführt wurde, liegt häufig eine Lücke zwischen den aktuellen Daten und dem letzten Backup.

**Erheblicher Zeitaufwand für den Restore** – Häufig kann der für einen Restore benötigte Zeitaufwand zu erheblichen Finanz- und Produktivitätsverlusten führen.

**Unpraktische oder unmögliche Neuerstellung der Daten** – Die Neuerstellung von Daten kann durch Zeitverlust, Kosten oder qualitative Einschränkungen zu einer unmöglichen oder nicht praktikablen Option werden.

**Nicht bootendes System** – Selbst kleine Beschädigungen der Betriebssystemstruktur können das Hochfahren des Systems verhindern.

**Fehler in gespiegelten oder RAID-Systemen** – Viele Unternehmen speichern Daten auf zwei separaten Speichersystemen. Wenn Daten beschädigt werden, bevor sie auf das zweite System kopiert werden oder eines (oder beide) Speichersysteme versagen, kann dennoch ein Datenverlust auftreten. Auch in RAID-Systemen kann Datenverlust auftreten, wenn zwei oder mehr Laufwerke gleichzeitig ausfallen oder ein Rebuild eines ausgefallenen Laufwerks fehlschlägt. Weder RAID- noch gespiegelte Systeme können vor Viren, Softwarefehlern oder Bedienerfehlern schützen.

**Absichtlich geänderte oder zerstörte Daten** – Daten können durch Viren, Systemeinträge oder frustrierte Mitarbeiter absichtlich zerstört oder verändert werden.

**Unabsichtlich geänderte oder zerstörte Daten** – Anwenderfehler können zum Datenverlust oder zur unabsichtlichen Veränderung von Daten führen.

**Korrumpierte oder gelöschte Microsoft-SQL- oder Microsoft-Exchange-Datenbanken** – Systemfehler, Stromausfälle, unabsichtliche oder bewusste Löschungen können diese unternehmenskritischen Daten unzugänglich machen.

## **Worauf kommt es bei der Auswahl eines Datenretters an?**

### **Hat das Unternehmen Erfahrung?**

Datenrettung ist ein technologisch sehr komplexer Bereich und erfordert ein hohes Maß an Expertise und Erfahrung. Datenrettungsunternehmen sollten ein entsprechendes Investment in Forschung und Entwicklung vorweisen können und entsprechende eigene Werkzeuge und Techniken zur Datenrettung entwickelt haben. Eine große Zahl erfolgreicher Datenrettungen sollte als Referenz vorliegen. Sinnvoll ist ein Unternehmen, das sowohl Diagnose und Datenrettungsdienste anbietet, als auch eigne Softwarelösungen.

## **Kennt das Unternehmen die verwendete Hard- und Software?**

Ein Datenretter sollte zertifizierter Entwickler oder Solutions-Partner der führenden Hard- und Softwareanbieter wie Microsoft, Novell, Apple, Sun oder SCO sein. Der Datenretter sollte in der Lage sein, Daten jeden Typs und für jede Plattform wiederherstellen zu können – von DOS, Windows, NT über Netzwerke, Apple Macintosh, UNIX bis hin zu Systemen von HP, DEC oder IBM. Er sollte mit allen Medien arbeiten können und mit Festplatten, optische Medien, Wechsellplatten und Flash-Medien ebenso umgehen können wie mit RAID-Systemen und Tape-Formaten wie DAT, Travan, Exabyte, DLT und AIT. Gut ist es, wenn der Datenretter von führenden Festplattenherstellern empfohlen wird.

## **Sind die Daten sicher?**

Um die wertvollen Unternehmensdaten zu schützen, sollte der Datenretter über strenge Sicherheitsvorkehrungen verfügen und proprietäre Protokolle, Datenverschlüsselung und andere Sicherheitsvorkehrungen einsetzen.

## **Wird eine Lösung zur Ferndatenrettung (RDR) angeboten?**

Viele Datenretter erwarten, dass die betroffenen Laufwerke zur Rettung eingeschickt werden. Ein Vorgang, der unter Umständen teuer und langwierig sein kann. Bei manchen Systemen ist ein Ausbau gar nicht möglich. Um die Daten schnell und kostengünstig zurückzuerhalten, ist eine Ferndatenrettung notwendig, bei der in Laborqualität über eine gesicherte Internet- oder Modemverbindung direkt auf dem betroffenen Server oder PC gearbeitet wird.

## **Maßnahmen im Schadensfall**

### **Expertentipp für den Notfall**

- Zunächst gilt es, Ruhe zu bewahren. Egal, was passiert ist, gehen Sie davon aus, dass Ihre Daten mit sehr hoher Wahrscheinlichkeit wieder herstellbar sind.
- Defekte Hardware führt oft zu Fehlverhalten der Datenträger. Schalten Sie den PC deshalb nicht ein, wenn Sie vermuten, dass es - zum Beispiel bei einem Blitzeinschlag - zu Überspannung in Ihrem Netz gekommen ist. Lassen Sie den PC ausgeschaltet. Treffen Sie keine voreiligen Entscheidungen!
- Bei einem Festplatten-crash hören Sie oft ungewöhnliche Geräusche, z. B. ein Klackern, Reiben oder sehr hohe Töne. In diesem Fall gilt es, keinesfalls selbst Hand an die Hardware zu legen. Ein Neustart könnte die Festplatte endgültig zerstören. Wenden Sie sich stattdessen umgehend an ein professionelles Datenrettungsunternehmen wie Kroll Ontrack.
- Verwenden Sie keine Datenträger, die Hitze, Feuchtigkeit oder Verrußung ausgesetzt waren, da die Daten unwiderruflich verloren gehen können, wenn der Datenträger nicht in der staubfreien Umgebung eines Reinraums behandelt wird.
- Schütteln Sie den Datenträger nicht und entfernen Sie bei Festplatten nicht das Gehäuse.
- Durch Wasser beschädigte Datenträger sollten feucht gehalten werden - im Wasser belassen oder in feuchte Tücher einwickeln - und sofort in ein Datenrettungslabor gebracht werden. Versuchen Sie niemals, durch Wasser beschädigte Datenträger durch Wärmebehandlung (z. B. mit dem Föhn) zu trocknen!
- Festplatten, die mit Salzwasser in Berührung gekommen sind, erfordern eine spezielle Behandlung. Salz beschleunigt die Korrosion (Zerstörung). Der Datenträger sollte daher unverzüglich in einem luftdichten Behälter an Kroll Ontrack geschickt werden.
- Versuchen Sie nicht, offensichtlich beschädigte Datenträger weiter zu verwenden.
- Probieren Sie niemals, Datenträger selbst zu säubern.
- In vielen Fällen lassen sich die verlorenen Daten mit speziellen Softwareprogrammen (z. B. Ontrack EasyRecovery™) in Eigenregie wieder herstellen. Setzen Sie solche Tools jedoch nicht ein, wenn die Anzeichen auf einen Hardware-Defekt deuten und der Computer beispielsweise ungewöhnliche Geräusche von sich gibt.

## **Praktisch und schnell: Online-Datenrettung**

Logische Problemfälle können fast immer mit der Ferndatenrettung (RDR) gelöst werden. Es gibt eine Reihe typischer Situationen, in denen dieses Verfahren die schnellste und kostengünstigste Variante darstellt.

## **Wiederherstellung von RAID-Systemen**

Wenn die Störung an einem RAID-System dazu führt, dass dieses vom Fileserver-Betriebssystem nicht mehr erkannt wird, stehen die gespeicherten Daten nicht mehr zur Verfügung. Bisher war die einzige Lösung, den RAID-Server neu aufzusetzen und die Daten von Backup-Bändern zu restaurieren. Im Extremfall führt dies zu einem mehrtägigen Systemausfall.

Kroll Ontracks „Remote Data Recovery“ (RDR) hilft hier, da sich der RDR-Ingenieur in den RAID-Server einklinken, dort die Diagnose und schließlich die Datenrettung durchführen kann. In der Regel ist dies eine Sache von wenigen Stunden.

## **Wiederherstellung von Microsoft-Exchange Servern**

Der Ausfall eines Mailservers ist für viele Unternehmen einer der schlimmstmöglichen Unfälle, da oft stunden-, wenn nicht tagelang keine E-Mails und Faxe empfangen und versendet werden können und so die Kommunikation mit Kunden und Partnern praktisch zum Erliegen kommt. Da sich die Daten auf einem solchen Mailserver durch ein- und ausgehende Mails und Faxe im Sekundentakt ändern, hilft ein Restore von Sicherungsbändern, die in der Regel einmal täglich erzeugt werden, meist nicht weiter. Bei einem Microsoft-Exchange-Server kann es zu Inkonsistenzen in der Datenbank kommen, wenn z. B. kurzzeitig die Stromversorgung ausfällt.

In diesem Fall kann der RDR-Ingenieur die Datenbankstruktur per Remote-Zugriff analysieren, die einzelnen Mailboxen der Anwender als PST-Dateien extrahieren und dem Kunden zur Verfügung stellen. Diese PST-Dateien zu importieren und daraus eine neue Exchange-Datenbank aufzubauen, ist dann für den Systemverwalter nur noch eine Routinetätigkeit.

## **Wiederherstellung von Microsoft-SQL-Servern**

Ganz ähnlich kann auch der Ausfall eines Datenbank-Servers vom Typ Microsoft-SQL behoben werden. Auch hier analysiert der RDR-Ingenieur zunächst die Struktur, sucht intakte Datensätze und überführt diese in eine intakte Datenbank. Diese enthält dann alle Datensätze bis auf die beschädigten.

## **Wiederherstellung nach einem Virusangriff**

Der Schlüssel zum Erfolg der Ferndatenrettung RDR nach einem Virenangriff ist die RDR-QuickStart-Software. Mit der bootfähigen Version kann das betroffene System neu gestartet werden, ohne dass die Gefahr besteht, dass der Virus weiteren Schaden anrichtet. Der RDR-Ingenieur kann sich auf dem befallenen System einloggen, den Virus entfernen und beschädigte Daten rekonstruieren.

## **Wiederherstellung versehentlich gelöschter Daten**

Wer hat noch nie versehentlich wichtige Dateien gelöscht? Meist passiert das unterwegs auf dem Notebook – weit ab von jeder Hilfe durch den IT-Administrator des Unternehmens. Auch hier kann eine RDR helfen, da man als Betroffener von jedem Ort der Erde aus mit einem RDR-Ingenieur in Verbindung treten kann, der den Schaden behebt und die gelöschte Datei online wiederbelebt.

## Datenrettungstipps für Server

Der erste Schritt ist, die Realität eines möglichen Datenverlustes zu akzeptieren. Zusätzlich ist es unerlässlich und sehr empfehlenswert, einen verständlichen Notfallplan zu erarbeiten. Wenn ein Datenverlust eintritt, läuft die Zeit immer gegen das IT-Team. Darum ist es gut, bestimmte Szenarien durchzuspielen um gegen alle Eventualitäten/ Unregelmäßigkeiten gewappnet zu sein.

Professionelle Datenretter wie Kroll Ontrack können heute auch die Daten von RAID-Systemen wiederherstellen. Im Falle eines Datenverlustes sollte also unbedingt ein professioneller Datenretter kontaktiert werden. Während eines Ausfalls kommt es zunächst aber darauf an, nicht die falschen Maßnahmen zu ergreifen, denn im schlimmsten Fall können die Daten unwiederbringlich verloren gehen.

- Bei einem Datenverlust nie die Daten auf den gleichen Server wieder aufspielen, auf dem der Datenverlust eingetreten ist. Immer einen separaten Server hinzuziehen oder eine andere separate Lokation wiederherstellen.
- Bei Ausfällen von Microsoft-Exchange- oder SQL-Servern nie versuchen, die Originaldateien zu reparieren. Immer zuerst eine Sicherungskopie der Daten erstellen und mit diesen arbeiten.
- Im Falle gelöschter Daten sollte Windows nicht heruntergefahren werden - stattdessen ist es ratsam, den Rechner sofort auszuschalten. Dies schützt vor dem Überschreiben von Daten.
- Wenn eine Platte in einem RAID-System versagt, niemals die defekte Platte durch eine Neue ersetzen, die vorher in einem anderen RAID-System eingebaut war - immer zuerst die zu ersetzende Platte bzw. deren Daten lowlevel löschen, bevor sie wieder neu eingebaut und genutzt wird.
- Auf möglicherweise fehlerhaften Festplatten keine Volume-Repair-Utilities laufen lassen oder Defragmentier-Tools verwenden.
- Bei Stromausfall eines RAID-Verbundes, bei einem möglicherweise fehlerhaften und nicht wieder hochzufahrenden Dateisystem oder bei fehlendem Zugriff auf die Daten auf keinen Fall die Volume-Repair-Utilities starten.
- Wenn eine Festplatte im RAID-Verband ungewöhnliche Geräusche macht, umgehend den Computer ausschalten und bei einer professionellen Datenrettungsfirma Hilfe suchen.
- Erstellen eines funktionierenden Backups, bevor Hardware- oder Software-Änderungen vorgenommen werden.
- Markieren der Platten und deren Position im RAID-Verbund.

Ein professioneller Datenretter wie Kroll Ontrack sollte ein wichtiger Bestandteil des „Disaster-Recovery-Plans“ eines Unternehmens sein. Das Management-Team bzw. Schlüsselpersonen des Unternehmens sollten über Rettungsmöglichkeiten ausreichend Bescheid wissen. Während eines Ausfalls ist es üblich, mehrere Rettungsversuche gleichzeitig zu starten. Der Schlüssel zum Erfolg ist es, den Datenretter so früh wie möglich zu involvieren, um die Daten so schnell wie möglich wieder verfügbar zu machen.

## Anhang

### Zuverlässigkeitskriterien

Zuverlässigkeit ist durch die Wahrscheinlichkeit definiert, dass ein System ohne Ausfall eine vorgegebene Betriebsdauer übersteht. Die nachfolgenden Angaben bieten Beurteilungskriterien für die Qualität von Informationssystemen.

### Mean Time Between Failures

Ein Maß für die Zuverlässigkeit ist die durchschnittliche Zeit bis zum Auftreten eines Fehlers bzw. zwischen zwei Fehlern. Die „Mean Time Between Failures“ (MTBF) wird normalerweise in Stunden angegeben. Sie besitzt allerdings nur eine begrenzte Aussagekraft, da sie auf Erfahrungswerten beruht, die nicht die Belastungen von individuell eingesetzten Komponenten berücksichtigen. Da ein System aus unterschiedlichen Komponenten besteht, die in Abhängigkeit von ihrer Belastung eine unterschiedliche Lebensdauer aufweisen, muss das Verhalten der Komponenten in die Berechnung der MTBF des Gesamtsystems eingehen. Die MTBF eines Gesamtsystems ergibt sich aus den MTBF-Zeiten der Einzelkomponenten, die mit ihrer angenommenen individuellen Belastung gewichtet sind.

### Verfügbarkeit

Die Verfügbarkeit gibt die Wahrscheinlichkeit an, das System zu einem bestimmten Zeitpunkt in einem funktionsfähigen Zustand anzutreffen. Einen wesentlichen Effekt auf die Gesamtverfügbarkeit des Systems stellt die Fehlerhäufigkeit dar. Auch sehr kurze Ausfälle können durch notwendigen Neustart von Applikationen zu längeren Verzögerungen führen.

Die Verfügbarkeit eines Gesamtsystems setzt sich aus der Funktionstüchtigkeit seiner Einzelkomponenten zusammen. Bei serieller Anordnung ist bei Ausfall einer Komponente die Verfügbarkeit des Systems gefährdet. Eine Komponente, die bei Ausfall das gesamte System zum Erliegen bringt, wird als „Single Point of Failure“ bezeichnet. Bei serieller Anordnung ist die Gesamtverfügbarkeit kleiner als die der Einzelkomponenten.

Die Verfügbarkeit setzt sich damit aus der prozentualen Wahrscheinlichkeit der Verfügbarkeit der Einzelkomponenten zusammen. So ergeben zwei in Reihe geschaltete Einzelkomponenten mit einer Verfügbarkeit von je 97,5%, was einem Ausfall von etwa 9 Tagen im Jahr entspricht, eine Verfügbarkeit des Systems von nur noch 95,06%, was einen Ausfall von 18 Tagen im Jahr bedeuten würde. Somit sind serielle Systeme sehr verletzlich, da der Ausfall nur einer Komponente ausreicht, um das Gesamtsystem zum Erliegen zu bringen. Durch Parallelsysteme können solche Ausfälle maskiert werden. Die Problematik wird insbesondere dann deutlich, wenn man sich vor Augen hält, dass ein System aus einer Vielzahl von Einzelkomponenten besteht und somit die Ausfallwahrscheinlichkeit stark ansteigt.

### Antwortzeiten

Die Antwortzeit stellt die Zeitspanne zwischen dem Ende einer Eingabe und dem Ende der Ausgabe dar. Damit hat sie entscheidende Wirkung auf die Benutzerakzeptanz eines Systems. Wenn der Nutzer aufgrund eines nicht verfügbaren oder überlasteten Systems spürbar warten muss, wird der Nutzer in seinem Arbeitsablauf behindert und empfindet die Arbeit mit dem System als störend.

### Ausfallzeiten

Ausfallzeiten setzen sich aus geplanten und ungeplanten Ausfallzeiten zusammen. Geplante Ausfallzeiten werden in der Regel durch routinemäßige Wartungsarbeiten ausgelöst, da es für viele Arbeiten an Hard- und Software notwendig ist, das System herunterzufahren. Sie können in Zeitfenstern bei niedriger Systemauslastung durchgeführt werden, damit bleiben die Folgekosten kalkulierbar. Gravierender wirken sich jedoch ungeplante Ausfälle aus, vor allem wenn sie zu Spitzenbelastungszeiten auftreten.

## Technische Maßnahmen

Nachfolgend werden technische Maßnahmen für ausfallsichere Systeme und Schutz der Daten aufgezeigt.

### Hardware-Redundanz

Redundanz ist das Vorhandensein von mehr als für die Ausführung der vorgesehenen Aufgaben an sich notwendigen Mittel. Die Ausfallsicherheit redundanter Systeme ergibt sich aus der doppelten Auslegung kritischer Einzelkomponenten. Um einen Ausfall des Gesamtsystems herbeizuführen, müssten beide gleichzeitig ausfallen. Bei zwei Komponenten mit einer Verfügbarkeit von jeweils 93% kann demnach bei redundanter Auslegung im statistischen Mittel eine Verfügbarkeit von 99,51% erreicht werden. Durch die redundante Auslegung von Prozessoren, Netzwerkkarten und Lüftern und dem Einsatz von unterbrechungsfreier Stromversorgung lässt sich immerhin eine Verfügbarkeit von 99% bei Unix-Systemen und noch 97% bei NT-Systemen erreichen. Dies entspricht einer Ausfallzeit von 88 bzw. 263 Stunden pro Jahr. Je nach unternehmensabhängiger Bewertung der Gefährdung kann die redundante Auslegung bis zu Ausweichrechenzentren führen.

### Redundanz in Speicherbausteinen

Arbeitsspeicher und Pufferspeicher sind flüchtige Speicher, somit geht deren Inhalt bei Störung des Rechnerbetriebs durch Stromausfall oder Absturz der Software verloren. Die geänderten Daten müssen deshalb in periodischen Abständen auf einen permanenten Speicher geschrieben werden. Durch die Generierung von Paritätsinformationen, dem „Error Correction Code“, kann in Speicherbausteinen eine Informationsredundanz erzeugt werden, die die Erkennung und Korrektur von Bitfehlern ermöglicht. Fortschrittliche Versionen verkraften sogar den Ausfall eines kompletten Speichermoduls, ohne dass der Server abstürzt.

### Sicherung der Stromversorgung

Grundvoraussetzung für den störungsfreien Betrieb von Computersystemen ist eine kontinuierliche Sicherstellung der Stromversorgung. Bei Spannungsschwankungen reagieren die Komponenten mit Datenverlust. Dabei ist ein Stromausfall gar nicht so unwahrscheinlich: Bei einer Ausfallquote von 0,02 Prozent pro Jahr summieren sich die Störungen der Stromversorgung durchschnittlich zu 105 Minuten Ausfall. Dabei sind weniger die eher seltenen „echten“ Stromausfälle ein Problem. Wesentlich übler wirken sich vielmehr die kurzzeitigen Schwankungen der Stromstärke und der Spannung aus. Sie dauern oft nur einige Millisekunden an, können aber empfindliche Systeme zum Absturz bringen.

Um strombedingte Ausfälle zu verhindern, wird eine Unterbrechungsfreie Stromversorgung (USV) zwischen Strom-netz und Computersystem geschaltet, sodass bei Netzschwankungen oder Stromausfall die Versorgung unmittelbar über die Batterien der USV erfolgt. Kurze Ausfälle können mit einer USV auf Basis von Akkumulatoren überbrückt werden. Für längere Zeiträume muss die Stromversorgung jedoch mit Hilfe von Generatoren sichergestellt werden. Die Überbrückungszeit muss dabei so bemessen sein, dass zumindest der Server ordnungsgemäß heruntergefahren werden kann oder Notstromaggregate anlaufen können. Die USV sollte dabei so geschaltet sein, dass ein Austausch der USV im laufenden Betrieb möglich ist.

Die USV-Systeme stellen selbst einen „Single Point of Failure“ dar, deshalb müssen sie bei hohen Sicherheitsanforderungen durch Parallelschaltung redundant ausgelegt sein. Dadurch soll sichergestellt werden, dass bei Ausfall einer USV alle Verbraucher ausreichend versorgt werden. Durch ein automatisches Herunterfahren der Systeme bei einem Stromausfall kann der Inhalt des Arbeitsspeichers gesichert und die offenen Dateien geschlossen werden.

Für den Schutz von Unternehmensnetzwerken haben sich drei Arten von USV-Systemen etabliert. Die einfachste und damit billigste Lösung stellt eine Offline-USV dar. Im Normalbetrieb wird der Strom direkt vom Netz zu den Verbrauchern geleitet und erst bei Unterschreiten einer bestimmten Spannung schaltet sie auf Batteriebetrieb um. Allerdings können solche Anlagen

in der Regel keine Spannungsschwankungen ausgleichen und benötigen für den Umschaltvorgang einige Millisekunden, was bei empfindlichen Systemen bereits zu Ausfällen führen kann.

Line-Interactive-Systeme können im Gegensatz zu Offline-Systemen Spannungsschwankungen ausgleichen und bieten damit einen besseren Schutz, sind aber auch teurer.

Die sicherste Lösung stellen Online-USV-Systeme dar. Die Rechner werden kontinuierlich aus den Akkumulatoren versorgt, die ständig aufgeladen werden. Damit werden Spannungsschwankungen völlig beseitigt und es sind auch bei Stromausfall keine Umschaltzeiten nötig. Allerdings besitzen Online-USV-Systeme einen schlechteren Wirkungsgrad und die Akkus werden stärker belastet.

## Netzabsicherung durch Firewalls

Wegen der zunehmenden Vernetzung muss sichergestellt werden, dass von außen keine Angriffe auf das firmeninterne Netz möglich sind. Um das Netz nach außen abzuschirmen, werden deshalb Firewall-Systeme eingesetzt. Diese erlauben, ähnlich der Zugbrücke einer Burg, den Zugang zum internen Netz an nur einer definierten Stelle. Die Firewall überwacht den gesamten Netzwerkverkehr von einem öffentlichen zu einem privaten Netz und lässt nur bestimmte Datenpakete anhand von Regeln passieren.

Normalerweise erfolgt die Überwachung des Netzwerkverkehrs, indem nur bestimmte IP-Adressen mit den entsprechenden Gegenstellen kommunizieren dürfen, d. h. es erfolgt eine Zugangskontrolle auf Netzwerkebene. Damit soll verhindert werden, dass Systeme durch vorsätzliche Handlungen in ihrer Funktion beeinträchtigt oder Daten manipuliert, ausgespäht oder zerstört werden.

Der Bereich hinter einer Firewall ist zwar geschützt, aber für einzelne Dienste noch erreichbar. Sie erlaubt eine Zugangskontrolle auf Benutzerebene, indem die Authentizität und die Zugangsberechtigung des Benutzers überprüft werden. Mittels einer Rechteverwaltung können Dienste festgelegt werden, mit denen eine Kommunikation stattfinden darf. Die Firewall sollte ebenfalls hochverfügbar ausgelegt sein und gegen Angriffe resistent sein, sonst stellt sie auch einen „Single Point of Failure“ dar.

**Kroll Ontrack GmbH**  
**Hauptsitz Böblingen**  
Hanns-Klemm-Str. 5  
71034 Böblingen  
Fon +49 (0)7031 644-0  
Fax +49 (0)7031 644-100  
Datenrettungs-Hotline:  
0800 10 12 13 14  
  
info@krollontrack.de  
[www.ontrackdatarecovery.de](http://www.ontrackdatarecovery.de)

**Kroll Ontrack S.a.g.l.**  
Piazza Boffalora, 4  
P.O. Box 191  
6830 Chiasso 3 Boffalora  
Fon +41 (0)91 68286-92  
Fax +41 (0)91 68286-94  
Datenrettungs-Hotline:  
0800 880 100  
  
info@krollontrack.ch  
[www.ontrackdatarecovery.ch](http://www.ontrackdatarecovery.ch)

**Kroll Ontrack GmbH**  
**Zweigniederlassung Österreich**  
Landstraßer Hauptstraße 71/2  
1030 Wien  
Fon +43 (0)1 71728-380  
Fax +43 (0)1 71728-110  
Datenrettungs-Hotline:  
0800 644 150  
  
office@krollontrack.at  
[www.ontrackdatarecovery.at](http://www.ontrackdatarecovery.at)

Copyright © 2008 Kroll Ontrack Inc.  
All Rights Reserved.

All other brands and product names are  
trademarks or registered trademarks of

**KROLL ONTRACK®**

**Vertrauen Sie auf die Besten.**