

Ontrack® Data Recovery



Fachinformation **Server Recovery**

KROLL ONTRACK®

Vertrauen Sie auf die Besten.

Die Kroll Ontrack GmbH:

Kroll Ontrack mit Sitz in Böblingen ist ein Anbieter von Services und Software in den Bereichen Datenrettung und Computer Forensik (elektronische Beweissicherung). Das Unternehmen Ontrack wurde 1985 in den USA gegründet und ist eine hundertprozentige Tochter des amerikanischen Risk-Consulting-Unternehmens Kroll Inc. (Hauptsitz New York), welches 2004 von Marsh & Mc Lennan Companies Inc. akquiriert wurde, einem führenden Anbieter von Risikomanagement und Versicherungsdienstleistungen.

Die speziell geschulten Experten von Kroll Ontrack machen logisch oder physikalisch beschädigte Daten auf allen Speichermedien durch die Bearbeitung in Labor und Reinraum wieder verfügbar. Die Daten werden mit eigens entwickelten Tools ausgelesen und anschließend auf einem beliebigen Medium gesichert. Kroll Ontrack kann dabei auf die branchenweit höchste Wiederherstellungsrate pro Jahr verweisen und nimmt dabei jährlich weltweit über 100.000 Anfragen zur Datenrettung von Kunden entgegen. Über 50 Ingenieure von Kroll Ontrack arbeiten zudem an der Weiterentwicklung der Tools und Softwareprodukte. Darüber hinaus ermöglicht das von Kroll Ontrack patentierte Remote Data Recovery exklusiv die Online-Datenrettung über gesicherte Modem- oder Internetverbindung.

Kroll Ontrack ist auch im Bereich der elektronischen Beweissicherung (Computer Forensik) tätig. Dazu zählt neben der Sicherstellung von Indizien auch die genaue Protokollierung aller durchgeführten Aktionen, um die Verwertbarkeit vor Gericht zu gewährleisten. Die Forensik-Experten von Kroll Ontrack rekonstruieren alle Eingriffe in die Unternehmensdaten und tragen so zur Schadensminimierung bei.

Zudem bietet Kroll Ontrack eine Reihe mehrfach ausgezeichneten Software-Produkte an. Ontrack EasyRecovery stellt gelöschte oder korrupte Daten wieder her. Ontrack PowerControls extrahiert Microsoft Exchange Mailboxen oder einzelne Inhalte schnell und einfach direkt aus dem .edb-File ohne Aufsetzen eines parallelen Exchange Servers. Ontrack DataEraser garantiert eine sichere Datenlöschung.

Niederlassungen befinden sich in Deutschland, der Schweiz, Österreich, Polen, Italien, Frankreich, Großbritannien, Spanien, Australien, Japan, Kanada und den USA.

Sie finden Kroll Ontrack im Internet unter:

www.krollontrack.de

www.ontrack.de

Kroll Ontrack GmbH
Hanns-Klemm-Straße 5
71034 Böblingen

Kostenfreie Rufnummer:

0800 10 12 13 14 (D)

0800 644 150 (A)

0800 880 100 (CH)

800 44 00 33 (I)

oder

+49 7031 644 150 (andere Länder)

Inhalt

Kapitel 1: Speicherlandschaft heute	5
Speicherbedarf und seine Bewältigung	5
Wertvolle Daten in Serverumgebungen	6
Datensicherung in deutschen Unternehmen	8
Kapitel 2: Gefährdete Speichermedien	9
Magnetisch und optisch gespeicherte Daten auf stationären Systemen	9
Speichermethoden	10
Kapitel 3: Speichersysteme	13
RAID-Systeme - die Lebensader der Geschäftstätigkeit	13
Network-Attached-Storage-Systeme (NAS)	13
Storage Area Network (SAN)	14
Kapitel 4: Risiken von Speicherlösungen	15
RAID-Fehler und andere Ausfälle	15
Ausfälle kosten Zeit und Geld	18
Mögliche Fehler, die eine Datenrettung erforderlich machen	19
Fallbeispiel: Bedienerfehler	20
Fallbeispiel: Saveset kann nicht zurückgespielt werden	21
„Sonderfall“ Exchange Server	21
Fallbeispiel: Mail-Datei im Exchange-Server beschädigt	21
Remote-Datenrettung (RDR)	25
Fallbeispiel: Controllerfehler	25
Funktionsweise der RDR	25
Wie sicher ist die RDR?	26
Mindestvoraussetzungen für RDR	26
Praktische Anwendungsfälle für die Online-Datenrettung	27
Kapitel 5: Wann brauchen Sie einen Datenrettungs-Spezialisten?	28
Worauf kommt es bei der Auswahl eines Datenretters an?	29
In fünf Schritten zur Wiederherstellung der Daten	30
Datenrettungs-Tipps für Server	31
Datenrettung als Bestandteil des Disaster Recovery Plans	32
Referenzen	34

Kapitel 1: Speicherlandschaft heute

Speicherbedarf und seine Bewältigung

Professionelle und effiziente Datenspeicherung ist längst nicht mehr nur ein Thema für große Unternehmen. Auch kleine und mittlere Unternehmen sind heute auf die ständige Verfügbarkeit der elektronisch abgelegten Informationen angewiesen; auch sie werden durch den drohenden Verlust wichtiger Geschäftsdaten bedroht.

Der Speicherbedarf eines Unternehmens hängt natürlich nicht zuletzt von seiner Größe und der Branche ab. Allen gemein sind jedoch die gesetzlichen Vorschriften, die den Speicherbedarf unweigerlich immer weiter in die Höhe treiben. Hinzu kommt eine stetig steigende Flut von E-Mails, die für geschäftliche Vorgänge wichtig sind. Entsprechend wächst die Menge der gespeicherten Daten unablässig an. Pro Tag entstehen weltweit rund 52 Milliarden Megabyte an Daten –Tendenz weiter steigend.

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

Aktuellen Untersuchungen zufolge nutzen viele Mittelständler, insbesondere Unternehmen mit weniger als 500 Mitarbeitern, hauptsächlich direkt angeschlossene Speichersysteme. Gleichzeitig gibt es einen Trend zur Konsolidierung verteilter Speicher bei Unternehmen, die mehrere Server einsetzen. So wird der Bedarf an hochwertigen Speicherlösungen weiter wachsen – Experten gehen sogar davon aus, dass der Bedarf an Storage im Mittelstand deutlich stärker wachsen wird als bei Großunternehmen.

Nicht nur die bereits erwähnten gesetzlichen Regelungen und Vorschriften, die beispielsweise ausführliche Dokumentationen und eine langfristige Speicherung der Geschäftsvorgänge bindend vorschreiben, tragen zu diesem Trend bei. Gerade auch der zunehmende E-Mail-Verkehr fordert mit teilweise umfangreichen Anhängen wie Präsentationen oder Bildern seinen Tribut. Hinzu kommen Daten, die durch Customer-Relationship-Management-Systeme (CRM), Supply-Chain-Management- (SCM) oder Enterprise-Resource-Planning-Lösungen (ERP) über Kunden, Lieferanten und Produktionsabläufe erfasst werden.

Von Unternehmen wird heute weit mehr geschäftliche Transparenz verlangt, als dies noch vor wenigen Jahren der Fall war. Es müssen daher mehr Daten bereitgestellt und revisionssicher gespeichert werden. Als „Faustregel“ kann mittlerweile von einer jährlichen Verdoppelung bis Verdreifachung des Speicherbedarfs der Unternehmen ausgegangen werden.

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. Beim SAN handelt es sich um ein spezielles Speichernetzwerk, bei dem alle Server über Hochgeschwindigkeitskabel und Switches mit zentralen Speichereinheiten verbunden sind. Der Vorteil dieser aufwändigen Architektur: Das lokale Netzwerk wird nicht zusätzlich belastet.

Im Gegensatz dazu findet beim NAS der Datenaustausch über das lokale Netzwerk statt. Network Attached Storage (NAS) wird meist in großen Unternehmen verwendet. Dort sorgen an das lokale Netzwerk angeschlossene Massenspeichereinheiten für die Erweiterung der Speicherkapazität. NAS funktioniert ähnlich wie ein Dateiserver, ist aber hoch skalierbar, einfacher zu administrieren und weniger aufwändig bei der Installation.

NAS kann entweder eigenen Festplatten-Speicher besitzen (NAS Appliance) oder an ein Storage Area Network (SAN) angeschlossen sein (NAS Head) und Speicher von angeschlossenen Storage-Systemen nutzen.

Wertvolle Daten in Serverumgebungen

Unternehmen speichern heute ihr gesamtes Wissen fast ausschließlich elektronisch. Ob Buchhaltungsdaten, Planungsdaten, Konzepte oder Budgets – von Patenten über Schriftwechsel bis zu Angeboten und Rechnungen befinden sich alle wichtigen und unternehmenskritischen Daten auf den Firmenservern.

Immer mehr Teile eines Unternehmens sind so abhängig von der Struktur der Firmen-Server und des Speichervolumens. Manche Firmen sind komplett von ihrem Datenbank-System abhängig. Hier werden Finanzdaten, Auftragsdaten oder Kundendaten verwaltet. Wieder andere Firmen sind einzig und allein von ihrem E-Mail-Server abhängig, ein nicht weniger kritischer Zustand. Manche Telefon-Systeme wandeln mündliche Nachrichten in E-Mail-Notizen um, wobei der E-Mail-Server als Teil des Kommunikations-Systems fungiert. Zudem sind die Systeme heutzutage auch Speichersysteme für alle Dokumente, die ein Anwender erstellt.

Von der einfachen internen Kommunikation über wichtige Verkaufsgespräche mit Kunden bis zu Buchhaltungs- und Rechnungsfragen und wichtigen Unternehmensentscheidungen ist die E-Mail – und damit der Microsoft Exchange Server – in jede Station des Geschäftslebens einbezogen. Heutige Unternehmen können ebenso wenig ohne E-Mail auskommen, wie sie ohne Telefon oder Elektrizität auskommen könnten. Darüber hinaus sorgt die E-Mail nicht nur dafür, dass Mitarbeiter und Geschäftsprozesse effizienter sein können, sondern sie ist auch die kostengünstigste Form der Kommunikation.

Beachten Sie diese Statistiken:

- Nach einer Studie von *The Radicati Group, Inc.* aus dem Jahr 2004 gibt es weltweit rund 980 Millionen aktiver E-Mail-Konten. Davon sind 49% Mailboxen in Unternehmen.
- Im Jahr 2002 wurden, einer Untersuchung des Marktforschungsunternehmens *IDC* täglich durchschnittlich 31 Milliarden E-Mails verschickt. Bis 2006 wird diese Zahl auf dramatische 60 Milliarden pro Tag ansteigen.
- Der durchschnittliche US-amerikanische Angestellte sendet und empfängt zwischen 60 und 200 Nachrichten pro Tag, berichtet Kevin Craine in dem Artikel „*Here Come the Lawyers. Is your IT Department Ready?*“
- Der *Collaborative Electronic Notebook Systems Association (CENSA)* zufolge, einer internationalen Industrie-Statistik-Organisation, wird sich in den nächsten zehn Jahren die Anzahl der elektronisch gespeicherten Dokumente alle 60 Minuten verdoppeln.
- In einigen Industrien gibt es im Durchschnitt mehr als eine Mailbox pro Angestellten. In der Telekommunikationsindustrie sind es beispielsweise 1,14 Mailboxen pro Mitarbeiter, bei Hightech- und Finanzdienstleistern sind es 1,07 Mailboxen pro Mitarbeiter.

Es ist eindeutig, Unternehmen werden weltweit mit E-Mail überflutet. Und diese E-Mails müssen verwaltet werden – aus rechtlichen, strukturellen und geschäftlichen Gründen.

Geschäftsanforderungen an das Wiederherstellen von E-Mail

Geschäftliche Gründe sind die treibende Kraft bei der Forderung nach E-Mail-Management. Der Hauptgrund dafür ist, dass viele Unternehmen Ihre E-Mails auf nur einem Server speichern. Das ist das Ergebnis einer In einer Umfrage unter 177 E-Mail-Administratoren, die 250 oder mehr Mailboxen verwalten. In dieser Umfrage hat Kroll Ontrack herausgefunden, dass immerhin 37 Prozent der Unternehmen nur einen Server zur E-Mail-Speicherung einsetzen.

Da die Mitarbeiter auch Mails löschen, die wichtig für ihre Tätigkeit sind, steigt die Zahl der Anfragen bei den IT-Abteilungen, diese Mails – die in vielen Fällen nur noch als Backup existieren – wiederherzustellen. Während das Speichern von E-Mails auf dem Server und das Setzen von Mailbox-Größenbeschränkungen den Speicherwaltungsbedürfnissen der IT entgegenkommt, erzeugt dieses Vorgehen gleichzeitig einen Konflikt mit den Geschäftsanforderungen der Angestellten. Das führt wiederum zu einer Erhöhung der Zahl der Anfragen nach der Wiederherstellung von Mail-Nachrichten vom Backup.

Eine sichere und unmittelbare Verfügbarkeit dieser Daten ist daher für Unternehmen heute bereits überlebenswichtig. Dennoch ist in vielen Firmen das Bewusstsein für den Wert dieser Daten nur gering ausgeprägt – man wiegt sich in der Sicherheit, dass die hochwertigen Komponenten auch weiterhin ihren Dienst tun werden.

Während der private Anwender oder das Kleinunternehmen seine Daten noch auf der Festplatte des PCs lagert und im Falle eines Schadens – sei es durch Fehlbedienung oder Ausfälle von Hard- oder Software – mit dem Verlust seiner wesentlichen Betriebsdaten rechnen muss, fühlt sich der IT-Verantwortliche in größeren Unternehmen zunehmend besser geschützt. Schließlich setzt er auf hochwertige RAID-, NAS- oder SAN-Systeme. Was soll da schon schief gehen? Die Verfügbarkeit der wichtigen kaufmännischen und produktions-technischen 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 schwerwiegenden 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.

Auch wenn sich Unternehmen darüber im Klaren sind, wie wichtig ihre Daten sind, gibt es doch Bereiche, in denen die Notwendigkeit einer professionellen Speicher- und Sicherungs-Lösung nicht sofort offensichtlich wird. Einer dieser Bereiche ist die Speicherung von E-Mails – immerhin müssen Geschäftsbriefe zehn Jahre aufbewahrt werden. Entsprechend stellen sich gerade mittelständische Unternehmen die Frage, ob sie E-Mails als Geschäftsbriefe betrachten müssen und ob sie pauschal alle E-Mails archivieren können. Hinzu kommt die Frage nach der Sicherung und Wiederherstellbarkeit der Exchange-Daten. Eine frühzeitige Klärung dieser Fragen kann für Unternehmen essentiell sein, denn nach fundierten Expertenschätzungen gelingen 15 bis 20 Prozent aller Backups nicht. Das Recovery würde im Fehlerfall nicht funktionieren.

An die professionelle Datenrettung wird meist viel zu spät gedacht – oft gehen Unternehmen davon aus, dass eine Datenrettung überhaupt nur bei Desktop-Systemen funktioniert und die Festplatte mit den sensiblen Daten eingeschickt werden muss.

Beide Vermutungen sind längst überholt. Professionelle Datenretter können heute auch die Daten von RAID-, NAS- oder SAN-Systemen wiederherstellen. Häufig kann dies sogar innerhalb weniger Stunden mittels der 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 defekte Speichermedien. Diese können soweit 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 Datenrecherche eingeleitet werden.

Die Gründe für Datenverlust können vielfältig sein: Daten können durch Katastrophen wie zum Beispiel Brand, Explosion oder Wasserschaden verloren gehen. Datenträger versagen durch Überalterung oder technische Defekte. Sehr oft wird der Verlust auch durch Unachtsamkeit wie versehentliches Löschen oder Formatieren verursacht. Auch durch Angriffe von Computerviren und Computerwürmern können Daten verloren gehen.

Kroll Ontrack ist darauf spezialisiert, Daten wiederherzustellen, die durch mechanische und elektromagnetische Defekte, Bedienungsfehler, Viren, Naturkatastrophen, Computerkriminalität oder ähnliche Ereignisse nicht mehr verfügbar sind. Das Unternehmen hat Werkzeuge für die Datenrettung von nahezu jeglichen Speichermedien und Betriebssystemen entwickelt und bietet einen herausragenden Service mit einer hohen Erfolgsquote.

Datensicherung in deutschen Unternehmen

Wie eine im Dezember 2004 erstellte Studie¹ feststellte, gehören Backups zwar zum unverzichtbaren Alltag der IT-Abteilungen, doch in Fragen der Priorität, Art und Häufigkeit existieren nach wie vor große Unterschiede. 98,5 Prozent der Befragten berücksichtigen bei ihren Backups die Fileserver, Applikationsserver und Webserver. 74,9 Prozent gaben gleichzeitig an, keine Desktop-PCs zu sichern und für 83,3 Prozent gehörten Notebooks nicht in den Datensicherungsplan. Nur gut 47,8 Prozent führen ein tägliches System-Backup durch, bei immerhin 42,4 Prozent werden Systemsicherungen einmal pro Woche oder sogar seltener durchgeführt. 67,9 Prozent der Befragten sehen keine Notwendigkeit für häufigere Backups oder führten mangelnde Ressourcen und eine Beeinträchtigung der Netzwerk- bzw. Serverleistung als Gründe an.

Gleichwohl fällt bei 50,7 Prozent der Server ein bis zweimal im Jahr aus, bei immerhin 11 Prozent sogar häufiger. Die so hervorgerufenen Schäden sind beträchtlich: 30,7 Prozent der Befragten gaben ihre Verluste im Hinblick auf Produktivität und Umsatz mit bis zu 10.000 Euro pro Ausfall an, 48 Prozent konnte ihre Verluste nicht beziffern.

Insgesamt ist ein Wechsel der Prioritäten notwendig: War bisher die Bewältigung der stark ansteigenden Datenmengen wichtig, stehen nun Fragen nach sicheren Backup-Möglichkeiten und unterbrechungsfreier Gewährleistung der 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 Magnetbändern 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.

¹ Umfrage von Symantec in Zusammenarbeit mit research+consulting zum Thema „System- und Datenbackup“ bei Unternehmen mit mehr als 150 Mitarbeitern, Dezember 2004.

Kapitel 2: Gefährdete Speichermedien

Grundsätzlich sind elektronisch gespeicherte Daten stärker gefährdet als Informationen, die auf Papier aufbewahrt werden. Zwar kann auch ein Aktenordner versehentlich weggeworfen werden oder einem Brand zum Opfer fallen – es gibt aber viel mehr mögliche Ursachen für den Verlust digitaler Daten. Hinzu kommt, dass digitale Informationen bis auf wenige Ausnahmen entweder in einem flüchtigen Speicher liegen, dessen Inhalt verloren geht, sobald die Stromzufuhr unterbrochen wird, oder auf Medien, die Daten magnetisch oder optisch aufzeichnen (Diskette, Festplatte, Magnetband, CD, DVD). Die Struktur solcher Medien kann durch eine Reihe von äußeren Einflüssen verändert werden (mechanisch, thermisch, magnetisch). Geschieht dies, so werden auch die gespeicherten Daten verändert. Wird z.B. durch den Magnetismus, den ein Lautsprecher abgibt, nur die geringe Anzahl von fünfzig Bytes einer Programmdatei auf einer Diskette verändert, kann dies dazu führen, dass diese Anwendung nicht mehr funktionsfähig ist.

Magnetisch und optisch gespeicherte Daten auf stationären Systemen

Die magnetische Speicherung von Daten hat eine lange Tradition, die bis zu den Kernspeichern von Großrechnern der 50er Jahre zurückreicht. Das Prinzip hat sich nicht wesentlich verändert: Jedes einzelne Bit (die kleinste digitale Informationseinheit, die jeweils den Wert 1 oder 0 darstellen kann) wird durch eine definierte Menge an Partikeln eines magnetisierbaren Materials dargestellt. Diese Menge ergibt sich aus der Fläche auf dem Datenträger, der wiederum als kleinste physikalische Speichereinheit definiert wird. Der Unterschied zwischen 1 und 0 wird durch die unterschiedliche Polung ausgedrückt. Ist die Mehrzahl der Partikel in einem Bereich in Nord-Süd-Richtung ausgerichtet, gilt dies als 0, ist sie in west-östlicher-Richtung gepolt, als 1.

Datenspeicher physikalisch betrachtet

Ausgerichtet werden die magnetisierbaren Partikel durch elektrische Spannung. In einer Festplatte ist dafür der Schreib-/Lesekopf zuständig, der die Polung von Partikeln in Mikrosekundengeschwindigkeit verändert. Beim Lesen der Daten wird dann je nach der Polung im Schreib-/Lesekopf eine negative oder positive Spannung erzeugt. Diese wird dann als Wert 1 oder 0 interpretiert.

Zu Beginn der Festplattenära wurden Platten mit Durchmessern von bis zu 12 Zoll (= ca. 30 cm) eingesetzt. Entsprechend groß waren die Bereiche, die für die Speicherung von einem Byte genutzt wurden. Bei modernen Festplatten sind diese Bereiche extrem kleiner geworden. Eine übliche 2,5-Zoll-Festplatte mit 40 GByte Kapazität besteht beispielsweise aus drei einzelnen Leichtmetallplatten, die jeweils auf der Ober- und Unterseite beschrieben werden. Jede Oberfläche speichert rund 2,5 GByte. Damit werden auf nur 400.000 mm² immerhin 2,7 Milliarden Bytes abgebildet. Die Datendichte pro Quadratmillimeter liegt bei über 6.500 Bytes.

Inzwischen gibt es durch ein neues Aufzeichnungsformat, bei dem die Daten „hochkant“ geschrieben werden, noch weitaus höhere Speicherdichten. Die dazu notwendige Technologie heißt: "Perpendicular Recording", zu deutsch: "Senkrechte Aufzeichnung". Mit dieser neuen Technologie ist es möglich, die Kapazitäten der Festplatten bis auf das Zehnfache zu steigern.

Derzeit sind auf den Festplatten die Bits parallel zur Rotationsrichtung angeordnet - sie liegen gewissermaßen ausgestreckt auf der Festplatte. Um höhere Speicherkapazitäten zu erreichen, müssen nun diese Bits immer näher aneinanderrücken. Dabei entsteht ein Effekt wie an einem vollbesetzten Strand – man hat kaum noch Platz für das eigene Handtuch und kollidiert mit dem Nachbarn. Bei den Bits wird diese „Strand“-Situation als superparamagnetischer Effekt beschrieben, bei dem die Bits ihre gegenseitige magnetische Polung beeinflussen und so Datenverluste verursachen.

Bei der senkrechten Aufzeichnung folgt man nun einer ganz einleuchtenden Idee: Man lässt die Bits nicht mehr liegen, sondern aufstehen, wodurch deutlich mehr Platz zur Verfügung steht. Sind die Bits senkrecht zur Rotationsrichtung aufgestellt, können daher viel mehr Bits auf der gleichen Fläche angeordnet werden, ohne dass sie sich gegenseitig beeinflussen.

Beeinflusst werden Magnetpartikel übrigens nicht nur durch magnetische Einwirkung. Der klassische ‚Headcrash‘, bei dem ein Schreib-/Lesekopf die Oberfläche berührt, führt zu einer physikalischen Beschädigung und damit zu Datenverlust. Hitze und Feuchtigkeit, die im Katastrophenfall einwirken, verändern meist die Struktur des Trägermaterials, so dass sich entweder die Magnetschicht teilweise ablöst oder aber der Träger (die ‚Platte‘) nicht mehr eben ist oder „eiert“, was einen Headcrash zur Folge haben kann.

Die Daten eines Unternehmens werden heutzutage in der Regel zentral gelagert. Der so genannte ‚Fileserver‘ muss dabei aber nicht unbedingt ein Rechner mit einem Festplattensystem sein. Die Datenspeicherung kann durchaus auch verteilt stattfinden – z.B. auf mehreren Festplattensystemen an verschiedenen Orten oder in einem eigenen oder angemieteten Data-Center. Zum Einsatz kommen dabei meist so genannte ‚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 erscheinen lässt und durch automatisiertes Spiegeln und Verteilen von Daten für eine Redundanz der Informationen sorgt.

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 magneto-optische Träger (MOs) eingesetzt. Diese sind zwar unempfindlich gegenüber externem Magnetismus, aber vor Datenverlust durch mechanische Beschädigung oder Hitze nicht gefeit.

Speichermethoden

Grundsätzlich unterscheiden sich die Speichermethoden bei Platten und Bändern voneinander. Während bei Platten (einschließlich CD-ROMs, DVDs und MOs) die Daten wahlfrei geschrieben und gelesen werden können, sind sie auf Bändern sequenziell gespeichert. Das bedeutet, dass einzelne Datenbereiche bzw. ganze Dateien auf einem Band nur durch Vor- und Rücklauf angesteuert werden können. Bei einer Festplatte sorgt das jeweilige Dateisystem dafür, dass der physikalische Aufbewahrungsort eines Datenpartikels in Tabellen abgelegt wird. Diese Information wird dann zur Ansteuerung der gewünschten Information genutzt.

Bei einer klassischen Festplatte ist das Dateisystem dafür verantwortlich, eine solche Tabelle (in der DOS-/Windows-Welt File Allocation Table = FAT genannt) zu erzeugen und zu verwalten. Was PC-Anwender möglicherweise als ‚Formatieren‘ kennen, ist der Vorgang, bei dem eine solche Tabelle angelegt wird. Vereinfacht dargestellt: Einer Speicherfläche für eine Dateneinheit (in der Regel: ein Byte) wird eine feste Adresse zugeschrieben. Üblicherweise wird dazu die Oberfläche der Festplatte in Spuren unterteilt. Diese Spuren bestehen aus konzentrischen Kreisen, die eine festgelegte Breite haben. Eine weitere Unterteilung erfolgt in die so genannten Sektoren. Sie unterteilen die Spuren in einzelne „Tortestücke“. Auf diese Weise kann ein bestimmter Speicherort auf der Festplatte, beispielsweise der Sektor 112 auf Spur 18, gezielt angesteuert werden.

Die kleinsten adressierbaren Einheiten dieser FAT-Dateizuordnungstabelle sind die Cluster. Ein Cluster fasst mehrere Sektoren zusammen. Die Anzahl hängt dabei von der Partitionsgröße und dem Dateisystem ab. Die maximale Größe einer Partition berechnet sich dabei wie folgt: max. Anzahl der FAT Einträge * Sektoren pro Cluster * 512 Byte/Sektor.

Die verschiedenen FATs

Der „Urvater“ der heute in der Windows-Welt genutzten „File Allocation Tables“ ist **FAT12**. FAT12 wurde 1980 als Dateisystem für QDOS, den direkten Vorläufer von MS-DOS, von Seattle Computer Products entwickelt. Mit ihm können 2^{12} oder 4.096 Cluster adressiert werden.

Sein Nachfolger wurde 1983 der von Microsoft entwickelte **FAT16**. Bei einer FAT16-Partition können maximal 2^{16} Cluster adressiert werden. Dies ist gleichbedeutend mit 65.536 Einträgen in der FAT oder auch 65.536 Clustern, die benannt werden können.

Folgende Tabelle veranschaulicht die Berechnung:

PARTITIONSGRÖÙE IN MB	SEKTOREN PRO CLUSTER	BYTES PRO CLUSTER
16 – 127	4	2.048
128 - 255	8	4.096
256 - 511	16	8.192
512 - 1023	32	16.384
1024 - 2047	64	32.768

FAT32 ist eine Weiterentwicklung des FAT16-Dateisystems von Microsoft. Er erschien 1997 und wurde mit Windows 95B eingeführt. Die Datenbreite wurde von 16 auf 32 Bit erweitert. Entsprechend stehen mehr Einträge für die Datei-Zuordnungstabelle zur Verfügung. FAT32 bietet zwei grundlegende Vorteile: Durch die Erweiterung der Datenbreite auf 32 Bit können wesentlich größere Partitionen verwendet werden als mit FAT16. Außerdem verwendet FAT32 wesentlich kleinere Cluster, wodurch Festplattenspeicher im Vergleich zu FAT 16 effizienter genutzt wird. FAT32 kann durch die höhere Datenbreite 2^{28} bzw. 268.435.356 Cluster adressieren.

Diese Darstellung gilt in dieser Form natürlich nur für FAT-Dateisysteme. Festplatten, die mit einem anderen Dateisystem, beispielsweise dem aus der Windows-Welt bekannten NTFS, arbeiten, können hier andere Ordnungsstrukturen aufweisen.

NTFS steht für "New-Technologie-File-System" und wurde analog zum Betriebssystem Windows NT von Microsoft entwickelt und eingeführt. Im Gegensatz zu FAT16 oder FAT32 basiert NTFS auf 64 Bit Datenbreite. NTFS ist nicht nur das Dateisystem für Windows NT, sondern auch für Windows 2000 und Windows XP.

NTFS nutzt ein gegenüber FAT deutlich verbessertes Indexsystem namens MFT (Master-File-Table) und bietet die Möglichkeit, ein Software-RAID-System zu nutzen und so mehrere physikalische Festplatten zusammenzufassen.

NTFS5 ist das Dateisystem von Windows 2000 und, trotz des irreführenden Namens, zu keinem anderen Betriebssystem kompatibel. NTFS5 stellt eine Erweiterung von NTFS(4) von Windows NT4 dar. Als Erweiterungen sind die Datenverschlüsselung und die dynamische Datenkompression besonders zu erwähnen. Das "neue" Dateisystem unterstützt. Um Platz zu sparen, können Dateien, Verzeichnisse oder ganze Partitionen dynamisch komprimiert werden. Mit der dynamischen Echtzeitverschlüsselung können einzelne Dateien, Verzeichnissen oder Partitionen zusätzlich abgesichert werden. Es ist jedoch nicht möglich, verschlüsselte Bereiche zusätzlich auch zu komprimieren.

Es kann nach der Datenverschlüsselung zu Problemen mit Defragmentierungsprogrammen kommen. Diese verweigern möglicherweise beim Auffinden verschlüsselter Daten ihren Dienst. Aus Sicherheitsgründen sollte die Echtzeitverschlüsselung nicht auf die Systempartition angewendet werden. Ebenso können komprimierte Daten nicht zusätzlich verschlüsselt werden.

Gelöschte Daten

Wird in einem Dateisystem eine Datei gespeichert, sucht das Betriebssystem nach einem freien - genauer: freigegebenen Cluster und schreibt die Bytes der Datei dort hinein.

Wird eine Datei gelöscht, gibt das Dateisystem diesen Sektor wieder frei – aber: die physikalische Datenspeicherung, also die Polung der Magnetpartikel wird dabei nicht verändert. Gelöschte Dateien werden nur aus dem „Inhaltsverzeichnis“ der Festplatte gelöscht, damit der benutzte Speicherplatz überschrieben werden kann.

Da ein Cluster idealtypisch (dies variiert von Betriebssystem zu Betriebssystem und von Festplattensystem zu Festplattensystem) 512 Byte speichert und eine Datei in der Regel aus Tausenden von Bytes (= KByte) besteht, müssen mehrere Cluster beschrieben werden. Da oft nicht der physikalisch nächstliegende Sektor frei ist, muss ein Ort für die Folge-Bytes gesucht werden. Deshalb verzeichnet die Dateitabelle nicht nur, welche Cluster frei(gegeben) sind und in welchen Clustern welche Bytes liegen, sondern auch, in welchem Cluster eine Datei beginnt und wo sie weitergeht. So entsteht eine Kette aus Clustern, die aufeinander verweisen und nacheinander ausgelesen die Datei ergeben, die benutzt werden soll.

Diese grundsätzliche Methode hat aber auch Nachteile. Da in Wirklichkeit eine Datei nicht nur einen Cluster umfasst, sondern um ein Vielfaches größer ist, kann es sein, dass der letzte Rest einer Datei einen Cluster nicht ausfüllt. Es bleibt Platz (der so genannte Slack) übrig, der eventuell noch physikalisch Daten enthält. Diese werden jedoch im Dateisystem nicht mehr zugeordnet, da sie zu keiner aktuell genutzten Datei gehören.

Da diese Daten physikalisch noch vorhanden sind, also in Form unterschiedlicher Polung von Magnetpartikeln existieren, können sie mit großer Sicherheit wiederhergestellt werden. Das gilt genauso auch für Daten auf Magnetbändern und ähnlich für optisch gespeicherte Daten.

Auch aus formatierten Festplatten und beschädigten Datenträgern lassen sich Daten gezielt wiederherstellen, wobei auch zunächst nicht mehr lesbare, korrupte Dateistrukturen kein dauerhaftes Hindernis bieten. Selbst bei beschädigten Datenträgern liegt die Quote der erfolgreichen Datenwiederherstellung bei rund 80 Prozent.

Kapitel 3: Speichersysteme

RAID-Systeme - die Lebensader der Geschäftstätigkeit

Ein RAID-System (Abkürzung für „Redundant Array of Inexpensive Disks“, oft aber auch „Redundant Array of Independent Disks“) dient zur Organisation mehrerer physikalischer Festplatten eines Computers zu einem leistungsfähigen und sicheren logischen Laufwerk. Durch solche Disk-Arrays sollen Systemstillstandzeiten durch Festplattenausfälle verhindert oder doch zumindest minimiert werden.

Mittlerweile gehören RAID-Systeme unterschiedlichster Kapazitätsgrößen auch in kleinen und mittleren Betrieben zur Standardausstattung. RAID-Systeme werden mit unterschiedlichen Anschlussarten als »Direct Attached Storage« (DAS), NAS- (Network Attached Storage) oder SAN-System (Storage Area Network) genutzt.

Ein Festplatten-Array bietet nicht nur mehr Speicherplatz, sondern ermöglicht einen schnellen Datenzugriff und mindert vor allem das Datenverlustrisiko. Ein typisches, kleines Disk-Array ist heute mit vier bis fünf Platten ausgestattet. Die entsprechenden Storage-Systeme werden bei kleineren Unternehmen meist direkt in den Server eingebaut – eine komfortable Lösung, die jedoch auch ein Problem birgt, denn während eines Ausfalls werden so möglicherweise mehrere Abteilungen lahm gelegt.

Der Einsatz von RAID-Systemen hängt weniger von der Größe des Unternehmens ab, als von den Anforderungen an Verfügbarkeit und Wiederanlaufzeit. Die Geschäftsprozesse bestimmen die Notwendigkeit eines RAID-Systems.

Der nächste Schritt zu erhöhter Ausfallsicherheit ist daher der Einsatz externer RAID-Systeme, etwa als NAS oder SAN, die durch günstigere Lösungen auch vermehrt Einzug in den Mittelstand halten. Durch RAID-Systeme kann die Betriebssicherheit, Leistung und Kapazität von Massenspeichern erhöht werden. Die Möglichkeiten, fehlertolerante RAID-Systeme aufzubauen, sind in den so genannten RAID-Leveln standardisiert. Diese Level repräsentieren verschiedene Kombinationen aus Leistung, Zuverlässigkeit und Kosten. Durch die Verknüpfung mehrerer Festplatten im RAID erhält man eine

- Erhöhung der Datensicherheit (Redundanz)
- Steigerung der Transferraten (Performance)
- Aufbau großer, logischer Laufwerke

Network-Attached-Storage-Systeme (NAS)

NAS-Systeme zeichnen sich durch relativ geringe Betriebskosten und eine schnelle Inbetriebnahme aus. Hier wird im Prinzip einfach ein Kasten mit einem Netzwerkadapter an die bestehende Infrastruktur angeschlossen.

Mit vernetzten NAS-Speichersystemen soll einerseits eine Konsolidierung des Speicherplatzes erreicht und andererseits eine bessere Zusammenarbeit und Verteilung gewährleistet werden. Speicher werden zusammengeführt, um so kostengünstiger eingesetzt und zentral verwaltet zu werden. Im Durchschnitt sollen 30 bis 50 Prozent aller Daten auf Plattensystemen aus Home-Verzeichnissen, gemeinsam genutzten Dokumenten oder anderen unstrukturierten Daten bestehen, die über ein NAS zusammengeführt und den Anwendern zentral im Netzwerk zur Verfügung gestellt werden können. Der grundlegende Vorteil der NAS-Technologie liegt im gemeinsamen Datenzugriff von unterschiedlichen Systemen und in einer effizienten Nutzung der Bandbreiten und der Zugriffszeiten sowie der Verfügbarkeit der Daten. NAS-Systeme bestehen zumeist aus einer oder mehreren Festplatten die entweder als RAID (Redundant Array of Independent Disks) oder als JBOD (Just a Bunch Of Disks) konfiguriert sind.

Die Vernetzung der NAS-Systeme erfolgt über IP-Netze, die nahezu überall als Ethernet-LANs implementiert sind. LANs stellen als ausgereifte und etablierte Technologie eine häufig genutzte Alternative zu den Kanalnetzen der SAN-Architektur dar. Sie können relativ problemlos ausgebaut und verwaltet werden, da die benötigte Kompetenz und Infrastruktur in den meisten Unternehmen bereits vorhanden ist. Daten lassen sich problemlos transportieren, allerdings ist die Leistung bei hoher Netzwerkauslastung in IP-Netzen nicht vorhersehbar.

Der Zugriff auf die Daten erfolgt im NAS per Dateizugriff. Beim Dateizugriff erfolgt die Adressierung der Daten, im Gegensatz zum Blockzugriff, über ihren Namen. Dadurch wird ein spezieller Fileserver nötig, der die Lese- und Schreibenfragen verwaltet und intern wiederum im Blockzugriff auf die Daten zugreift. Die angeschlossenen Rechner kennen die physikalische Adresse der Dateien nicht, sondern senden eine Namensanfrage an den Fileserver. Dieser verwaltet die entsprechenden Aufrufe. So können mehrere Systeme gleichzeitig auf den Datenbestand zugreifen.

Dedizierte NAS-Systeme dienen nur als Fileserver und verfügen über darauf spezialisierte Betriebssysteme wie NFS (Network File System) für Unix oder CIFS (Common Internet File System) für Windows. Sie benötigen keine zusätzliche Software auf den angeschlossenen Rechnern, können aber auch keine weiteren Anwendungen ausführen. Spezialisierte NAS-Systeme eignen sich vor allem für den Einsatz in leistungshungrigen Umgebungen, die zudem eine hohe Verfügbarkeit erfordern.

Storage Area Network (SAN)

Die Kombination aus IP-Netz und Dateizugriff gilt als typische NAS-Architektur, während Kanalnetze und Blockzugriff dem Segment der SAN (Storage Area Network) zugerechnet werden.

Ein SAN ist, nach der ursprünglichen Investition, relativ kostengünstig, da gerade in kleinen und mittleren Unternehmen das SAN kaum geändert wird. Die entsprechenden Switches werden zumeist vom Integrator konfiguriert und später nicht mehr geändert. Ein SAN wird allerdings erst bei einer größeren Datenmenge interessant oder bei sich ändernden Business-Prozessen, durch die sich der Speicherbedarf häufig ändert.

In einer SAN-Umgebung wird der Speicherplatz für die Client-Rechner über ein Disk-Array zur Verfügung gestellt. Auf diese Weise kann die Hardware konsolidiert werden – durch den Einsatz weniger, großer Subsysteme reduziert sich der Bedarf an lokalen bzw. dezentralen Festplatten und der Verwaltungsaufwand wird deutlich verringert. Backups im SAN können direkt auf dedizierte Tape-Libraries erfolgen.

Kanalnetze dienen der Anbindung von Storage-Systemen über eine Hochgeschwindigkeitsverbindung an die jeweiligen Server. Diese Verbindung verhält sich wie ein dedizierter Kanal und erlaubt Servern und Speichersystemen, Signale über eine gemeinsame Verbindung zu senden, ohne sich gegenseitig zu stören. Kabelnetze erfordern allerdings zusätzlichen Aufwand, da zusätzliche Technologien wie beispielsweise „Fibre Channel“ installiert und gewartet werden müssen.

Der Zugriff auf die Daten erfolgt beim SAN per Blockzugriff. Hier werden die Daten direkt Block für Block vom Datenträger auf den Rechner übermittelt. Gesteuert wird der Zugriff über Dateitabellen des Betriebssystems des anfragenden Rechners. Blockzugriff ist aufgrund seiner Struktur sehr schnell, ist jedoch, da der Datenzugriff über den einzelnen Rechner erfolgt, nur schwer verteilbar.

Ein großer Vorteil von SANs ist ihre Disaster-Toleranz. Alle wichtigen Elemente, etwa Platten-Subsysteme, Host-Adapter oder ganze Server-Systeme, können mehrfach redundant im SAN vorhanden sein.

Kapitel 4: Risiken von Speicherlösungen

Nahezu jedes Unternehmen arbeitet heute mit digitalen Daten und benötigt daher auch entsprechende Speicherlösungen. NAS-Systeme sind hier vorteilhaft, da sie die Verfügbarkeit der Daten deutlich besser sichern können, als DAS-Lösungen. Allerdings belasten sie das Netzwerk zusätzlich. Daher ist es erforderlich, dass das System sicher arbeitet, was, in Abhängigkeit der benutzten Komponenten, nicht bei allen Systemen der Fall ist.

Im Falle eines Systemausfalls besteht sowohl bei DAS- als auch bei NAS-Speichern das Risiko, dass Daten unwiederbringlich verloren gehen. Auch Backup-Lösungen sind hier nicht immer die endgültige Lösung, denn bei großen Datenmengen kann es durchaus sein, dass das verfügbare Backup-Zeitintervall oder auch die Bandbreite des Netzwerkes nicht ausreichen, um alle Daten zu sichern.

RAID-Fehler und andere Ausfälle

RAID – dieser Begriff drückt aus, dass bei Ausfall einer Platte kein anderes Laufwerk in seiner Funktion betroffen ist. Werden Daten z.B. auf ein RAID5 Array geschrieben, wird gleichzeitig auch ein Fehlercode (Parity) generiert, der ebenfalls auf dem Array abgelegt wird. Beschädigte Dateien lassen sich so im Notfall über den Fehlercode wieder herstellen - der Ausfall einer einzelnen Platte bleibt ohne Auswirkung auf den Datenbestand.

Fällt beispielsweise bei einem RAID5-System eine Festplatte aus, sollte im Normalfall kein anderes Laufwerk in seiner Funktion betroffen sein. Werden Daten auf ein RAID5-Array geschrieben, wird gleichzeitig auch ein Fehlercode generiert, der ebenfalls auf dem Array abgelegt wird. Beschädigte Dateien lassen sich so im Notfall über den Paritycode wiederherstellen. Der Ausfall einer einzelnen Festplatte sollte daher ohne Auswirkung auf den Datenbestand bleiben. In der Realität kommt es jedoch auch bei RAID-Systemen mit Paritycode immer wieder zu größeren Problemen. Trotz modernster Speicher-Technologie kann sich innerhalb kürzester Zeit ein Desaster anbahnen. Mit der Komplexität des Systems erhöht sich auch die Zahl der potenziellen Fehlermöglichkeiten. Manche Datenverlust-Situationen gehen auf Hardware-Fehler zurück - besonders wenn mehrere Festplatten ausfallen oder der RAID-Controller defekt ist - bei anderen ist die Software verantwortlich.

In der Realität sind auch RAID-Systeme keine Wundermittel im Alltag eines IT-Technikers:

3:00 Uhr. Das Bereitschafts-Handy klingelt. Das könnte alles Mögliche bedeuten: Feuer, Einbruch, Ausfall der Klima-Anlage im Server-Raum 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 Server-Raum 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 UPS-Einheiten 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 des Applikations-Servers 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 Firmware zeigt, dass der Festplatten-Verbund 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 Firmware, 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 Festplatten-Verbund 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.

Soweit unser Beispiel. Es wird sichtbar, wie schnell sich trotz modernster Speicher-Technologie ein Desaster anbahnen kann. System-Unfälle passieren täglich. Trotz der Vielschichtigkeit von SAN-/NAS-Systemen kommen Ausfälle vor. Manche Datenverlust-Situationen sind Hardware bezogen, bei anderen liegt es an der Software. Als weitere Ursachen gelten menschliches Versagen oder Naturkatastrophen.

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.

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.

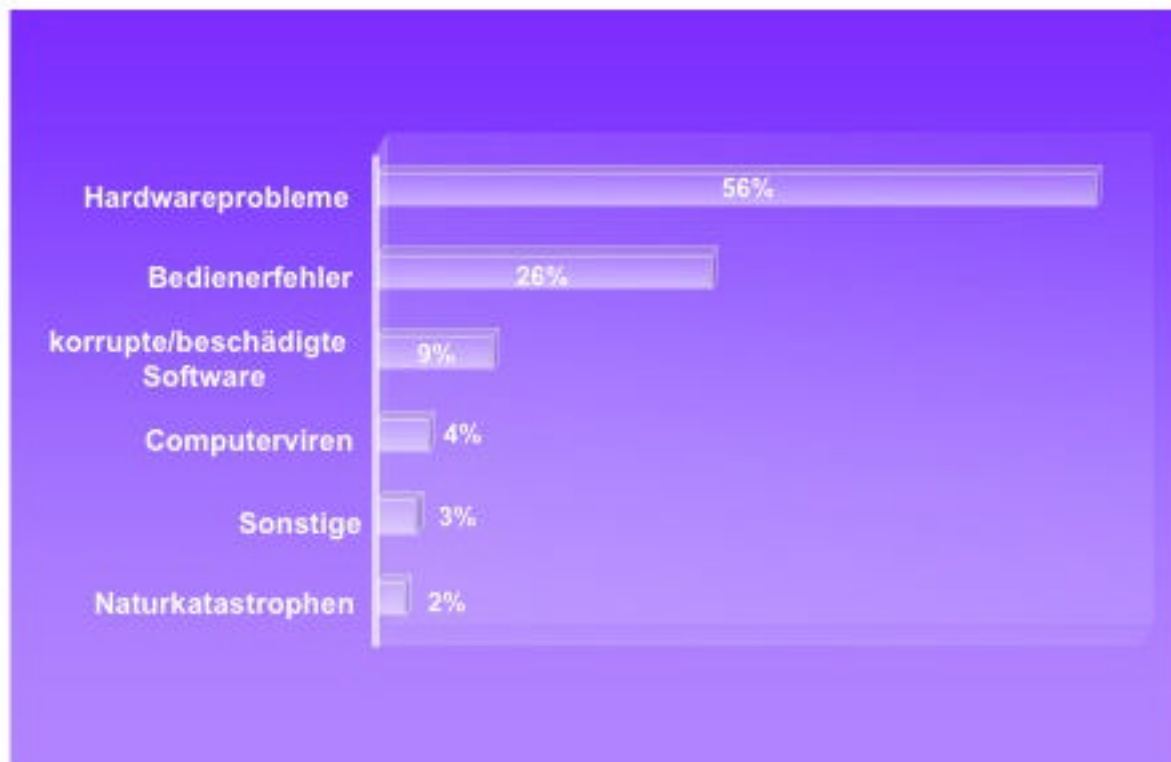
Häufig werden RAID-Systeme mit günstigen IDE-Festplatten zusammengestellt, die jedoch nicht für eine Dauerbelastung ausgelegt sind. Hohe Ausfallquoten nach zwei bis drei Betriebsjahren sind hier vorprogrammiert.

Im Schadensfall offenbaren sich dann häufig auch noch bisher verborgen gebliebene Ausfälle anderer Komponenten. So kann sich im Krisenfall herausstellen, dass das Bandlaufwerk sich im Laufe der Zeit dejustiert hat und ältere Bänder nun nicht mehr lesbar sind. Möglicherweise sind Tapes auch durch Alterung und Verschleiß unbrauchbar geworden.

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. Es kommt auch vor, dass Software an sich problemlos läuft und es daran scheitert, dass sich keine Treiber für neue Hardware finden lassen. Die hier auftretenden Probleme können häufig auch mit einer Hochverfügbarkeitslösung nicht behoben werden.

Fazit: Auch wenn das RAID-System fehlerfrei arbeitet, gibt es weitere Ursachen, die zu Datenverlust führen können wie menschliches Versagen oder äußere Einwirkungen wie Brand- oder Wasserschäden.

Laut einer Erhebung von Kroll Ontrack¹ teilen sich die Fehlfunktionen wie folgt auf:



Fast die Hälfte der Ausfallursachen, wie etwa Bedienerfehler oder Softwarekorruption, sind durch eine RAID-Lösung kaum abzusichern. Trotz ständiger technologischer Fortschritte und Verbesserungen der Zuverlässigkeit von magnetischen Speichermedien kommt es immer häufiger zu einem Datenverlust. Professionelle und qualifizierte Datenrettung wird wichtiger denn je. Die Ingenieure von Kroll Ontrack haben drei Hauptgründe für diese Entwicklung identifiziert:

1. Immer größere Datenmengen werden auf immer kleinerem Raum gespeichert.

Die Speicherkapazität der Festplattenlaufwerke von heute ist im Vergleich zu den Festplattenlaufwerken von vor 10 Jahren mindestens 500-mal so hoch. Höhere Speicherkapazitäten verstärken jedoch die Auswirkungen eines Datenverlusts, die mechanische Genauigkeit ist dabei ein entscheidender Faktor.

2. Die Daten sind potenziell kritischer als früher.

Krankenakten in Krankenhäusern, akademische Arbeiten, wichtige Finanz- und Steuerinformationen, Verdienstbescheinigungen, sensible Daten im Bereich Online-Banking etc. - heutzutage speichert ein Großteil der Benutzer Informationen ausschließlich elektronisch. Der Verlust kritischer Daten führt zu erheblichen finanziellen, rechtlichen und produktivitätsbezogenen Nachteilen für Unternehmen und Privatnutzer.

3. Tools und Techniken zur Datensicherung sind nicht zu 100% zuverlässig.

Die meisten Computerbenutzer verlassen sich auf ihre Sicherungskopien. Forschungsergebnisse des Datenrettungs-Unternehmens Kroll Ontrack zeigen jedoch, dass immerhin 80% der Kunden ihre Daten regelmäßig sichern, jedoch sind sie für den kritischen Moment der Wiederherstellung nur ungenügend vorbereitet. Bei der Sicherung wird vorausgesetzt, dass Hardware und Speichermedien voll funktionsfähig, die Daten nicht beschädigt sind, und die letzte Sicherung vor nicht allzu langer Zeit durchgeführt wurde, damit eine vollständige Wiederherstellung überhaupt erst möglich wird.

Auch die fortschrittlichste Technik ist nicht immer perfekt: Hardware und Software können durchaus versagen und Sicherungen enthalten nicht immer die aktuellsten Daten!

¹ Kroll Ontrack Inc. 2004

Ausfälle kosten Zeit und Geld

Hardware-Ausfälle ziehen im Durchschnitt einen Systemausfall von vier Stunden bis zu zwei Tagen nach sich. Hinzu kommt der Zeitaufwand für die Wiederherstellung bzw. Rücksicherung der Daten und Applikationen, die auch noch einmal rund vier bis zwölf Stunden dauert. Im Schadensfall ist also mit einer Mindestausfallzeit von acht Stunden zu rechnen – vorausgesetzt, alle erforderlichen Schritte sind problemlos durchführbar. Der Folgeaufwand bei einem Datenverlust durch Probleme bei der Wiederherstellung ist jedoch kaum zu beziffern und kann ein Unternehmen massiv schädigen.

Unternehmen bzw. Institutionen riskieren, ohne Zugriff auf ihre Daten, hunderttausende von Euro an Umsatz zu verlieren. Jeden Tag. Tatsache ist, dass wir alle heutzutage von unseren konsistenten und zugänglichen Daten abhängig sind.

Ein ausführlicher „Desaster Recovery Plan“ kann hier helfen. Alle Schritte, die zur Rettung und Wiederherstellung des Systems notwendig sind, sollten hier minutiös verzeichnet sein. Nur ein sicherer und getesteter Fahrplan, der auch eine mögliche externe Datenrettung einschließt, kann im Ernstfall helfen, Folgefehler durch Fehlbedienung in Folge von Stress und Druck zu vermeiden.

Kroll Ontrack Datenrettung bietet folgende Datenrettungs-Lösungen für Server und RAID-Systeme:

REMOTE DATA RECOVERY™ SERVICE	DATENRETTUNGS-SERVICE IN LABOR UND REINRAUM	ONTRACK POWERCONTROLS™ SOFTWARE
In Situationen, in welchen die Hardware noch problemlos funktioniert, bietet sich die Remote Data Recovery™ als schnellste, bequemste und kostengünstigste Datenrettungs-Variante an. Bei dieser Service-Variante wird die Datenrettung in Labor-Qualität direkt auf dem Server durchgeführt - mittels einer gesicherten Modem- bzw. Internet-Verbindung. Die RDR™ erweckt den Server wieder zum Leben - und zwar im Bruchteil der Zeit, welche die Datenrettung von einem Backup in Anspruch nehmen würde.	In Situationen, in welchen die Hardware physikalisch beschädigt ist, hilft der Labor-Service: Die Festplatte wird im Reinraum von erfahrenen Datenrettungs-Ingenieuren geöffnet und bearbeitet. Der Service in Labor und Reinraum ist besonders zu empfehlen, wenn es sich um besonders komplexe und extreme Datenrettungsfälle handelt.	In Datenrettungsfällen, in welchen Daten von einem Exchange-Server wiederhergestellt werden müssen, ist die bewährte Mailbox-Recovery-Software Ontrack PowerControls™ die geeignete Lösung. Mit diesem Tool können mühelos einzelne Inhalte bzw. ganze Mailboxen einer Exchange Datenbank (*.edb-Datei) wiederhergestellt, kopiert und durchsucht werden.

Kroll Ontrack hat bei unter Anderem bei folgenden Betriebssystemen und Speichermedien erfolgreiche Datenrettungen durchgeführt:

HERSTELLER VON SPEICHERMEDIEN		DATENBANKEN	BETRIEBSSYSTEME	
Adaptec AMIBus Compaq Dell HP QLogic Mylex Network Appliance PERC Intel ICP-Vortex IBM Hitachi	EMC Pinnacle Promise Raidtec Software RAIDs Storage Dimensions Sun Infotrend Arena Areca Samsung Maxtor	Microsoft Exchange Microsoft SQL	BSD HP UX IBM® AIX® Linux Novell® NetWare® Macintosh Server SCO	Sun™ Solaris™ UNIX® Windows NT® Windows® 2000 Windows Server™ Windows 2003

Mögliche Fehler, die eine Datenrettung erforderlich machen

Die häufigsten Ursachen für Datenverlust

- Hardware- oder Systemfehlfunktionen (56% aller Datenverluste)
Datenverlust entsteht beispielsweise durch Stromausfall, Lesekopf-/Plattencrash oder Controllerfehler.

Fallbeispiel: Systemzugriff nicht möglich

System:

RAID 5 mit 4 Maxtor-Festplatten
4 x 160 GB mit ca. 240-350 GB Daten
Betriebssystem: Linux

Problem:

Keinen Zugriff auf das System. Als Ausfallgrund wird eine Überspannung vermutet. Der Administrator hat keinen Rebuild versucht. Es werden Audio-Dateien benötigt, die mit einer proprietären Software erstellt wurden.

Datum: 30.03.04 Zeit: 22:30

Die vier Festplatten werden am selben Tag vom Administrator persönlich vorbeigebracht. Das Flugzeug landet um 22:30

Datum: 30.03.04 Zeit: 23:30

Der Kunde wurde abgeholt und in einem Hotel in der Nähe des Labors untergebracht.

Der Ingenieur im Labor legt Images der Festplatten an. Die Datenretter haben sich zur Erstellung von Kopien der Festplatten entschlossen, da die physikalische Unversehrtheit der Festplatten aufgrund der vermuteten Überspannung nicht sicher war.

Datum: 31.03.04 Zeit: 22:00

Die Images sind fertig gestellt und der Ingenieur beginnt die RAID-Struktur über eine Simulation des RAID-Controllers zurückzubauen.

Datum: 01.04.04 Zeit: 5:35

Die Bearbeitung der logischen Struktur ist abgeschlossen. Es wird eine Dateiliste erstellt.

Datum: 01.04.04 Zeit: 9:00

Die Dateiliste kann vom Kunden eingesehen werden und ein Datensatz wird zu Testzwecken wiederhergestellt. Der Kunde installiert die proprietäre Software auf einem Testrechner und verifiziert die Integrität der Daten.

Es können 620.000 Dateien mit einer Gesamtkapazität von 390 GB gerettet werden. Das Datenrettungsangebot wird angenommen und die Daten werden auf externe Festplatten gespielt.

- Bedienungsfehler (26% aller Datenverluste)
Datenverlust tritt auf beispielsweise durch versehentliches Löschen oder Formatieren der Festplatte oder durch Aufprall oder Fall.

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 WIN-System angehängt. Die schwerwiegend 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.

- Beschädigte Software (9% aller Datenverluste)
Datenverlust kann geschehen beispielsweise durch eine Beschädigung durch Diagnose- oder Reparatur-Tools, fehlgeschlagene Sicherungsprozesse oder die Komplexität der Konfiguration.

Fallbeispiel: Saveset kann nicht zurückgespielt werden

System:

6 Super-DLT-Bänder im logischen Verbund

Problem:

Der Server war abgestürzt und wurde neu aufgebaut. In der Folge konnte das Saveset nicht zurückgespielt werden. Der Restore-Prozess konnte von der Backup-Software nicht initialisiert werden, da eines der im logischen Verbund stehenden Bänder einen Defekt hatte.

Benötigt wurde eine Datenbank eines Warenwirtschaftssystems. Die Datenbank macht 10 GB der 700 GB auf den Backupmedien aus.

Mit Kroll Ontrack-Tools waren die Datenretter in der Lage, die Bänder einzeln zu katalogisieren und sich auf die Suche nach der Datenbank zu machen. Auf dem vierten Band wurde sie schließlich gefunden.

Die Datei wurde vom Kunden verifiziert und die Wiederherstellung beauftragt. Die Datenbank wurde umgehend auf eine externe Festplatte gespielt. Die Firma des Kunden konnte die Arbeit wieder aufnehmen.

- Computerviren (4% aller Datenverluste)
Datenverlust wird hervorgerufen beispielsweise durch dateiinfizierende oder polymorphe Viren.
- Höhere Gewalt (5% aller Datenverluste)
Datenverlust tritt ein beispielsweise durch Feuer, Hochwasser oder Spannungsabfall.

„Sonderfall“ Exchange Server

Fallbeispiel: Mail-Datei im Exchange-Server beschädigt

System:

Exchange-Server
edb-Datei von ca. 50 GB

Problem:

Die Datei Priv.edb weist eine Datenkorruption auf.

Datum: 23.xx.xx **Zeit: 11:00**

Der Kunde hat sich dazu entschlossen, zunächst selbst einen Reparaturversuch zu starten.

Datum: 24.xx.xx **Zeit: 8:00**

Der Reparaturversuch des Kunden war nicht erfolgreich. Der Kunde nutzte die Remote-Datenrettung (RDR) und hat die Festplatte an ein bootfähiges WIN-System angeschlossen. Anschließend konnte er sich in den Kroll Ontrack-Server einwählen.

Die Ferndiagnose begann um ca. 10:00 Uhr..

Datum: 24.xx.xx **Zeit: 22:54**

Kroll Ontrack generierte eine Dateiliste. Die Datei war 51 GB groß und beinhaltete 495 Mailboxen.

Datum: 25.xx.xx **Zeit: 00:20**

Die Datenrettung wurde beauftragt und die Datei wurde sofort auf eine Backup-Platte des Kunden kopiert.

Datum: 25.xx.xx **Zeit: 11:00**

Der Kopierprozess war abgeschlossen und der Kunde hatte seine E-Mails zurück.

Wie das Exchange-Backup arbeitet

Um zu verstehen, wie Daten wiederhergestellt werden, ist es wichtig, zu verstehen, wie ein Backup unter Exchange funktioniert. Die Beschaffenheit dieser Backups macht es, kombiniert mit der Datenbank-Struktur von Exchange, sehr schwer, Daten wiederherzustellen.

Es gibt zwei grundlegende Arten von Exchange-Backups: Online-Backups und Offline-Backups. Bei einem Online-Backup arbeitet der Server weiter, während das Backup durchgeführt wird und E-Mails können weiterhin gesendet und empfangen werden – es gibt keine Unterbrechung des Mailsdienstes. Bei einem Offline-Backup wird der Server während des Backups heruntergefahren und der Mailservice wird unterbrochen. Offline-Backups haben den Vorteil, schneller zu sein und die Administratoren müssen bei der Entscheidung für ein Online- oder Offline-Backup zwischen dem Wunsch nach schnellen Backups und der Unterbrechung des Mailsdienstes abwägen.

Die Administratoren müssen sich außerdem entscheiden, ob sie ein vollständiges Backup durchführen wollen oder eine oder mehrere einzelne Mailboxen sichern wollen (Das Backup einzelner Mailboxen wird Brick-Level-Backup genannt.). Bei einem vollständigen Backup werden die gesamte Priv.edb und die zugehörigen Log-Dateien gesichert. Diese Art des Backups ist ideal zur „Disaster Recovery“ – falls ein Server oder eine Festplatte ausfällt, kann die gesamte Exchange-Datenbank wiederhergestellt werden. So können auch alle E-Mails und Mailboxen wiederhergestellt werden.

Nun wirft diese Form des kompletten Backups aber ein schwerwiegendes Problem auf: Es kann nämlich nur jeweils die gesamte Datenbank mit allen Mailboxen und Nachrichten wiederhergestellt werden. Um das zu tun, muss ein Duplikat des Exchange Servers aufgebaut werden, der so genannten Recovery Server. Dann wird das Backup auf diesen Server kopiert. Von diesem Server aus können dann einzelne Mailboxen in PST-Dateien kopiert werden. Erst dann kann in diesen PST-Dateien nach den Nachrichten gesucht werden, die wiederhergestellt werden sollen. Diese Nachrichten werden dann auf den ursprünglichen Server kopiert. Dieser Vorgang ist teuer, umständlich und kann nicht in jedem Fall durchgeführt werden. Der Recovery Server muss genauso konfiguriert sein wie der Exchange Server. Wenn die Konfiguration nicht genau dokumentiert ist, kann das Backup nicht durchgeführt werden. Außerdem sind der Kauf und die Wartung des Recovery Servers alles andere als unaufwendig. Der Recovery Server kann natürlich auch nur dann aufgesetzt werden, wenn er benötigt wird, aber dieser Vorgang kostet im Schnitt einen ganzen Tag, was für eine Unternehmensumgebung, in der Informationen schnell benötigt werden, absolut unpraktikabel ist.

Mit einem Brick-Level-Backup können einzelne Mailboxen wiederhergestellt werden, so dass man in der Lage ist, einzelne Mailboxen ebenso wiederherzustellen wie Mailbox-Gruppen, einzelne oder mehrere Nachrichten. Allerdings ist auch dieses Verfahren mit Nachteilen behaftet. Aufgrund der ineffizienten Art, in der die Daten gespeichert werden, benötigt ein Brick-Level-Backup erheblich mehr Speicherplatz als ein komplettes Backup. Dazu dauert der Backup-Vorgang auch deutlich länger. Ein Server mit 400 Mailboxen benötigt beispielsweise rund eine Stunde für ein komplettes Online-Backup. Wenn auf demselben Server ein Brick-Level-Backup läuft, kann das Backup der 400 Mailboxen gut 18 Stunden dauern. Ein weiterer Nachteil ist, dass nicht die gesamte Exchange-Datenbank mit dem Brick-Level-Backup gesichert werden kann – dafür muss ein komplettes Backup durchgeführt werden.

Probleme mit Exchange Backups

Die Administratoren haben aufgrund dieser Gegebenheiten bei der Backup-Strategie eine schwere Entscheidung zu treffen. Sollen nur komplette Backups durchgeführt werden, weil sie kostengünstiger und platzsparender sind als Brick-Level-Backups? Mit kompletten Backups gibt es keinen einfachen Weg, einzelne Mailboxen und Nachrichten wiederherzustellen, was ein Problem für das Unternehmen werden kann, wenn einzelne Mailboxen oder Nachrichten gefunden und wiederhergestellt werden sollen.

Brick-Level-Backups sind auf der anderen Seite oft nicht praktikabel, weil sie zeitaufwendig und teurer sind. Hinzu kommt das Problem, das beim Brick-Level-Backup nicht die gesamte Datenbank wiederhergestellt werden kann. Als Ergebnis bleibt Unternehmen in der Backup-Frage nur die Wahl zwischen zwei Übeln. Einige versuchen einen gemischten Ansatz und führen beide Arten von Backups, komplette Backups und Brick-Level-Backups, zu unterschiedlichen Zeiten durch. Da aber Brick-Level-Backups so zeitaufwendig und teuer sind, sichern einige Unternehmen nur ausgewählte Mailboxen, beispielsweise die der Top-Manager, mit dem Brick-Level-Backup.

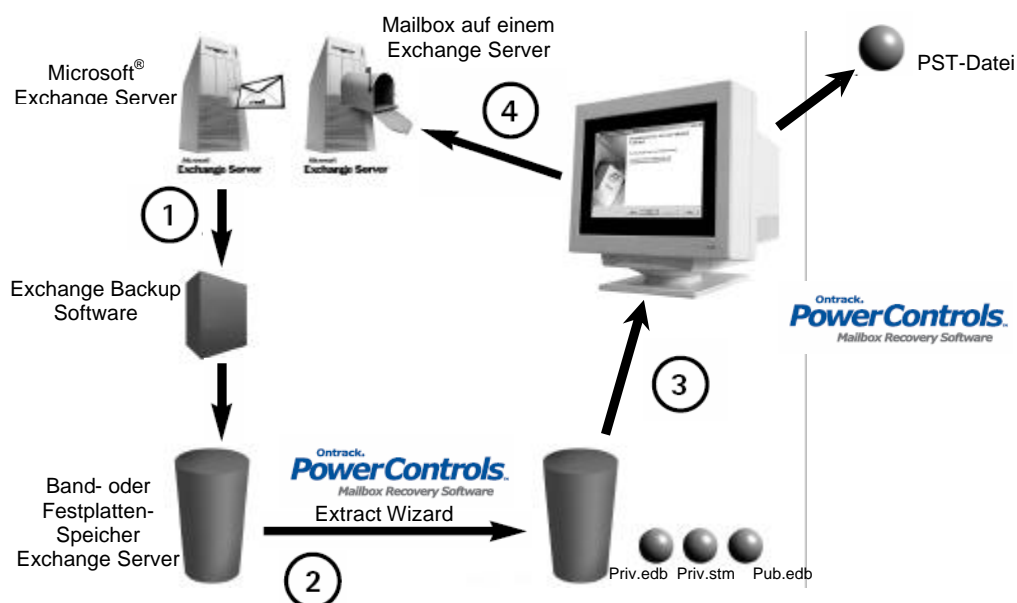
Wie PowerControls das Problem löst

PowerControls, die Mailbox Recovery Software von Ontrack Data Recovery™, löst dieses Problem, indem es den Administratoren ermöglicht, einzelne Nachrichten, Mailboxen, Dateianhänge und sogar Notizen, Kontakte und Aufgaben aus einem kompletten Backup wiederherzustellen. Die Software kann direkt auf die EDB-Dateien zugreifen, so dass es nicht nötig ist, ein Brick-Level-Backup durchzuführen, um einzelne Nachrichten und Mailboxen wiederherzustellen. Statt jeweils nur eine Mailbox zu durchsuchen oder ein altes Backup zur Analyse einzuspielen, können Sie gleichzeitig alle Mailboxen, die sich in einer EDB-Archivdatei befinden, durchsuchen. Dabei können verschiedene Kriterien wie Schlüsselwörter, Betreff, Datum oder spezielle Benutzernamen eingesetzt werden. Einzelne Mailboxen müssen nicht gesondert gesichert werden, da sie direkt aus der EDB-Datei wiederhergestellt werden können.

Mit PowerControls muss der normale Backup-Prozess nicht verändert werden – es arbeitet im Rahmen der normalen Backup-Prozeduren. Wenn diese Prozeduren geändert werden, passt sich PowerControls an und arbeitet mit den neuen Prozeduren. Darüber hinaus arbeitet PowerControls auch mit bereits erstellten Backups, so dass auch Daten von Backups wiederhergestellt werden können, die vor der Installation von PowerControls angelegt wurden.

Wie PowerControls arbeitet

Um besser zu verstehen, wie PowerControls eingesetzt werden kann, ist es hilfreich, die Architektur von PowerControls zu betrachten. Die Abbildung zeigt den schematischen Ablauf.



Die Schlüsselfunktion von PowerControls ist seine Fähigkeit, EDB-Dateien direkt verarbeiten zu können. Damit ist es nicht notwendig, die Backup-Prozeduren zu ändern – PowerControls greift auf die Dateien zu, nachdem ein Backup abgeschlossen wurde.

Schritt 1: Die Backup-Software sichert die Exchange-Datenbank und legt ein Exchange-Backup an.

Schritt 2: Der ExtractWizard von PowerControls stellt die Datenbank an einem anderen Speicherort, der kein Exchange Server ist, wieder her.
Hinweis: Für Backup-Formate, die derzeit vom ExtractWizard nicht unterstützt werden, stellt die Exchange Backup-Software die Datenbank an einem Speicherort, der kein Exchange-Server ist, wieder her.

Dann...

Schritt 3: PowerControls kann nun eingesetzt werden, um einzelne Mailboxen, Nachrichten und Dateianhänge zu durchsuchen und anzusehen.

Schritt 4: PowerControls kann eine einzelne Mailbox, Nachrichten oder Dateianhänge auf dem Exchange Server wiederherstellen oder sie in einer neuen PST-Datei an einem anderen Speicherort ablegen.

Remote-Datenrettung (RDR)

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.

Remote Data Recovery (RDR) ist eine von Kroll Ontrack patentierte Technologie, die Daten auf dem Server, Desktop oder Laptop innerhalb weniger Stunden wieder verfügbar macht.

Benötigt wird dazu nur ein Modem oder ein Internetzugang, über den einer der Datenrettungsingenieure direkt mit dem fehlerhaften Laufwerk über eine verschlüsselte Verbindung kommuniziert. Diese Technologie kann erfahrungsgemäß in mehr als 50% aller Fälle eingesetzt werden.

Der Datenträger muss nicht ausgebaut werden und es wird so wertvolle Arbeitszeit gespart. Gleichzeitig wird die Ausfallzeit des Systems minimiert. In Fällen von NAS- oder SAN-Systemen, Microsoft Exchange oder SQL-Datenbanken, RAID-Systemen mit beschädigter Festplatte oder Controller-Fehlern ist RDR oft die einzige Lösung.

Fallbeispiel: Controllerfehler

System:

Novell Netware 6.x

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 eingeschickt werden, da sich die verlorenen Daten physikalisch auf mehrere RAID-Systeme im SAN verteilten.

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.

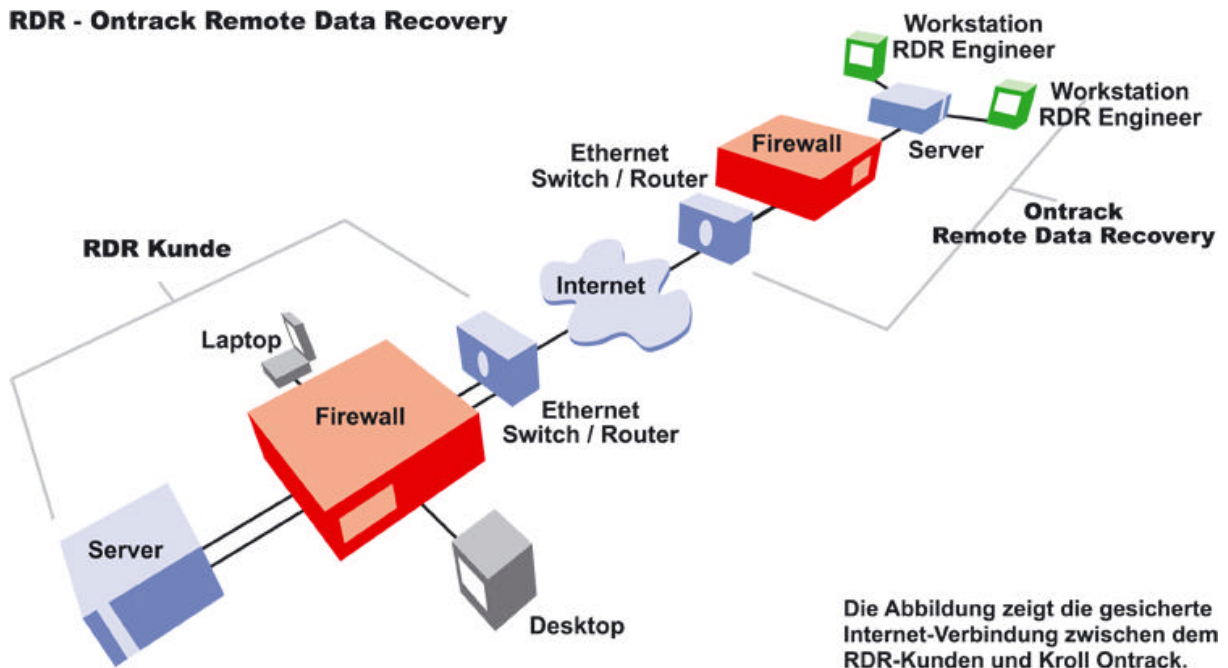
Nach wenigen Stunden gaben die Datenrettungsingenieure einen ersten Zwischenstand. Durch das logisch verloren gegangene RAID sind die Strukturen des Dateisystems im SAN beschädigt worden. Mit Hilfe der Kroll Ontrack-Werkzeuge konnten die Dateistrukturen erfolgreich wiederhergestellt werden.

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.

Funktionsweise der RDR

1. Anfrage des Kunden wegen Datenverlust.
2. Ingenieur überprüft Möglichkeiten zur RDR®.
3. Persönliches Gespräch von Kunde und RDR-Ingenieur.
4. Der Kunde installiert den Ontrack-Verbindungsassistenten „ConnectionClient“.
5. Der Ingenieur rettet die Daten mit speziellen Tools - von alle Arten von Speichermedien, Plattformen und Betriebssystemen.
6. Besonders geeignet für große Storage-Systeme: RAID, NAS, SAN.
7. Der Kunde erhält eine umfassende Diagnose: eine Liste mit allen wiederherstellbaren Files und entscheidet dann, ob die Datenrettung durchgeführt werden soll.
8. Datenrettung: die verlorenen Daten werden wiederhergestellt und auf das Kundensystem gespeichert.
9. Der RDR-Spezialist meldet sich ab, und der Kunde startet seinen Computer neu. Der Kunde kann nun wieder auf die eigenen Daten zugreifen.

RDR - Ontrack Remote Data Recovery



Wie sicher ist die RDR?

Die RDR von Kroll Ontrack erfüllt die allerhöchsten Sicherheitsstandards: Die gesamte Kommunikation erfolgt über eine verschlüsselte Verbindung. Es wird ein proprietäres Kommunikationsprotokoll verwendet, die Pakete sind verschlüsselt, die Strukturen sicher.

Zusätzlich wird der Ontrack SecurityLayer verwendet, der in der Diagnosephase nicht auf die Datenträger schreibt und mit dessen Hilfe sehr schnell eine Analyse durchgeführt werden kann. Kroll Ontrack arbeitet tagtäglich mit wichtigen Daten; verantwortungsbewusster Umgang mit vertraulichen Daten und rigorose Sicherheitsprozesse sind daher selbstverständlich. All Mitarbeiter sind gemäß §5 BDSG dem Datenschutz verpflichtet.

Mindestvoraussetzungen für RDR

Mit RDR können derzeit Daten aus **Windows 3.x, 95, 98, Me, XP, 2000, NT, Linux, Novell NetWare** und **NSS** wiederhergestellt werden. Dazu wird ein Modem oder einen Internetzugang über ein unternehmensweites LAN oder einen ISP (Internet Service Provider) benötigt. Einer der Datenrettungsingenieure arbeitet mit diesem Modem- oder Internetzugang, um direkt mit dem fehlerhaften Laufwerk zu kommunizieren.

Praktische Anwendungsfälle für die Online-Datenrettung

Logische Problemfälle können fast immer mit der Remote Data Recovery 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 Ontrack 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 MS 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 MS 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 MS 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 Online-Datenrettung 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.

Kapitel 5: Wann brauchen Sie einen Datenrettungs-Spezialisten?

Nahezu alle Daten lassen sich im Schadensfalle wiederherstellen. Doch wann benötigen Sie eigentlich einen Datenrettungsspezialisten?

Unzuverlässiges Backup-System – Ohne ein getestetes und zuverlässiges Backup-System 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 Backup-Prozeduren 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 ein 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 Betriebssystem-Struktur 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, Systemeinbrüche oder frustrierte Mitarbeiter absichtlich zerstört oder verändert werden.

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

Korrupte oder gelöschte MS SQL- oder MS 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, Wechselplatten 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 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 Internet- oder Modemverbindung direkt auf dem betroffenen Server oder PC gearbeitet wird.

Kapitel 6: Tipps zur Datenrettung für Server

In fünf Schritten zur Wiederherstellung der Daten

				
<p>Kontaktaufnahme unter 0800 10 12 13 14 oder Online</p> <p>Bei einem ausführlichen Gespräch mit einem Kundenberater wird festgehalten, wie der Schaden zustande gekommen ist, um was für ein Speichermedium es sich handelt, um welche Datenmenge es sich handelt, welches Betriebssystem vorliegt und wie schnell die Daten wieder benötigt werden. Es folgt ein professioneller Lösungsvorschlag für den speziellen Fall.</p>	<p>Erweiterte Diagnose</p> <p>Die erweiterte Diagnose beinhaltet die Summe vieler hochwertiger Ontrack-Einzelservices. Beispielsweise wird das Medium abgeholt und der Kunde erhält exklusiv ein komplettes Verzeichnis, in dem alle wieder herstellbaren Dateien aufgeführt sind. Erst danach wird entschieden, ob der Datenrettungsauftrag erteilt wird. Wenn es ganz besonders schnell gehen muss, empfiehlt sich die patentierte Online-Datenrettung (RDR™).</p>	<p>Datenwiederherstellung</p> <p>Nach Eingang des Datenrettungsauftrags machen sich die Ingenieure im Datenrettungslabor an die Arbeit. Alle Daten werden Bit für Bit wiederhergestellt. Dabei wird mit selbst entwickelten Werkzeugen und Programmen gearbeitet, die optimal auf die unterschiedlichen Betriebssysteme und Dateistrukturen abgestimmt sind. Aufgrund genauer Systemkenntnisse wissen die Ingenieure, welche Daten in welchen Verzeichnissen, Sektoren oder Segmenten von Datenträgern zu finden sind und wie die gelöschten Dateien wieder hergestellt werden können. Ist die Hardware so schwer beschädigt, dass sie im Reinraum bearbeitet werden muss, wird der Datenträger in einer sicheren, staubfreien Umgebung geöffnet und Images der Rohdaten werden erstellt. In einem hochspezialisierten Prozess werden hier die auf der Festplatte gespeicherten Daten wieder verfügbar gemacht und so wiederhergestellt, dass auf die verlorenen, korrupten oder beschädigten Daten erneut zugegriffen werden kann.</p>	<p>Aktualität</p> <p>Der zuständige Kundenberater ist stets über den Stand der Datenrettung auf dem Laufenden. Der Kunde ist so über jeden einzelnen Schritt des Datenrettungs-Prozesses informiert und kann rund um die Uhr auf die kostenlose Datenrettungs-Hotline unter 0800 10 12 13 14 zugreifen. Die professionelle und kompetente Dienstleistung hilft, das Herzstück des Unternehmens - die Daten - schnell zurückzuerhalten.</p>	<p>Datenaufbereitung</p> <p>Nach erfolgreichem Abschluss der Datenrettung werden die Daten auf einen Datenträger nach Wahl gespeichert, der dem Kunden - zusammen mit einer genauen Anleitung zum Wiederaufspielen der wiederhergestellten Daten – zugesandt bekommt. Aber auch in diesem Moment wird der Kunden nicht alleingelassen. Sollten noch Fragen offen sein, hilft der Support unter 0800 10 12 13 14 oder +49 (0)7031 644-244 selbstverständlich jederzeit gerne weiter.</p>

Datenrettungs-Tipps 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 durch zu spielen um gegen alle Etwaigkeiten/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 MS 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 Datei-System 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 Teil des „Desaster Recovery Plans“ des 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. Dies ist sinnvoll, da das Ziel ist, der Firma so schnell wie möglich ihre Daten wieder verfügbar zu machen. Der Schlüssel zum Erfolg ist es, den Datenretter so früh wie möglich zu involvieren.

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 unterschiedliche 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 Notfall-Prozeduren, 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 berücksichtigt, um die Gefahr des Ausfalls durch Bandfehler zu minimieren.

RAID-Systeme

Auch RAID-Speichersysteme, SAN-Systeme, JBOD- und NAS-Systeme sollten in den Disaster Recovery Plan mit aufgenommen werden. Diese Speichersysteme verfügen über Redundanz-Architekturen, 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 schalte 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-Reparierprogramm 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 das effektivste Hilfsmittel für den Kunden.

Dieses Beispiel ist interessant, weil es zeigt, wie in schneller Folge kaskadieren können. 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.

Daten-Desaster 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 Anbietern. 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, hochspezialisierte Ingenieure und 24 Stunden Support und Hilfe.

Referenzen

Kroll Ontrack konnte schon bei vielen Unternehmen erfolgreiche Datenrettungen durchführen. Hier ein Auszug aus der Kundenliste:

- A&R Yabuno, Bonn
- AOK Sachsen, Dresden
- ARAL
- Artservice Gerhard auf der Heide GmbH, Düsseldorf
- Badenia Bausparkasse
- BAG Raiffeisen E.G.
- bfw-medcom GmbH
- BIOS Beratung in Organisation und Software GmbH
- BK Giuliani
- BMW AG, München
- Chemie Technik
- Connex
- Continental
- D. Logistics Services NV, Tienen, Belgien
- D. Logistics Services NV, Tienen, Belgien
- Spett. Telma srl, Treviso, Italien
- DAS
- Data Quest AG, Luzern
- Deloitte
- Deutsche Telekom
- Diakonie
- Ecofit
- Edeka
- EP: R&C
- Ernst & Young
- Festo
- Firmenich
- Forschungszentrum Rossendorf, Dresden
- Gyseler Consuling
- HeizungsSanitär Günther Marx GmbH, Kusterdingen
- HewlettPackard
- Hyundai
- IBM
- Jena Optik
- Karl Pönighaus Systemhaus GmbH
- Klinikum Großhadern
- Landesbetrieb "Liegenschafts und Baubetreuung, Mainz
- Magna Steyr
- Marimex Industires GmbH, Bottrop
- Massivholzmöbel Hartmann
- MaxPlanck Institut
- Ministerium für Umwelt und Verkehr BadenWürttemberg
- Norddeutscher Rundfunk,
- Nozag Antriebstechnik
- ÖBB
- Oberösterreichische Kraftwerke
- Pixel Connection, München
- Plan@EDVService, Offenbach
- Porsche
- Price Waterhouse
- ReiseBank
- Reuters
- SAB GmbH, Staufenberg
- Siemens AG
- Sig. Salvetti Vigilio, Garag. Die S.A. Valpolicalla VR
- Smart
- SMART GmbH, Böblingen
- SOSPC. Ch Sàrl, Mézières, Schweiz
- Spett. Ciba Speciality Chemicals S.p.a., Origgio (Va), Italia
- Spett. Consorzio Depurazione Acque Biasca, Biasca, Schweiz
- Spett. Elettronica Sillaro, Castel San Pietro Terme, Italia
- Spett. Nèmesi IT srl, Vicenza
- Spett. Tecno General srl, Fermo
- Spett. Telma srl, Treviso, Italien
- Spett. UniCredit Xellon Banca S.p.a., Milano
- SSC-Services
- Stadt Kitzingen
- Stadt Köln
- TC Logopak
- Universität Bremen
- Universitätsklinikum Bremen
- Weisser + Böhle GmbH
- Westdeutscher Rundfunk
- Willi Geller GmbH, Köln
- ZF

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

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

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

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.