

Das verdrängte Risiko Datenverlust

Erfahrung von Datenrettern zeigt Probleme der Business-Continuity-Planung



Bild: CBL Datenrettung

Unternehmen sind nur handlungsfähig, wenn sie auf ihre Daten zugreifen können und von Datenverlust betroffene Firmen erleiden allzu oft schwere wirtschaftliche Schäden oder müssen sogar schließen. Umfragen wie die AT&T Business Continuity Study 2007 belegen, dass nur etwa 70 Prozent der Unternehmen Pläne für die Erhaltung der Geschäftskontinuität im Krisenfall haben und weniger als die Hälfte der Firmen mit Notfallplan diesen auch testen. Dass die tatsächlichen Risiken im eigenen Unternehmen häufig völlig falsch eingeschätzt wurden, erleben Datenrettungsdienstleister täglich. Die Erfahrungen derer, die zum Einsatz kommen, wenn Daten nicht sicher waren, geben Einblicke in die Bedrohung der Business Continuity.

■ Gerlinde Wolf

Datenverlust kann die Funktionsfähigkeit oder das Überleben eines Unternehmens auf ganz unterschiedliche Weisen bedrohen, je nach Art der Daten und ihres Stadiums im „Lebenszyklus“ zwischen Erstellung und geplanter Vernichtung. Am augenscheinlichsten ist dies bei aktuellen Daten der zentralen IT-Systeme wie etwa bei der Buchhaltung oder bei der Auftragsbearbeitung. Je nach Branche kann der Verlust solcher Daten innerhalb von Tagen oder sogar Stunden zu schweren wirtschaftlichen Schäden oder gar zu Handlungsunfähigkeit führen. Im Bereich un-

ternehmenskritischer Systeme ist die Sicherheit im Allgemeinen durch Backup- und Recovery-Lösungen am besten gewährleistet.

Gefährdet sind Daten auch kurz nach ihrer Erzeugung, wenn sie noch nicht von den Datensicherungsstrategien erfasst werden. Zu dieser Gruppe gehören beispielsweise Entwürfe, Konzepte und Kommunikationsdaten, die nur auf lokalen PC-Festplatten oder Notebooks gespeichert sind. Der Schaden ist beim Verlust solcher „vorläufiger“ Daten zwar meist geringer, aber das Risiko eines Verlusts sehr groß. Dies gilt vor allem bei Notebooks, die nicht nur leichter gestohlen >



Gerlinde Wolf
ist Channel Manager
bei CBL Datenrettung in Kaiserslautern
T +49/631/34289-10
F +49/631/34289-28
gwolf@cbltech.de



Beitrag als PDF auf
www.sui24.net

TECHNIK

oder verloren werden, sondern deren Festplatten anfälliger sind als stationäre.

Eine dritte Gruppe stellen archivierte Daten dar. Auf Grund geänderter gesetzlicher Bestimmungen ist bei diesen ein gewaltiges Wachstum zu verzeichnen. Datenverluste bei archivierten Daten bedrohen zwar gewöhnlich nicht den Fortbestand eines Unternehmens können aber rechtliche Konsequenzen haben, wenn Aufbewahrungspflichten nicht eingehalten werden. „Compliance“ ist in den letzten Jahren das große Thema der Speicherbranche. Bestimmungen wie der Sarbanes-Oxley Act, GDPdU und GoBS verlangen Aufbewahrungszeiten zwischen sechs und zehn Jahren.

Die Masse der Daten, die sicher gespeichert werden muss, ist daher gewaltig und Unternehmen investieren steigende Summen in Backup und Archivierung. Trotz des großen Aufwands kommt es immer wieder zum Verlust von Daten. Wo liegen die Risiken?

Ursachen des Datenverlusts

Es gibt eine Reihe von Ursachen für den Verlust digitaler Information. Dabei machen offensichtliche Gefahren wie mutwillige Manipulationen, Computerviren und Naturkatastrophen nur rund 25 Prozent aus. Mit rund 75 Prozent überwiegen Funktionsstörungen von Hardware und Software sowie menschliches Versagen.

Hardwarebezogene Ursachen fallen im Wesentlichen in die folgenden Kategorien:

- Headcrash (Aufsetzen des Schreib-/Lesekopfes auf der Datenträgeroberfläche) oder Dejustierung der Festplatte durch starke Erschütterung des Gerätes
- Dauerhafte Einwirkung elektrostatischer Ladungen oder Spannungsspitzen führen zur Zerstörung von Laufwerksplatinen oder RAID-Controllern
- Extreme Umgebungsbedingungen, zum Beispiel starke Temperaturschwankungen oder längere Einwirkung von Feuchtigkeit führen zur Beschädigung von Magnetbändern
- Magnetfelder schwächen die Signale auf Bandspeichermedien
- Verschmutzungen auf Leseköpfen führen zum Reißen von Magnetbändern

Fehler in der Software können dafür verantwortlich sein, dass Sicherungen nicht gespeichert oder überschrieben werden. Bei Datenverlust ohne Hardware-Beteiligung sind die Grenzen zwischen Bedienfehler und Softwarefehler fließend.

Dass Daten sabotiert oder IT-Einrichtungen durch Feuer, Flut und Beben beschädigt werden können, ist natürlich bekannt und eine ganze Industrie bietet Backuplösungen, unterbrechungsfreie Stromversorgung, Firewalls und Antiviren-



Selbst bei Datenträgern, die durch einen Brand beschädigt wurden, ist häufig die Rettung der Daten möglich.

software an. Vor allem in großen Unternehmen und Organisationen wird auch tatsächlich mit großem Aufwand redundante Datenhaltung, Backup und Archivierung betrieben. Warum also wächst ständig der Bedarf an Dienstleistern, die Daten von logisch korrupten oder physikalisch beschädigten Datenträgern rekonstruieren?

Trügerische Sicherheit

Trotz ausgeklügelter Backup-Strategien werden viele Daten bei der Sicherung schlicht vergessen. Laut einer IDC Studie aus dem Jahr 2002 lagen damals bereits bis zu 60 Prozent der Unternehmensdaten ungesichert auf PCs und Notebooks. Mit der steigenden Zahl mobiler Rechner dürfte dieser Anteil bis heute sogar noch gestiegen sein. Backup-Strategien dürfen sich daher nicht auf die zentralen Systeme beschränken, sondern müssen dezentral erzeugte und (zwischen-)gelagerte Daten mit einbeziehen. Dabei ist es notwendig, bei den Mitarbeitern ein Problembewusstsein zu schaffen und einen verantwortlichen Umgang mit digitalen Informationen zu fördern. Ein weiterer Bereich in dem häufig überhaupt keine Datensicherung vorgenommen wird, sind Daten aus dem Produktionsbereich, beispielsweise Steuerungsdaten von CNC-Maschinen.

Bei der Datensicherung können Fehler auftreten, sei es, dass Backups wegen offener Dateien unvollständig sind, nicht die richtigen Da-

ten gespeichert werden, technische Probleme bei den Speichergeräten oder Medien unbemerkt bleiben oder weil Backupsoftware nicht richtig bedient wird. Nach einem White Paper von Veritas sind 97% aller unvollständigen Backups auf geöffnete Dateien zurückzuführen. Die Erfahrung der Datenrettungsdienstleister zeigt außerdem, dass Backup-Zeitfenster zu knapp gewählt werden und die Organisation von Datensicherung und Rücksicherung unzureichend geplant und überprüft wird.

Selbst wenn die gesicherten Daten eine Rücksicherung erlauben würden, gehen sie nach den Erfahrungen der Datenretter erstaunlich oft durch falsche Lagerung der Speichermedien verloren. Doug Owens, der seit über 18 Jahren bei dem weltweit tätigen Datenrettungsdienstleister CBL Data Recovery Technologies Methoden für die Bandspeicherdatenrettung entwickelt, hat eine erschreckende Sorglosigkeit in der Lagerung von Magnetbändern und der Wartung von Laufwerken festgestellt. Nach seiner Schätzung lagern nur 50% der Anwender ihre Bänder korrekt. Beschädigungen oder Bandrisse sind normalerweise auf ein fehlerhaftes Laufwerk oder mangelhafte Lagerung der Bänder zurückzuführen, beispielsweise wenn die Datenträger in extrem warmen Räumen oder solchen mit hohen Temperaturschwankungen gelagert werden. Schlecht gewartete Laufwerke sind ein Hauptgrund für Bänderrisse. Wenn eine Verunreinigung auf einem Kopf nicht entfernt wird, verhärtet sie sich und zieht noch mehr Schmutz an.

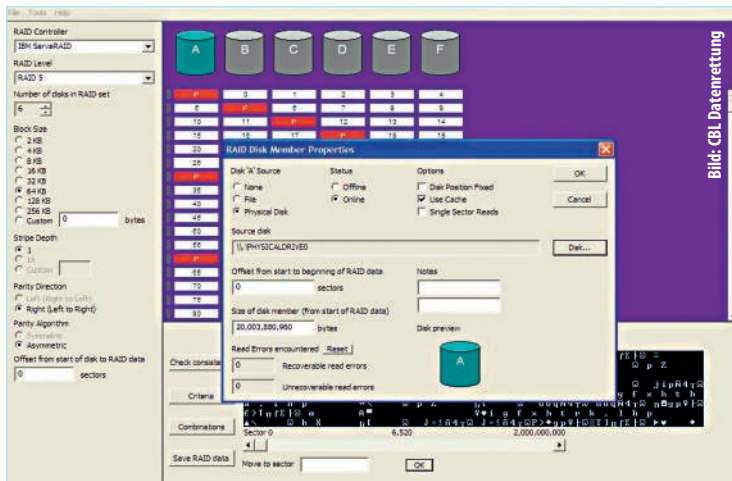


Bild: CBI Datenrettung

Mit Hilfe von Spezialsoftware können RAID-Daten auch ohne RAID-Controller rekonstruiert werden.



Bild: CBI Datenrettung

Wenn Datenrettung als Option in der Notfallplanung vorgesehen ist, können sich Datenrettlabors ohne Verzögerung an die Arbeit machen – die Erfolgsquoten liegen bei über 85 %.

Sobald sich genug Schmutz angesammelt hat, kann dies zu einer Beschädigung oder zum Reißen des Bandes führen. Die Praxis der Schadensfälle zeigt, dass viele Anwender dazu neigen, das Problem immer zuerst beim Medium zu sehen. Reißt ein Band im Laufwerk oder wird von der Spule abgewickelt, sollte man davon ausgehen, dass dies beim nächsten Band, das ins Gerät eingelegt wird, ebenfalls passieren könnte. Oft genug werden aber weitere Versuche mit anderen Bändern gestartet.

Während der Datenverlust bei einem einzelnen gerissenen Band meist relativ gering ist, kann der allmähliche Datenverlust durch Magnetisierung verheerende Folgen haben – und hierzu reicht unter Umständen schon das Magnetfeld einer Leuchtstoffröhre aus. Schleichender Datenverlust ist häufig das heimtückischste Problem, da er erst entdeckt wird, wenn ein Datensicherungszyklus bereits längere Zeit läuft.

Der menschliche Faktor

Ein trügerisches Gefühl der Sicherheit und eine Leugnung der Gefahren erhöht nicht nur das Risiko eines Datenverlusts sondern verzögert außerdem unnötig die Datenrettung durch professionelle Dienstleister. Immerhin können in über 85% der Fälle verlorene Daten rekonstruiert werden. Zu den psychologischen Faktoren gehören die Auswirkungen der Unternehmenshierarchie, wodurch Risiken verschleiert und Probleme verzögert zugegeben werden. Dilettantische Rettungsversuche machen einen Datenverlust oft erst endgültig. Häufig wird zum Beispiel durch Versuche, einen Rechner neu zu starten, der seltsame Geräusche von sich gegeben hat, der mechanische Schaden einer Festplatte verschlimmert. Ein beliebter Fehler ist auch, Hardwarefehlern mit Datenrettungssoftware beikommen zu wollen.

Durch die damit verbundenen Zugriffe auf eine beschädigte Festplatte kann die Datenträgeroberfläche endgültig zerstört werden.

Ein nicht zu unterschätzendes Risiko stellt die Kombination aus falschem Sicherheitsgefühl und hierarchischen Machtverhältnissen dar. Bei der Einrichtung von Backup- und Archivierungssystemen werden mögliche Schwachstellen und die Restrisiken von Dienstleistern und IT-Verantwortlichen gegenüber Vorgesetzten in der Regel nicht thematisiert – schließlich gibt man ja viel Geld aus, um sicher zu sein. Tritt dann doch ein Datenverlust auf, wird er zunächst nicht zugegeben und mit dilettantischen Rettungsversuchen wertvolle Zeit verloren. Die Angst der IT-Mitarbeiter ist nicht unbegründet, wie Datenretter in ihrer Kommunikation mit den Kunden feststellen müssen. Immer wieder werden gerade die Mitarbeiter fristlos entlassen, die als einzige für die Datenrettung nötige Auskünfte hätten geben können. Die Angst, die durch den Verlust unternehmenswichtiger Daten hervorgerufen wird, führt zu kontraproduktiven irrationalen Reaktionen. Datenverlust ist immer eine Ausnahmesituation, doch können größere Schäden durch falsche Reaktionen vermieden werden, wenn man sich der Möglichkeit bewusst ist und entsprechende Notfallpläne entwickelt hat.

Empfehlungen

Die Möglichkeit des Datenverlusts muss bei der Bewertung der IT-bezogenen Risiken trotz bestehender Datensicherungsmaßnahmen mit einbezogen werden und Teil jedes Notfallplans sein. Die Wiederherstellung der Daten aus dem Backup muss im Sinne einer Feuerwehübung praktisch getestet und geübt werden. Das Wissen darüber und die Zuständigkeiten sollten auf mehrere Schultern verteilt und Dokumentatio-

nen getrennt von den gesicherten Daten aufbewahrt werden.

Für Sicherung und Wiederherstellung ist es wesentlich, Prioritäten festzulegen. Die Frage, die sich jedes Unternehmen stellen muss, ist: Welche Daten sind für die Handlungsfähigkeit des Unternehmens unverzichtbar, was wird also so schnell wie möglich gebraucht und was zum Beispiel erst innerhalb einer Woche? Auf diese Weise wird im Notfallplan eine Reihenfolge der Datenwiederherstellung festgelegt. Dies gilt sowohl für planmäßiges Rücksichern aus Backupdaten wie auch für die Datenrettung im Falle des Versagens von Sicherungsmechanismen.

Um im Ernstfall zusätzlich Zeit zu sparen und so die wirtschaftlichen Folgen zu minimieren, bietet es sich an, Datenrettung zu einem Teil von Wartungsverträgen zu machen. So muss nicht erst darüber entschieden werden, ob die Datenrettung z.B. von einer Notebook-Festplatte versucht werden soll, ein Dienstleister gesucht, eine Diagnose erstellt, ein Kostenvoranschlag eingeholt werden müssen. Die Daten werden stattdessen einfach so schnell wie technisch möglich von dem Datenretter, mit dem man einen entsprechenden Vertrag hat, wiederhergestellt.

Zusammenfassend lässt sich feststellen, dass selbst bei optimaler Datensicherheit ein schwer zu kalkulierendes Restrisiko bleibt, durch den Verlust von Daten wirtschaftlichen Schaden zu erleiden. Wird der „Gau“ bei der Erstellung von Sicherheitsbestimmungen, Verfahrensweisen und Notfallplänen thematisiert, lassen sich die Risiken insofern minimieren, als die technischen Möglichkeiten zur Rettung auch tatsächlich ohne zeitliche Verzögerung ausgeschöpft werden können. ■

Weiterführende Infos auf www.sui24.net

more @ click **SIO38500**