




**CA Security Management**

- Umfassende, komplette Lösung
- Unübertroffene Skalierbarkeit
- Integrierbar und modular

Hier klicken und White Paper Security Management herunterladen:  
 "Wie Sie die Sicherheit mit den Geschäftsabläufen in Einklang bringen"

Transforming  
IT Management



**SearchSecurity.de**

Entscheidungswissen für Security-Professionals

[Erweiterte Suche](#)

HOME
INHALTE
MEINUNG
WHITEPAPER
WEBCASTS
SPECIALS
SERVICE
ÜBER UNS
MEINE SEITE

Netzwerksicherheit | Identity- und Access-Management | Plattformsicherheit | Applikationssicherheit | Bedrohungen | Security-Management

HOME > Security-Management > Business Continuity

**Security-Konzepte für Datensicherung und Business Continuity**

**Zeitversetzte Datenspiegelung erlaubt Disaster Recovery auch im WAN**

04.03.2008 | Autor: Lars Albrecht



Datenspiegelung ermöglicht Disaster Recovery auch über große Entfernungen hinweg. Bild: Fotolia/Libelle

**Haftungsrechtlich wird die Sicherung geschäftskritischer Daten zur Chefsache – es gilt, den fortlaufenden Betrieb zu gewährleisten. Disaster-Recovery-Konzepte wie Storage- oder Clustertechnologien verhindern Datenverlust und hohe Folgekosten, schützen jedoch nicht vor logischen Fehlern. Standby-Systeme sichern kritische Daten dank zeitversetzter Spiegelung über weite Entfernungen hinweg. Erfahren Sie in diesem Beitrag mehr über technische Möglichkeiten hinsichtlich Business Continuity.**

Business Continuity hat laut einer Umfrage von Steeleye Technology für vier von fünf IT-Managern höchste Priorität. Über die Hälfte der befragten IT-

Entscheider rechnen mit fatalen Folgen für ein Unternehmen, wenn geschäftskritische Systeme länger als 24 Stunden ausfallen.

Gehen durch einen Fehler kritische Daten verloren, entstehen nicht nur finanzielle Nachteile. Auch immaterielle Schäden wie Imageverlust und Kundenzufriedenheit sind zu befürchten.

Anzeige



Old Server: wenig Leistung, viel Verbrauch.  
Wecken Sie ihn!





**Kraftvoll. Effizient.**

Ein Fehlerfall kann neben Datenverlust und Systemstillständen auch haftungsrechtliche Konsequenzen haben. Die aktuelle Rechtsprechung verpflichtet IT-Verantwortliche, wichtige Systeme und geschäftskritische Daten gemäß gesetzlicher Vorschriften und Rahmenbedingungen vor Ausfällen zu schützen.

Wird die Datensicherung vernachlässigt, ist dies laut Gesetz grob fahrlässig und kann den Fortbestand des Betriebs gefährden. Fällt ein System aus und gehen wichtige Daten verloren, weil kein oder nur ein mangelhaftes Sicherheitskonzept vorhanden ist, haften die IT-Verantwortlichen und die Geschäftsleitung.

**Datenverlust oft durch logische Fehler verursacht**

Aktuelle Studien belegen, dass etwa 70 Prozent aller Ursachen, die zu Datenverlusten führen, auf logische Fehler zurückgehen. Zu den Fehlerquellen gehören

- ▶ beschädigte Datenimporte,
- ▶ Sabotage durch Dritte,
- ▶ fehlgeschlagene Wartungsarbeiten,
- ▶ unbeabsichtigtes Löschen oder
- ▶ Fehler bei der Bedienung komplexer IT-Umgebungen.

Weitere mögliche Fehlerquellen beziehen sich auf die Hardware. So erfolgt die Datenhaltung bei Storage-Technologien wie RAID synchron. Dadurch werden die zerstörten Daten der Originaldatenbank auch fehlerhaft auf das Ausfallsystem übertragen.

In solchen Fällen hilft nur noch eine zeitaufwändige Rücksicherung der Datenbank. Hierbei ist zu beachten, dass neben der Rücksicherung ein umfangreicher Datenverlust von durchschnittlich einem Arbeitstag droht, der nachträglich wieder erfasst werden muss. Kaum ein Unternehmen kann sich einen so langen Systemstillstand leisten.

**Storage-Technologien schützen nicht vor logischen Fehlern**

**WEITERE INHALTE ZUM THEMA**

**Übersicht**

- ▶ **Die nächste unvermeidbare Katastrophe?**  
McAfee bewertet die Auswirkungen von Datenverlusten auf Grundlage einer Online-Befragung.
- ▶ **Gastvortrag ComConsult: Dual-Vendor-Strategie**  
Die Integration von Produkten verschiedener Hersteller in einem Netzwerk wird von vielen Admins verschmäht – zu Unrecht?
- ▶ **Datenvielfalt in IP-Netzen – Herausforderung Voice & Video**  
Voice und Video over IP stellen hohe und völlig neue Anforderungen an die Netzwerkinfrastruktur und die Administratoren.
- ▶ **Prophylaxe gegen Stromausfall & Co.**  
Statistisch gesehen kommt es in Deutschland alle zwei Jahre zu einem Stromausfall.
- ▶ **WLAN-Netze richtig konzipieren und administrieren**  
Drahtlose Netze sind im Firmenumfeld ebenso erwünscht wie gefürchtet – doch auch das größte Problem lässt sich meistern!
- ▶ **Die Roadshow-Agenda und das ProCurve-Team im Überblick**  
Alle Veranstaltungsinhalte im Überblick und die strategischen Ziele der Adaptive Networks Vision im Detail.

Anzeige



PARTNER SOLUTION DAYS & IT-ENTSCHEIDER KONGRESS 2008

EXPERTENTREFFEN
FACHVORTRÄGE
HERSTELLERMESSE



**Anmeldung und Infos hier klicken!**

**TOP 5 - MEIST GELESEN**

**News & Artikel**

1. **Sicheres Dokumentenmanagement für vertrauliche Informationen:** Brainloop Secure Dataroom 7.0 unterstützt Microsoft XPS
2. **Aufrechterhaltung des Geschäftsbetriebs hat für die IT oberste Priorität:** Umfrage von Steeleye über die Bedeutung von Business Continuity
3. **Algin Umove sichert Active Directory:** Active Directory verschieben, klonen und wiederherstellen
4. **In sechs Schritten zum effektiveren Information Leakage Management:** Maßnahmen gegen Datenverlust und Insider Threats im Unternehmen
5. **Erzwingener Neustart von Cisco-Appliances durch Dauerbeschuß von IP-Paketen:** PIX- und ASA-Appliances von Cisco durch DoS-Attacken angreifbar

STORAGE & ARCHIVIERUNG

PARTNER SOLUTION DAYS & IT-ENTSCHEIDER KONGRESS 2008

Storage-Technologien wie RAID (Redundant Array of Independent Disks) oder SAN (Storage Area Network) legen den Fokus auf die Datenabsicherung. Dies geschieht auf einer sogenannten Block-Level-Ebene.

Dabei werden Daten redundant auf mehrere Speichermedien geschrieben, um den Betrieb des Gesamtsystems bei einem IT-Notfall aufrecht zu erhalten. Fällt ein Speichermedium aus, sind die Datenbestände auf einer weiteren Komponente verfügbar.

Vor logischen Fehlern mit korrupten oder gelöschten Daten schützt dies jedoch nicht. Insgesamt sichern die Technologien zwar Server- und Storage-Systeme ab. Sie wurden aber primär für den Bereich der Hochverfügbarkeit entwickelt und reichen für ein verlässliches IT-Disaster-Recovery-Konzept nicht aus.

### **Spiegelsysteme gewährleisten konsistente und korrekte Daten**

Standby-Systeme bieten im Gegensatz zu den Hardware-Technologien speziell für Datenbanken die Möglichkeit, einen Datenbestand vor logischen Fehlern zu schützen.

Zunächst wird die Originaldatenbank auf ein anderes System im LAN oder WAN kopiert. Danach werden alle Veränderungen der Echtdatenbank kontinuierlich auf das Spiegelsystem übertragen. Geschieht das zudem zeitversetzt, bietet diese Lösung einen optimalen Schutz vor logischen Fehlern.

Löscht zum Beispiel ein Mitarbeiter um elf Uhr unbeabsichtigt die Vertriebsdaten, kann auf das Spiegelsystem mit dem Datenbestand von 10:59 Uhr umgeschaltet werden. Damit ist innerhalb weniger Minuten ein Spiegelsystem mit konsistenten und korrekten Daten verfügbar.

Im Vergleich zu den hardwarebasierten Disaster-Recovery-Lösungen oder manuellen Rücksicherungen ist dieses Verfahren deutlich effektiver und effizienter.

### **Disaster-Recovery-Lösungen für Business Continuity**

Insgesamt rücken die Vorteile einer Disaster-Recovery-Lösung immer mehr in das Bewusstsein der Unternehmen. So planen 79 Prozent der von SteelEye befragten IT-Manager, zusätzliche Technologien für eine höhere Verfügbarkeit von IT-Systemen bereitzustellen, um einen fortlaufenden Betrieb zu gewährleisten und damit die Zukunftsfähigkeit des Unternehmens zu sichern.

### **Software überträgt Daten zeitversetzt auf Spiegelserver**

Libelle ist Software-Spezialist im Bereich Disaster Recovery und Hochverfügbarkeit und hat seine Lösung für die zeitversetzte Datenspiegelung konzipiert. So erstellt und verwaltet die Spiegelsoftware automatisch insbesondere Standby-Datenbanken.

Dabei wird die Lösung sowohl auf dem Echt- als auch auf dem Spiegelsystem implementiert. Im laufenden Betrieb und bei voller Verfügbarkeit der Produktivsysteme werden zunächst alle wichtigen Dateien und Datenbanken initial auf das Spiegelsystem übertragen.

Änderungen der Echtseite werden in einen Zeitrichter gelegt. Dieser wirkt zwischen Echt- und Spiegelsystem, indem er die Transaktionen vorübergehend zwischenspeichert. Physisch befindet sich der Trichter auf dem Spiegelsystem, damit er bei Ausfall des Originalsystems zugänglich ist.

Dabei lässt sich dynamisch einstellen, wann die Daten aus dem Zeitrichter auch logisch an den Spiegelserver weitergegeben werden. Fällt die Originaldatenbank aus, lässt sich der Datenbestand vollständig oder bis kurz vor den Zeitpunkt des Fehlers wiederherstellen.

Auf das Spiegelsystem schaltet die Software manuell per Mausklick oder automatisch um. Darauf zugreifende Systeme und Benutzer arbeiten so innerhalb kürzester Zeit mit einem konsistenten Datenbestand weiter.

### **Datenspiegelung über weite Entfernungen**

Neben lokalen Spiegelungen zwischen räumlich nahestehenden Systemen sind durch eine zusätzliche WAN-Funktionalität auch Spiegelungen über weite Entfernungen möglich. Durch die Skalierbarkeit können sowohl KMUs als auch internationale Unternehmen mit weltweit verteilten Rechenzentren globale Disaster-Recovery-Konzepte umsetzen, in denen beispielsweise Systeme interkontinental abgesichert werden.

**Lars Albrecht ist Sales Director der Libelle Sales + Services GmbH & Co. KG.**

Redakteur: Stephan Augsten