

Durchdachte IT-Disaster-Recovery-Konzepte verhindern Datenverlust

Sichere Daten dank zeitversetzter Spiegelung

Fällt ein System aus, gehen meist wichtige Daten verloren. Verschiedene IT-Disaster-Recovery-Konzepte schützen geschäftskritische Daten bei Systemausfällen. Stora- getechnologien wie RAID oder Cluster sichern dabei eher die Hardware ab, während Standby-Systeme mit zeitversetzter Spiegelung die Daten selbst schützen.

Unternehmen erkennen zunehmend die Vorteile und Notwendigkeit einer Disaster-Recovery-Lösung. So hat eine kürzliche Umfrage von Symantec ergeben, dass in jedem zweiten der 900 weltweit befragten Betriebe eine Disaster-Recovery-Lösung bereits zum Einsatz kommt. Rund 45 Prozent der Unternehmen, die kein Sicherheitskonzept besitzen, sahen sich schon mit einem IT-Notfall konfrontiert. Etwa jeder vierte Betrieb (26 Prozent) musste sogar mit zwei IT-Notfällen umgehen.

Logische Fehler hauptverantwortlich

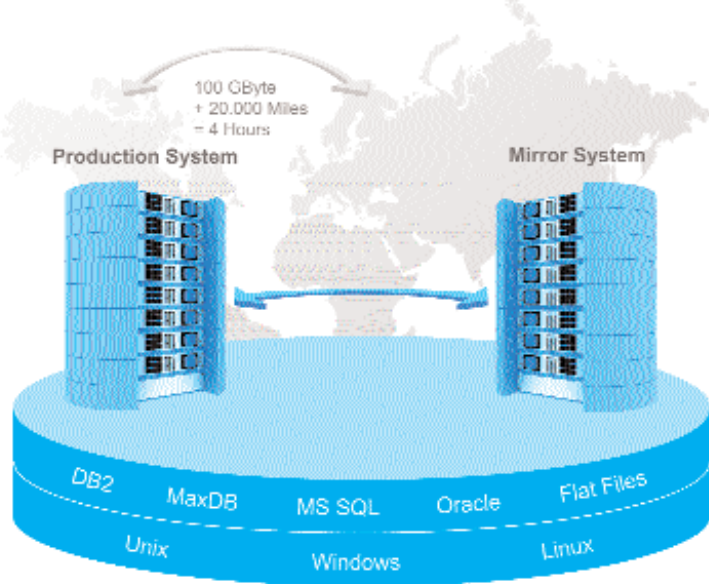
In Sachen Datenverlust gibt es bereits umfangreiche Ursachenforschung. Interessantes Ergebnis: Nicht die Hardware ist die Hauptursache, sondern logische Fehler. Auf diese gehen etwa 70 Prozent der Datenverluste zurück. Zu den häufigsten Fehlerquellen gehören unter anderem beschädigte Datenimporte, Sabotage durch Dritte, fehl-

geschlagene Wartungsarbeiten, vorsätzliche Manipulation oder Löschung von Daten, ungewollte Veränderungen oder Verlust des Datenbestandes durch Benutzerfehler, fehlerhafte Softwareupdates und Skripte. Etwa 30 Prozent der Fehlerquellen beziehen sich auf die Hardware. Storage-Technologien wie RAID (Redundant Array of Independent Disks) oder SAN (Storage Area Network) legen den Fokus auf die Datenabsicherung auf Block-Level-Ebene. Dabei werden Daten redundant auf mehrere Speichermedien geschrieben, um den Betrieb des Gesamtsystems bei einem IT-Notfall aufrechtzuerhalten. Fällt ein Speichermedium aus, sind die Datenbestände auf einer weiteren Komponente verfügbar. Vor logischen Fehlern mit korrupten oder gelöschten Daten schützt dies jedoch nicht: Da die Datenhaltung synchron erfolgt, werden die zerstörten Daten der Originaldatenbank auch fehlerhaft auf das Ausfallsystem übertragen. In diesen Fällen hilft nur noch eine zeitaufwändige Rücksicherung der Daten-

bank. Hierbei ist zu beachten, dass neben der Rücksicherung auch ein umfangreicher Datenverlust von durchschnittlich einem Arbeitstag droht, der nachträglich wieder erfasst werden muss. Kaum ein Unternehmen kann sich einen so langen Systemstillstand leisten. Eine weitere Sicherungsmaßnahme für Datenbestände sind Snapshots. Das sind Momentaufnahmen der gespeicherten Daten beispielsweise in einem SAN. Um den konsistenten Bestand einer Datenbank zu erhalten, ist es nicht möglich, während des Snapshots schreibende Aktionen auf der Datenbank durchzuführen. Daher werden alle Schreibzugriffe gesperrt, die die Produktivdaten verändern können. Das führt allerdings vorübergehend zu einer Unterbrechung der IT-gestützten Geschäftsprozesse. Für ein verlässliches IT-Disaster-Recovery-Konzept sind Technologien, die auf die Hochverfügbarkeit von Server- und Stora- gesystemen zielen, erheblich zu kurz ge- griffen. Spezialisten empfehlen im Rahmen solcher Konzepte, die Systeme räumlich zu trennen, was aber einen immensen techni- schen Mehraufwand und hohe Kosten mit sich bringt. Die Maßnahme verhindert, dass Feuer oder Naturkatastrophen wie Hoch- wasser die Hardware schädigen und die darauf gespeicherten Daten zerstören. Auch sie adressiert jedoch nicht das Haupt- übel der logischen Fehler.

Schutz vor logischen Fehlern durch Standby-Datenbanken

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 Echtzeitdatenbank kontinuierlich auf das Spiegelsystem übertragen. Geschieht das zeitversetzt, übertragen sich logische Fehler nicht gleich automatisch auf das Spiegelsystem. 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 Di-



Grafik (Server_Production_Mirror): Spiegeldatenbanken lassen sich über geeignete WAN-Links auch über weite Entfernungen realisieren. Quelle: Libelle

aster-Recovery-Lösungen oder manuellen Rücksicherungen ist dieses Verfahren deutlich effektiver und effizienter.

Knackpunkt bei diesem Verfahren ist die zeitversetzte Spiegelung, wie sie etwa bei den Disaster-Recovery-Lösungen von Libelle zum Einsatz kommt. Dabei wird die Software 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 Zeittrichter als Zwischenspeicher gelegt. 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 Zeittrichter auch logisch an den Spiegelserver weitergegeben werden. Fällt die Originaldatenbank aus, lässt sich der Datenbestand vollständig oder bis kurz vor dem Zeitpunkt des Fehlers wiederherstellen. Manuell per Mausklick oder automatisch schaltet die Software auf das Spiegelsystem um.

Datenspiegelung über weite Entfernungen möglich

Neben lokalen Spiegelungen zwischen räumlich nahestehenden Systemen sind über eine WAN-Funktion auch Spiegelungen über weite Entfernungen möglich. Dies erlaubt Unternehmen mit weltweit verteilten Rechenzentren, globale Disaster-Recovery-Konzepte umzusetzen, in denen beispielsweise Systeme interkontinental abgesichert werden. Da die Lösung hardware-unabhängig konzipiert ist, lässt sie sich ohne großen Aufwand in die bestehende IT-Landschaft integrieren. Bereits vorhandene Hochverfügbarkeitskonzepte wie Storage- oder Cluster-Technologien können eingebunden und somit weiterhin verwendet werden. Standardschnittstellen gewährleisten die Anbindung der Spiegelungen an System-Monitoring-Umgebungen.

Neben der originären Aufgabe der Systemabsicherung bietet die Softwarelösung einen weiteren Mehrwert. Das Spiegelsystem kann für zusätzliche Aufgaben verwendet werden wie das Auswerten von

Daten oder das Sichern durch klassische Backup-Verfahren. Steht ein Umzug der gesamten Serverlandschaft eines Konzerns an, bleibt das IT-Umfeld dank der Lösung konstant funktionsfähig. Denn die Systeme sind durch die Spiegelseite nahezu unterbrechungsfrei verfügbar. Da der laufende Betrieb bis zur Freigabe des Produktivsystems über das Spiegelsystem abgedeckt wird, lassen sich auch Upgrades und Updates als Gefahrenquellen entschärfen. Daher befinden sich Unternehmen insgesamt mit einem gut durchdachten Disaster-Recovery-Konzept und einem darauf basierenden Notfallplan auf der sicheren Seite.



Lars Albrecht,
Sales Director,
Libelle Sales +
Services GmbH &
Co. KG



Sicher ist besser!
www.lampertz.de

IT-Schutz risk protector LSR

Wirkstoff: Hochverfügbarkeitschutz

Feuer- und Einbruchschutz auf höchstem Niveau

Schützt vor

Wirkt sofort!

IT-Rechenzentren von Lampertz bieten Ihnen extremen Schutz Ihrer IT-Systeme. Ohne Kopf- oder Bauchschmerzen – ohne Wenn und Aber! Zum Beispiel: der einzigartige RISK PROTECTOR LSR 18.6 E – unabhängig zertifiziert (ECB-S) und hochverfügbar.



Info-Hotline 02 6 61/952-2 00
www.lampertz.de

Besuchen Sie uns in
Halle 2, Stand 838
Halle 12, Stand 826





Kompetenz mit Sicherheit