

Das Leistungsportfolio:

Der **IT-SERVICE**

und die **IT-WERTSCHÖPFUNGSTIEFE**

RISIKOMANAGEMENT

IT Effectiveness

BUSINESS IT ALIGNMENT

Capability Maturity Model
Integration

DISASTER RECOVERY

Logische Fehler
als Gefahrenquelle
ausschalten

NEUE ABSATZWEGE

! Frischer Wind • IN DER B2B-WELT

►► Konferenz: 15.-16.4.2008 – München

itsecurity

2008



Enterprise Security

Neu mit Track »Hack Attack«

NEUE ABSATZWEGE
IM INTERNET
Sebastian Neubeck
und Frank Müller
im Interview



Zeitversetzte Spiegelung sichert Daten bei Systemausfällen

Logische Fehler



Das Volumen an digitalen Daten wächst stetig. Laut einer Studie des Marktforschungsinstituts IDC nimmt das Datenwachstum jährlich um 57 Prozent zu. Allein in Deutschland gab es 2006 ein Datenaufkommen von zehn Exabyte¹. Bis 2010 erwarten die Experten ein Volumen von rund 70 Exabyte. Bei diesen großen Datenmen-

Systemausfälle gefährden die Zukunftsfähigkeit eines Unternehmens. Neben Verfahren wie Storage- und Clustertechnolo-

gen werden Sicherung und Speicherung immer mehr zu einer Herausforderung. Gehen geschäftskritische Informationen wie Produktionsdaten, Kundendaten und Geschäftskorrespondenz durch Systemausfälle verloren, kommen hohe Folgekosten auf die betroffenen Unternehmen zu. Diese entstehen beispielsweise durch einen Betriebsstillstand. Die daraus resultierenden Nachteile



als **Gefahrenquelle** ausschalten

sind nicht nur finanzieller Art. Auch immaterielle Schäden wie Imageverlust und Kundenunzufriedenheit gehen damit einher.

Neben dem reinen Datenverlust und möglichen Systemstillständen kann ein Fehlerfall auch haftungsrechtliche Konsequenzen haben. Die Sicherung der Daten wird zur Chefsache. Denn die aktuelle Gesetzgebung nimmt auch die IT-

mangelhaftes Sicherheitskonzept vorhanden ist, haften die IT-Verantwortlichen und die Geschäftsleitung.

Systemausfälle und ihre Ursachen

Hardwareausfall, Software- oder Anwenderfehler, Naturkatastrophen oder Sabotage: Systemausfälle können viele Ursachen haben. Dabei ist in den Köp-

werden. Geschäftsschädigende Auswirkungen sind die Folge. So fand die Symantec Corporation in einer Umfrage heraus, dass 75 Prozent der befragten deutschen Unternehmen große Wettbewerbsnachteile befürchten, wenn ein System ausfällt. Über die Hälfte (54 Prozent) rechnen mit verärgerten Kunden, Reputations- und Vertrauensverlust.

Bild: iStockphoto

nehmens. Unterschiedliche IT-Disaster-Recovery-Konzepte verhindern Auswirkungen wie Datenverlust und hohe Folgen sichern Standby-Systeme mit zeitversetzter Spiegelung geschäftskritische Daten über weite Entfernungen hinweg.

Verantwortlichen in die Pflicht, wichtige Systeme und damit geschäftskritische Daten gemäß den aktuellen gesetzlichen Vorschriften und Rahmenbedingungen vor Ausfällen zu schützen. Wird die Datensicherung vernachlässigt, ist dies laut Gesetz grob fahrlässig und kann den Fortbestand des Betriebes gefährden. Fällt ein System aus und gehen wichtige Daten verloren, weil kein oder nur ein

fen der IT-Verantwortlichen meist noch der Grundsatz verankert, dass die physische Absicherung im Bereich der Server- und Storage-Systeme die Herausforderung eines IT-Notfalls löst. Das ist jedoch nicht umfassend genug gedacht. Hardware ist zwar ersetzbar. Ein korrekter Datenbestand sowie individuelle Anwendungen können damit jedoch nicht wieder beschafft

Logische Fehler häufigster Grund

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. Da bei Storage-Technologien wie RAID 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 Datenbank. 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.'

WEB-TIPP:

www.libelle.com

Hardware-Technologien: sinnvoll aber nicht ausreichend

Die einzelnen Hardwarekomponenten wie Server- und Stagesysteme können durch verschiedene Ansätze abgesichert werden. Bei Serversystemen spielen Cluster-Technologien eine große Rolle, da sie vor Serverausfällen schützen. Aufgrund des komplexen Systems ist der Administrationsaufwand hoch und eine regelmäßige, intensive Pflege unerlässlich. Gehen Daten bei einem Systemausfall verloren, bietet das Clustersystem keinen Schutz.

Storage-Technologien speichern Daten redundant

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. Darüber hinaus können Snapshots eingesetzt werden, um die Datenbestände zusätzlich abzusichern. Snapshots sind Momentaufnahmen der gespeicherten Daten beispielsweise in einem SAN. Um den konsistenten Bestand einer Datenbank

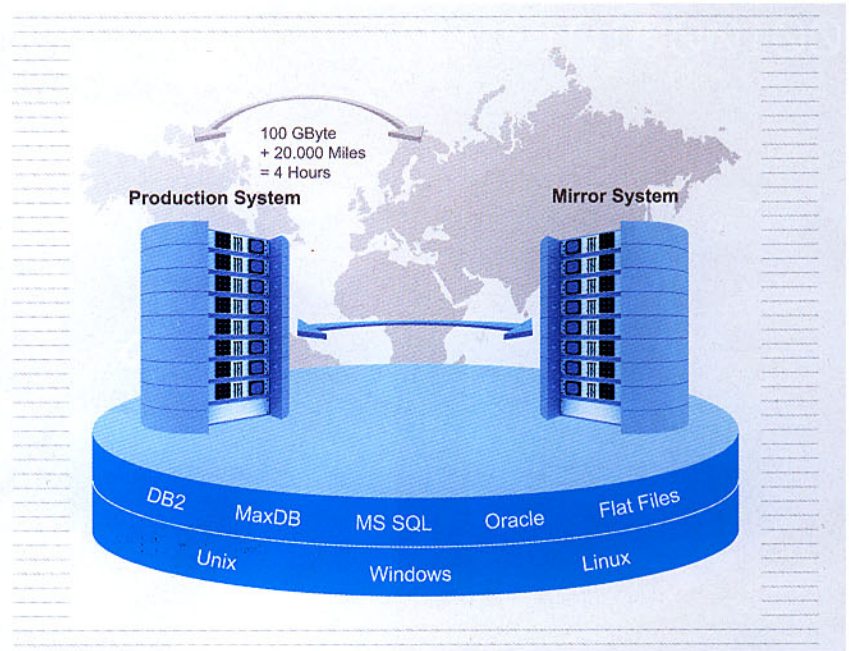


Bild 1: Ein Spiegelsystem als Disaster-Recovery-Lösung ermöglicht es, Daten interkontinental abzusichern.

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.

Räumliche Trennung mit hohem Aufwand verbunden

Insgesamt sichern die Technologien zwar Server- und Stagesysteme ab. Sie wurden aber primär für den Bereich der Hochverfügbarkeit entwickelt und reichen für ein verlässliches IT-Disaster-Recovery-Konzept nicht aus. Spezialisten empfehlen im Rahmen solcher Konzepte, die Systeme räumlich zu trennen, was einen erheblichen technischen Mehraufwand und hohe Kosten mit sich bringt. Nur dadurch lässt sich verhindern, dass Feuer oder Naturkatastrophen wie Hochwasser die Hardware schädigen und die darauf gespeicherten Daten zerstören. Logische Fehler stellen darüber hinaus auch weiterhin eine Gefahr dar. Dazu gehören neben Sabotage, insbesondere der vorsätzlichen Manipulation oder Löschung von Daten, ungewollte Veränderungen oder Verlust des Datenbestandes durch Benutzerfehler, fehlerhafte Softwareupdates und Skripte.

Standby-Datenbanken – Spiegelung von Transaktionen

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 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.

Software automatisiert zeitversetztes Recovery

Die patentierte Lösung von Libelle, Softwareanbieter im Bereich Disaster Recovery und Hochverfügbarkeit, würde für die zeitversetzte Datenspiegelung konzi-

piert. So erstellt und verwaltet die Software 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 Zeittrichter 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 Zeittrichter auch logisch an den Spiegelsystem weitergegeben werden. Fällt die Originaldatenbank aus, lässt sich der Datenbestand vollständig oder bis kurz vor den Zeitpunkt des Feh-

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

Interkontinentale Sicherung der Systeme möglich

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

Einfache Integration in bestehende IT-Landschaft

Da die Lösung hardwareunabhängig konzipiert ist, lässt sie sich ohne großen Aufwand in die bestehende IT-Landschaft integrieren. Bereits vorhandene Hochverfügbarkeitskonzepte können eingebunden und somit weiterhin verwendet werden. Standardschnittstellen gewährleisten die Anbindung an System-Monitoring-Umgebungen.

Entlastung des Produktivsystems

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.

Sicherheitskonzepte gewährleisten Zukunftsfähigkeit

Die Vorteile einer Disaster-Recovery-Lösung rücken immer mehr in das Bewusstsein der Unternehmen. So hat eine Umfrage von Symantec ergeben, dass in jedem zweiten der befragten Unternehmen 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. Für jedes Unternehmen ist es daher unerlässlich, Vorsorgemaßnahmen zu treffen. Dabei gilt es, konkrete Anforderungen an ein Sicherheitskonzept im Vorfeld zu definieren. Mit einem gut durchdachten Disaster-Recovery-Konzept und einem darauf basierenden Notfallplan befinden sich Unternehmen auf der sicheren Seite. So tragen Sicherheitskonzepte zur Zukunftsfähigkeit eines Unternehmens bei.

LARS ALBRECHT

Disaster-Recovery-Lösungen

Leitfaden für die Auswahl einer IT-Disaster-Recovery-Lösung.

- 1 Geschäftskritische Prozesse und Daten identifizieren**
Bei geschäftskritischen Prozessen und Daten handelt es sich meist um zentrale Systeme wie ERP oder Informationssysteme, die für den Betrieb einer Organisation überlebensnotwendig sind.
- 2 Risiken definieren**
Vulkanausbrüche, Kriege oder Tsunamis bergen für in Deutschland ansässige Unternehmen ein geringes Risiko. Ausbrechendes Feuer, Naturkatastrophen wie Hochwasser oder Sabotage sind viel wahrscheinlicher für Systemausfälle. Risiken bergen beispielsweise auch häufige Softwareupdates der kritischen Systeme.
- 3 Lösungsszenarien erarbeiten**
Sind die Risiken definiert, sollten Unternehmen unterschiedliche Lösungsszenarien erarbeiten. Wie lassen sich Daten schützen, wenn Feuer ausbricht, Softwareupdates fehlschlagen oder Bestände gelöscht werden?
- 4 Dienstleister vergleichen – Referenzen einfordern**
Zahlreiche IT-Dienstleister bieten mittlerweile Disaster-Recovery-Lösungen an. Zu vergleichen sind dabei die jeweiligen Sicherheitsverfahren, auf die die Anbieter setzen. In einem weiteren Schritt gilt es, die Angebote verschiedener Dienstleister zu prüfen und Referenzen einzufordern.
- 5 Lösung in Testumfeld prüfen**
Hat sich ein Unternehmen für eine Lösung entschieden, sollte sie in einer Testumgebung vorab geprüft werden: Hierbei ist es notwendig, die erarbeiteten Lösungsszenarien zu simulieren, um deren Praxistauglichkeit sicherzustellen.
- 6 Regelmäßige Notfallübungen**
Ergänzend dazu raten Experten, regelmäßig organisatorische und technische Notfallübungen für den Katastrophenfall durchzuführen. Diese sollten auch dokumentiert und ausgewertet werden.