

Backup und Archivierung

Virtualisierung
UMTS-Backup
Enterprise Search
Notfallplanung
mit Marktübersicht
E-Mail-Archivierung



Zahlreiche Teilnehmer auf Frühjahrskonferenzen

Cisco Expo, Troopers 08,
RSA Conference

Update bei Kabelsystemen

Normierungsfortschritt
für 40GbE und 100GbE

Carrier und Service-Provider

mit Anbieterübersicht
VPNs als Service

Vorausschau verhindert Katastrophen

Notfallplanung für Backups und Restore

Viele Unternehmen vernachlässigen ihre Datensicherung – und wenn regelmäßig gesichert wird, findet oft kaum ein Test zur Rücksicherung statt. Noch weniger existiert ein konkreter Notfallplan, der genau beschreibt, welche Maßnahmen im Falle eines Datenverlustes ergriffen werden müssen, um zügig wieder zum Geschäftsalltag zurückkehren zu können. Dabei kann gerade eine gute Notfallplanung helfen, lange Ausfallzeiten zu verhindern und den Schaden eines Datenverlustes möglichst gering zu halten.

Jeder kennt diese Situation: Die Chefsekretärin sucht eine Präsentation für ein Meeting mit einem wichtigen Kunden, die sie Tags zuvor angefertigt hat. Sie kann sie jedoch nicht finden, aus welchen Gründen auch immer. Für eine Neuauflage fehlen wichtige Daten und vor allem Zeit. Existiert in diesem Unternehmen keine klare Notfallplanung, passiert daraufhin vielleicht Folgendes: Verzweifelt ruft die Mitarbeiterin beim Administrator an, muss jedoch feststellen, dass dieser im Urlaub ist. Es vergeht wertvolle Zeit, bis sie endlich einen anderen Ansprechpartner aus der Technik erreicht. Dieser Mitarbeiter aber kennt sich mit dem Sicherungssystem nur mäßig aus, eine Rücksicherung hat er noch nie gemacht. Bis er sich zurechtfindet und die passende Datei wiederherstellen kann, ist ein halber Tag vergangen und der Termin mit dem wichtigen Kunden geplatzt.

Bei einer korrekten Notfallplanung wüsste die Chefsekretärin sofort, wer der Zuständige oder in diesem Falle sein Stellvertreter ist und könnte diesen unverzüglich alarmieren. Da der fragliche Mitarbeiter mit dem System bestens vertraut wäre, erfolgte eine Rücksicherung der Präsentation relativ schnell, und der Kundentermin könnte wie geplant stattfinden.

Ebenso unentbehrlich ist ein ausgeklügelter Notfallplan im Falle eines Komplettver-

lusts der elektronischen Daten. Eine zügige Rücksicherung und damit die zeitnahe Wiederaufnahme des Geschäftsalltags können für den Fortbestand eines Unternehmens entscheidend sein. Daher gehört ein Notfallplan zu jedem guten IT-Security-Konzept. Bei der Ausgestaltung spielt vor allem die Frage nach der Wichtigkeit



Ohne gute Planung und Übung gehen gerade im Notfall oft die einfachsten Handgriffe schief
Quelle: Netcos/Tatjana Schötz

der elektronischen Daten für ein Unternehmen eine große Rolle. Wichtige Überlegungen hierzu sind:

- Zu welchem Zweck nutzt das Unternehmen elektronische Daten? Zu welchem Zeitpunkt nutzt das Unternehmen die Daten?
- Welche Auswirkungen hat es für die Geschäftsprozesse, wenn die Daten mehr als einen Tag nicht verfügbar oder ganz verloren sind?

Es gibt einige Punkte, die beim Erstellen eines geeigneten Notfallplans unbedingt beachtet werden sollten. So müssen bereits im Vorfeld die Zuständigkeiten geklärt werden. Insbesondere muss feststehen, wer für die Durchführung der Maßnahmen im Notfall die Verantwortung trägt und wer im Fall des Falles die Vertretung übernimmt. Nach Möglichkeit sollte auch ein Manager in die Planung einbezogen werden, um mit seiner Hilfe schnell auf unvorhergesehen Umstände reagieren zu können. Wichtig ist, die Mitarbeiter mit der Notfallplanung vertraut zu machen und sie regelmäßig zu schulen. Außerdem ist zu klären, wie sich eine schnellstmögliche Alarmierung umsetzen lässt und wer genau im Notfall zu benachrichtigen ist.

Der Notfallplan muss ausgewählten Mitarbeitern, die auf ihre elektronischen Daten angewiesen sind, geläufig und gut zugänglich sein. Dies muss auch nach einem Komplettausfall und nach einem Katastrophenfall gelten, weshalb der Plan nicht etwa nur im Haus ausgedruckt hinterlegt sein sollte, sondern auch an einem räumlich getrennten Ort.

Je nach Geschäftsfeld des Unternehmens und Bedeutung der Daten für das Unternehmen ist auch die Frage zu klären, ob es nötig ist, bei einem Datenverlust außerhalb der Bürozeiten sofort zu reagieren – oder ob ein Restore zu normalen Geschäftszeiten ausreicht. Aus diesen Aspekten leitet sich ab, ob ein Bereitschaftsdienst dafür eingerichtet werden muss. Im Bereitschaftsfall ist noch zu klären, welche Daten derart wichtig sind, dass sie sofort zurückgesichert werden müssen, und welche Daten zu einem späteren Zeitpunkt wiederhergestellt werden können. Der Notfallplan muss folgende Informationen enthalten:

- sämtliche Kontaktdaten der zu alarmierenden Personen,
- die der Zuständigen und Stellvertreter sowie zum Beispiel des Stromversorgers,
- des Ausweichrechenzentrums (falls vorhanden),
- des externen Datenträgerarchivs,
- aller IT-Wartungsfirmen, mit denen Supportverträge bestehen, und
- der Hersteller und Händler, bei denen die Hardware und Software bezogen wurde.

Es sollten klare Handlungsanweisungen für bestimmte Stufen eines Datenverlustnotfalls ausformuliert werden, gestuft nach Wichtigkeit der Daten und Umfang des Schadens – zum Beispiel Verlust einer einzelnen Datei, Kompletterverlust oder Defekt eines Systems. Nicht nur Anweisungen für die Mitarbeiter, sondern vor allem Handlungsanweisungen für die zuständigen Personen sollten genau dokumentiert sein. Extrem wichtig ist, dass eine ausführliche Dokumentation über die Durchführung einer Rücksicherung existiert und für den Verantwortlichen schnell greifbar ist. Diese Dokumentation sollte alle Maßnahmen für ein Restore Schritt für Schritt auflisten und so verfasst sein, dass notfalls auch eine außenstehende IT-versierte Person damit zurechtkommt.

Ein wichtiger Bestandteil außerdem: Wo liegen die Sicherungen und wie kommt man an sie heran? Da diese Dokumentation vertrauliche Daten enthält, sollte sie nur für

Verantwortliche zugänglich sein. Bei einer Neuerung des Sicherungssystems oder einer Änderung der Zuständigkeiten oder sonstigen Änderungen müssen die Dokumentationen und Notfallanweisungen sich immer auf den neuesten Stand befinden. Die Mitarbeiter sollten über Änderungen auf dem Laufenden gehalten werden. Bei der Formulierung eines Notfallkatalogs ist darauf zu achten, klare, kurze Aussagen zu treffen, die prägnante, leicht verständliche Handlungsanweisungen darstellen. Für ein leichteres Erfassen der Zusammenhänge können Grafiken eingearbeitet sein. Ein Unternehmen sollte mindestens einmal im Jahr regelmäßige Probedurchläufe verschiedener Notfallsituationen anhand des Notfallplans durchführen, und zwar mit den Verantwortlichen und allen Mitarbeitern, damit diese das richtige Verhalten in einer kritischen Situation üben können. Sinnvoll ist es, auch hier einen Verantwortlichen zu benennen, der die Probeläufe re-

gelmäßig initiiert und überwacht. Dieser kann bei Unregelmäßigkeiten im Ablauf oder bei auftauchenden Defiziten im Notfallplan Anpassungen anstoßen. Nach einem kompletten Restore ist zu prüfen, ob tatsächlich alle Daten zurückgesichert wurden. Je nach System und Wichtigkeit der Daten werden bei Totalverlust oft nicht sofort alle Dateien wiederhergestellt. Das kann unter Umständen zu Problemen führen, wenn später vergessen wird, die noch fehlenden Daten zurückzuspielen. Auf neuen Sicherungen sind diese Daten dann nicht mehr vorhanden, und nach einer bestimmten Zeit besteht die Gefahr, dass die Daten über eine möglicherweise aktive Retention Policy gelöscht werden.

Jeder noch so gute Notfallplan setzt ein notfallgerechtes Backup voraus. Auch bei den Sicherungsmethoden gibt es einige Unterschiede. Man sollte sich vor allem die wichtigsten Vor- und Nachteile der inhouse betriebenen Bandsicherung gegenüber ei-



Wenn nichts mehr geht...

Disaster Recovery mit BusinessShadow®

Wir können keinen Systemcrash vermeiden. Aber die Folgen blitzschnell rückgängig machen.

Wenn Ihr System nach Software-, Hardware- oder Eingabefehlern ausfällt oder Katastrophen auftreten, drehen Sie einfach die Zeit zurück – mit Libelle BusinessShadow®.

Egal, ob die Entfernung zum Spiegelserver 100 Meter oder tausende von Kilometern beträgt. Durch die zeitversetzte Datenspiegelung stehen Ihnen Ihre Datenbanken, File-Systeme und Anwendungen jederzeit zur Verfügung. Innerhalb von Minuten. Mit dem fehlerfreien Datenbestand vor dem Systemausfall.

Erfahren Sie alles über den kosteneffizienten Schutz Ihrer Daten im Katastrophenfall unter

www.libelle.com/de oder
Tel. +49 (0)711 / 78335-0

Libelle

Libelle Sales + Services GmbH & Co. KG
Gewerbestraße 42 | D - 70565 Stuttgart

T 0711 / 78335-0 | F 0711 / 78335-148
sales@libelle.com | www.libelle.com

Unterschiedliche Rücksicherungsverfahren

Rücksicherungsverfahren einer Datei bei herkömmlicher Bandsicherung:

- Anhand der Katalogdatei wird ermittelt, auf welchem Band die Datei liegt.
- Das Band wird verfügbar gemacht, entweder per Library oder von Hand.
- Voraussetzung: Band und Laufwerk waren in Ordnung, die Sicherung ist gelaufen.
- Die Datei wird auf dem Band gesucht, das Band muss bis zur betreffenden Datei durchgelesen werden.
- Die Datei wird zurückgesichert.

Rücksicherungsverfahren einer Datei bei Remote Backup:

- Am Sicherungs-Client wird eine Verbindung zum Serviceanbieter aufgenommen.
- Über den Rücksicherungsassistenten des Sicherungs-Clients wird die Datei bestimmt, die zurückgesichert werden soll.
- Es erfolgt ein direkter Zugriff auf sämtliche Versionen dieser Datei.
- Die Datei wird wiederhergestellt.
- Die Zeiten der Rücksicherung sind nur durch die Bandbreite der verfügbaren Internetverbindung limitiert.

nem Remote-Backup bewusst machen. Viele Firmen sichern ihre Datenbestände auf Bändern, doch diese Art der Sicherung birgt viele mechanische Schwachstellen. Bänder haben nur eine bestimmte Lebensdauer und können nicht beliebig oft überspielt werden. Da aber deren Anschaffung teuer ist, erneuern Unternehmen Bänder nicht allzu oft. Dies erhöht die Gefahr, dass Bänder aufgrund von Defekten irgendwann nicht mehr lesbar sind und Verschleißerscheinungen zeigen. Zudem ist eine Sicherung mit Band sehr zeitintensiv. Bänder

wollen eingelegt, das System verwaltet und regelmäßig gewartet sein. Die Bänder sind regelmäßig auf ihre Funktionalität hin zu überprüfen. Diese Zeit sowie die zugehörigen Ressourcen fehlen den Unternehmen oft.

Besonders wichtig ist es, die Sicherungsbänder, ein zugehöriges Laufwerk sowie die Software inklusive Lizenzschlüssel und die Katalogdatei räumlich getrennt vom übrigen System zu lagern. Die Sicherungsträger müssen zudem vor möglichen Zugriffen Dritter geschützt vorliegen.

Was gehört zu einer guten Backup-Restore-Notfallplanung?

Voraussetzung: ein funktionierendes Datensicherungssystem, eine regelmäßige und zuverlässige Sicherung der Daten sowie die geregelte Auslagerung der Datensicherungsmedien.

- Benennung der Verantwortlichen, der Stellvertreter und Bevollmächtigten,
- Aufstellen von Vertretungsregeln, eventuell auch eines Bereitschaftsplans,
- Aufstellung eines Alarmierungsplans,
- umfangreiche Adress- und Kontaktdatenliste,
- Definition der möglichen Notfälle,
- allgemeine Verhaltensregeln in Notfällen,
- detaillierte Handlungsanweisungen für klar definierte Notfallsituationen,
- Beurteilung der Wichtigkeit von bestimmten Daten,
- Auflistung der Verfügbarkeitsanforderung für bestimmte Dateien,
- IT-Inseln im Backup-Konzept sowie im Restore-Plan nicht vergessen,
- ausführliche Dokumentation über eine Rücksicherung,
- Aufbewahrungskonzept für die Notfallanweisungen und der Dokumentationen,
- regelmäßige Notfalltests,
- Schulung, Sensibilisierung und Einbezug der Mitarbeiter und
- Überprüfung der Daten auf Vollständigkeit nach einem Komplett-Restore.

Eine Alternative zur herkömmlichen Bandsicherung bietet das Remote-Backup. Hier werden die Daten bereits vor der Übertragung stark verschlüsselt und dann über eine Internetdatenleitung zu einem entfernten Rechenzentrum gesendet und dort gespeichert. Dieses Verfahren bietet einige Vorteile. Der Zeitaufwand für eine ordnungsgemäße Sicherung reduziert sich enorm, und das Backup läuft vollautomatisch im Hintergrund. Es entfallen die Wartung des Systems und das lästige Bandwechseln. Es müssen außerdem keine Sicherungsmedien angeschafft werden, und das Problem der Lagerung erledigt sich auch, da die Sicherung stets räumlich getrennt zum System im Rechenzentrum des Backup-Providers liegt. Beim Remote Backup kann ein Unternehmen die Regel der zeitlichen Sicherungsabstände selbst bestimmen, möglich ist sogar eine permanente Sicherung (CDP, Continuous Data Protection), sobald Daten sich geändert haben. Eine Bandsicherung läuft dagegen oft nicht einmal täglich ab.

Meist spielen Sicherheitsbedenken vor allem im Hinblick auf die Übertragung der Daten eine große Rolle bei der Wahl des Sicherungssystems. Aber gerade vor Gefahren aus dem Netz, wie zum Beispiel Hackerangriffen, braucht man sich bei den ausgelagerten Daten keine Sorgen zu machen, wenn man einige Qualitätsmerkmale bei der Auswahl des Anbieters beachtet. Wichtig ist, dass die zu sichernden Daten bereits vor der Übertragung lokal stark verschlüsselt und auch auf dem Zielsystem verschlüsselt abgelegt sind. Es ist auch darauf zu achten, dass der Anwender selbst seinen Schlüssel generiert. Damit ist nur er in der Lage, seine gesicherten Daten auszulesen. Dritte können mit den verschlüsselten Daten nichts anfangen. Wichtig bei Remote Backup ist die sichere Hinterlegung des Schlüssels, er muss gut aufbewahrt und vor Zugriffen Dritter geschützt werden.

Tatjana Schötz, Gunther Pipperr
und Stanislaw Panow/wj

Gunther Pipperr und Stanislaw Panow sind Geschäftsführer von Netcos. Tatjana Schötz ist freie Journalistin.