

BACKUP

Die Lebensversicherung der Daten

In jedem Unternehmen fallen tagtäglich eine Vielzahl von Daten an. Der Verlust dieser kann weit reichende Konsequenzen haben. Aus diesem Grund gilt es, diese Daten sicher aufzubewahren und bei Bedarf wiederherzustellen.

AUTOR: ANDREAS WISLER

Welche Daten müssen gesichert werden?

Als erstes stellt sich die Frage, was überhaupt gesichert werden soll und muss. Dies global zu beantworten ist praktisch nicht möglich. Zu unterschiedlich sind die Anforderungen. Daher gilt es vor dem Einsatz eines Backup-systems zu überlegen, welche Daten für das Überleben der Firma notwendig sind. Nicht zu vergessen sind die portablen Geräte, wie Handhelds, Memory Sticks, Laptops etc. Anschliessend müssen die verschiedenen Abteilungen und Personen für Ihren Bereich angeben, auf welche Daten sie in welcher Zeit wieder zugreifen müssen. Mit diesen Angaben kann anschliessend mit der Planung des Backups begonnen werden.

Backupmöglichkeiten

Die Backupmöglichkeiten sind sehr vielfältig. Die gebräuchlichsten sind nachfolgend mit ihren Vor- und Nachteilen aufgelistet. Beachten Sie, dass ein RAID, Diskmirroring oder ein zweiter Server zwar die Datensicherheit erhöhen, jedoch können diese nicht so schnell ausser Haus gebracht werden.

Speicherung auf Tape(s)

Der Markt bietet hier eine Vielzahl von Möglichkeiten: DAT, DLT, LTO, AIT sind typische Bezeichnungen dafür. Doch welche Lösung ist nun die richtige? Dies hängt mit den zu sichernden Daten zusammen. Wie viel Platz wird benötigt? Wie stark können die Daten komprimiert werden? In welcher Zeit muss das Backup durchgeführt sein? Mit den An-

gaben aus dem ersten Abschnitt kann das richtige Medium bestimmt werden. Wenn bei der Planung klar wird, dass ein Band alleine nicht ausreicht, kann ein Bandroboter in Betracht gezogen werden.

Backup auf Wechsel-Harddisk

Der Zeitfaktor spielt immer eine grössere Rolle, vor allem in Betrieben, in welcher ein 24h-Betrieb herrscht. Die billigste und oft auch einfachste Möglichkeit ist es, die Daten auf eine Wechsel-Harddisk oder eine SAN-Station zu sichern. Der Schreibzugriff auf diese Datenträger ist um ein x-faches schneller als auf das Band. Diese Sicherungs-Festplatte muss, wie das Band auch, sicher aufbewahrt werden.

Daten auf CD oder DVD brennen

Viele Rechner werden heute mit einem CD- oder gar DVD-Brenner ausgeliefert. Da liegt es natürlich nahe, dieses Medium auch für das Backup zu verwenden. Obwohl auch eine DVD nicht an die Kapazität eines Bandes herankommt, kann sich dies lohnen. Sicherheitshalber sollten nur vollständige Backups gemacht werden. Dabei muss jeden Tag ein neues Medium eingelegt werden.

Images

Eine immer populärer werdende Sicherungsart ist das Erstellen eines Images. Dies kann nach dem Starten eines speziellen Betriebssystemes (für Serversysteme vermutlich nicht durchführbar) oder im laufenden Betrieb erfolgen. Dabei wird eine 1:1-Kopie der ge-

samten Platte erstellt. Bei einer Wiederherstellung muss nur die entsprechende Datei wiederhergestellt werden.

Arten des Backups

Die Durchführung des Backups kann auf verschiedene Arten erfolgen:

Full-Backup

Beim Fullbackup werden alle markierten Daten gesichert.

Differential Backup

Bei dieser Art des Backups werden nur die seit dem letzten Backup neuen oder veränderten Daten gesichert.

Inkremental Backup

Dabei werden alle Veränderungen seit dem letzten Full-Backup gesichert.

Welche Art nun ausgewählt wird, hängt davon ab, wie viele Daten gesichert werden, wie viel Platz zur Verfügung steht und wie schnell die Daten bei einem Verlust wieder hergestellt werden müssen. Einzelne Dateien wieder herzustellen kann sehr schnell geschehen, jedoch eine komplette Wiederherstellung dauert bei einem differentiellen Backup länger als bei einem inkrementellen oder vollständigen Backup.

Rotationsverfahren

Um eine optimale Sicherung auch über einen grösseren Zeithorizont gewährleisten zu können, existieren verschiedene Rotations-

verfahren. Der Hauptunterschied zwischen diesen Verfahren liegt in der Anzahl der benötigten Medien und im Zeitraum, nach dem die Medien in das Rotationsschema zurückkehren (Sicherungshorizont).

Sicherungsstrategie: Sohn

Medien: mindestens 1;
Sicherungshorizont: letzte Sicherung



Beim Sohn-Schema wird jeden Tag eine Gesamtsicherung durchgeführt. Bei einem Band wird dieses jeden Tag überschrieben und bietet keine Möglichkeit an ältere gelöschte Daten zu gelangen.

Sicherungsstrategie: Vater/Sohn

Medien: mindestens 6;
Sicherungshorizont: zwei Wochen

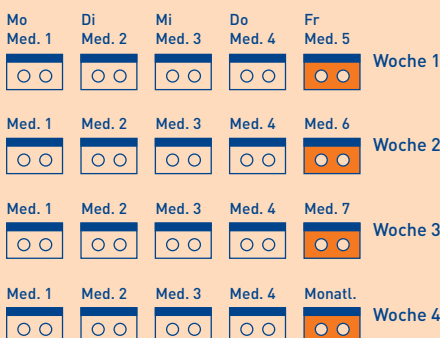


Das Vater/Sohn Schema ist eine Kombination aus Gesamtsicherungen und Differential- bzw. Inkremental-Sicherung über einen Zeitraum von zwei Wochen.

Bei dieser Strategie werden vier Medien für die Differential- oder Inkrementalsicherung von Montag bis Donnerstag benötigt. Die restlichen zwei Medien enthalten Gesamtsicherungen und werden erst nach zwei Wochen wieder überschrieben.

Sicherungsstrategie: Grossvater

Medien: mindestens 19;
Sicherungshorizont: ein Jahr



Das Grossvater Schema ist eine der am häufigsten verwendeten Backupstrategien. Bei dieser Sicherungsstrategie werden vier Medien für die Differentialsicherung von Montag bis Donnerstag gebraucht. Drei Medien enthalten die Gesamtsicherung am Freitag. Die restlichen zwölf Medien sind für monatliche Sicherung reserviert (Woche 4) und werden nicht mehr überschrieben.

Lagerung der Datenträger

Die Sicherungsmedien gehören zwingend an einen anderen Ort. Sie dies nun extern, zum Beispiel in einem Banksafe, oder mindestens in einem anderen Brandabschnitt. Oft werden die Backup-Datenträger aus Bequemlichkeitsgründen direkt neben der Sicherungsstation deponiert. Bei einem Brand sind diese Medien mit den Originaldaten zusammen verloren.

Generell gilt, dass die Medien in einen feuer-, rauch- und wasserfesten Tresor gehören. Wasserfest, da zur Bekämpfung eines Brandes Wasser zum Einsatz kommt. Es wäre schade, wenn die Datenträger das Feuer überstanden haben, jedoch „untergegangen“ sind.

Wiederherstellung von Daten

Einzelne Dateien wieder herzustellen, gehört für Administratoren fast schon zu den täglichen Arbeiten. Sehr schnell ist eine Datei absichtlich oder unabsichtlich gelöscht und muss von den Sicherungsbändern zurückgeholt werden. Ob dabei auch in einem Notfall schnell auf die Daten zurückgegriffen werden kann, ist aber meistens nicht bekannt.

Ein Desaster liegt unter anderem dann vor, wenn nicht mehr auf dem üblichen System eine Wiederherstellung durchgeführt werden kann. Daher sollte in regelmässigen Abständen, mindestens nach einer Anpassung des Backup-Plans, ein Desaster-Recovery (d.h. eine vollständige Wiederherstellung) durchgeführt werden. Dazu sollte ein neues System so vorbereitet sein, dass ein Bandlaufwerk angeschlossen werden kann. Nun gilt es, alle Daten von den entsprechenden Medien zurück zu holen. Sollten nur Daten darauf gespeichert sein, ist dies weiter nicht problematisch. Schwieriger wird es, wenn auch das Betriebssystem und Applikationen darauf gesichert wurden. Oft klappt die Wiederherstellung dieser Daten nur noch auf einem baugleichen System. Daher sollte hier

zusätzlich ein identisches Ersatz-Gerät bereit stehen oder ein entsprechendes Konzept vorhanden sein.

Kontrollen

Mit dem Durchführen des Backups alleine ist es jedoch nicht getan. Nach jeder Sicherung sollte das Ergebnis kontrolliert werden. Meistens genügt ein Blick in die Logdatei des entsprechenden Programms. Wurden alle Daten gesichert? Sind Störungen aufgetreten (Daten gesperrt, zu wenig Platz auf dem eingelegten Medium oder ähnliches)? Wie sieht der Zustand des Bandes aus? Welches Medium muss als nächstes eingelegt werden? Dies sind Fragen, die jeden Tag beantwortet werden müssen. Diese Kontrollen und das Ersetzen eines Mediums sollte schriftlich festgehalten werden.

Mit der optimalen Vorbereitung und der korrekten Umsetzung kann jederzeit auf die Daten zurückgegriffen und diese verlustfrei wiederhergestellt werden. Wappnen Sie sich jetzt, bevor es zu einem Datenverlust kommt. ◆

ZUM AUTOR

Andreas Wisler

(Tel. 052 320 91 20)
ist Geschäftsführer der GO OUT Production GmbH, welche sich mit IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt.

Er unterrichtet in der Klubschule Migros den Lehrgang „IT-Security Manager“, darüber hinaus veröffentlicht er regelmässig einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.goSecurity.ch bestellt werden kann.

Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.

