

## Zuverlässige Datensicherung am Computer - ein Muss für jedes Unternehmen

**Datensicherung ist unerlässlich, nicht nur in großen Firmen, sondern auch in mittelständischen und kleinen Betrieben bis hin zu Einzelunternehmern.**

**Sie sind sogar verpflichtet, geschäftsrelevante Daten in angemessenen Abständen zu sichern und zugriffssicher aufzubewahren. Dies ergibt sich schon aus den Vorschriften der ordnungsgemäßen, nachvollziehbaren und revisionssicheren Buchhaltung. Geschieht dies nicht und sind wichtige Daten erst einmal verloren, so kann der Schaden in's schier unermessliche steigen.**

### Ziemlicher Aufwand

Da müssen Medien und Laufwerke angeschafft werden, eine spezielle Software ist nötig. Zudem sind personelle Kapazitäten extra dafür frei zu stellen. Es muss ein Verantwortlicher dafür benannt und eventuell sogar geschult werden. Das bedeutet einen enormen Zeit- und Kostenaufwand für die Firmen. Oftmals fehlen den Firmen jedoch diese Kapazitäten, sie haben nicht genügend Personal und können oder wollen niemanden extra einstellen.

### Abhilfe ist möglich

ACM-Mitglied Stanislaw Panow kennt diese Probleme als ehemaliger Leiter der IT-Abteilung eines großen Bauträgers nur allzu gut; er ist jetzt Geschäftsführer

der im Juni 2002 gegründeten Firma netcos AG. Deren Schwerpunkte: Know How in den Bereichen EDV-Beratung, e-Security, Projektmanagement, Datenbank- und Softwareentwicklung bis hin zum IT-Service.

### Wie man den Aufwand reduzieren kann

Die Netcos AG bietet den Firmen folgenden Service:

- eine automatische Datensicherung, die weder personelle, noch zeitliche oder materielle Ressourcen frisst und absolut sicher ist.
- Zudem ist eine Rücksicherung ohne großen Aufwand für das Unternehmen zu jeder Zeit möglich, und das ohne einen Backup-Spezialisten im Hause zu haben. Mehr dazu siehe weiter hinten.

### Nachlässigkeit macht sich nicht bezahlt

“Die Unternehmen reagieren durchweg positiv auf unseren Service. Jedoch wird das Thema meist wieder verdrängt, wenn es darum geht, die Sache professionell anzupacken. Datensicherung nimmt viel Zeit in Anspruch und keiner will oder kann diese lästige Aufgabe übernehmen. Da wird dann schon mal geschludert bei der Sicherung, wenn denn überhaupt eine stattfindet”, weiß Stanislaw Panow aus Erfahrung. Erst bei einem Datenverlust wird die Ernsthaftigkeit deutlich und erwacht das Bewusstsein für richtiges Backup. Wenn dann Firmendaten verlo-

ren gehen und keine Sicherung gemacht wurde, sei der Schaden groß. “Oftmals kommen Kunden erst zu uns wenn es zu spät ist und alle Daten weg sind”, so der netcos AG-Geschäftsführer. Zwar gibt es die Möglichkeit des “Desaster Recovery”, also von Datenrettungseinsätzen, jedoch kann nicht gewährleistet werden, dass die Daten tatsächlich wieder hergestellt werden können. Und das geht dann richtig ins Geld.

In vielen Fällen droht einer Firma das Aus nach einem Datencrash. Laut einer Studie des Recovering-Spezialisten Jon W. Toigo erholen sich 43% der Unternehmen nach einem Totalverlust nicht mehr, weitere 29% schließen innerhalb der kommenden 2 Jahre.

### Mangelhafte Sicherungsmoral

Alarmierende Prognosen angesichts der derzeit verbreiteten Sicherungsmoral, denn 40% aller Unternehmen sichern ihre Daten weniger als einmal pro Woche, wie eine weitere Studie aufzeigt. Die häufigsten Gründe für eine unzureichende Datensicherung in Firmen sind fehlendes bis mangelhaftes Equipment, zu wenig Know How und Zeitmangel. Es findet auch keine regelmäßige Überwachung oder Überprüfung statt, ob das Backup richtig gelaufen ist. Einige Firmen verzichten sogar bewusst auf Datensicherung, da wichtige Dokumente in Papierform ausgedruckt und archiviert wurden. Um diese Daten dann wieder zu digitalisieren bedarf es eines enormen Zeitaufwands.

### Netzattacken, Datenklau und dergleichen

In der heutigen Zeit steigender Attacken aus dem Internet fast undenkbar, denn schnell ist mal ein ganzes Firmennetz lahm gelegt und das trotz der oftmals hohen Sicherheitsmaßnahmen. Es gibt kaum eine Firma, die nicht schon mit Attacken aus dem Netz gekämpft hätte. Gefahren drohen aber auch von innerhalb. Nach der IT-Security Studie 2005 von InformationWeek stieg in den letzten Jahren der Angriff durch unternehmenseigene Mitarbeiter und damit verbundene Datenverluste und Komplettausfälle enorm. Jeder 12. Zwischenfall hatte einen Totalausfall zur Folge. Und nur 20% dieser Firmen erlitten keinen nennenswerten Schaden. Auch Katastrophen wie Feuer oder Wasser können zu einem Datenverlust führen und das, obwohl vielleicht sogar regelmäßig eine Sicherung gemacht wurde. Ebenso können Datenträger verloren gehen. Denn auch mit der Aufbewahrung nimmt man es hierzulande nicht so ernst, oftmals sind die Sicherungsmedien nicht separat verwahrt und meist sogar noch für jeden zugänglich. Da ist Datenmissbrauch bzw. Diebstahl Tür und Tor geöffnet. Ein weiterer Unsicherheitsfaktor sind diverse Speichermedien. Diese können defekt sein, ohne dass dies bemerkt wird. Gibt es dann nur diese einzige Sicherung, hat auch das fatale Folgen, genauso wie unregelmäßige bis seltene Sicherungen. Wird nicht wenigstens einmal pro Woche, besser jedoch jeden Tag gesichert, sind die zurück zu sichernden Daten veraltet

*Fortsetzung nächste Seite*

und bedürfen eines enormen Aufwands, um wieder aktualisiert zu werden. (Einige Daten sind jedoch für immer verloren, das könnte den Verlust eines wichtigen Kunden bedeuten oder die Arbeit der letzten Wochen zunichte machen.)

#### Was also tun?

Es empfiehlt sich ein so genanntes Remote Backup, d.h. eine Datensicherung via Internet, wie sie auch netcos AG mit Ihrem Reback Service anbietet.

Wie funktioniert das?

Die Daten werden über eine verschlüsselte Datenleitung via DSL-Anschluss gesichert und im Falle eines Datenverlustes wieder hergestellt. Dies betrifft nicht nur Daten vom zentralen Server, sondern auch von Niederlassungen, Heimarbeitsplätzen, Außendienstmitarbeitern usw., egal ob diese sich auf Servern unter Windows, Unix, AS 400, PCs oder Notebooks befinden. Die Datenspeicherung selbst erfolgt dann im gesicherten und permanent überwachten Rechenzentrum. Bereits vor der Übermittlung werden die Daten verschlüsselt. Mit einem persönlichen Schlüssel, und nur mit diesem können die Daten zurück gesichert werden. Diesen Schlüssel besitzt nur der Kunde. Für Reback wird kein eigenes zusätzliches Hard- und Software System benötigt. Die Anschaffung von Bandlaufwerken, Wechslem, Tape Libraries sowie Speichermedien entfällt. Eine einzige Software reicht aus für alle Aufgaben. Das Aufsetzen ist leicht und macht einen Einstieg sofort möglich, es sind keine Spezialkenntnisse nötig. Das Backup selbst läuft vollautomatisch im Hintergrund, und das Tag für Tag. Einzige Voraussetzung dafür ist, man muss online sein. Eine

Rücksicherung ist zu jeder Zeit möglich, egal ob tags oder nachts. Eine Besonderheit der Datenübernahme bei Reback ist, dass z.B. identische Dateien, auch von verschiedenen Rechnern, nur ein einziges Mal gesichert werden müssen, damit reduziert sich das zu sichernde Datenvolumen enorm. Die Datensicherung erfolgt mit Versionierung; dabei kann der Kunde festlegen, in welchen Zyklen gesichert werden soll und auf wie viele vergangene Sicherungen er zurückgreifen möchte. Diese Art der Datensicherung erfolgt unter nachweisbarer Einhaltung der Richtlinien und Vorschriften für Datensicherung in Unternehmen.

#### Für Idealisten mit Eigeninitiative

Auch wer seine Daten selbst sichern möchte, für den hat Stanislaw Panow einige Tipps parat:

- Gesichert werden sollte laut Gesetz mindestens einmal pro Woche, am besten jedoch jeden Tag. Je öfter gesichert wird, umso weniger Rückstand bezüglich aktuellem Datenstand hat eine Firma im Falle einer Rücksicherung.

- Software und Hardware für Backup gibt es genügend auf dem Markt, doch meist sind diese wenig sicher oder sie funktionieren nicht richtig bzw. sind schwierig zu bedienen. Hier sollte genau geprüft werden, was in Frage kommt und nicht am falschen Platz gespart werden. Hier gilt: Erst testen dann kaufen. Wichtig ist vor allem: Auch eine Rücksicherung muss getestet werden. Manchmal treten erst hier Schwierigkeiten auf.

- Speichermedien sollten regelmäßig auf

ihre Funktionalität hin überprüft werden. Am wirkungsvollsten ist eine doppelte Sicherung auf verschiedenen Medien.

- Speichermedien sollten sicher verwahrt und vor einem möglichen Zugriff Dritter geschützt werden. Um auch im Katastrophenfall gewappnet zu sein, sollten doppelte Sicherungen an verschiedenen Orten sicher verwahrt werden.

- Will man seine Sicherungen archivieren, sollte man darauf achten, dass auch ein passendes und funktionsfähiges Leselaufwerk dazugehört, um diese Daten wieder lesen zu können. Oftmals wechselt

die Technik schnell und für bestimmte Medientypen sind kaum noch Laufwerke erhältlich.

- Zu einer vernünftigen Datensicherung gehört auch ein Notfallplan. Das heißt konkret, schnelle unkomplizierte und vollständige Rücksicherung der Daten innerhalb eines angemessenen Zeitraumes. Aus diesem Grunde sollten in regelmäßigen Abständen Rücksicherungstests erfolgen und ein Krisenverantwortlicher benannt werden.

Tatjana Schötz und Stanislaw Panow,  
netcos AG

## ■ Rent your IT.

individuell · flexibel · partnerschaftlich

Von der Verkabelung, dem IT/TK Umzug, dem Einrichten Ihrer Systeme bis zur Wartung und Betreuung hilft Ihnen die netcos AG.

info@rent-your-it.de  
www.rent-your-it.de

Wenn Sie heute Ihre Daten verlieren,

sind Sie morgen noch im Geschäft?

**Datensicherung** einfach, schnell und zuverlässig

reback@netcos.de  
www.re-back.de

re  back  
remote backup services

## NETCOS AG

Herr Stanislaw Panow  
(Geschäftsleitung)

Richard-Strauss-Str. 71  
81679 München

Tel.: 089/45 22 16 0  
Fax: 089/45 22 16 99