Wie wichtig die gespeicherten Daten sind, erkennen viele erst, wenn der erste Systemcrash auftritt und ein Großteil der Informationen verloren geht. Leider stellen fast ebenso viele erst in diesem Moment fest, dass die Datensicherung nicht korrekt durchgeführt wurde. Wer sich auf die wichtigsten Fehlerquellen des Daten-Backups konzentriert, kann einem teuren Verlust jedoch erfolgreich vorbeugen.

1. Zu seltene Datensicherung
Die Abstände zwischen den Sicherungen sollten dem regelmäßigen Datenfluss angemessen sein. Zu viele verlassen sich auf einen festen Rhythmus, in dem die Datensicherung vorgenommen wird, ohne auf besondere Ereignisse einzugehen. Wenn zum Beispiel besondere Erkenntnisse gewonnen wurden, ist dies ein Zeitpunkt, zu dem zwingend die Datensicherung aktualisiert werden sollte. Wird dagegen einige Tage nicht gearbeitet, ist im Anschluss eine erneute Sicherung der unveränderten Daten eher unwichtig.

2. Ein RAID-System mit einer Datensicherung verwechseln
RAID steht für Redundant Array of Independent Disks. Bei einem solchen System werden regelmäßig redundante Daten gespeichert. Hiermit wird auf das Ausfallrisiko der im Verbund arbeitenden Festplatten reagiert. Ein echter Systemcrash oder gar die physische Zerstörung des Rechners wird durch diese Redundanz nicht aufgefangen. Eine zusätzliche Datensicherung ist zwingend notwendig.

3. Die Kopie immer in der Nähe haben
Nach dem Einsturz des Stadtarchivs in Köln wurde ein Doktorand bekannt, der seine Aufzeichnungen verloren hatte. Er war zwar stets sorgfältig mit dem Erstellen seiner Sicherungskopien. Doch der Stick, auf dem diese gespeichert waren, lag jederzeit griffbereit neben seinem Laptop. Dieser Doktorand hatte zwar das Glück, dass der Stick aus den Trümmern geborgen werden konnte, doch das Beispiel macht eines sehr deutlich: Eine Sicherungskopie ist nur dann sicher, wenn sie in einem anderen Gebäude aufbewahrt wird als die Originale. Bei Unternehmen kann es auch genügen, wenn die entsprechenden Datenspeicher in einem anderen Brandschutzbereich untergebracht sind als die Server des internen Netzwerkes.

4. Zu schnelles Überschreiben der Daten
Viele kleine Unternehmen arbeiten nach dem altbekannten Großvater-Vater-Sohn-Prinzip. Bei diesem ergänzen sich tägliche, wöchentliche und monatliche Datensicherung. Gerade die täglichen Sicherungskopien werden jedoch bei diesem Prinzip viel zu schnell überschrieben. Der Datenspeicher, der noch die Kopie von Montag enthält, wird am Dienstag bereits mit der nächsten täglichen Sicherung überschrieben. Sinnvoller wäre es, alle täglichen Datensicherungen aufzubewahren, bis die nächste Wochensicherung abgeschlossen wurde. So lässt sich auch am Ende einer Woche noch eine vollständige Systemwiederherstellung

bewerkstelligen.

5. Kein Konzept für den Restore
Dass eine Datensicherung wichtig ist, wird immer mehr Menschen sehr bewusst. In Unternehmen ist sie je nach Art der aufkommenden Daten sogar gesetzlich vorgeschrieben. Doch noch zu wenige Nutzer und Administratoren denken an den Moment, in dem die Datensicherung benötigt wird. Das Wiederherstellen des Systems ist nicht selten das eigentliche Problem, über das Unternehmen stolpern. Ein gut durchdachtes Sicherungskonzept hält auch stets einen vollständigen Plan zur Wiederherstellung der Daten bereit. Dies sollte bei einem reinen Software-Problem nicht länger als einige Minuten dauern.

6. Unflexible Sicherungssoftware
Bei kleinen Unternehmen oder Neugründungen wird meist eine Softwarelösung für die Datensicherung gesucht, die aktuell zum üblichen Datenumlauf passt. Da die Software immer zuverlässig gearbeitet hat, scheint eine Veränderung an der Stelle nicht notwendig zu werden. Wächst das Unternehmen jedoch, gelangt die Datensicherung nicht selten an ihre Grenzen. Findige Administratoren können häufig noch Erweiterungen basteln, mit denen das System auch bei dem größeren Datendurchsatz ohne weiteres läuft. Doch spätestens, wenn die Wiederherstellung der Daten notwendig wird, rächt sich diese Sparsamkeit. Ein individuell zurechtgezimmertes System lässt sich meist nur mit großem Aufwand wiederherstellen. Besser ist es, von Anfang an auf eine Software zu setzen, bei der die Erweiterung der Aufgaben bereits vorgesehen ist.

7. Ungeklärte Zuständigkeiten
Wenn es um die Sicherung sensibler Daten geht, ist natürlich größte Vorsicht angebracht. Die Daten müssen so gesichert werden, dass sie nicht nur nicht verloren gehen, sondern auch Unbefugten nicht in die Hände gelangen können. Doch gerade durch diese Absicherungen können mitunter wichtige Informationen verloren gehen. Es sollte daher stets geklärt sein, wer für einen bestimmten Datenbereich verantwortlich ist, wer die Passwörter kennt und wer die Wiederherstellung starten kann. Hierfür sollten jederzeit mindestens zwei Personen ausgewählt werden. Sollte eine der Personen das Unternehmen verlassen, ist sicherzustellen, dass die Zuständigkeiten für die Daten auch an deren Nachfolger übertragen werden.

8. Die Kosten für Sicherheit unterschätzen
In vielen Unternehmen muss gespart werden. Doch viel zu oft unterschätzen Vorstände den Wert eines gut funktionierenden IT-Systems. Die Hardware soll möglichst wenig kosten und die Software am besten nur ein einziges Mal installiert werden. Um die Kosten für Neuanschaffungen so gering wie möglich zu halten, kann es sinnvoll sein, die Hardware

lediglich zu mieten. Auf diese Weise werden die Mitarbeiter regelmäßig mit den neuesten technischen Möglichkeiten ausgestattet, ohne hierdurch die Kosten in die Höhe zu treiben. Doch gerade diese Sparmaßnahme stellt auch eine sehr große Gefahrenquelle dar. Durch die zeitlich begrenzten Mietverhältnisse muss regelmäßig am funktionierenden System gearbeitet werden. Die Datensicherung wird umso wichtiger, da kein Mitarbeiter mehr seine eigenen Projekte selbst absichern kann. Eine gute Datensicherung steht und fällt mit der Redundanz.

Gen. Quelle: http://www.langmeier-software.com/seiten/news/die-acht-haeufigsten-backup-fehler