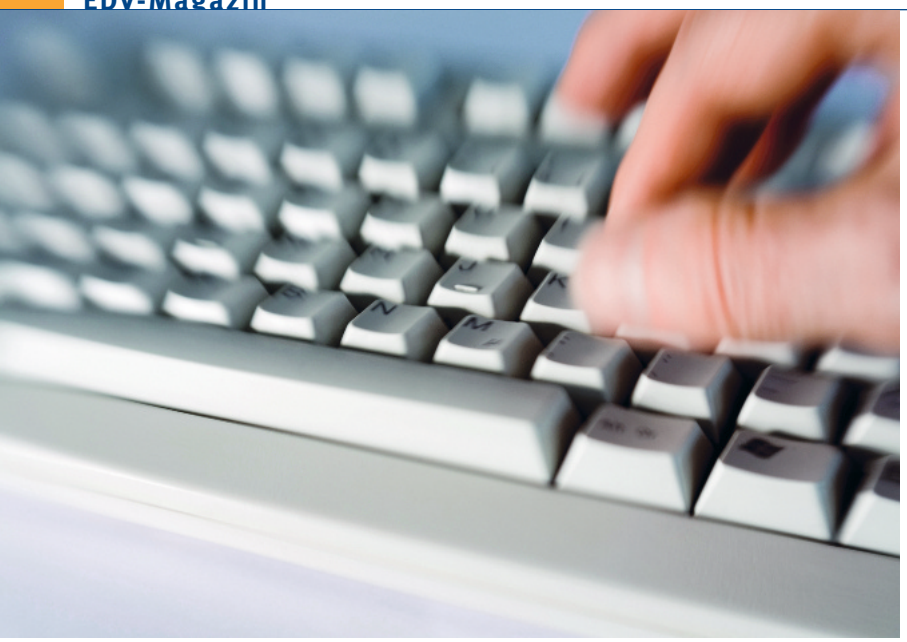

Datensicherung

Kein Frust durch Datenverlust

Je nach Intensität der Computernutzung, kann ein Datenverlust für einen Betrieb durchaus katastrophale Folgen haben. Josef Fenninger gibt Tipps und praxisorientierte Beispiele, wie Sie wirkungsvoll ein schlüssiges Datensicherungskonzept für den eigenen Betrieb entwickeln.

Für einen Schreiner-, Tischler- oder Fensterbauerbetrieb, der ausschließlich die Textverarbeitung nutzt, ist es noch relativ verschmerzbar, wenn seine Daten plötzlich weg sind. Sie liegen zumindest meistens noch ausgedruckt in Papierform vor.
Bei einem Betrieb mit höherem Technisierungsgrad (z. B. CAD-Arbeitsplätze, Bearbeitungszentrum) kann der Verlust von Daten den Geschäftsbetrieb vollkommen lahm legen und daher sehr viel Geld kosten. Hier kommt ein zweiter Aspekt mit einer ganz wesentlichen Frage zum Tragen: Wie lange kann es sich der Betrieb leisten, dass das Produktivsystem nicht funktioniert?
Auch äußere Zwänge können einen zur regelmäßigen und durchdachten Datensicherung verpflichten: Der Gesetzgeber verlangt für eine revisionssichere Buchführung, dass die Buchungsdaten 10 Jahre lang aufbewahrt werden. Viele Banken haben in ihren Fragebögen zum Rating nach Basel II Fragen zum Datensicherungskonzept integriert. Die Gründe für Datenverlust sind vielfältig. Hier einige Beispiele:

- Der Computer wird durch Brand, Überspannung oder Überschwemmung komplett zerstört.
- Der Computer wird gestohlen.
- Festplatte kann kaputt gehen.
- Durch einen Bedienungsfehler wurden Daten versehentlich gelöscht oder überschrieben.
- Ein böswilliger Mitarbeiter löscht Daten absichtlich.
- Schadsoftware (z. B. Virus, Trojaner) hat Daten zerstört.
- Ein Softwarefehler hat Daten in einem inkonsistenten Zustand hinterlassen.
- Ein Hardwaredefekt in einem Server verursacht, dass dieser nicht mehr läuft. Ein Ersatzteil ist beispielsweise erst frühestens in 48 Stunden verfügbar.

Ein gern gemachter Fehler: Man schreibt in der Textbearbeitung einen Brief. Dabei lädt man sich als Vorlage den Brief an einen anderen Kunden, ändert ihn ab und möchte ihn unter dem Namen eines anderen Kunden speichern. Zu spät merkt man, dass man die ursprüngliche Version überschrieben hat, da man statt „Speichern unter" einfach nur „Speichern" geklickt hat. Mit einer funktionierenden Datensicherung kann man sich das ursprüngliche Dokument in wenigen Minuten problemlos wieder zurückholen.
Für jeden dieser Fälle ist es notwendig, sich zu überlegen, wie man darauf reagiert. Man sollte sich also in jedem Fall die Mühe machen und ein schlüssiges Datensicherungskonzept für den eigenen Betrieb entwickeln.

Der erste Schritt: Wo sind meine Daten gespeichert?

Um die erzeugten Daten sinnvoll sichern zu können, muss man sich zuerst Gedanken machen, wo man seine Daten speichert. Auf einem Einplatzsystem wäre es ein sinnvoller Weg, das Verzeichnis „Eigene Dateien" für alle selbst erzeugten Daten zu verwenden und dieses in die Sicherung mit einzubeziehen. Viele Softwareprodukte halten sich leider nicht an diese Vorgabe und speichern ihre Daten in anderen Verzeichnissen.
Noch schwieriger ist es im Netzwerkbetrieb. Hier ist es wichtig, dass alle Benutzer ihre Daten auf dem Server ablegen und nicht lokal auf dem eigenen Rechner. Lokale Datenbestände sind sehr schwierig in eine Datensicherung mit einzubeziehen. Außerdem existieren die Daten dann oft im Netzwerk und auf den lokalen Computern mehrfach in verschiedenen Versionen, was die Arbeit mit den Dokumenten sehr erschwert. Grundsätzlich gilt: Alle Daten so zentral wie möglich speichern.

Der zweite Schritt: Welche Medien sind sinnvoll?

Mit bestem Gewissen kann ich die Verwendung von externen Festplatten empfehlen. In den Punkten Speichergröße, Geschwindigkeit und Zuverlässigkeit schlagen sie CD, DVD und Bänder um Längen. Die Preise sind in den letzten Jahren auf ein erschwingliches Niveau gefallen. Außerdem kann man auch sehr große Datenbestände mit einer externen Festplatte unbeaufsichtigt sichern, ohne ständig ein volles Medium gegen ein leeres

Der Autor

Josef Fenninger ist Schreinermeister, Betriebswirt des Handwerks, Dozent in der Meisterausbildung und entwickelt Branchensoftware

auswechseln zu müssen. Da vielerorts breitbandige Internetverbindungen verfügbar sind, ist in jüngster Zeit die Online-Datensicherung als Alternative entstanden. Dabei wird von einer Firma Speicherplatz auf einem Server zur Verfügung gestellt, auf den man seine Daten sichert.

Der dritte Schritt: Was will ich erreichen?

Die verschiedenen Möglichkeiten, seine Daten zu verlieren, verlangen auch unterschiedliche Reaktionen darauf.
Um zu verhindern, dass eine defekte Festplatte einen Datenverlust nach sich zieht, ist es eine sehr gute Lösung, mit Plattenspiegelung zu arbeiten. Dabei werden die Daten nicht nur auf einer, sondern gleich auf mehreren Platten gespeichert (ein so genannter RAID Verbund). Geht eine Platte kaputt, können die Daten aus dem Inhalt der anderen Platten wieder hergestellt werden.
Der Knackpunkt an dieser Methode ist, dass man überhaupt bemerkt, dass eine Platte kaputt gegangen ist, da die verbliebenen Platten einfach weiterarbeiten. Dazu ist es nötig, die Ereignisprotokolle des Computers regelmäßig zu überprüfen, ob ein Fehler aufgetreten ist, damit man entsprechend darauf reagieren kann.
Wird die Computeranlage zerstört oder gestohlen, ist es wichtig, eine aktuelle Vollsicherung zur Verfügung zu haben, damit man die Daten schnell wieder restaurieren kann. Dabei sollte man auch bedenken, dass eine Datensicherung auch immer außerhalb des Betriebes im örtlich entfernten Privathaus oder einem Bankschließfach aufbewahrt werden sollte.
Werden Daten gelöscht oder überschrieben, so merkt man das oft erst Tage oder Wochen nach der „Tat". Das Gleiche gilt bei einem Virenbefall oder Softwarefehler. Jetzt ist es wichtig, die verschiedenen Versionen eines Dokumentes, die sich im Laufe der Zeit angesammelt haben, in der Datensicherung zu haben.
Ist man im Betrieb auf einen funktionierenden Server angewiesen, dann wird das Datensicherungskonzept etwas schwieriger. Meist laufen auf Servern auch Datenbank- und Kommunikationsdienste, die man nicht so ohne weiteres im laufenden Betrieb sichern kann. Der zuverlässigste Weg, eine hohe Verfügbarkeit zu erreichen ist, einen zweiten Server mitlaufen zu lassen, der die gleichen Daten wie der erste Server enthält. Fällt der erste Server aus, übernimmt der zweite, ohne dass es ein Benutzer merkt. Der EDV-Administrator hat dann genügend Zeit, den Server zu reparieren.
Ist eine Hochverfügbarkeit nicht notwendig und man kann mit einer Ausfallzeit bis zu einem Tag leben, so ist es möglich, vom Server ein Abbild (ein so genanntes Image) anzulegen. Dieses ist eine 1:1 Kopie der Festplatten. Fällt eine Platte aus, baut man eine neue ein und kopiert das Image darauf. Dadurch entfällt das Installieren und Einrichten des Betriebssystems. Unter Umständen kann es auch sinnvoll sein, aus diesem Abbild eine virtuelle Maschine zu erzeugen. Mit dieser kann man den Server schnell auf einen anderen Computer „umziehen", ohne dass dieser die gleiche Hardware haben muss.
Es hat sich auch als sinnvoll erwiesen, einen Zuständigen zu benennen, der für die Datensicherung im Betrieb verantwortlich ist.
Die Datensicherung sollte weitgehend automatisch ablaufen. Dazu kann man die im Betriebssystem oder in der Sicherungssoftware enthaltenen Zeitpläne verwenden.
Um die Datensicherung vor unbefugtem Zugriff zu schützen, kann man diese mittels Verschlüsselung schützen. Im Ernstfall muss man schnell das Passwort für die Verschlüsselung zur Hand haben. In der Hektik, die ein Datenverlust auslöst, kann man ein Passwort schnell vergessen. Deshalb empfehle ich, die Datensicherungen lieber in einen Tresor zu sperren.

Datensicherungsstrategie – zwei Beispiele

Bei einem Einplatzsystem ohne Netzwerk mit geringem Datenaufkommen und ausschließlichem Einsatz von Standard Office-Software kann folgende Strategie sinnvoll sein:
Man speichert die Daten in ein gemeinsames Verzeichnis, das man regelmäßig (täglich oder wöchentlich) auf eine CD / DVD brennt. Diese bewahrt man sauber beschriftet mit Datum auf. Ebenfalls regelmäßig (z. B. monatlich) bewahrt man eine der Silberscheiben örtlich getrennt vom Büro auf. Fällt der PC aus, hat man alle Daten auf der zuletzt gebrannten Scheibe beisammen.
Ein Betrieb mit mehreren Arbeitsplätzen und Maschinen, die auf Serverzugriff angewiesen sind, hat es da schon schwerer, da bei einem Serverausfall auch die Fertigung ausfällt:
Alle Daten sollten auf einem Serverlaufwerk gespeichert werden. Meistens laufen auch Datenbank- und Kommunikationsdienste auf dem Rechner. Diese Serverprogramme haben zwar zumeist eigene Datensicherungsmöglichkeiten, aber damit hat man einfach zu viele Datensicherungs-Baustellen offen. Deshalb kommt man um die Anschaffung einer geeigneten Datensicherungssoftware, die alles auf einmal sichern kann, meist nicht herum. Diese sollte die Daten auf verschiedene externe Festplatten sichern. Eine Platte für die tägliche Datensicherung. Diese sollte inkrementell, d. h. aufbauend erfolgen. Hier werden nur die veränderten Daten gesichert, das spart Plattenplatz und Zeit. Diese tägliche Sicherung dient dazu, versehentlich gelöschte oder veränderte Dateien schnell wieder herzustellen.
Zwei weitere externe Festplatten verwendet man für die wöchentliche Sicherung. Dabei wird der komplette Serverinhalt gespeichert. Die beiden Platten werden im Wechsel verwendet. Die jeweils nicht verwendete Platte wird örtlich getrennt vom Büro aufbewahrt.
Zusätzlich legt man sich ein Image des Servers an, baut daraus eine virtuelle Maschine und hat damit einen Ersatzserver, der in wenigen Stunden einsatzbereit ist. Dieser muss aber im Vorfeld ausgiebig getestet werden, ob er wirklich alle benötigten Dienste zur Verfügung stellt.

Sichern alleine ist nicht ausreichend

Die schönste Datensicherungsstrategie nützt nichts, wenn man im Ernstfall bemerkt, dass die Sicherungsmedien leer sind. Kontrolle ist ein weiterer, sehr wichtiger Aspekt. Datensicherungsprogramme legen zumeist Protokolle ihrer Arbeit an. Diese gilt es wöchentlich zu prüfen, ob dort Fehler protokolliert sind. In einem weiteren Schritt sollte man regelmäßig Stichproben machen und die Daten wieder herstellen, um zu prüfen, ob das auch wirklich klappt. Ich habe schon einen Bandsicherungs-Server erlebt, der immer brav eine erfolgreiche Datensicherung protokolliert hat. Im Ernstfall hat man dann bemerkt, dass die Bänder leer waren. Vor allem bei der Datensicherung gilt: Vertrauen ist gut, Kontrolle ist besser.

Gerüstet sein: Im Notfall alles zur Hand

Um im Fall des Falles strategisch vorgehen zu können empfehle ich, ein Notfall-Strategie-Papier anzufertigen. In diesem wird beschrieben, wie im Falle eines Datenverlustes oder Serverausfalles vorzugehen ist. Damit spart man sich wertvolle Zeit.
Ein letzter Punkt für Datensicherheit in der Schreinerei: Alle paar Monate die Computergehäuse öffnen und den Staub daraus absaugen (dabei auf statische Aufladung achten!). Da sammelt sich sehr viel Dreck an, der schnell zu Hardwaredefekten führen kann. ■

Infobox

Virtuelle Maschine

Eine virtuelle Maschine besteht im Wesentlichen aus zwei Komponenten:
1. Hostsystem
2. Gastsystem

Das Hostsystem ist eine Software. Diese wird auf einem Rechner installiert, der genügend Prozessorleistung, Arbeitsspeicher und Plattenplatz hat, um zwei oder mehrere Betriebssysteme parallel ausführen zu können. Das ist heute in der Regel ein handelsüblicher PC mit schnellem Dual-Core Prozessor, 3 - 4 Gigabyte Arbeitsspeicher und ab 250 Gigabyte Festplatte.
Das Gastsystem ist ein beliebiges Betriebssystem (z. B. Windows oder Linux). Dieses wird in das Hostsystem installiert. Das Betriebssystem wird also nicht direkt auf die Festplatte des PC kopiert, sondern nur virtuell in das Hostsystem. So ist es möglich - neben dem eigentlichen Betriebssystem - mehrere Betriebssysteme gleichzeitig und unabhängig voneinander laufen zu lassen.