Datensicherung

Strategien und Maßnahmen gegen Datenverlust

Datensicherung und Notfallwiederherstellungsmaßnahmen helfen bei der Schadensbegrenzung nach Systemausfällen, dem Verlust einzelner Dateien oder im schlimmsten Fall der Zerstörung der gesamten IT-Infrastruktur. Verschiedene Maßnahmen sind nötig, um die Sicherheit von digitalen Daten sicherzustellen.

Voraussetzung für jede Notfallvorsorge sind die Planung und Durchführung regelmäßiger Datensicherungen. In vielen Fällen müssen auch die Mitarbeiterinnen und Mitarbeiter zur Einhaltung und Unterstützung der Datensicherungsmaßnahmen verpflichtet werden.

Warum Datensicherung?

Heute werden oft Technologien eingesetzt, die bestimmte typische Einsatzzwecke von Datensicherungen abdecken: RAID-Laufwerke bieten Schutz vor dem mechanischen Ausfall einzelner Festplatten, Snapshot-Technologien ermöglichen das Wiederherstellen versehentlich gelöschter Dateien.

Der Nutzen von Datensicherungen geht aber weit über diese begrenzten Einsatzbereiche hinaus: Sie können bestimmte Datenstände zu Beweisführungszwecken wiederherstellen (Jahres-, Monatssicherungen) oder Daten retten, die von Schadsoftware verfälscht oder zerstört wurden.

Vor allem aber ermöglichen sie, die Daten nach schwerwiegenden Vorfällen, wie z. B. einem Brand im Serverraum oder dem Diebstahl von Rechnern, wiederherzustellen. Durch die geringe Größe der Sicherungsmedien ist auch die Auslagerung an einen sicheren Ort ohne großen Aufwand möglich.

Datensicherungskonzept und Datensicherungsplanung

Zunächst sollte in schriftlicher Form festgelegt werden, welche Daten von wem zu welchem Zeitpunkt gesichert werden.

Folgende Punkte müssen dabei in jedem Fall behandelt werden:

- Umfang und Klassifizierung der zu sichernden Daten (z. B. Geschäfts- und Produktionsdaten, Systemdateien, Datenbanken, Laufwerke)
- Sicherungstechnologie und -medien (z. B. Sicherungsbänder, Wechselfestplatten, Cloud-Speicher, USB-Sticks, CD/DVD)
- Zeitintervall und Zeitpunkt der Sicherungen (z. B. täglich, wöchentlich, an Werktagen)
- Anzahl der aufzubewahrenden Sicherungen aus der Vergangenheit
- Zuständigkeit für Durchführung, Überwachung und Dokumentation der Sicherungen
- Aufbewahrung der Backup-Datenträger
- Überprüfung der Datensicherungen, Wiederherstellungstests und -übungen

Voraussetzung regelmäßiger Datensicherungen ist die zentrale Speicherung aller wichtigen Daten, die auch hinsichtlich der Datensicherheit zu empfehlen ist.

Benutzerinnen und Benutzer müssen dazu angehalten werden, ihre Daten auf den Servern (und nicht den Festplatten ihrer Arbeitsplatzrechner) abzuspeichern.
Vorrangig müssen Geschäfts- und Produktionsdaten (selbst erstellte Daten wie z. B. Dokumente, Kundendatei, Buchhaltung, E-Mail) gesichert werden, außerdem noch eventuelle Konfigurationsdateien der eingesetzten Software.

Wichtige Computer, die nach einem Ausfall schnell wieder zur Verfügung stehen müssen, sollten dagegen (z. B. mittels Image-Sicherung) vollständig gesichert werden.

Grundsätzlich sind alle Arten von Wechseldatenträgern als Sicherungsmedien geeignet. Im einfachsten Fall kann es ausreichen, die Produktionsdaten wöchentlich auf eine CD-ROM oder DVD zu brennen. Auch externe USB-Festplatten und Cloud-Speicher, eventuell auch USB-Sticks, können verwendet werden.

Sicherungssoftware, Sicherungslaufwerke

Allerdings erfordert dieses Vorgehen hohen Arbeits- und Zeitaufwand und lässt sich schlecht automatisieren. Ab einer bestimmten Datenmenge ist es daher sinnvoller, geeignete Sicherungssoftware und spezielle Sicherungslaufwerke einzusetzen.

Server-Betriebssystemen liegen einfache Versionen von Backup-Software bei, die bereits ausreichen können. Im Handel erhältliche Sicherungssoftware ist dagegen für komplexe Sicherungsaufgaben (z. B. dem Sichern eines Datenbank- oder Mailservers) besser geeignet und kann mit einer größeren Auswahl verschiedener Sicherungsmedien (z. B. Bandsicherungen) umgehen.

Als Sicherungshardware können **USB-Festplatten** oder **Bandlaufwerke** eingesetzt werden. Die Daten können auch auf einen eigenen Storage-Server (**NAS** – Network Attached Storage) gesichert werden. Dies ist aber nur dann sinnvoll, wenn dieser räumlich und vor allem brandschutztechnisch von den gesicherten Computern getrennt ist.

Online-Datensicherung

Für kleine bis mittlere Datenmengen lässt sich die Möglichkeit der **Online-Datensicherung** nützen. Dabei werden Daten über das Internet zu Anbietern von Cloud-Speicher übertragen, von denen sie im Notfall wieder abgerufen werden können. Der Vorteil dieser Methode ist, dass die Daten außer Haus gespeichert werden und dadurch eine räumliche Trennung der Sicherungen von den Originaldaten gegeben ist.

Bei einer Online-Sicherung ist aber großes Augenmerk auf die Seriosität und Sicherheit des Anbieters zu legen. Die Zuverlässigkeit und Verfügbarkeit muss wie bei jedem Cloud-Dienst genau geprüft werden.

Wenn sensible Daten auch vor Zugriffen des Anbieters sicher sein sollen, müssen sie bereits vor der Übertragung verschlüsselt werden. Zu bedenken ist auch, dass der Datentransport über das Internet sehr lange dauern kann, vor allem, wenn nach einem Totalausfall der gesamte Datenbestand wiederhergestellt werden soll.

Verschiedene Datensicherungsarten sind in Gebrauch. Hier nur die Wichtigsten:

- **Volldatensicherung:**
  Bei dieser Methode werden sämtliche zur Sicherung vorgesehenen Dateien einzeln gesichert. Volldatensicherungen sind einfach durchzuführen, und auch die Wiederherstellung der Daten ist einfach.
  Allerdings verbrauchen sie viel Speicherplatz auf den Sicherungsdatenträgern und dauern lange.
  Sie sind ideal für unbeaufsichtigte, in der Nacht oder am Wochenende durchgeführte Sicherungsläufe.
- **Inkrementelle Sicherung:**
  Bei inkrementellen Sicherungen werden nur jene Dateien gesichert, die sich seit der letzten Vollsicherung geändert haben. Da üblicherweise der Großteil der Daten unverändert bleibt, ist der Umfang dieser Datensicherung deutlich geringer.
  Für die Wiederherstellung werden aber die letzte Volldatensicherung sowie alle darauffolgenden inkrementellen Sicherungen benötigt. Da eine einzige fehlgeschlagene Sicherung ausreicht, um alle darauffolgenden Sicherungen unbrauchbar zu machen, müssen in größeren Abständen (z. B. wöchentlich) zusätzliche Volldatensicherungen durchgeführt werden.
- **Differenzielle Sicherung:**
  Bei der differenziellen Methode wird zunächst eine Volldatensicherung gemacht. Bei den nächsten Sicherungen werden nur die Dateien, die seit dieser geändert wurden, gesichert.
  Der Sicherungsumfang ist dadurch höher als bei der inkrementellen, aber niedriger als bei einer Volldatensicherung.
  Zur Wiederherstellung werden nur mehr zwei Sicherungsmedien benötigt: Das der letzten Volldatensicherung sowie das der letzten differentiellen Datensicherung.
- **Image-Sicherung:**
  Bei Image-Sicherungen wird ein "Image" (Speicherabbild) der Festplatte eines Rechners erstellt und auf einen Datenträger gespeichert.
  Im Bedarfsfall kann der Rechner damit in kurzer Zeit wieder in den exakten Zustand zum Zeitpunkt der Imageerstellung versetzt werden.
  Diese Methode ist auch für Backups gut geeignet, verbraucht aber ähnlich viel Platz wie eine Volldatensicherung.

Um sicherzustellen, dass die Datensicherung richtig eingerichtet wurde, muss unbedingt die Wiederherstellung der gesicherten Daten getestet werden.

Besonders gilt dies für die Wiederherstellung komplexer Server (Datenbank-, Mailserver, Domänencontroller).

Die Notfallwiederherstellung solcher Server, von der neuen Hardware bis zur produktionsreifen Maschine, muss mindestens einmal durchgeführt und dokumentiert werden.

Ohne einen derartigen Test ist es sehr wahrscheinlich, dass im Ernstfall Probleme auftreten, die eine erfolgreiche Wiederherstellung verhindern.

Geeignete Aufbewahrung der Backup-Datenträger

Bei der Aufbewahrung der Backup-Datenträger ist aus zwei Gründen besondere Sorgfalt angebracht. Die Entwendung eines Sicherungsmediums würde einem Angreifer den einfachen Zugriff auf die wichtigsten Unternehmensdaten ermöglichen.

Im Katastrophenfall, etwa nach der Zerstörung der IT-Systeme durch einen Brand, sind die Sicherungen die einzige Chance, den elektronisch gespeicherten Datenbestand zu retten.

Folgende Anforderungen sollten erfüllt sein:

- Der **Zugriff** auf Backup-Datenträger darf **nur befugten Personen** möglich sein. Sie sollten idealerweise in einem Safe, jedenfalls aber geschützt gelagert werden.
  Auch die Sicherungslaufwerke sollten nur den zuständigen Mitarbeitern zugänglich sein, um zu verhindern, dass Medien unbemerkt ausgetauscht werden können.
- Die **Backup-Datenträger** müssen von den gesicherten Rechnern **räumlich getrennt** aufbewahrt werden, um zu vermeiden, dass bei einem Brand, Wasserschaden, Einbruch etc. Computer und Datensicherungen gleichzeitig zerstört werden.
- In **regelmäßigen Abständen** – z. B. einmal wöchentlich – sollte ein vollständiger **Sicherungssatz** an einen anderen Ort (ein Nebenstandort des Unternehmens, ein Bankschließfach, evtl. auch der Wohnsitz einer Mitarbeiterin oder eines Mitarbeiters) **ausgelagert** werden.
- Im Notfall muss es möglich sein, auf die benötigten Sicherungsmedien ohne größere Verzögerung zugreifen zu können.

Schriftliche Aufzeichnung von Konfigurationsdaten

Zusätzlich zur eigentlichen Datensicherung sollten verschiedene Konfigurationsdaten ausgedruckt und an sicherer Stelle aufbewahrt werden.

Selbst wenn sämtliche Konfigurationseinstellungen in elektronischer Form gespeichert werden können, ist es von Vorteil, in Notfällen auf Ausdrucke der wichtigsten Einstellungen zurückgreifen zu können.

Beispielsweise sollten die Zugangsdaten zum Internet-Provider, einschließlich der Konfigurationsdetails für den Netzwerkzugang und der Passwörter (z. B. für evtl. Mail-Accounts), gesondert zugreifbar sein.

Auch für Konfigurationseinstellungen der Netzwerkrouter und Switches sind schriftliche Aufzeichnungen oder Bildschirmausdrucke bei der Wiederherstellung wichtig.

Sicherungsvarianten im Überblick:

- **Sicherung auf externe Festplatten, Wechselfestplatten oder USB-Sticks:**
  pro: kostengünstig, einfach
  kontra:Versionsmanagement problematisch, hoher Bedienungsaufwand
- **Bandsicherung:**
  pro: Archivierung und räumliche Trennung leicht möglich, große Datenmengen, automatisierbar
  kontra: Einrichtungs- und Bedienungsaufwand, Anschaffungskosten
- **Online-Sicherung:**
  pro: räumliche Trennung, Sicherheit bei seriösen Anbietern
  kontra: laufende Kosten, eher für kleinen Datenmengen geeignet, kaum für Komplettsicherungen. abhängig von Internetverbindung, Abhängigkeit von Anbieter
- **Imagesicherung:**
  pro: sehr schnell, gut für Sicherung kompletter Systeme geeignet, schnelle Wiederherstellung, gut automatisierbar
  kontra: Wiederherstellung einzelner Dateien teilweise kompliziert, Einrichtungs- und Bedienungsaufwand, Anschaffungskosten

Diese Aufzeichnungen müssen an sicherer Stelle, d.h. vor Zerstörung und unbefugten Zugriffen geschützt, gelagert werden. Bei Änderungen an den Einstellungen oder Passwörtern müssen sie umgehend aktualisiert werden.

Datensicherung bei mobilen IT-Systemen (Notebooks, Smartphones etc.)

Wenn Notebooks oder Smartphones verwendet werden, um wichtige Daten unterwegs zu erfassen oder zu bearbeiten, muss dafür gesorgt werden, dass auch die auf diesen Geräten abgelegten Daten gesichert werden.

Dazu bieten sich folgende Verfahren an:

- **Datensicherung auf externen Datenträgern (externe Festplatten, USB-Sticks, DVD-ROMs etc.)**
  Die Datenträger müssen getrennt von den zugehörigen Computern aufbewahrt werden, um den gleichzeitigen Verlust, etwa bei einem Diebstahl, zu verhindern.
  Die Sicherungsdaten müssen verschlüsselt sein, um Missbrauch beim Verlust eines Sicherungsdatenträgers ausschließen zu können.
- **Datensicherung über Fernverbindung zum Firmennetzwerk**
  Dabei werden die Daten vom Standort der Mitarbeiterin oder des Mitarbeiters zu einem zentralen Firmenserver übertragen.
  Ausreichende Übertragungsgeschwindigkeit sowie die verschlüsselte Übertragung der Daten sind dafür unbedingte Voraussetzungen.
  Diese Methode ist daher nur dann einsetzbar, wenn auf der Firewall des Unternehmens verschlüsselte Fernzugänge z. B. für Telearbeit eingerichtet wurden.
- **Datensicherung auf Cloud-Speicher**
  Sicherungsdaten von Mobilgeräten können in der Cloud gespeichert werden, wenn das Unternehmen über eigenen Online-Speicher verfügt.
  Cloud-Speicher für Privatkunden (z. B. iCloud, Google Drive) ist aber ungeeignet und darf nicht verwendet werden, da Datenverlust auftreten könnte (z. B. bei einem Personalwechsel). Die Mitarbeiterinnen und Mitarbeiter müssen darauf entsprechend hingewiesen werden.
- **Datensicherung bei der Rückkehr ins Firmennetzwerk**
  Dieses Verfahren ist nur dann empfehlenswert, wenn die Mitarbeiterin oder der Mitarbeiter regelmäßig (z. B. wöchentlich) in das Unternehmen zurückkehrt und der mögliche Verlust der zwischenzeitlich geänderten Daten tragbar erscheint.

Die ersten drei Verfahren bringen zusätzlichen Aufwand und Verantwortung für die Benutzerinnen und Benutzer mit sich. Durch den Einsatz geeigneter Software-Tools ist es möglich, den nötigen Arbeitsaufwand zu verringern.

Mitarbeiterinnen und Mitarbeiter mit mobilen IT-Systemen müssen aber besonders auf die Wichtigkeit regelmäßiger Datensicherungen und ihre Eigenverantwortung beim Schutz der Daten hingewiesen werden.

Stand: 23.05.2018