it-safe.at

it-safe: Achten Sie gerade jetzt auf Cybersicherheit!

Datensicherung mit Konzept – darauf müssen Sie bei der Planung achten

Wie Sie zum Datensicherungskonzept kommen

Stand: 02.07.2018

Wenn der Daten-Ernstfall eintritt – etwa nach Systemausfällen, dem Verlust einzelner Dateien oder im schlimmsten Fall der Zerstörung der gesamten IT-Infrastruktur –helfen Notfall-Wiederherstellungsmaßnahmen bei der Schadensbegrenzung. Voraussetzung für jede erfolgreiche Notfallvorsorge ist die Planung und regelmäßige Durchführung einer vernünftigen Datensicherung.

Meist sind verschiedene, miteinander verknüpfte Maßnahmen nötig, um sicherzustellen, dass die IT-Systeme innerhalb eines definierten Zeitraums wieder funktionsfähig sind. Auch die Mitarbeiterinnen und Mitarbeiter müssen mit einbezogen werden und sich zur Einhaltung und Unterstützung der Datensicherungsmaßnahmen verpflichten.

Im 1. Teil unserer Serie zeigen wir, wie Sie zum Datensicherungskonzept kommen.

Mithilfe einer vollständigen Datensicherung können bestimmte Datenstände zu Beweisführungszwecken wiederhergestellt werden (z. B. Jahres-, Monatssicherungen). Oder Sie können Daten retten, die von Schadsoftware verfälscht oder zerstört wurden. Vor allem aber ermöglicht 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.

Darüber hinaus können für bestimmte typische Einsatzzwecke zusätzlich spezifische Technologien eingesetzt werden, die die Datensicherung im Arbeitsalltag unterstützen, z. B.:

- RAID-Laufwerke, die Schutz vor dem mechanischen Ausfall einzelner Festplatten bieten
- Snapshot-Technologien, die das Wiederherstellen versehentlich gelöschter Dateien ermöglichen usw.

Datensicherungskonzept und -planung

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

Dazu sind Überlegungen zu den folgenden Punkte anzustellen:

1. Welchen **Umfang** (Speicherplatz) haben die Daten, die gesichert werden sollen, und wie können sie **klassifiziert** werden:
   z. B. Geschäfts- und Produktionsdaten, Systemdateien, Datenbanken, bestimmte Laufwerke etc.
2. Welche **Sicherungstechnologie und -medien** werden zum Einsatz kommen:
   z. B. Sicherungsbänder, Wechselfestplatten, Cloud-Speicher, USB-Sticks, CD/DVD etc.
3. Zu welchem **Zeitpunkt** und in welchem **Intervall** sollen welche Daten gesichert werden: täglich, wöchentlich, an Werktagen etc.
4. Wie viele **Sicherungen aus der Vergangenheit** sollen aufbewahrt werden:
   z. B. bis zu 6 Monate zurückliegend, bis zu einem Jahr etc.
5. Wer ist für die **Durchführung**, Überwachung und Dokumentation der Sicherungen zuständig?
6. Wo und wie können die **Backup-Datenträger aufbewahrt** werden?

7. Wer kümmert sich um die **Uberprüfung** der Datensicherungen bzw. um Wiederherstellungstests und -übungen?

Wichtig:

Damit alle wichtigen Daten verlässlich und regelmäßig gesichert werden können, müssen diese **zentral gespeichert** werden. Es ist daher sinnvoll, alle Benutzerinnen und Benutzer zu informieren und immer wieder daran zu erinnern, dass sie ihre Daten **auf den Servern** (und nicht den Festplatten ihrer Arbeitsplatzrechner) abspeichern.

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.

Geeignete Sicherungsmedien und Methoden

Manuelle Sicherung mit Wechseldatenträgern:

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. Allerdings erfordert dieses Vorgehen hohen Arbeits- und Zeitaufwand, lässt sich schlecht automatisieren und ist damit fehleranfällig.

Pro: kostengünstig, einfach

Kontra: Versionsmanagement problematisch, hoher Bedienungsaufwand

Sicherungssoftware:

Ab einer bestimmten Datenmenge ist es daher sinnvoller, geeignete Sicherungssoftware und spezielle Sicherungslaufwerke einzusetzen, z. B.:

- **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. Sie kann mit einer größeren Auswahl verschiedener Sicherungsmedien (z.B. Bandsicherungen) umgehen.

Sicherungshardware:

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.

Pro Bandsicherung: Archivierung und räumliche Trennung leicht möglich, große Datenmengen, automatisierbar

Kontra Bandsicherung: Einrichtungs- und Bedienungsaufwand, Anschaffungskosten

Online-Datensicherung (Cloud-Speicher):

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.

Pro: räumliche Trennung, Sicherheit bei seriösen Anbietern

Kontra: laufende Kosten, eher für kleinen Datenmengen geeignet, kaum für Komplettsicherungen. abhängig von Internetverbindung, Abhängigkeit von Anbieter

Tipp: Cloud-Dienstleister, die Daten garantiert in Österreich speichern, sind am Gütesiegel „**Austrian Cloud**“ erkennbar.

» Weitere Infos