Datensicherung

Datensicherheit
(*data security)*
Maßnahmen zur Sicherstellung des Erhaltes von gespeicherten Daten

Maßnahmen sind erforderlich, um digitale Daten durch Einflüsse außerhalb des IT-Systems:

- durch Menschen
- durch Hardwaredefekte
- durch Softwarefehler oder
- durch Einwirkungen von Computerviren

zu schützen.

Schutz vor:

- Ø Verlust
- Ø Zerstörung
- Ø Verfälschung
- Ø Unbefugter Kenntnisnahme
- Ø Unberechtigte Verarbeitung

Ziele:

- Ø Ständige Verfügbarkeit der Anlage und der Daten
- Ø Korrektheit der Daten und der Programme
- Ø Zugriffsschutz vor unberechtigtem Zugriff

Maßnahmen bei der Hardware:

- Ø Zutrittskontrolle
  Schlüssel, Karten, Chip, Magnetstreifen, Finger, Augen, usw.
- Ø Abschließen und Verschließen der Anlage vor Unbefugten
- Ø Speicherschutz
  Schreibschutz an Diskette, Stick, Band
- Ø Notstromaggregate
  USV
- Ø Blitzschutz
- Ø Passwortschutz
  BIOS

Maßnahmen bei der Software:

- Ø Programmschutz durch Passwort
- Ø Automatische Abspeicherung
- Ø Automatische Abspeicherung unter anderem Namen
- Ø Plausibilitätskontrolle
  Verhinderung von Falscheingaben
- Ø Prüfbit-Technik
  Fehlervermeidung bei der Datenübertragung durch ein Prüfbit

- Ø Prüfziffernverfahren
  Ermittlung einer Nummer aus einer anderen (Konto/Artikel)-Nummer
- Ø Virenschutzprogramme

Sonstige Sicherungsmaßnahmen:

- Ø Backup-Verfahren
  Sicherungskopien von Dateien, Verzeichnissen oder der ganzen Festplatte, xcopy, robocopy, backup, RAID-Verfahren, usw.
- Ø Aufbewahren von Ursprungsdateien
  falls sie später benötigt werden
- Ø Aufbewahren von Jahresenddateien
  Jahresendbestand für Bilanzauswertung
- Ø Anlegen einer Sicherungskopie für jeden Tag, Woche, Monat usw.
  Unterschiedliche Strategien der Sicherung
- Ø Bautechnik: Aufbewahrung der Sicherheitskopien in einem anderen Raum: Feuer, Wasser, Blitz
- Ø Benutzerprotokoll
  Wer hat wann was genutzt? Fehler oder Manipulation?

Datensicherungsstrategien

Das Resultat der durchgeführte Datensicherung wird als Sicherungskopie oder **Backup** bezeichnet. Die Wiederherstellung wird als Datenrücksicherung oder **Restore** bezeichnet.

Die vorhandenen und sich ständig ändernden Daten müssen:

- o **Regelmäßig** gesichert werden (privater User oder z. B. Bank)
- o **Aktuell** und sicher sein (abhängig von der Änderungshäufigkeit und ihrer Wichtigkeit, Lagerung und Ort)
- o Auch im gesicherten Zustand dem **Datenschutz** entsprechen (Schutz personenbezogener Daten vor unbefugtem Zugriff)
- o **Vollständig** in einer bestimmten Zeitrahmen **fehlerfrei** wieder herstellbar sein
- o **automatisch** und **mehrfach** gesichert werden
- o unterliegen **wirtschaftlichen Kriterien**

Die Strategie oder Vorgehensweise ergibt sich aus den folgenden **Überlegungen/Fragen**

- Wie die Datensicherung zu erfolgen hat.
- Wer ist für die Datensicherung verantwortlich?
- Wann und wie oft wird sie durchgeführt?
- Welche Daten werden gesichert?
- Auf welchem Speichergerät oder Speichermedium wird gespeichert?
- Wo werden die gesicherten Daten aufbewahrt?
- Ist die Datensicherung vor Diebstahl zu sichern ist und ist eine zusätzliche Verschlüsselung notwendig?
- Wie lange werden sie aufbewahrt?
- Wann und wie werden die Daten auf ihre Wiederherstellbarkeit geprüft?
- Welche Datensicherungsstrategie (siehe unten) wird umgesetzt?

- Sind Datenbanken zu sicher? Gerade bei Datenbanken müssen Besonderheiten beachtet werden:
  Datenbanken müssen in einem konsistenten Zustand gesichert werden (Datenkonsistenz). Dies erreicht man durch Herunterfahren der Datenbank (Cold Backup). Die Datenbank ist off-line und der Produktivbetrieb ist unterbrochen.
  Ein Hot Backup ist eine Sicherung, die möglichst aktuell gehalten wird (optimal wäre ein gleicher Stand wie das Live-System). Beim Systemabsturz wäre die Datensicherung sofort einsatzbereit (z. B. durch RAID1, Mirroring).
- Wer erstellt die Dokumentation?
- Wie wird bei der Rücksicherung vorgegangen und wie sieht der Wiederanlaufplan aus? Wer ist in diesem Fall verantwortlich?

Es gibt unterschiedliche Datensicherungen

Eine vollständige Datensicherung:
die Sicherung aller Daten, unabhängig vom Datum ihrer letzten Sicherung.

Eine differenzielle Datensicherung:
die seit der letzten vollständigen Datensicherung geänderten Daten werden vollständig gespeichert.

Inkrementelle Datensicherung:
nur die Daten werden gesichert, die sich seit der letzten Datensicherung (meist der letzten inkrementellen Sicherung) verändert haben. Die inkrementelle Datensicherung geht schnell, aber es ist ein relativ großer Aufwand bei der Wiederherstellung von Daten. Es müssen mehrere Sicherungen hintereinander zurück überspielt werden.

Das Generationenprinzip oder die Großvater-Vater-Sohn Datensicherung:
Von dem Datenbestand wird ständig ein dreifaches Backup mit unterschiedlichem Alters durchgeführt (Großvater, Vater, Sohn). Veränderungen und Verluste der Daten können wieder Rückgängig gemacht werden.