

Strg, Alt, Entf ? !

Hilfe bei Hard- und Softwareproblemen, Auf- u. Umrüstung, Reparatur, Wartung, Beratung u. Schulung

Jochen Semmelhaack

Kuhle 13, 25335 Neuendorf

☎ 0 41 28 – 9 6 3 2

☎ 0 41 28 – 9 6 3 9

☎ 0 162 – 31 23 288

info@pc-hilfe-semmelhaack.de

Haben Sie ein Sicherheitskonzept für Ihr EDV- System?

Besitzen Sie eine Datensicherung Ihrer Fotos, Programmeinstellungen oder Firmendaten? Ist Ihr System vor Fremdzugriffen geschützt und werden diese Schutzmaßnahmen regelmäßig kontrolliert?

1. Datensicherung

Unter Datensicherung versteht man das teilweise oder gesamte Kopieren der in einem Computersystem vorhandenen Daten auf ein alternatives Speichermedium. Das Ziel ist, den Datenverlust bei Systemausfällen, wie z. B. Festplattendefekt zu begrenzen. Die Wiederherstellung einer Sicherungskopie bezeichnet man auch als Datenrücksicherung oder Restore.

Die Datensicherung dient dem Schutz vor Datenverlust durch:

- Hardware-Schäden (z. B. durch Überspannung, Materialermüdung, Verschleiß oder Naturgewalten wie Feuer, Wasser, etc.)
- Diebstahl oder absichtliches Löschen der Daten
- Computerviren, -würmer und Trojanische Pferde
- versehentliches Überschreiben oder Löschen der Daten
- technische Fehler innerhalb der Daten

Die Aufbewahrung von Datensicherungen sollte örtlich entfernt von der EDV-Anlage in einer sicheren Umgebung erfolgen. Für **kleinere Unternehmen** eignen sich z. B. Bankschließfächer. **Größere Unternehmen** können z. B. speziell gesicherte Safes oder Räumlichkeiten zur feuersicheren Unterbringung der Daten benutzen und/oder die gesicherten Daten auf mehrere Standorte verteilen. Datensicherung auf dem heimischen **Privat-PC** ist davon abhängig, welche Speichermedien zur Verfügung stehen. Meist werden günstige Medien für bereits vorhandene Geräte wie CDs, DVDs, Memory-Sticks oder externe Festplatten gewählt.

Der einzig sichere Beweis einer erfolgreichen Datensicherung ist der Nachweis, dass die gesicherten Daten auch vollständig und innerhalb eines angemessenen Zeitraums wiederhergestellt werden können. Aus diesem Grund sollten in regelmäßigen Abständen **Rücksicherungstests** erfolgen.



In Unternehmen sollte die Datensicherung gemäß einer Datensicherungsstrategie durchgeführt werden. In ihr sollte festgelegt werden:

- Wie die Datensicherung zu erfolgen hat.
- Wer für die Datensicherung verantwortlich ist.
- Wann Datensicherungen durchgeführt werden.
- Welche Daten gesichert werden sollen.
- Welches Speichermedium zu verwenden ist.
- Wo die Datensicherung sicher aufbewahrt wird.
- Wie lange Datensicherungen aufzubewahren sind.
- Wann und wie Datensicherungen auf ihre Wiederherstellbarkeit überprüft werden.

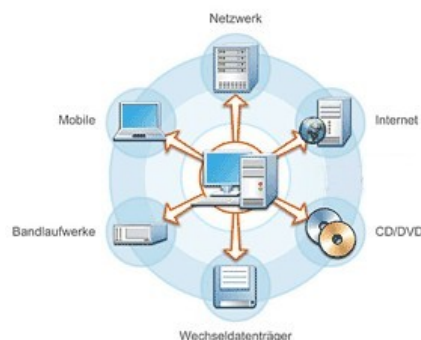
Datensicherungen sollten in Unternehmen automatisch erfolgen, da manuelle Datensicherungen durch menschliche Fehler beeinflusst werden können. Die Anfertigung von zwei räumlich getrennten Datensicherungen eines Datenbestandes erhöht die Zuverlässigkeit der Datenwiederherstellung, um die Auswirkungen plötzlich auftretender Ereignisse wie Feuer oder physikalische Zufälle zu minimieren. Die Verwendung von Standards macht die Datenwiederherstellung einfacher.

Folgende Möglichkeiten stehen zur Verfügung:

- Manuelle Sicherung
- Software- und zeitgesteuerte automatische Sicherung
- auf Externe Festplatte
- DVD / CD
- auf Memory-Stick
- bei DSL-Verbindungen auf Datenserver von Dienstleistern im Internet

Der wirtschaftliche Nutzen von Datensicherungen sollte sich in einem wirtschaftlich sinnvollen Verhältnis zu dem für die Datensicherung betriebenen Aufwand verhalten. Eine Wiederherstellung der Daten von einem Spezialunternehmen i. d. R. weitaus kostspieliger, als die Anschaffung von passender Software und Hardware zur Sicherung. Zudem gibt es auch hier keine Garantie des Erfolgs.

Steht besondere Software zur Verfügung, empfiehlt sich eine differenzielle Sicherung. Die technisch einfachste Möglichkeit, die ohne Software und Hintergrundwissen auskommt, ist die Anlage von mindestens zwei Sicherungen im regelmäßigen Abstand auf einem physisch unabhängigen Datenträger. Sind die Daten auf der ursprünglichen Festplatte entsprechend sortiert, kann die Sicherung aktueller oder besonders wichtiger Daten in kürzeren Zeitabständen erfolgen (z. B. täglich), als die der übrigen Bestände.



2. Weitere Sicherheitsmerkmale

- Gibt es einen ausreichenden Virenschutz?
Wird die Aktualität und Wirksamkeit regelmäßig geprüft?
- Gibt es eine Firewall?
Wissen Sie was diese leistet und was nicht?
- Sind die vorhandene Installation und die dazugehörigen Einstellungen ausführlich dokumentiert (Software mit Keys oder Passwörtern)? Gibt es eine Anleitung zur Installation für den Notfall?
- Bezieht die Sicherung auch Netzwerk-Rechner, Notebooks und die Daten auf diesen ein?
- Werden vertrauliche Informationen von Datenträgern oder IT-Systemen sicher gelöscht? (z.B. alte Festplatten)
- Gibt es einen Schutz Überspannung (Blitz), Stromausfall und Diebstahl?
- Ist Ihr Passwortschutz ausreichend?
- Werden Arbeitsplatzrechner bei Verlassen und Kennwort gesichert?

Gerne sind wir Ihnen bei einer sicheren und wirtschaftlichen Lösung dieser Thematik behilflich. Bei Fragen und Problemen können Sie sich jederzeit an uns wenden.

