Datensicherung: Grundsätzliches zum Sichern von Daten

IHK München und Oberbayern

Wirtschaft für Zukunft

Datensicherung: Grundsätzliches zum Sichern von Daten

Wo und wie sichere ich welche Daten, damit diese im Notfall gerettet werden können? Das IHK-Merkblatt informiert dazu über Grundsätzliches.

1. **Um was geht es?**
   Die Nutzung eines PCs, Tablets oder Smartphones ist immer mit der Nutzung von Software und Daten auf Datenträgern verbunden: Ein Betriebssystem (Windows, iOS, Linux, Android,...) stellt die grundsätzlichen Funktionen bereit, Anwendungsprogramme ermöglichen die Arbeit mit dem Rechner und das Ergebnis der Arbeit wird in Dateien (Text, Word, Excel...) gespeichert. Diese Kombination kann durch Ausfälle der Hardware (z.B. Festplatte), fehlende Onlineverbindung (z.B. zur Cloud) oder unsachgemäße Handhabung gestört oder zerstört werden.

   Kann im Problemfall auf eine Sicherungskopie zurückgegriffen werden, ist eine Schadensbegrenzung über die Rekonstruktion der Informationen möglich.

   Voraussetzung ist aber eine aktuelle und verwertbare Sicherungskopie.

2. **Daten auf der Festplatte**
   Es gibt unterschiedlich wichtige Daten auf einem Rechner:
   - **Eigene Dateien**
     Die von Ihnen eingegebenen und gesammelten Daten sind die wichtigsten Daten auf einem Rechner und unbedingt regelmäßig zu sichern.
     Wobei Sie auch hier zwischen wichtigen und unwichtigen, aktuellen und veralteten Daten unterscheiden können. Wichtig ist, dass Sie Ihre persönlichen, wichtigen Daten von den Daten für Betriebssystem und Anwendungsprogramme, trennen. Legen Sie z.B. auf dem PC ein Basisverzeichnis (z.B. Meine Daten) und darin eigene Verzeichnisse für Ihre Zwecke an. Oder sichern Sie in der Cloud gesicherte Daten nochmals an anderer Stelle.

   - **Betriebssystem und Anwendungsprogramme**
     Betriebssystem und Anwendungsprogramm sind im Allgemeinen über die beim Kauf mitgelieferten Speichermedien oder Downloads wieder

installierbar oder reparierbar. Ebenso Treiber für Geräte wie Drucker, Kameras etc.
Aber:
a. Aus dem Internet geladene Anwendungsprogramme müssen ggf. erneut geladen werden. Legen Sie für solche Programme einen eigenen Ordner an (z.B. Downloads), den Sie wie Ihre eigenen Dateien sichern (s.o.).
b. Falls Sie Software direkt aus dem Internet gekauft haben und die Seriennummer per E-Mail erhalten haben: Kopieren Sie den Inhalt dieser E-Mails in eine Datei und sichern auch diese Datei so wie Ihre eigenen Dateien (s.o.).
c. Anwendungsprogramme können auf Ihre Bedürfnisse hin konfiguriert werden. Bzw. Sie fügen ggf. den Programmen oft Information hinzu (z.B. Lesezeichen bei Browsern). Auch diese Informationen sind so wie Ihre eigenen Dateien (s.o.). Wo die Anwendungsprogramme diese Informationen sichern ist sehr unterschiedlich und im Einzelfall zu recherchieren: Manche Programme bieten in den Menüs die Optionen wie Exportieren an (z.B. Lesezeichen-Manager von Browsern).

- **Netzwerke**
  Sollten Sie mehrere Rechner in einem Netzwerk betreiben, empfiehlt sich der Einsatz von Netzwerklaufwerken (=ein eigens dafür vorgesehener Rechner oder Cloudspeicher) oder Datenaustauschplattformen (z. B. Wikis), auf denen alle Mitarbeiter Daten ablegen können. Dieses Netzwerklaufwerk kann dann zentral gesichert werden. Allerdings müssen Sie dafür sorgen, dass die Zugriffsrechte für die Mitarbeiter geregelt sind und die Kapazität des Netzwerklaufwerkes ausreicht bzw. pro Mitarbeiter begrenzt wird.
  Noch konsequenter in der zentralen Datenhaltung sind Terminal-Netzwerke mit virtuellen Maschinen: Dort dient der Rechner am Arbeitsplatz nur noch der Bildschirmanzeige. Die Programme laufen auf einem Zentralrechner, die Tastaturanschläge werden diesem sofort übermittelt. Neben der damit möglichen zentralen Sicherung ist ein weiterer Vorteil die Zugriffsmöglichkeit darauf: Über gesicherte Internet-Verbindungen können Außendienstmitarbeiter so weltweit auf das Firmennetzwerk zugreifen und Baupläne, Kundendaten, Telefonnummer etc. nutzen.

3. **Was sichert man wie?**
   Bei der Sicherung kann man immer wieder alles komplett kopieren oder nur die Änderungen sichern:
   - **Volldatensicherung**
     Alle Daten werden zu einem bestimmten Zeitpunkt gesichert.
     Vorteil: Alles schnell wieder verfügbar

Nachteil: Zeitaufwändig, viel Speicherplatz nötig
Empfehlung: Regelmäßig Volldatensicherung durchführen, insbesondere wenn neue Programme oder Programmversionen eingespielt wurden.

- **Partielle Sicherung**
  Nur die als wichtig erachteten Daten werden gesichert. Programmdateien oder temporäre Dateien werden zum Beispiel nicht gesichert. Hier kann man nach Dateityp die Häufigkeit der Speicherung differenzieren. Systemdateien und Programmdateien ändern sich nur nach Änderungen im System oder in Programmen wogegen bei einer Datenpartition(Trennung der Benutzerdaten von den Systemdaten) die tägliche Speicherung der Daten notwendig ist.
  Vorteil: Zeitersparnis, weniger Speicherbedarf
  Nachteil: Etwas mehr Verwaltungsaufwand als bei der Vollsicherung

- **Inkrementelle Datensicherung**
  Die Änderungen seit der letzten Vollsicherung bzw. inkrementellen Sicherung werden gesichert.
  Vorteil: Schnell, wenige Speicherplatz nötig
  Nachteil: Wiederherstellung der Daten aufwändig

- **Differentielle Datensicherung**
  Nur die Änderungen seit der letzten Vollsicherung werden gesichert.
  Vorteil: Weniger Zeit & Speicherplatz als bei Volldatensicherung nötig
  Nachteil: Mehr Zeit & Speicherplatz als bei inkrementeller Sicherung nötig

- **Inkrementelle oder differentielle Datensicherung?**
  Im Schadensfall ist mit einer differentiellen Datensicherung der Rechner schneller rekonstruierbar. Allerdings muss bei der täglichen Sicherung mehr Zeit und Hardware investiert werden.

4. Worauf und mit welcher Software kann man sichern?

- **Speichermedien**
  Regelmäßige Kontrolle der Speichermedien ist nötig und ggf. müssen die Daten von einem alten auf ein neues Speichermedium überspielt werden.
  - DVD: Wenige Gigabyte (GB) sicherbar, Für vereinzelte Sicherungen und für Auslandseinsätze z. B. China ggf. geeignet
  - USB-Stick: Ein USB-Stick (mehrere hundert GB möglich,) ist klein, handlich und schnell an einen Rechner angeschlossen. Daher ist besondere Sorgfalt gefragt bei der Aufbewahrung

(sicher lagern) und Absicherung (Passwort- und Fingerabdruckschutz möglich).

- Externe Festplatten: Am USB-Anschluss sind externe Festplatten mit einigen tausend GB anschließbar. Die Lagerung und die Sicherung der Festplatte ist hier besonders wichtig. USB 3.0. Festplatten vergrößern die Datenübertragungsgeschwindigkeit stark. Raid-Festplatten spiegeln gegenseitig die Daten, so dass beim Ausfall einer Festplatte die Daten noch auf einer zweite Festplatte vorhanden sind.

- Bandlaufwerke: Daten werden auf Kassetten gesichert, die mehrere hundert GB schnell aufnehmen können. Allerdings sind Bandlaufwerke teuer und die Suchzeit für Dateien relativ lange.

- Cloud: Daten werden per Internet auf Speichernetzwerke hochgeladen. Dazu ist eine schnelle und zuverlässige Breitbandanbindung nötig. Zudem sollte genau geprüft werden, wie die Daten in der Cloud gelagert werden: Das betrifft z. B. den Datenschutz (werden personenbezogene Daten außerhalb der EU gelagert?) und den Zugriffsschutz (werden die Daten verschlüsselt abgelegt?).

- **Empfehlung:** Mit einer externen Festplatte erhalten Sie für relativ wenig Geld ein einfach zu bedienendes lokales Speichermedium. Ergänzt um verschlüsselt abgelegte Onlinesicherungen.
  s.a. BSI Datensicherungskonzept

- **Datenspiegelung**
  Datenspiegelung ist der Ansatz zur kostengünstigen und schnellen Erstellung redundanter Kopien von Daten. Auf zwei gleichartigen Speichermeiden wird der gleiche Datenbestand gespeichert. Das wird erreicht, indem man eine Hardware- oder eine Softwarelösung zur Synchronisierung einsetzt. Das eine Medium wird als Primärmedium bezeichnet auf dem gearbeitet wird. Für den Fall, dass dieses Primärmedium ausfällt, kann man durch die Synchronisierung auf das Sekundärmedium wechseln. Will man kritische IT-Systeme absichern, sollten alle Schreibvorgänge auf beiden Medien gleichzeitig durchgeführt werden.

- **Datenlagerung**
  Unabhängig vom Speichermedium sollten Sie dieses kennzeichnen und beschriften. Schließlich wollen Sie das Sicherungsmedium nicht irrtümlicherweise entsorgen oder Unbefugten aushändigen. Ebenso empfiehlt es sich, das Speichermedium hin und wieder zu testen, ob es

noch lesbar ist. Hinsichtlich des Ortes ist zu beachten, dass Temperatur, Luftfeuchtigkeit, Staub das Speichermedium nicht gefährden. Man schätzt die Lebensdauer einer DVD auf 40 bis 200 Jahre, aber nur unter optimalen Bedingungen. s.a. BSI zu Archivierung.
Im Idealfall bewahren Sie die Sicherungen diebstahlgesichert und nicht am gleichen Ort wie das Original auf.

- **Software**
  - Sicherung auf externen Festplatten ohne zusätzliche Software: https://www.youtube.com/watch?v=mOZfbZqGjd4
  - Sicherung mittels Windows-Onedrive: https://www.youtube.com/watch?v=I1IvF8lri5U
  - Sicherung von iPhones / iPads: https://www.youtube.com/watch?v=in7HzmmDl0I
    Z. B. Windows 10 verfügt über einen Sicherungs- und Wiederherstellungsassistenten: Start > Alle Programme > Wartung > Sichern und Wiederherstellen, mehr dazu
  - Tests von zusätzlicher Software für die Datensicherung:
    - Stiftung Warentest: https://www.test.de/Backup-Software-im-Test-4622858-0/
    - Computerbild:https://www.computerbild.de/artikel/cb-Ratgeber-Sicherheit-Bac
    - heise Verlag: https://www.heise.de/download/specials/Die-beste-Backup-Software-Tools-fu

- **Verschlüsselungsprogramme**
  Um die Daten zusätzlich vor unberechtigtem Zugriff zu sichern, ist die Verschlüsselung der Daten möglich. Insbesondere bei den kleinen USB-Sticks ist das empfehlenswert.
  - Übersicht von Verschlüsselungsprogrammen: https://www.heise.de/download/search?terms=verschl%C3%BCsselung
  - PGP: http://www.iks-jena.de/mitarb/lutz/anon/pgp.html

- **Verschlüsselung für die Cloud**
  Die Verschlüsselung erfolgt auf einem virtuellen Laufwerk auf Ihrem PC. Eine Übersicht von Software dafür finden sie hier.
- **Online-Sicherung**
  Neben der bisher vorgestellten Datensicherung auf Speichermedien können wichtige Daten auch in gesicherten Rechenzentren abgelegt werden. Verschiedene Firmen bieten eine verschlüsselte Datenübertragung per Internet, Speicherplatz in einem Rechenzentrum und automatisierende Software an.

- Vorrausetzungen an sich selbst: Breitband-Internetverbindung
- Vorrausetzungen an den Online-Sicherungsanbieter: Gesicherte Übertragungswege ins Rechenzentrum, tadelloser Ruf, Größe und (EU?) Standort des Rechenzentrums?
- Vertrauen zum Anbieter: Ist er morgen auch noch da? Vertragsbedingungen?

- **Virtuelle Datenräume**
  Neben der simplen Aufbewahrung von Daten kann man Online-Plattformen zum gegenseitigen Austausch von Daten und Informationen nutzen. Als Nebeneffekt werden vertrauliche Daten gesichert.
  Übersicht von Anbietern von Datenräumen:
  https://www.capterra.com.de/directory/30783/virtual-data-room/software
  Allgemeine Übersicht von Software zu Datensicherung, Datenschutz:
  http://www.softguide.de/software/datensicherung-datenschutz.htm

5. **Was tun wenn das Speichermedium kaputt ist?**
   Ist die Festplatte oder das Bandlaufwerk kaputt, ist professionelle Hilfe nötig.
   - Kriterien für Anbieter von Datenrettung:
     https://www.recoverylab.de/serioese-datenrettung-datenrettungsfirmen-kriterien/
   - Softwareübersicht Datenrettung:
     https://www.chip.de/download/tag_datenrettung_Datenrettung/gesamt-charts/
   - Test von Datenrettungsangeboten: Stiftung Warentest:
     https://www.test.de/Datenrettungssoftware-im-Test-Nur-eine-hilft-in-allen-Situationen

ANSPRECHPARTNER

Bernhard Kux
089-5116-1705
bernhard.kux@muenchen.ihk.de