JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN

UNIVERSITÄTSBIBLIOTHEK

e-Coffee-Lecture: Datensicherheit und Backupstrategien

Gliederung

(1) Datenverlust: ein Worst-Case-Scenario **Warum?**

(2) Grundlegendes zur Datensicherheit **Was?**

(3) Maßnahmen für Datensicherheit **Wie?**

Datenverlust: ein Worst-Case-Scenario

Person X wertet in ihrem Büro bereits den ganzen Tag Daten für seine Dissertation aus. Die sensiblen Daten hat sie, wie immer, auf ihrem USB-Stick mitgebracht. Eine Sicherung liegt daheim sicher in einer ihrer Schreibtischschubladen. Da es spät wird und sie noch einen Termin hat, beendet sie ihre Arbeit hastig, speichert die Datei auf dem Stick aus Zeitgründen unverschlüsselt ab und räumt diesen, wie üblich, in ihre Tasche. Sie macht sich auf den Weg nach Hause und stellt ihre Tasche ab.

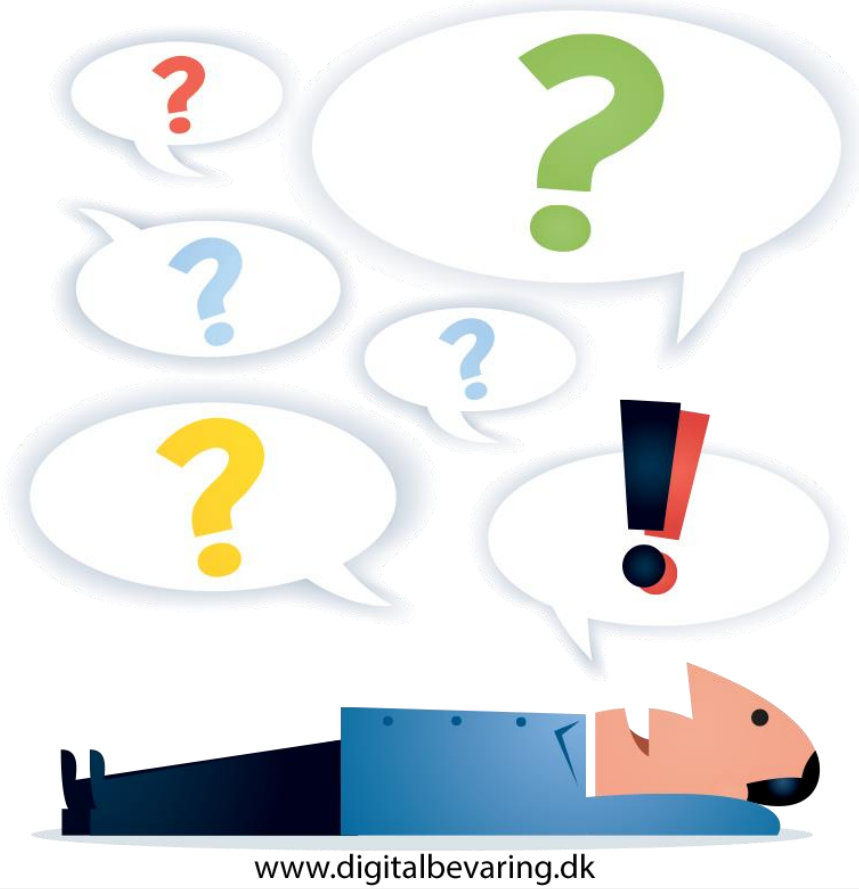
Datenverlust: ein Worst-Case-Scenario

Als sie am nächsten Tag wieder im Büro ist, merkt sie, dass der Stick verschwunden ist. Glücklicherweise sichert sie ihre Dateien aber auch immer noch in einer Cloud. Da fällt ihr ein, dass sie am Vortag ja schnell weg musste und das Cloud-Backup deshalb vergessen hat. Auch die Tage davor musste sie ihre Arbeit hastig beenden, die letzte Sicherung ist von vor 3 Tagen, die Sicherung auf der externen Festplatte daheim bereits mehrere Wochen alt. Verärgert macht sie sich an die Arbeit und wiederholt ihre Auswertungen in der Hoffnung, dass niemand den verlorenen Stick mit den unverschlüsselten sensiblen Daten findet.

Datenverlust: ein Worst-Case-Scenario

Was hat Person X denn falsch gemacht?

- unsichere Ablage der Datenträger
- nur eine Version/Kopie der aktuellen Daten
- manuelle Backups
- keine Verschlüsselung der sensiblen Daten



Grundlegendes zur Datensicherheit

Was ist eigentlich Datensicherheit?

- genereller Schutz von Daten
- bezieht sich sowohl auf analoge als auch digitale Daten
- Frage nach den technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Daten
- hohe Datensicherheit als angestrebter Zustand durch diese Maßnahmen

Quelle: colourbox.com/search/find?supplier=80700

Grundlegendes zur Datensicherheit

Was umfasst Datensicherheit?

- Schutz vor Verlust und Diebstahl
- Schutz vor höherer Gewalt (z.B. Feuer)
- Datenlöschung/-vernichtung
- Datenspeicherung und -aufbewahrung
- Verschlüsselung
- …

Quelle: colourbox.com/supplier/bigp-105393

Maßnahmen für Datensicherheit

1) sicherer Ablage-/Aufbewahrungsort für Datenträger
   a. abschließbarer Raum
   b. Tresor / (Bank-)Schließfach
   c. Brandschutzkassetten
   d. für tragbare Geräte: Organizer/zusätzliche Aufbewahrungstasche
2) Nutzung von vornherein geschützten Geräten
   a. wasserdichte USB-Sticks
   b. externe Anti-Shock Festplatten

Maßnahmen für Datensicherheit

3) Verschlüsselung von Dateien und Ordnern
   - VeraCrypt
   - Rohos Mini Drive
   - Passwortvergabe für gezippte Dateien/Ordner
4) Ablage von Daten in einer Cloud oder auf Netzlaufwerk
   - JLUbox (Mitarbeiter: 100GB / Studierende: 30GB)
   - winfile (Mitarbeiter/Studierende: 50GB)

Maßnahmen für Datensicherheit

5) Datenlöschung/-vernichtung

- Tiefenformatierung mit DBAN oder HDD LLF Low Level Format Tool
- Demagnetisieren mit Degausser (nur bei HDDs)
- Professionelle Datenträgervernichtung gemäß DIN66399
- Private Zwecke: Festplatten bzw. Platter mehrfach durchbohren

Maßnahmen für Datensicherheit

6) Backupstrategien
   - ➢ 3-2-1 Regel einhalten
   - ➢ Arten von Backups:
     a. vollständig
     b. inkrementell
     c. differenziell