Backup-Konzepte

Datensicherung einfach gemacht

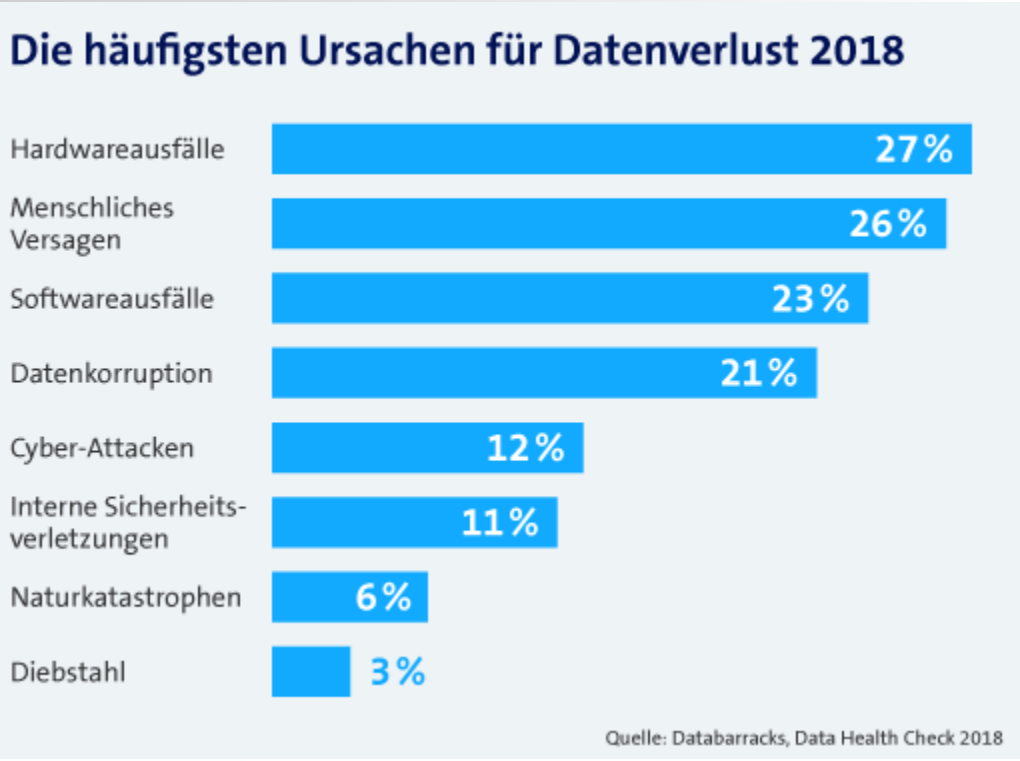
Inhalt

Sinn und Zweck der Datensicherung

- **Eine Datensicherung schützt vor den Folgen von Datenverlust**
  - Es muss nicht immer Cyber-Kriminalität sein:
    - Versehentliches Löschen / Verändern der eigenen Daten ist die häufigste Ursache!
    - Bekannte Gefahren: via Phishing-Mails werden IT Systeme angegriffen
    - Aber natürlich können IT Systeme (Hardware oder Software!) auch einfach mal ausfallen
- **Was ist eine Datensicherung („Backup“)?**
  - das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren / wiederherstellen zu können!
- **Backups sind eine Maßnahme des Datenschutzes (→ „Verfügbarkeit“)**
  - Dies ist aber nur eines der Schutzziele (dazu zählen auch: Vertraulichkeit, Integrität)
  - Betriebe haben die Pflicht Datenschutz zu implementieren (→ gemäß HGB, GoBD, DSGVO, GDPdU et.al.)
  - Ein Backup-Konzept sollte eingebettet sein in das übergreifende Datenschutz- und Datensicherheitskonzept (→ BSI Grundschutz), und das Notfall-Management (→ ITIL SM)
  - Die Backup- **und Restore**-Verfahren **müssen erprobt und dokumentiert sein!!**

Ursachen für Datenverluste

- **Menschliches Versagen**
  - Versehentliches Löschen oder Überschreiben von Dateien / Inhalten
  - Fehlerhafte Konfiguration von PC / Server
- **Technische Probleme + höhere Gewalt**
  - Verschleiß (Festplatten altern, SSDs ebenso)
    → beachte „MTBF“ und „SMART“-Werte
  - Mechanische Defekte (z.B. durch Sturz, Erschütterung, Hitze, Kälte)
  - Elektrische Defekte (Kurzschlüsse, Überspannung, defekte Netzteile!)
  - Äußere Einflüsse (Einbruch, Blitzschlag, Brand, Überflutungen!)
- **Cyber-Kriminalität + interne Prozesse**
  - Phishing, Hacker-Angriffe, Ransom-Ware (Daten-Verschlüsselung + Erpressung)
  - Absichtliches Löschen / Beschädigen („Rache-Akte“), Zugriffe trotz/nach Mitarbeiter-Kündigung, Daten-Diebstahl
- **Betriebssystem- oder Softwarefehler**
  - Sporadisch werden Fehler in Betriebssystemen bekannt, z.B. Windows-10 Update im Okt. 2018 (nach dem Update fehlten zahlreiche Programme und Benutzerdaten)
  - Fehler in Anwendungs-Programmen und/oder Datenbanken sind relativ häufig!



Was umfasst ein Backup-Konzept?

- **Ermittlung und Bewertung der eigenen Anforderungen**
  - Welche IT Systeme sind zu schützen, um welche Daten geht es?
  - Welche (Geschäfts-)Prozesse hängen von den Systemen + Daten ab?
  - Wie aktuell müssen im Notfall die wiederhergestellten Daten sein?
    - = Menge/Zeitspanne der Daten, die verloren gehen dürfen (RPO, Recovery Point Objective)
  - Wie lange darf die im Notfall erforderliche Wiederherstellung maximal dauern?
    - = Zeitraum bis „die IT“ nach dem Notfall wieder verfügbar ist (RTO, Recovery Time Objective)
  - Wie lange müssen gelöschte Daten wiederherstellbar sein? (Backup-Historie, kein Archiv!)
- **Auswahl / Festlegung einer „Backup-Strategie**
  - „High-Level“ Beschreibung: was, wie, wo, worauf/wohin, wie oft, wie lange, durch wen
- **Auswahl und Beschaffung benötigter Backup-Hardware + -Software**
  - Backup-Medien, Aufbewahrungs-Behälter, Beschriftung, Backup-Programm(e), …
  - „Aufrüstungen“ der Infrastruktur? (Stromversorgung, Klima, Netzwerk LAN + WAN)
- **Implementierung, Test und Dokumentation der Backup-Verfahren**
  - Software installieren und konfigurieren, Backup-Medien vorbereiten, Prozesse einrichten
  - Backup und Restore probeweise durchführen und dabei dokumentieren (auch: Zeit)
  - Backup-Konzept und Backup-/Restore-Verfahren mehrfach ausdrucken und verteilen

Verwendung mehrerer Backup-Medien

- **Beispiel: „Die 3-2-1 Regel“**
- **<u>Drei</u> Kopien der Daten herstellen**
  - (die Original-Daten werden mitgezählt)
  - Also zeitlich gestaffelt mindestens noch zwei Kopien der Daten erstellen
- **<u>Zwei</u> unterschiedliche Medientypen verwenden**
  - z.B. Festplatten und CDs, oder Festplatten und Magnetband (ggf. auch Cloud)
- **<u>Eins</u> der Backup-Sets an einem externen Ort verwahren**
  - z.B. in einem Tresor (Brandklassen beachten!) oder Bank-Schließfach
  - oder „auslagern“ in Privaträume (→ Backups verschlüsseln!)
  - Ganz wichtig: nur das „**Air Gap**“ schützt vor Cyber-Kriminalität!
- **Diese „3-2-1“-Regel ist besser als nichts – aber: es kein Backup-Konzept!**
  - Beispiel: zwar gibt es dann zwei unabhängige Daten-Kopien, aber es gibt noch keine Versionierung (die letzten x Backups?) und keine ausreichende Historie (x Monate?)
  - Und es gibt viele andere Regeln: z.B. „Großvater-Vater-Sohn“ oder „Türme von Hanoi“

Technik: unterschiedliche Backup-Arten

- **Es gibt eine Reihe unterschiedlicher Arten Backups zu erstellen:**
- **Backup von Dateien und Ordnern**
  - Entspricht der „intuitiven“ manuellen Methode: kopiert Dateien von A nach B
  - Backup-Programme fügen aber noch „Meta-Daten“ hinzu (Version, Datum, etc.)
  - Intelligente Backup-Verfahren können die Menge der zu sichernden Daten reduzieren:
    - Komplette Sicherung: es werden alle Dateien + Ordnern gesichert
    - Differenzielle Sicherung: es werden nur die Daten gesichert, die gegenüber der letzten Komplett-Sicherung hinzu kamen oder geändert wurden
    - Inkrementelle Sicherung: es werden nur gegenüber der letzten Komplett- oder Inkrementell-Sicherung neue oder geänderte Daten gesichert (→ Backup-Kette!)
- **Backup kompletter Filesysteme („Volumes“)**
  - Bei diesem Backup wird eine 1:1-Kopie der Festplatte (bzw. Partition) erstellt, die auch Betriebssystem- und Boot-Dateien sowie sämtliche Nutzer-Konfigurationen umfasst.
  - Dieses „Clonen“ der Volumes / Partitions geschieht meist als „offline“-Backup !
- **oft sinnvoll:**
  - Eine (zeitlich gestaffelte) Kombination von Volume- und Datei-Backups

Tools

- **Backup-Programme des jeweiligen Betriebssystems**
  - (Windows-7: unsicher, veraltet, nicht mehr einsetzbar!)
  - Windows-10: „Systemwiederherstellung“ mit vielen Tücken, „Datensicherung“
  - MacOS: „TimeMachine“ funktioniert sehr gut für Nutzer-Daten, nicht für das Betriebssystem selbst
  - Linux: viele gut funktionierende Tools (tar, rsync, ...), aber: Konfigurations-Aufwand
- **Andere kostenpflichtige Backup-Programme (kommerzielle Anbieter)**
  - Viele Anbieter, viele Tools, aber: fast alles ist „proprietär, d.h. nicht mit anderen Methoden lesbar
  - Ggf. nutzbar: Acronis True Image, Aomei Backupper Professional, Veeam Agent for Windows
- **Andere kostenlose Backup-Programme**
  - Anbieter von Festplatten oder NAS bieten teilweise eigene Tools an: zwar kostenlos, aber ebenfalls „proprietär
  - Freeware: die Heise-Redaktion bietet z.B. „c’t-WIMage“ an, das Windows-10 Volume-Backups erstellt
  - Open-Source: zahlreiche Tools auf Basis von bewährten Verfahren, z.B. Clonezilla, Borg, Duplicati
- **Empfehlung: ausschließlich Tools einsetzen, die "frei und offen" sind!**
  - Das betrifft sowohl den Programm-Quelltext als auch die Backup-Datenformate! (muss dokumentiert sein!)

    → ein Backup muss später auch mit anderen Programm-Versionen oder auf anderen Systemen lesbar sein!
- **Die Goldene Regel: „Ein Backup ist kein Backup, wenn man es nicht überprüft hat!“**
  - Dazu sollte man die „Verifikation“ der Backup-Tools nutzen, aber auch eine echte Wiederherstellung durchführen
- **Unbedingt eine Statistik / Übersicht führen**
  - Wann wurde welches Backup mit welchem Inhalt auf welchem Backup-Medium erstellt
  - Diese Übersicht entweder ausdrucken+verteilen, oder unabhängig von den Backup-Medien speichern (z.B. Cloud)

Beispiel für ein minimales Backup-Konzept

Auch Kleinbetriebe oder Freiberufler ohne „Rechenzentrum“ oder Server-Infrastruktur brauchen ein Backup-Konzept!

Für einen einzelnen PC oder Laptop könnte das zum Beispiel so aussehen:

- **An jedem Monats-Anfang:**
  - Backup aller Partitions mit „CloneZilla“ (offline) auf 2..3 externe USB-Disks im Wechsel
    (damit kann der PC oder ein Ersatzgerät komplett wiederhergestellt werden)
- **Täglich (abends):**
  - Backup aller „User Home“-Verzeichnisse mit „Duplicati“ o.ä. (online) auf zentrales NAS
    (damit werden Benutzer-Daten relativ aktuell gesichert)
- **Wöchentlich (oder am Wochenende):**
  - Replikation der NAS-Disks auf wechselnde externe Festplatten, oder in eine Cloud
    (damit werden Benutzer-Daten an einem redundanten Ort hinterlegt)

Das ist nicht perfekt, erfüllt aber einige grundlegende Anforderungen:

- RPO für Betriebssystem: 1 Monat, für User-Daten: 1 Tag
- RTO ca. 2 Std., + evtl. Hardware-Beschaffung, + Windows-Updates ...
- Versehentlich gelöschte Daten sind in Minuten wieder da (Stand vom Vortag)

Wie man Datensicherung NICHT machen sollte

- **An einem Smartphone**
  - Gar keine Datensicherung („ich hab' da keine Daten drauf...“)
    - Wird oft übersehen: Konfiguration / Zugangsdaten installierter Apps, Fotos, Notizen, …
  - Duplizierung lokaler Daten, Fotos + Dokumente in eine (vordefinierte?) Public Cloud
    - Keine Kontrolle: Zugriffe? Lebensdauer? „Vendor-Lock-In“? Vorsicht vor „Zwei-Wege-Sync“!!
- **An einem einzelnen PC oder Laptop**
  - Sporadisches manuelles Kopieren von Daten oder Ordnern auf USB-Stick(s)
    - Wird oft vergessen, keiner weiß welche Daten von wann auf welchem Stick sind
    - Evtl. sind die Nutzerdaten gesichert, aber Betriebssystem und Anwendungen???
  - Automatisches regelmäßiges Sichern von Ordnern auf eine externe Festplatte
    - Die Festplatte muss dazu permanent angeschlossen bleiben: schlechte Idee!
    - Rest-Risiko ist viel zu hoch (nur 1 Medium, nur 1 Ort), unklare Versionierung
  - Automatisiertes regelmäßiges Sichern von Ordnern auf eine mehrere Festplatten im Wechsel
    - Schon besser, aber verlangt viel Disziplin (Austausch und Lagerung der Medien)
- **Auf einem Server oder NAS**
  - Vertrauen auf „RAID“ (redundante Festplatten) und/oder Snapshots von Filesystemen
    - RAID ist KEIN BACKUP! Snapshots sind KEIN BACKUP!

Fun Facts

Quelle: pixabay.com

- **Hund zerbeißt den USB-Stick mit dem einzigen Backup**
  - Blöd, dass der PC danach noch am selben Tag kaputt ging…
    (eine wahre Geschichte, berichtet von Kroll Ontrack unter
    https://www.security-insider.de/kroll-ontrack-praesentiert-die-kuriosesten-datenverluste-gal-467690)
- **Das älteste Backup-Medium: Lochkarten …**
  - Das erste Speichermedium, das zur Datensicherung verwendet wurde.
    1890 entwickelt von Herman Hollerith zur Beschleunigung der Volkszählung.

Klassische Antwort eines IT-System-Admins auf die verzweifelte Frage eines Anwenders, ob er denn bitte die verlorenen Daten wieder herstellen könnte, und zwar ganz ganz schnell!!

- **Am 31. März ist „World Backup day“ → mach’ mit!**

DER "WORLD BACKUP DAY" EID

“Ich schwöre feierlich, am 31. März ein Backup meiner wichtigen Dokumente und wertvollen Erinnerungen zu machen.”

Ich werde auch meine Freunde und meine Familie über den "World Backup Day" informieren – Freunde lassen Freunde nicht ohne Backup steh'n.

Quelle: http://www.worldbackupday.com - This page is not officially supported or endorsed by „World Backup Day“.