zurück

Backup – Grundlagen, 3-2-1-Regel, Backup-Arten, RPO/RTO

Backups schützen Daten vor Verlust durch:

- Hardwaredefekte
- versehentliches Löschen
- Malware / Ransomware
- Fehlkonfigurationen
- Naturkatastrophen
- Softwarefehler

Ein Backup ist nur dann ein Backup, wenn es:

1. unabhängig,
2. regelmäßig,
3. testbar
   ist.

---

1. Warum Backups?

Ohne Backup kann ein Datenverlust existenzbedrohend sein – privat wie beruflich.

Typische Verluste:

- Familienfotos
- Projektdaten
- Buchhaltung
- Konfigurationsdateien
- Server (VMs, Container-Daten)
- E-Mail-Archive

Professionelle IT ist OHNE Backup nicht denkbar.

---

2. 3-2-1-Regel (wichtigste Backup-Regel)

Die 3-2-1-Regel lautet:

- **3 Kopien** deiner Daten

- auf **2 unterschiedlichen Medientypen**
- **1 Kopie extern/offsite**

ASCII:

```
Original
    + Backup auf NAS
    + Backup auf USB/Cloud (Offsite)
```

Warum?

- Ransomware kann lokale Backups zerstören
- Feuer/Einbruch kann Geräte vernichten
- Medien können ausfallen

3-2-1 gehört zum Pflichtwissen der IHK.

---

3. Backup-Arten

Es gibt drei klassische Backup-Arten:

a) Vollbackup

Alle Daten werden vollständig gesichert.

Vorteile:

- komplette Datensicherung
- einfach wiederherzustellen

Nachteile:

- höchste Speicherlast
- dauert am längsten

b) Inkrementelles Backup

Nur Änderungen seit dem letzten **irgendeinem** Backup werden gespeichert.

ASCII:

```
V1 (voll) → I2 → I3 → I4 → ...
```

Wiederherstellung:

- Vollbackup + alle Inkremente seitdem

Vorteile:

- sehr schnell
- sehr effizient

Nachteile:

- Wiederherstellung dauert länger
- Kette darf nicht defekt sein

c) Differenzielles Backup

Sichert Änderungen seit dem letzten **Vollbackup**.

ASCII:

```
V1 (voll)
D2 (alles seit V1)
D3 (alles seit V1)
```

Vorteile:

- einfacher wiederherzustellen
- mittlere Geschwindigkeit

Nachteile:

- großer Speicherbedarf nach einigen Tagen

Überblick

Art	Speed	Speicher	Restore-Zeit
Voll	langsam	hoch	schnell
Differenziell	mittel	mittel-hoch	mittel
Inkrementell	sehr schnell	niedrig	langsam

4. RPO & RTO

RPO – Recovery Point Objective

Frage: **Wie viele Datenverlust können wir verkraften?**

Beispiel:

- RPO 1 Stunde → Backups jede Stunde
- RPO 24 h → täglich

RTO – Recovery Time Objective

Frage: **Wie lange darf die Wiederherstellung dauern?**

Beispiel:

- RTO 5 Minuten → Snapshots / HA
  * RTO 2 Stunden → Backup-Server
  * RTO 48 h → Low-Priority-IT

RTO & RPO müssen zur Firma passen und sind Prüfungsstoff.

---

5. Backup-Medien (was ist sinnvoll?)

- **NAS** – zentral, schnell
    - **USB-Festplatten** – günstig, offline sicher
      * **LTO-Bänder** – langfristige Archivierung
      * **Cloud** – Offsite automatisch
      * **Snapshots** – zusätzlicher Schutz (aber kein echtes Backup!)
    - **Rsync / ZFS / Btrfs** – sehr effizient
      * **Hypervisor Backups (Proxmox, Hyper-V)** – vollständige VM-Sicherung

—

6. Snapshots vs Backups

Viele verwechseln das.

Snapshots

- sind „Zeitpunkte“ im Dateisystem
    - sehr schnell
      * kein Ersatz für Backups
      * gehen verloren, wenn Hauptspeicher verloren geht

Backups

- Kopie auf ein **unabhängiges** System
    - physisch getrennt vom Original
      * schützt vor Hardwaredefekt, Malware, Feuer

Wichtig: Snapshots sind NICHT zu 3–2–1 zählbar.

---

7. Offsite & Offline Backups

Offsite

- Backup liegt an einem anderen Ort
  * z. B. Cloud, Zweitstandort

Offline

- Backup-Medium ist NICHT dauerhaft verbunden
  * schützt vor Ransomware

Beides zusammen = maximale Sicherheit.

---

8. Backup-Strategien

a) GFS – Grandfather-Father-Son

klassische Rotation:

- Daily (Son)
    - Weekly (Father)
      * Monthly (Grandfather)

b) 3-Generationen-Backup

- heute
    - gestern
      * letzte Woche

c) 2-Stufen-Konzept

- lokales schnelles Backup
    - zusätzlich Offsite-Backup

d) Cloud-Hybrid

- lokales NAS + Cloud-Sicherung
    - perfekt gegen Katastrophen

—

9. Tools & Systeme für Backups

Private Umgebung

- BorgBackup
    - Restic
      * Rsync
      * Duplicati
      * Veeam (Free)
      * Synology HyperBackup
      * Proxmox Backup Server

Unternehmensumgebung

- Veeam Backup & Replication
    - Bacula
      * Commvault
      * NetBackup
      * Rubrik
      * Datto

Container / Docker

- Volumerotate
    - Restic + Cron
      * Borg + bind-mount
      * Proxmox VM-Backup → sehr sauber für Docker-Hosts

—

10. Was muss gesichert werden?

- Benutzerverzeichnisse
  - Dokumente
    * Serverdaten
    * VM-Images
    * Container-Volumes
    * Datenbanken (MySQL, MariaDB, Postgres)
    * Konfigurationsdateien (/etc)
    * Netzwerkkonfigurationen (Switches, Firewalls)
    * Zertifikate
    * wichtige Schlüssel (SSH, WireGuard, GPG)

  Backups **von Konfigurationen** sind extrem wichtig.

---

11. Testen von Backups

Ein Backup ist nur gut, wenn es wiederhergestellt werden kann.

Testen:

- Checksum-Prüfung
  - Teilweise Wiederherstellung
    * VM in isoliertem Netzwerk booten
    * Restore-Protokolle prüfen

  Viele Firmen scheitern hier → restore nicht getestet = kein Backup.

Zusammenfassung

- 3-2-1 ist die goldene Regel
  - Voll/Ink/Diff bestimmen Speicher & Geschwindigkeit
    * RPO = erlaubter Datenverlust
    * RTO = erlaubte Wiederherstellungszeit
    * Snapshots sind KEINE Backups
    * Offsite & Offline sind entscheidend gegen Ransomware
    * Backups müssen getestet werden

* Backups sind Pflicht für jede IT-Infrastruktur