



Backup Checkliste

Sind Ihre Backups wirklich bereit für 2027?

Die meisten Unternehmen gehen davon aus, dass ihre Backups funktionieren – bis zum Ernstfall. Diese Checkliste hilft Ihnen, in wenigen Minuten zu prüfen, ob Ihre Backup-Strategie wirklich sicher, vollständig und wiederherstellbar ist.

1. Vollständigkeit der Backups

- ☐ Sind **alle kritischen Systeme** im Backup enthalten (Server, SaaS, Cloud, Endpoints)?
- ☐ Gibt es einen Prozess, mit dem neue Systeme, SaaS-Dienste und nicht zentral beschaffte Anwendungen erkannt und in die Backup-Strategie aufgenommen werden?
- ☐ Werden auch **Microsoft 365 / Google Workspace** Daten gesichert?
- ☐ Gibt es eine aktuelle Übersicht aller gesicherten Systeme?

2. Backup Frequenz

- ☐ Entspricht die Backup-Frequenz Ihren Geschäftsanforderungen?
- ☐ Sind für kritische Systeme sowohl die **maximale Wiederherstellungszeit (RTO)** als auch der **maximal akzeptable Datenverlust (RPO)** definiert?

3. Schutz vor Ransomware & Angriffen

- ☐ Ist mindestens eine Backup-Kopie **unveränderbar (immutable)** und gegen Löschen geschützt?
- ☐ Gibt es **physisch oder logisch getrennte Backup-Standorte**?
- ☐ Sind Backup-Zugänge **separat abgesichert (MFA, Rollenrechte)**?
- ☐ Können Backups im Ernstfall **nicht gelöscht oder verschlüsselt** werden?

4. Wiederherstellbarkeit (der wichtigste Punkt)

- ☐ Wurden **Restore-Tests** in den letzten 6–12 Monaten durchgeführt?
- ☐ Ist klar definiert, **wie schnell Systeme wiederhergestellt werden müssen (RTO)**?
- ☐ Sind **Daten auch selektiv (Datei / Mail / User)** wiederherstellbar?
- ☐ Gibt es ein dokumentiertes **Recovery-Szenario für Notfälle**?
- ☐ Werden Backup-Daten regelmässig auf Integrität geprüft?
- ☐ Gibt es dokumentierte und regelmässig getestete Recovery- und Disaster-Recovery-Verfahren für unterschiedliche Ausfallszenarien?





Backup Checkliste

5. Offsite & Georedundanz

Sind Backups gegen folgende Risiken geschützt?

☐	Brand	☐	Stromausfall	☐	Naturkatastrophen	☐	Ransomware
--------------------------	-------	--------------------------	--------------	--------------------------	-------------------	--------------------------	------------

Viele Unternehmen folgen der 3-2-1-1-0-Regel:

3 Kopien der Daten / 2 unterschiedliche Speichermedien / 1 Offsite-Kopie / 1 Immutable Backup / 0 Fehler nach Recovery-Test

6. Monitoring & Alarmierung

☐	Werden Backup-Jobs automatisch überwacht?
☐	Werden Fehler sofort gemeldet?
☐	Prüft jemand regelmässig die Reports?
☐	Ist die Backup-Strategie dokumentiert und aktuell?

7. Kapazität & Wachstum

☐	Reicht der Backup-Speicher für das nächste Jahr?
☐	Gibt es eine Archivstrategie für alte Daten?

8. Compliance & Aufbewahrung

☐	Gibt es eine Archivstrategie für alte Daten?
☐	Existieren klare Löschrichtlinien?

9. Versteckte Risiken in der Backup-Strategie

☐	Gibt es Single Points of Failure (z. B. ein Backup-System ohne Redundanz)?
☐	Werden Backups nur „gespeichert“, aber nie aktiv überprüft?
☐	Ist klar, wer im Ernstfall Zugriff auf die Wiederherstellung hat?

Wenn Sie mehrere Punkte nicht sicher abhaken können, besteht kein unmittelbares Risiko – aber eine klare Lücke in der Resilienz Ihrer IT.

