Backup-Konzept für Unternehmen und Privatpersonen

Stand Nov 9, 2026

Kernaussage

Dieses Konzept verzichtet ausdrücklich auf USB-Sticks und USB-Festplatten als Backup-Medium. Dieser Verzicht ist nur sicher, wenn eine andere Kopie ihre Aufgabe übernimmt: eine Kopie, die ein Angreifer auch mit Administratorrechten nicht löschen oder verschlüsseln kann.

Wer USB streicht und sonst nur ein NAS im Heimnetz oder einen synchronisierten Cloud-Ordner hat, steht schlechter da als vorher. Deshalb nennt dieses Konzept für jede Zielgruppe einen konkreten Ersatz: unveränderlichen Cloud-Speicher (Object Lock / Immutable) oder ein zeitweise getrenntes Backup-System, das sich die Daten selbst holt.

Grundsatz: Ein Backup ist erst dann ein Backup, wenn die Wiederherstellung erfolgreich getestet wurde.

Grundprinzipien

Maßstab ist die 3-2-1-1-0-Regel, die erweiterte Form der klassischen 3-2-1-Regel für Zeiten von Ransomware.

Ziffer	Bedeutung	Umsetzung ohne USB
3	Drei Kopien: Original + zwei Backups	Arbeitsdaten, lokales Backup, Offsite-Backup
2	Zwei verschiedene Medien bzw. Systeme	z. B. NAS + Cloud-Objektspeicher
1	Eine Kopie an einem anderen Ort	Rechenzentrum in der EU, zweiter Standort
1	Eine Kopie unveränderlich oder getrennt	Object Lock / Immutable, Pull-Backup, Band (LTO)
0	Null Fehler beim Wiederherstellungstest	Regelmäßige, dokumentierte Restore-Tests

Weitere Pflichtprinzipien:

- **Versionierung statt Spiegelung.** Synchronisation (OneDrive, Dropbox, RAID) ist kein Backup: Gelöschte oder verschlüsselte Dateien werden mitsynchronisiert. Nötig sind Versionen über mindestens 30 Tage, besser 90.
- **Verschlüsselung vor dem Verlassen des Geräts.** Backups werden clientseitig verschlüsselt (AES-256). Der Schlüssel liegt getrennt vom Backup, z. B. im Passwortmanager und zusätzlich auf Papier im Safe.
- **Getrennte Zugangsdaten.** Das Backup-Konto hat eigene Zugangsdaten mit Zwei-Faktor-Anmeldung und ist nicht Teil der Windows-Domäne oder des normalen Benutzerkontos.
- **Automatisierung.** Ein Backup, das jemand von Hand anstoßen muss, fällt früher oder später aus.
- **Ziele festlegen.** RPO = wie viele Stunden Datenverlust maximal tragbar sind. RTO = wie schnell der Betrieb wieder laufen muss. Beides bestimmt Häufigkeit und Technik.

Verzicht auf USB-Datenträger

Regel: USB-Sticks, USB-Festplatten und USB-SSDs werden nicht als Backup-Medium eingesetzt – weder im Unternehmen noch privat. Bestehende USB-Backups werden nach Einführung des neuen Konzepts überführt und anschließend sicher gelöscht (Überschreiben oder physische Vernichtung, bei personenbezogenen Daten nach DIN 66399).

Begründung:

1. **Menschlicher Faktor.** USB-Backups hängen davon ab, dass jemand das Laufwerk anschließt, wechselt und wegbringt. In der Praxis bleibt das Laufwerk dauerhaft angesteckt oder wird wochenlang vergessen.
2. **Dauerhaft angesteckt = mitverschlüsselt.** Ein angeschlossenes USB-Laufwerk ist für Ransomware ein normales Laufwerk und wird im selben Durchgang verschlüsselt.
3. **Verlust und Diebstahl.** Kleine Datenträger gehen verloren, werden gestohlen oder im Auto vergessen. Bei personenbezogenen Daten ist das eine meldepflichtige Datenpanne nach Art. 33 DSGVO, wenn das Medium nicht verschlüsselt war.
4. **Schadsoftware-Einfallstor.** USB-Anschlüsse sind ein bekannter Infektionsweg. Unternehmen sollten USB-Massenspeicher per Geräterichtlinie sperren; Backup-Ausnahmen untergraben diese Sperre.
5. **Unzuverlässige Hardware.** Billige Sticks und externe Platten fallen ohne Vorwarnung aus, Flash-Speicher verliert stromlos über Jahre Daten. Eine Überwachung des Zustands findet praktisch nie statt.
6. **Keine Nachweisbarkeit.** Ob und wann gesichert wurde, ist bei USB selten protokolliert. Für Art. 32 DSGVO und die Rechenschaftspflicht fehlt damit der Beleg.

Ersatz für die Offline-Kopie (mindestens eine Variante ist Pflicht):

Variante	Geeignet für	Wie sie schützt
Cloud-Objektspeicher mit Object Lock (Immutable), EU-Rechenzentrum	Privat und Unternehmen	Daten sind für eine festgelegte Frist nicht löschbar, auch nicht mit Admin-Zugang
Pull-Backup: zweites NAS holt sich die Daten, Quelle hat keinen Schreibzugriff	Kleine Büros, ambitionierte Privatanwender	Kompromittierte PCs erreichen das Ziel nicht
Unveränderliche Snapshots auf dem NAS (z. B. WORM/Immutable Snapshots)	Privat und Unternehmen, als zusätzliche Schicht	Snapshots sind für die Sperrfrist nicht löschbar
LTO-Band oder RDX-Wechselmedien, ausgelagert	Unternehmen mit größeren Datenmengen	Physisch getrennt (Air Gap), lange haltbar

RDX-Kartuschen und LTO-Laufwerke werden teils über USB angeschlossen. Entscheidend ist hier nicht die Schnittstelle, sondern das Verfahren: Backup-Software mit Protokoll, Medienrotation und Auslagerung. Ob diese Ausnahme zulässig ist, legt das Unternehmen im Konzept ausdrücklich fest.

Konzept für Privatpersonen

Ziel: Fotos, Dokumente und Zugangsdaten überstehen Geräteausfall, Diebstahl, Wohnungsbrand und Ransomware – ohne dass jemand an Sicherungen denken muss.

Was gesichert wird (nach Priorität):

1. Passwortmanager-Tresor und Wiederherstellungscodes (2FA-Codes)
2. Fotos und Videos
3. Dokumente: Verträge, Steuer, Versicherungen, Zeugnisse
4. Handy-Daten (Kontakte, Chats)
5. Programme und Betriebssystem nur, wenn eine Neuinstallation unzumutbar wäre

Stufe A – Grundschutz (geringer Aufwand):

Kopie	Umsetzung	Häufigkeit
1. Original	PC/Laptop, Smartphone	–
2. Cloud-Backup mit Versionierung	Backup-Dienst mit clientseitiger Verschlüsselung und EU-Speicherort, alternativ Cloud-Speicher mit Versionsverlauf ≥ 30 Tage	automatisch, täglich
3. Zweite, unabhängige Cloud-Kopie	anderer Anbieter, mit Object Lock oder Papierkorb-Sperre; für Smartphones das Geräte-Backup des Herstellers	automatisch, wöchentlich

Stufe B – Erweiterter Schutz (Familie, viele Fotos, Homeoffice):

Kopie	Umsetzung	Häufigkeit
1. Original	PC/Laptop, Smartphone	–
2. Lokales Backup	NAS im Heimnetz mit RAID 1 und unveränderlichen Snapshots; PCs sichern per Backup-Software mit eigenem Backup-Benutzer	automatisch, täglich
3. Offsite + unveränderlich	NAS repliziert verschlüsselt in einen Cloud-Objektspeicher mit Object Lock (z. B. 30 Tage Sperrfrist)	automatisch, täglich

Regeln für den Alltag:

- Das normale Benutzerkonto hat keine Admin-Rechte und keinen Schreibzugriff auf das Backup-Ziel.
- Zugang zu Cloud-Konten nur mit Zwei-Faktor-Anmeldung.
- Verschlüsselungsschlüssel und Notfallzugang ausdrucken und an einem zweiten Ort hinterlegen (z. B. bei Angehörigen oder im Bankschließfach).
- Eine Vertrauensperson weiß, wo die Backups liegen (digitaler Nachlass).

- Einmal im Quartal einen Ordner testweise wiederherstellen, einmal im Jahr ein komplettes Gerät.

Konzept für Unternehmen (KMU)

Ziel: Der Betrieb läuft nach Hardwareausfall, Fehlbedienung oder Cyberangriff innerhalb der festgelegten RTO wieder, mit höchstens RPO an Datenverlust. Die Sicherung ist nach Art. 32 DSGVO dokumentiert und nachweisbar.

Schritt 1 – Bestandsaufnahme

- Alle Datenquellen erfassen: Server, Arbeitsplätze, NAS, Branchensoftware, Datenbanken, Website, E-Mail.
- Cloud-Dienste ausdrücklich mitzählen: Microsoft 365, Google Workspace, CRM, Buchhaltung. Der Anbieter sichert seine Infrastruktur, nicht zwingend Ihre Daten gegen Löschung durch eigene Nutzer oder Angreifer.
- Je Quelle RPO und RTO mit der Geschäftsleitung festlegen und unterschreiben lassen.

Schritt 2 – Architektur nach Unternehmensgröße

Ebene	Kleinstbetrieb (1–10 MA)	KMU (10–250 MA)
Ebene 1: Lokales Backup (schnelle Wiederherstellung)	NAS mit unveränderlichen Snapshots, eigene Backup-Zugangsdaten	Dedizierter Backup-Server oder gehärtetes Linux-Repository, nicht in der Windows-Domäne
Ebene 2: Offsite-Kopie	Verschlüsselte Replikation in EU-Cloud	Replikation an zweiten Standort oder in EU-Cloud
Ebene 3: Unveränderlich / Air Gap	Object Lock beim Cloud-Ziel, Sperrfrist ≥ 30 Tage	Object Lock und/oder LTO-Band mit Auslagerung; Sperrfrist ≥ 30 Tage
SaaS-Daten	Backup für Microsoft 365 / Google Workspace	Dto., zusätzlich CRM und Fachanwendungen
Website	Tägliches Hoster-Backup + eigene externe Kopie	Dto., inkl. Datenbank, Restore-Test pro Quartal

Schritt 3 – Sicherungsplan (Richtwerte)

Datenart	Häufigkeit	Aufbewahrung
Datenbanken, Buchhaltung, Warenwirtschaft	stündlich bis täglich (inkrementell)	30 Tage täglich, 12 Monate monatlich
Dateiablage	täglich, zusätzlich Snapshots alle 1–4 Stunden	30 Tage täglich, 12 Monate monatlich

Datenart	Häufigkeit	Aufbewahrung
Komplettabbild der Server	wöchentlich	4–8 Wochen
E-Mail und SaaS	täglich	12 Monate oder nach Archivierungsregel
Jahresabschluss-Stand	jährlich	nach steuerlicher Aufbewahrungsfrist (Archivierung, kein Backup-Ersatz)

Schritt 4 – Absicherung des Backup-Systems

- Backup-Konsole nur mit Zwei-Faktor-Anmeldung und eigenen Admin-Konten („Vier-Augen“ für Löschungen, sofern die Software das bietet).
- Backup-Netz vom Büronetz trennen (eigenes VLAN, Firewall-Regeln nur für nötige Ports).
- Updates für Backup-Software und NAS-Firmware zeitnah einspielen.
- Alarmierung bei fehlgeschlagenen Jobs per E-Mail an mindestens zwei Personen.
- USB-Massenspeicher per Geräterichtlinie (GPO/Intune) sperren.

Schritt 5 – Verantwortung

- Benannte Backup-Verantwortliche Person plus Vertretung.
- Dienstleister vertraglich einbinden: Leistungsumfang, Reaktionszeiten, Auftragsverarbeitungsvertrag (Art. 28 DSGVO).

Wiederherstellungstests und Notfallplan

Die „0“ der Regel ist die Stelle, an der die meisten Konzepte scheitern: Gesichert wird jahrelang, getestet wird erst im Ernstfall.

Test	Privat	Unternehmen	Nachweis
Einzelne Datei/Ordner wiederherstellen	vierteljährlich	monatlich	Testprotokoll
Komplettes Gerät / Server wiederherstellen	jährlich	halbjährlich, auf Ersatzhardware oder VM	Protokoll mit gemessener Dauer (vs. RTO)
Wiederherstellung aus der unveränderlichen Kopie	jährlich	jährlich	Protokoll
Notfallübung „Ransomware“ (alles lokal weg)	–	jährlich	Übungsbericht mit Maßnahmen

Notfallhandbuch (Unternehmen, ausgedruckt und offline verfügbar):

1. Meldeweg und Telefonliste: Geschäftsleitung, IT-Dienstleister, Datenschutzbeauftragter, Versicherung.
2. Erste Maßnahmen bei Verdacht auf Angriff: Netz trennen, Backup-Jobs anhalten, nichts löschen.
3. Reihenfolge der Wiederherstellung nach Geschäftskritikalität.
4. Zugangsdaten zur Backup-Umgebung und Verschlüsselungsschlüssel (versiegelt, Tresor).

5. Prüfung vor dem Restore: Ist der Wiederherstellungspunkt sauber, also vor Beginn des Angriffs?
6. Meldung an die Aufsichtsbehörde binnen 72 Stunden prüfen (Art. 33 DSGVO).

Datenschutz und rechtliche Pflichten (Unternehmen)

Die Datensicherung ist eine technische und organisatorische Maßnahme im Sinne von Art. 32 Abs. 1 lit. b und c DSGVO: Verfügbarkeit und rasche Wiederherstellung nach einem Zwischenfall.

- **Dokumentation:** Das Backup-Konzept gehört in die TOM-Dokumentation und wird im Verzeichnis der Verarbeitungstätigkeiten referenziert.
- **Auftragsverarbeitung:** Für Cloud-Backup-Anbieter und IT-Dienstleister ist ein AV-Vertrag nötig. Speicherort bevorzugt EU/EWR; bei Drittlandbezug Rechtsgrundlage für die Übermittlung prüfen.
- **Löschkonzept:** Personenbezogene Daten in Backups lassen sich meist nicht einzeln löschen. Üblich und vertretbar: Aufbewahrungsfristen der Backups begrenzen, Zugriff einschränken und nach einem Restore bereits gelöschte Daten erneut löschen. Das wird im Löschkonzept beschrieben.
- **Archiv ≠ Backup:** Steuerliche Aufbewahrungspflichten (GoBD) erfüllt ein revisionssicheres Archiv, nicht das Backup.
- **Verschlüsselung:** Verschlüsselte Backups senken das Risiko bei Verlust; ob eine Datenpanne dann noch meldepflichtig ist, hängt vom Einzelfall ab.
- **NIS2:** Unternehmen, die unter das NIS2-Umsetzungsgesetz fallen, müssen Backup-Management und Notfallwiederherstellung zusätzlich als Risikomanagementmaßnahme nachweisen.

Diese Hinweise ersetzen keine Rechtsberatung im Einzelfall.

Checkliste

- ☐ Alle Datenquellen inkl. Cloud-Dienste und Website erfasst
- ☐ RPO und RTO je Datenquelle festgelegt
- ☐ Drei Kopien auf zwei Systemen, eine davon an einem anderen Ort
- ☐ Mindestens eine Kopie unveränderlich (Object Lock) oder getrennt (Pull, Band)
- ☐ Keine USB-Datenträger als Backup-Medium; alte USB-Backups überführt und sicher gelöscht
- ☐ USB-Massenspeicher per Richtlinie gesperrt (Unternehmen)
- ☐ Versionierung ≥ 30 Tage aktiv
- ☐ Backups clientseitig verschlüsselt, Schlüssel getrennt hinterlegt
- ☐ Backup-Zugang mit eigenen Zugangsdaten und Zwei-Faktor-Anmeldung
- ☐ Alarmierung bei fehlgeschlagenen Sicherungen eingerichtet
- ☐ Restore-Test durchgeführt und protokolliert
- ☐ Notfallhandbuch ausgedruckt und offline verfügbar
- ☐ AV-Verträge mit Backup-Anbietern abgeschlossen
- ☐ Backup in TOM-Dokumentation und Löschkonzept aufgenommen
- ☐ Nächster Überprüfungstermin des Konzepts festgelegt (mindestens jährlich)

Weiterführende Quellen

- BSI IT-Grundschutz-Kompendium, Baustein CON.3 „Datensicherungskonzept“, und BSI-Maßnahmenkatalog Ransomware (Hinweis u. a. bei Identeco)
- 3-2-1-1-0-Regel – FAST LTA Glossar
- 3-2-1-1-Regel für Privatanwender – ESET
- Offline vs. Online Backup – Hagel IT