hostspezial

HS-AUDIT-BCK-02
REV. 2.0 · MAI 2026
PUBLIC · DE

BACKUP-AUDIT · KMU-TOOLKIT

Trägt Ihr Backup im Ernstfall?

14 Prüfpunkte aus 15 Jahren Praxis bei oberfränkischen Mittelständlern. Drucken, abhaken, auswerten — ohne E-Mail-Gate, ohne Tracking-Pixel.

14
PRÜFPUNKTE

5
THEMENBLÖCKE

~30 min
BEARBEITUNGSZEIT

INHALT · ÜBERSICHT

Was Sie in den nächsten 30 Minuten klären können.

So nutzen Sie diese Checkliste: Lesen Sie jeden Punkt durch. Wenn Sie spontan mit „Ja, dokumentiert und getestet" antworten können, kreuzen Sie an. Bei jedem „Hmm..." oder „muss ich nachschauen" lassen Sie das Feld leer — das ist ein offener Befund. Am Ende zählen Sie. Externe Validierung ist kostenlos auf Anfrage.

KAPITEL 01 · 3 PRÜFPUNKTE · STRATEGISCHE EBENE

Strategie & Konzept 01

Ohne dokumentierte Strategie operieren Sie blind. Erst beim Restore merken Sie, ob Sie das Richtige gesichert haben — diese drei Grundsatz-Punkte klären, ob das Konzept überhaupt funktionieren kann.

---

01 3-2-1-Regel umgesetzt

3 Datenkopien (Original + 2 Backups), auf **2 unterschiedlichen Medien**, **1 davon räumlich getrennt** (Off-Site). Mindeststandard — darunter ist es kein verlässliches Backup.

> NOTIZ Reine Cloud-Synchronisation (OneDrive, Dropbox) ist **kein Backup** — versehentliches Löschen wird in Minuten in die Cloud propagiert.

PRIORITÄT
Critical

AUFWAND
Low

☐ ERFÜLLT

---

02 RPO und RTO schriftlich definiert

Recovery Point Objective (max. zulässiger Datenverlust) und **Recovery Time Objective** (max. Wiederanlaufzeit) sind pro System dokumentiert und vom Management abgenommen.

> BEISPIEL „Buchhaltung darf max. 4 h Daten verlieren und muss in 8 h wieder laufen." Wer das nicht schreibt, kann nicht messen.

PRIORITÄT
High

AUFWAND
Medium

☐ ERFÜLLT

---

03 Air-Gap gegen Ransomware

Mindestens eine Backup-Kopie ist **aktiv vom Produktivnetz getrennt** — per Tape, Immutable Storage oder separatem Tenant. Ransomware kann diese Kopie technisch nicht erreichen.

> HÄUFIGER BEFUND NAS im selben Netz, Domain-Admin hat Schreibzugriff. Eine kompromittierte Domain reicht — Backup ist weg.

PRIORITÄT
Critical

AUFWAND
Medium

☐ ERFÜLLT

KAPITEL 02 · 4 PRÜFPUNKTE · TECHNISCHE EBENE

Technische Umsetzung 02

Konzept passt — jetzt geht es an die Stellschrauben, die im Ernstfall den Unterschied zwischen Wiederanlauf und Tagen Stillstand machen.

04 Verschlüsselung der Backup-Daten

Alle Backups sind **at-rest und in-transit verschlüsselt**. Schlüssel-Management ist dokumentiert; der Admin-Schlüssel liegt nicht ausschließlich auf demselben System.

PRIORITÄT
High

AUFWAND
Low

☐ ERFÜLLT

05 Off-Site-Lokation georedundant

Off-Site-Kopie liegt in einem **anderen Brandabschnitt oder Rechenzentrum** (mind. 5 km Entfernung). Lokaler Brand-, Wasser- oder Stromschaden vernichtet nicht beide Kopien.

> STANDARD Off-Site-Backup ins Lichtenfelser RZ kostet typisch **3–8 €/AP/Monat** — günstiger als die Wiederherstellung nach einem Brand.

PRIORITÄT
Critical

AUFWAND
Medium

☐ ERFÜLLT

06 Backup-Software aktuell und supportet

Eingesetzte Backup-Lösung (Veeam, Proxmox Backup, Acronis, Synology Active Backup) ist auf **aktueller Major-Version** mit aktivem Hersteller-Support.

PRIORITÄT
High

AUFWAND
Low

☐ ERFÜLLT

07 Microsoft 365 wird aktiv gesichert

Microsoft sichert M365-Daten **nicht** gegen versehentliches Löschen oder Ransomware. Eine separate Backup-Lösung für Exchange, OneDrive, SharePoint, Teams ist im Einsatz.

> VERGESSEN SIE NICHT Microsoft hält Mails 14 Tage in der „Wiederherstellbar"-Mailbox. Danach unwiderruflich weg.

PRIORITÄT
Critical

AUFWAND
Low

☐ ERFÜLLT

KAPITEL 03 · 3 PRÜFPUNKTE · VERIFIKATION

Test & Nachweis 03

Ein nicht getestetes Backup ist Schrödingers Backup: gleichzeitig vorhanden und nicht vorhanden, bis Sie es im Ernstfall öffnen. Der einzige verlässliche Beweis ist ein dokumentierter Restore.

08 Restore-Test in den letzten 90 Tagen

Dokumentierter, vollständiger Restore (mindestens VM, Datenbank, einzelne Datei) wurde in den letzten 90 Tagen erfolgreich durchgeführt. Niemand hat „nur" auf den Erfolg-Status der Backup-Software vertraut.

> **AUS DER PRAXIS** In über **60 %** unserer Erstanalysen scheitert der erste echte Restore-Test: falsches Boot-Medium, fehlende Treiber, abgelaufene Lizenzen.

PRIORITÄT
Critical

AUFWAND
Low

☐ ERFÜLLT

09 Test-Protokoll mit Zeitmessung

Restore-Zeit wurde gemessen und passt zum vereinbarten **RTO**. Ergebnis ist schriftlich dokumentiert und vom Management gegengezeichnet.

PRIORITÄT
High

AUFWAND
Low

☐ ERFÜLLT

10 Bare-Metal-Restore-Fähigkeit getestet

Im Notfall kann ein **komplettes System auf neuer Hardware** wiederhergestellt werden. Voraussetzungen (Boot-Medium, Treiber, Lizenzen) liegen griffbereit — nicht im verschlüsselten Server selbst.

PRIORITÄT
Critical

AUFWAND
Medium

☐ ERFÜLLT

KAPITEL 04 · 4 PRÜFPUNKTE · ORGANISATION

Organisation & Compliance 04

Technik ist die halbe Miete. Die andere Hälfte sind klare Verantwortlichkeiten und Compliance-Anforderungen Ihrer Branche.

11 Aufbewahrungs-Konzept GoBD-konform

Steuerlich relevante Daten werden **10 Jahre revisionssicher** aufbewahrt. Aufbewahrungs-Strategie unterscheidet zwischen Backup (operativ) und Archiv (langfristig).

PRIORITÄT
High

AUFWAND
Low

☐ ERFÜLLT

12 Verantwortlichkeiten dokumentiert

Wer prüft täglich oder wöchentlich den Backup-Status? Wer wird im Fehlerfall alarmiert? Vertretungsregelung im Urlaub und bei Krankheit? **Schriftlich** — nicht im Kopf eines Admins.

PRIORITÄT
High

AUFWAND
Very Low

☐ ERFÜLLT

13 Notfall-Plan inkl. Wiederanlauf-Reihenfolge

Bei Totalausfall: Welche Systeme werden in welcher Reihenfolge wiederhergestellt? Wer informiert Mitarbeiter, Kunden, Behörden? Schriftlich, nicht im Kopf eines Admins, der gerade im Urlaub ist.

PRIORITÄT
Critical

AUFWAND
Medium

☐ ERFÜLLT

14 Branchen-Compliance abgedeckt

Spezifische Anforderungen Ihrer Branche sind erfüllt: **HACCP** (Lebensmittel), **GAMP 5** (Pharma), **VAIT** (Versicherung), **TISAX** (Automotive), **NIS2** (kritische Infrastruktur), **DORA** (Finanzdienstleister).

PRIORITÄT
Critical

AUFWAND
High

☐ ERFÜLLT

KAPITEL 05 · AUSWERTUNG

So bewerten Sie Ihr Ergebnis

Zählen Sie, wie viele der 14 Punkte Sie klar mit „Ja" beantworten können. Überall wo Sie zögern oder „weiß ich nicht" denken, haben Sie eine offene Lücke.

14 / 14	**Top-Aufstellung** Jährlicher Review reicht aus. Ihre Backup-Strategie ist solide.	SOLID
10–13	**Punktuelle Lücken** Konkrete Maßnahmen-Liste sinnvoll, aber kein Notfall.	STABLE
5–9	**Substantielle Risiken** Backup-Strategie sollte zeitnah überarbeitet werden.	AT-RISK
< 5	**Akut** Externe Beratung dringend empfohlen, bevor der nächste Vorfall passiert.	CRITICAL

Drei nächste Schritte

Wenn die Selbst-Auswertung Lücken aufgedeckt hat, sind drei Schritte sinnvoll — in dieser Reihenfolge:

Schritt 01

Restore-Test einplanen

Nicht später als „in den nächsten 30 Tagen". Wählen Sie ein nicht-kritisches System und testen Sie den Wiederherstellungs-Weg inkl. Zeitmessung.

Schritt 02

Off-Site-Lücken schließen

Wenn alle Kopien im selben Gebäude liegen, ist eine Off-Site-Kopie der nächste Schritt. Cloud-Object-Storage oder zweiter Standort.

Schritt 03

Verantwortlichkeiten festhalten

30 Minuten reichen, um zu klären, wer was prüft. Die billigste Maßnahme mit dem höchsten Hebel.

SCHNUPPER-ANGEBOT · OHNE VERPFLICHTUNG

Halber Tag Senior-Consultant Vor-Ort-Inventur

Wir kommen vorbei, schauen Server, Backup, Switches und Doku an, liefern eine schriftliche Bewertung mit Risiko-Score und drei priorisierten Handlungsempfehlungen. Kein Verkauf, keine Verpflichtung.

WAS SIE NACH DEM TERMIN ERHALTEN

Ausgefüllte Audit-Checkliste · Risiko-Score 0–14 · Drei priorisierte Maßnahmen mit Aufwand-Schätzung · Optional: Angebot zur Umsetzung — komplett unverbindlich.

TELEFON
+49 9571 87314-9

E-MAIL
info@hostspezial.de

WEB
hostspezial.de