1.

Die 10 größten Backup-Fehler -

und wie du sie sofort vermeidest

Wie du in 5 Minuten erkennst, ob dein Backup-System im Ernstfall standhält.

mv it GmbH - Erkrather Straße 401, 40231 Düsseldorf - 0211 879 774-0 - www.mv-it.cloud - info@mv-it.cloud

Einleitung

Datenverlust gehört zu den teuersten IT-Risiken überhaupt – und trotzdem verlassen sich viele Unternehmen auf Sicherungssysteme, die im Ernstfall versagen.
Ein einziger Hardwarefehler, ein Cyberangriff oder ein versehentlich gelöschter Ordner kann reichen, um den Betrieb für Tage lahmzulegen.
Dieses kompakte Dokument hilft dir, **dein Backup-System in nur 5 Minuten zu überprüfen.**
Finde heraus, welche typischen Fehler auch in deinem Unternehmen lauern – und wie du sie **jetzt sofort ausschaltest.**

Warum dieser Self-Check wichtig ist

Viele IT-Verantwortliche wiegen sich in Sicherheit, weil täglich Backups laufen – aber kaum jemand überprüft, ob die Wiederherstellung tatsächlich funktioniert.
Erst im Ernstfall zeigt sich, ob das Backup-System wirklich hält, was es verspricht.
Mit diesem Self-Check erkennst du:

- welche Schwachstellen du übersehen könntest
- wie hoch dein aktuelles Risiko ist
- und welche 1-2 Maßnahmen du sofort umsetzen kannst, um sicherer zu werden.

👉 **Mach jetzt den Self-Check auf der nächsten Seite und finde heraus, wie sicher dein Backup wirklich ist.**

2.

Die 10 + 2 größten Backup-Fehler - dein 5-Minuten-Self-Check

So funktioniert's

Lies jeden Punkt und hake an, ob er in deinem Unternehmen zutrifft.

Am Ende zählst du deine Häkchen – dann siehst du sofort, wie sicher dein Backup wirklich ist.

Backup-Self-Check

Nr.	Typische Fehler	Trifft zu? Ja/Nein	Risiko / Auswirkung
1	Backups werden nie getestet	□ Ja / □ Nein	Keine Garantie, dass sie im Notfall funktionieren
2	Keine Offsite- oder Cloud-Kopie vorhanden	□ Ja / □ Nein	Totalverlust bei Brand, Diebstahl oder Ransomware
3	Backup liegt auf derselben Maschine wie das Produktivsystem	□ Ja / □ Nein	Kein Schutz bei Hardware- oder Systemausfall
4	Keine Versionierung aktiviert (ältere Stände überschrieben)	□ Ja / □ Nein	Kein Zugriff auf frühere, saubere Datenbestände

Nr.	Typische Fehler	Trifft zu? Ja/Nein	Risiko / Auswirkung
5	Kein Monitoring oder Altering aktiv	□ Ja / □ Nein	Fehler bleiben unbemerkt, bis es zu spät ist
6	Backup-Zeitfenster kollidiert mit Produktivsystem	□ Ja / □ Nein	Performance-Verlust und unvollständige Sicherungen
7	Backups sind unverschlüsselt	□ Ja / □ Nein	Datenschutzverletzung, DSGVO-Risiko
8	Kein Cloud-Backup vorhanden	□ Ja / □ Nein	Kein Schutz bei Standortausfall
9	Keine regelmäßige Validierung durch Dritte	□ Ja / □ Nein	Falsche Sicherheit durch ungetestete Systeme
10	Kein dokumentierter Notfallplan	□ Ja / □ Nein	Unklare Zuständigkeiten im Ernstfall, Zeitverlust
11	Keine Abstimmung mit Cyber-Versicherung oder externen Audit-Anforderungen	□ Ja / □ Nein	Versicherungsschutz kann Schadensfall entfallen
12	Keine Offline-/Cold-Storage-Sicherung außerhalb des Netzwerks	□ Ja / □ Nein	Ransomware kann alle Online-Backups verschlüsseln

Auswertung

Zähle deine “Ja”-Antworten:

0-3 Häkchen:

Dein Backup-System ist solide - sehr gut!

4-8 Häkchen:

Du hast erkennbare Lücken - Handlungsbedarf vorhanden.

9-12 Häkchen:

Kritischer Zustand - dein Backup ist akut gefährdet.

Tipp

Selbst moderne Backup-Lösungen scheitern nicht an der Technik, sondern daran, dass sie nie getestet werden oder nicht den Vorgaben der Cyber-Versicherung entsprechen.
Mach diesen Check mindestens einmal pro Quartal – am besten gemeinsam mit einem externen IT-Partner oder Auditor.

3.

Was du aus den Ergebnisse ableiten kannst

Jedes Kreuz in deinem Self-Check zeigt eine mögliche Schwachstelle in deiner Datensicherung.

Die gute Nachricht: Die meisten dieser Risiken lassen sich mit klaren Prozessen und moderner Cloud-Technologie schnell beheben.

Hier sind die drei wichtigsten Stellschrauben, mit denen du dein Backup-System zukunftssicher machst:

1. Organisatorische Sicherheit

- **Verantwortung klären:** Lege fest, wer für Backups zuständig ist und wann sie überprüft werden.
- **Tests einplanen:** Führe regelmäßige Wiederherstellungstests durch - nicht nur Backup-Logs prüfen, sondern wirklich Daten zurückspielen.
- **Dokumentation:** Halte Abläufe und Zuständigkeiten schriftlich fest. Im Ernstfall zählt jede Minute.
- **Erinnerungssystem:** Plane wiederkehrende Erinnerungen, damit Prüfungen nicht vergessen werden.

2. Technische Absicherung

- **Cloud-Backups mit Geo-Redundanz:** Sichere Daten an mindestens zwei physisch getrennten Standorten, idealerweise in zertifizierten Rechenzentren
- **Monitoring aktivieren:** Nutze Systeme, die dich automatisch benachrichtigen, wenn ein Backup fehlschlägt.
- **Verschlüsselung:** Alle Sicherungen sollten Ende-zu-Ende verschlüsselt sein - das schützt vor Datenlecks und erfüllt DSGVO-Anforderungen.
- **Automatisierung:** Reduziere manuelle Eingriffe - so minimierst du Fhler und sparst Zeit.

3. Strategische Planung

- **Disaster-Recovery-Strategie (DR):** Lege fest, wie schnell du nach einem Ausfall wieder arbeitsfähig sein musst (RTO/RPO).
- **Notfallplan:** Erstelle eine klare Schritt-für-Schritt-Anleitung, wie Systeme im Ernstfall wiederhergestellt werden.
- **Externe Validierung:** Lass dein Backup regelmäßig von einem neutralen IT-Partner prüfen, um blinde Flecken zu vermeiden.
- **Skalierbarkeit:** Plane jetzt schon für dein Wachstum - steigende Datenmengen sollten keine neuen Risiken schaffen.

Die meisten Backups schreitern nicht an der Technik - sondern daran, dass niemand prüft, ob sie wirklich funktionieren.

Ein funktionierendes Backup-System ist kein einmaliges Projekt, sondern ein fortlaufender Prozess aus **Testen, Überwachen und Optimieren.**

mv itgmbh

4.

Dein nächster Schritt

Fazit

Wenn du in deinem Self-Check mehr als drei Häkchen gesetzt hast, solltest du dein Backup-System genauer prüfen.

Selbst kleine IT-Ausfälle können in wenigen Stunden **vier- bis fünfstellige Schäden** verursachen – durch Stillstand, Datenverlust oder Betriebsunterbrechungen.

Die meisten Unternehmen merken erst **im Ernstfall**, dass ihr Backup nicht funktioniert.

Doch genau das kannst du mit wenigen einfachen Schritten verhindern.

📅 *Jetzt kostenlosen Backup-Check anfragen*

👉 Hier Termin buchen

(oder direkt per E-Mail an info@mv-it.cloud – Betreff: „Backup-Check“)

Was du jetzt tun kannst

Wir bieten dir einen **kostenlosen 15-Minuten-Backup-Check** an.
Dabei prüfen wir gemeinsam, ob dein aktuelles Sicherungssystem im Ernstfall wirklich hält, was es verspricht.
Du erhältst:

- ✅ Eine **klare technische Einschätzung** deines aktuellen Backup-Status
- ⚙️ Eine **kurze Risikoanalyse** zu Datenverlust, Wiederherstellungszeit und Ransomware-Schutz
- 🚀 **Konkrete Handlungsempfehlungen**, um dein System sofort abzusichern

Ohne Verkaufsgespräch. Ohne Verpflichtung.
Einfach ein ehrlicher, professioneller Blick auf dein System – damit du ruhig schlafen kannst.

Warum dieser Check sinnvoll ist

- Du siehst innerhalb von Minuten, ob deine Datensicherung wirklich funktioniert.
- Du erfährst, welche kleinen Änderungen deine Systemsicherheit massiv erhöhen.
- Du bekommst Klarheit, statt dich auf Hoffnung zu verlassen.

mv it GmbH - Erkrather Straße 401, 40231 Düsseldorf - 0211 879 774-0 - www.mv-it.cloud - info@mv-it.cloud

Abschlussnote

Dieses Dokument wurde erstellt, um Unternehmen dabei zu helfen, Risiken in der Datensicherung schnell zu erkennen und gezielt zu beseitigen.

© mv it GmbH – Ihr Partner für Cloud-Backup, Sicherheit und IT-Services.
Erkrather Straße 401, 40231 Düsseldorf | +49 (0) 211 879 774-0 | info@mv-it.cloud | mv-it.cloud