CHECKLISTE · 32 PRÜFPUNKTE

ITS AG

Backup-Strategie-Checkliste für den Mittelstand

32 Prüfpunkte, mit denen Sie Ihre aktuelle Backup-Strategie ehrlich gegen die Ransomware-Realität abklopfen – bevor es ein Angreifer für Sie tut.

Lesezeit	Format	Stand
20 Minuten	**Selbst-Audit**	**2026**

Ein Praxis-Leitfaden der ITS AG, Goldbach · Frankfurt · Darmstadt. Für IT-Verantwortliche in kleinen und mittelständischen Unternehmen.

WARUM DIESES DOKUMENT

01 Ein „grüner“ Backup-Job ist kein Wiederherstellungsversprechen

Fast jedes Unternehmen sichert seine Daten. Aber sichern und im Ernstfall wiederherstellen sind zwei verschiedene Dinge – und genau diese Lücke nutzen Angreifer aus. Moderne Ransomware verschlüsselt heute nicht nur Ihre Produktivsysteme, sie sucht gezielt nach Ihren Backups und löscht sie zuerst.

~80%
der angezeigten Ransomware-Angriffe richteten sich gegen kleine und mittlere Unternehmen.

89%
der Organisationen hatten bei einem Angriff ihre Backup-Speicher als Ziel.

34%
der Backup-Speicher wurden im Schnitt verändert oder gelöscht.

Die gefährliche Wahrnehmungslücke: Im Durchschnitt erfüllen mittelständische Unternehmen nur rund **56 %** der grundlegenden Sicherheitsanforderungen – während sich **91 %** selbst als „gut geschützt“ einschätzen. Diese Checkliste schließt die Lücke zwischen Gefühl und Faktenlage.

Die folgenden 32 Prüfpunkte sind so formuliert, dass Sie sie ehrlich mit *Ja* oder *Nein* beantworten können. Jedes „Nein“ ist kein Vorwurf, sondern eine konkrete To-do-Position. Nehmen Sie sich 20 Minuten und gehen Sie die Liste mit dem aktuellen Stand Ihrer Infrastruktur durch – nicht mit dem Soll-Zustand aus der Dokumentation.

ANLEITUNG

02 So nutzen Sie die Checkliste

Die drei Begriffe, die alles bestimmen

RPO (Recovery Point Objective): Wie viele Daten dürfen maximal verloren gehen? Bestimmt Ihr *Backup-Intervall*.

RTO (Recovery Time Objective): Wie lange darf der Wiederanlauf maximal dauern? Bestimmt Ihre *Wiederherstellungs-Architektur*.

3-2-1-1-0: 3 Kopien · 2 Medientypen · 1 außer Haus · 1 unveränderbar/offline · 0 Fehler im verifizierten Restore-Test.

Bewertung in fünf Blöcken

Die Prüfpunkte sind in fünf Themenblöcke gegliedert. Haken Sie jeden erfüllten Punkt ab und zählen Sie am Ende.

26–32 JA	Solide Basis – Feinschliff genügt.
16–25 JA	Spürbare Lücken – Handlungsbedarf.
0–15 JA	Kritisch – kein verlässlicher Schutz.

Wichtig vorab

Snapshots und Cloud-Synchronisation (z. B. OneDrive, Dropbox) sind **kein** Backup. Snapshots liegen meist auf demselben System; eine Synchronisation verteilt eine Verschlüsselung in Echtzeit auf alle Kopien. Behandeln Sie beides nicht als Sicherung.

DIE 32 PRÜFPUNKTE

03 Strategie & Verantwortung

A Grundlagen klären

1 Ist für jedes wichtige System ein RPO definiert (maximal tolerierbarer Datenverlust)? ☐

Ohne RPO ist jedes Backup-Intervall reine Annahme. ERP/Buchhaltung brauchen oft 1–4 h, eine Dokumentenablage verträgt 24 h.

2 Ist für jedes wichtige System ein RTO definiert (maximal tolerierbare Ausfallzeit)? ☐

Der RTO entscheidet über die Architektur: Eine Stunde Wiederanlauf erfordert eine ganz andere Lösung als ein Tag.

3 Wissen Sie, welche Systeme geschäftskritisch sind und in welcher Reihenfolge sie wieder laufen müssen? ☐

Eine kurze Business-Impact-Betrachtung verhindert, dass im Ernstfall an der falschen Stelle begonnen wird.

4 Gibt es eine benannte, namentlich verantwortliche Person für das Backup? ☐

„Alle“ verantwortlich heißt im Zweifel „niemand“. Vertretung inklusive.

5 Sind gesetzliche Aufbewahrungsfristen (HGB, GoBD) in der Aufbewahrungsdauer abgebildet? ☐

Handelsbücher und steuerrelevante Daten müssen revisionssicher und über Jahre verfügbar bleiben – nicht nur 14 Tage.

6 Hat die Geschäftsführung die definierten RPO/RTO-Werte freigegeben? ☐

Restrisiko ist eine Geschäftsentscheidung. Die Freigabe schützt die IT und macht Investitionen begründbar.

04 3-2-1-1-0 – die Abdeckung

B Kopien, Medien, Orte

7 **Existieren mindestens drei Kopien Ihrer Daten (Produktion + zwei Sicherungen)?** ☐
Eine einzige Sicherung ist ein Single Point of Failure.

8 **Liegen die Sicherungen auf mindestens zwei verschiedenen Medientypen?** ☐
Gleiche Technik = gleiche Schwachstelle. Z. B. Disk plus Tape oder Disk plus geprüfter Cloud-Speicher.

9 **Liegt mindestens eine Kopie räumlich außer Haus (Offsite)?** ☐
Brand, Wasser, Diebstahl, Beschlagnahme – lokale Ereignisse treffen sonst Original und Sicherung gleichzeitig.

10 **Gibt es eine unveränderbare (immutable) oder vom Netz getrennte (air-gapped) Kopie?** ☐
Das ist die entscheidende Erweiterung gegen Ransomware: eine Kopie, die selbst ein kompromittierter Administrator nicht löschen kann.

11 **Ist die Offsite-/Offline-Kopie wirklich vom Produktivnetz getrennt?** ☐
Eine zweite Kopie am selben Switch und im selben Active Directory ist mitverschlüsselt, bevor Sie es merken.

12 **Beträgt die Aufbewahrung der unveränderbaren Kopie mindestens 14–30 Tage?** ☐
Angreifer bewegen sich oft Wochen unentdeckt im Netz. Eine zu kurze Aufbewahrung sichert nur bereits kompromittierte Stände.

13 **Werden Microsoft-365-/Cloud-Daten (E-Mail, Teams, SharePoint) separat gesichert?** ☐
Microsoft verantwortet die Verfügbarkeit der Plattform – nicht die Wiederherstellung Ihrer gelöschten oder verschlüsselten Inhalte.

14 **Sind auch Endgeräte und mobile Daten erfasst, die nicht zentral abgelegt werden?** ☐
Lokale Projektordner, Notebooks im Außendienst – was nicht erfasst ist, ist nicht gesichert.

05 Ransomware-Härtung

Der Block, der den Unterschied macht

Ein Backup, das ein Angreifer mit erbeuteten Administrator-Rechten löschen kann, ist im Ernstfall wertlos. Die folgenden acht Punkte entscheiden darüber, ob Ihre Sicherung einen gezielten Angriff übersteht.

C Schutz vor gezielter Manipulation

- [ ] **15** Ist das Backup-Administrator-Konto vom normalen Domänen-Admin getrennt?
  Identische Zugangsdaten bedeuten: Wer die Domäne übernimmt, übernimmt auch die Backups.
- [ ] **16** Ist die Anmeldung an der Backup-Konsole durch Mehr-Faktor-Authentifizierung (MFA) geschützt?
  MFA stoppt den Großteil automatisierter Übernahmen kompromittierter Konten.
- [ ] **17** Läuft das Backup in einem eigenen, segmentierten Netzbereich?
  Netztrennung verhindert, dass sich Schadsoftware vom Produktiv- ins Backup-Segment ausbreitet.
- [ ] **18** Sind die Sicherungen verschlüsselt – sowohl bei der Übertragung als auch im Ruhezustand?
  Schützt vor Datenabfluss (Double Extortion) und ist datenschutzrechtlich (DSGVO) geboten.
- [ ] **19** Ist die Unveränderbarkeit technisch erzwungen (Object Lock / WORM / Hardened Repository)?
  Eine Richtlinie auf dem Papier reicht nicht – die Sperre muss auf Speicherebene durchgesetzt sein.
- [ ] **20** Sind Schattenkopien und Snapshots gegen Löschung geschützt?
  Standard-Ransomware löscht zuerst die Volume-Schattenkopien, um eine schnelle Wiederherstellung zu verhindern.
- [ ] **21** Ist die Backup-Software selbst aktuell gepatcht?
  Schwachstellen in Backup-Produkten sind ein beliebtes Einfallstor – im Schnitt erscheinen über 100 neue Schwachstellen pro Tag.
- [ ] **22** Werden Sie alarmiert, wenn Backups fehlschlagen oder verändert werden?
  Eine ungeprüfte rote Meldung über Wochen ist im Ernstfall ein böses Erwachen.

06 Test & Betrieb

D Beweisen statt vermuten

23 **Führen Sie regelmäßig einen echten Wiederherstellungstest durch (nicht nur „Job grün“)?** ☐
Erst die tatsächliche Rückspielung beweist, dass Ihre Daten lesbar und vollständig sind.

24 **Werden diese Restore-Tests dokumentiert (Datum, Umfang, Ergebnis)?** ☐
Nachweise sind im Schadensfall, gegenüber Versicherung und Aufsicht Gold wert.

25 **Haben Sie die tatsächliche Wiederherstellungszeit gemessen und mit Ihrem RTO verglichen?** ☐
Viele entdecken erst im Test, dass die reale Rückspielung um ein Vielfaches länger dauert als geplant.

26 **Wurde eine komplette System-/VM-Wiederherstellung getestet – nicht nur einzelne Dateien?** ☐
Ein zurückgeholtes Word-Dokument beweist nicht, dass Sie einen ausgefallenen Server komplett neu aufbauen können.

27 **Ist die Wiederanlauf-Reihenfolge festgelegt (z. B. Verzeichnisdienst → E-Mail → ERP → Arbeitsplätze)?** ☐
Abhängigkeiten in der falschen Reihenfolge kosten im Ernstfall Stunden.

28 **Können Sie einen „sauberen“ Wiederherstellungspunkt vor Angriffsbeginn identifizieren?** ☐
Maßgeblich ist der Stand vor dem ersten Eindringen – nicht vor der sichtbaren Verschlüsselung.

07 Notfall-Integration

E Vom Backup zum Wiederanlauf-Plan

29 **Ist das Backup Teil eines schriftlichen Notfall-/Wiederanlaufplans?** ☐
Sicherung und Notfallplan gehören zusammen – die beste Kopie nützt nichts ohne Ablauf.

30 **Liegt die Wiederherstellungsanleitung auch offline vor (Papier / getrenntes Medium)?** ☐
Wenn alle Systeme verschlüsselt sind, ist eine Anleitung im verschlüsselten Wiki wertlos.

31 **Sind Kontakt- und Eskalationswege (Dienstleister, Versicherung, Behörden) hinterlegt?** ☐
Im Ernstfall zählt jede Minute – Telefonnummern sucht man nicht erst während der Krise.

32 **Wird die Backup-Strategie mindestens jährlich und nach jeder Infrastrukturänderung überprüft?** ☐
Neue Server, neue Anwendungen, neue Standorte – ungeprüft fällt schnell etwas durchs Raster.

Auswertung

Zählen Sie Ihre „Ja"-Antworten: **26–32** = solide Basis, Feinschliff genügt. **16–25** = spürbare Lücken, vor allem in Block C und D priorisieren. **0–15** = aktuell kein verlässlicher Schutz gegen einen ernsthaften Angriff – hier sollte zeitnah gehandelt werden.

Quellen (Auswahl): BSI, Die Lage der IT-Sicherheit in Deutschland 2025 · Veeam Data Protection / Ransomware Trends Report 2025 · BKA, Bundeslagebild Cybercrime 2025 · Sophos, State of Ransomware 2025 · BSI IT-Grundschutz, Baustein CON.3 (Datensicherungskonzept). Kennzahlen gerundet; Studienjahre beachten.