

CHECKLISTE · BACKUP & RECOVERY

Backup-Strategie: 3-2-1-Regel umsetzen

Schritt für Schritt zu Sicherungen, die auch nach Ransomware, Fehlbedienung oder Hardwareausfall wiederherstellbar sind.

DAS ERHALTEN SIE

- RPO/RTO verständlich erklärt, mit Vorlage
- Speicherziele im Vergleich (lokal, Cloud, unveränderbar)
- Ransomware-sichere Backup-Architektur
- Restore-Testplan und Checkliste

AUF EINEN BLICK

Für	**Geschäftsleitung und IT-Verantwortliche in KMU**
Zeitbedarf	**ca. 1–2 Stunden pro Durchlauf**
Stand	**16. November 2026**
Version	**2.0**

1 Die Regel – und warum sie heute 3-2-1-1-0 heißt

> Eine Sicherung ist erst dann etwas wert, wenn die Wiederherstellung nachweislich funktioniert – rechtzeitig, vollständig und aus einer Kopie, die ein Angreifer nicht erreichen konnte.

Ziffer	Bedeutung	Praxis
3	Drei Kopien der Daten	Produktivdaten + zwei Sicherungen
2	Zwei unterschiedliche Medien/Systeme	z. B. Backup-Speicher (NAS/Backup-Appliance) und Cloud- oder Bandspeicher
1	Eine Kopie außerhalb des Standorts	Rechenzentrum, Cloud-Speicher oder ausgelagerte Medien
1	Eine Kopie offline oder unveränderbar	Unveränderbarer Objektspeicher (Object Lock), gehärtetes Linux-Repository, getrenntes Medium
0	Null Fehler bei der Prüfung	Automatische Prüfung der Sicherungen und regelmäßige Restore-Tests

Warum das wichtig ist

Bei Ransomware-Angriffen werden häufig zuerst die erreichbaren Sicherungen gelöscht oder verschlüsselt. Eine Kopie, die mit denselben Domänen-Zugangsdaten erreichbar ist, schützt deshalb nur gegen Hardwareausfall – nicht gegen Angriffe.

2 Schutzziele festlegen: RPO und RTO

- **RPO (Recovery Point Objective)**: Wie viel Datenverlust ist maximal tragbar? Ein RPO von 4 Stunden bedeutet: mindestens alle 4 Stunden sichern.
- **RTO (Recovery Time Objective)**: Wie lange darf die Wiederherstellung höchstens dauern, bis der Prozess wieder läuft?

RPO und RTO sind **Geschäftsentscheidungen**. Die IT liefert Aufwand und Kosten, die Geschäftsleitung entscheidet über das tragbare Risiko. Die Werte unten sind Beispiele zur Orientierung.

Datenklasse (Beispiel)	RPO	RTO	Sicherungsform
ERP/Warenwirtschaft, Buchhaltung	1–4 h	4–8 h	Image + Datenbank-konsistente Sicherung, mehrmals täglich
Dateiablagen, Projektdaten	24 h	1 Tag	Tägliche Sicherung, Versionierung
E-Mail und Microsoft 365	24 h	1–2 Tage	Separate M365-Sicherung (siehe Hinweis)
Server-Systeme (Domäne, Datei, Anwendungen)	24 h	1 Tag	Image-Sicherung inkl. Systemzustand

Datenklasse (Beispiel)	RPO	RTO	Sicherungsform
Notebooks/Clients	nach Bedarf	1–2 Tage	Daten zentral ablegen, Neuinstallation statt Client-Backup
Konfigurationen (Firewall, Switches, WLAN)	nach jeder Änderung	4 h	Konfigurationsexport, versioniert

Microsoft 365 und SaaS-Dienste

Cloud-Anbieter sichern ihre Plattform gegen Ausfälle, aber gelöschte oder verschlüsselte Inhalte sind nach Ablauf der Aufbewahrungsfristen nicht mehr wiederherstellbar. Prüfen Sie im Rahmen des geteilten Verantwortungsmodells, ob eine separate Sicherung von Exchange Online, SharePoint, OneDrive und Teams nötig ist.

3 Speicherziele im Vergleich

Ziel	Stärken	Grenzen	Rolle in 3-2-1
Lokales NAS / Backup-Appliance	Schnelle Wiederherstellung, planbare Kosten	Gleicher Standort, angreifbar wenn mit Domäne verbunden	Erste Kopie, schnelle Restores
Gehärtetes Linux-Repository	Unveränderbare Sicherungen möglich, lokal schnell	Erfordert sauberen Betrieb und Härtung	Unveränderbare lokale Kopie
Cloud-Objektspeicher mit Object Lock	Außer Haus, unveränderbar für definierte Frist	Restore-Dauer abhängig von Bandbreite; Kosten für Abruf prüfen	Offsite + unveränderbar
Band / Wechselmedien	Echte Offline-Kopie, lange Lagerung	Manueller Prozess, Disziplin nötig	Offline-Kopie
Externe USB-Platte	Günstig, einfach	Nur offline, wenn wirklich getrennt; fehleranfällig	Notlösung für sehr kleine Umgebungen

Ransomware-feste Architektur – Mindestanforderungen

- Backup-Server und Repository **nicht** in die Windows-Domäne aufnehmen; eigene Zugangsdaten mit MFA.
- Mindestens eine Kopie unveränderbar (Aufbewahrungssperre) oder physisch getrennt.
- Backup-Konsole nicht aus dem Client-Netz erreichbar; Zugriff nur aus dem Management-Netz.
- Sicherungen verschlüsseln; Schlüssel und Zugangsdaten sicher und getrennt verwahren (auch offline).
- Alarm bei fehlgeschlagenen Jobs, ungewöhnlich hohen Änderungsraten oder gelöschten Sicherungsketten.
- Aufbewahrung so wählen, dass auch ein spät entdeckter Angriff überbrückt wird (z. B. mehrere Wochen).

Backup ist kein Archiv

Gesetzliche Aufbewahrungspflichten (z. B. nach HGB und AO, GoBD) erfordern eine revisionssichere Archivierung. Eine Backup-Rotation erfüllt diese Anforderungen in der Regel nicht.

4 Umsetzung in sieben Schritten

Schritt	Was zu tun ist
1. Inventar	Alle zu sichernden Systeme, Datenbanken, SaaS-Dienste und Konfigurationen erfassen – inkl. „vergessener" Quellen.
2. Schutzziele	RPO/RTO je Datenklasse mit der Geschäftsleitung festlegen und dokumentieren.
3. Ziele wählen	Speicherziele nach 3-2-1-1-0 kombinieren; Kapazität und Wachstum für 2–3 Jahre einplanen.
4. Jobs konfigurieren	Anwendungskonsistente Sicherungen (Datenbanken, Domänencontroller), Zeitpläne, Aufbewahrung, Verschlüsselung.
5. Überwachung	Tägliche Erfolgskontrolle, Alarmierung an eine Person mit Vertretung, Kapazitätswarnungen.
6. Restore testen	Nach Testplan (nächste Seite) wiederherstellen, Dauer messen, Ergebnis protokollieren.
7. Dokumentation	Wiederherstellungsanleitung, Zugangsdaten-Verwahrung und Kontakte – auch ausgedruckt.

5 Restore-Testplan

Test	Intervall (Empfehlung)	Erfolgskriterium
Einzelne Datei / E-Mail wiederherstellen	monatlich	Datei vollständig, korrekte Version
Datenbank in Testumgebung wiederherstellen	vierteljährlich	Anwendung startet, Daten konsistent
Kompletten Server (VM) wiederherstellen	halbjährlich	System bootet, Dienste laufen, RTO eingehalten
Wiederherstellung aus der Offline-/unveränderbaren Kopie	jährlich	Restore ohne Zugriff auf Produktivumgebung möglich
Notfall-Szenario (z. B. Ransomware) als Übung	jährlich	Reihenfolge, Rollen und Zeiten dokumentiert

Restore-Protokoll

Datum / Durchgeführt von _____

Getestetes System / Daten _____

Quelle (Kopie, Medium) _____

Gemessene Dauer vs. RTO _____

Ergebnis / Abweichungen _____

Maßnahmen _____

6 Checkliste

	Prüfpunkt	Verantwortlich	Termin / Nachweis
PLANUNG			
☐	Alle Datenquellen inkl. SaaS und Konfigurationen sind erfasst.	_____	_____
☐	RPO/RTO sind je Datenklasse von der Geschäftsleitung freigegeben.	_____	_____
☐	Aufbewahrungsdauer überbrückt einen spät entdeckten Angriff.	_____	_____
ARCHITEKTUR			
☐	Drei Kopien auf zwei Medien, eine davon außer Haus.	_____	_____
☐	Mindestens eine Kopie ist offline oder unveränderbar.	_____	_____
☐	Backup-Infrastruktur ist von der Domäne getrennt und mit MFA geschützt.	_____	_____
☐	Sicherungen sind verschlüsselt, Schlüssel getrennt verwahrt.	_____	_____
BETRIEB			
☐	Jobs werden täglich kontrolliert; Alarmierung hat eine Vertretung.	_____	_____
☐	Restore-Tests erfolgen nach Plan und sind protokolliert.	_____	_____
☐	Wiederherstellungsanleitung liegt auch ausgedruckt vor.	_____	_____

Quellen & weiterführende Referenzen

- BSI IT-Grundschutz-Kompendium, Baustein CON.3 „Datensicherungskonzept“, bsi.bund.de
- BSI: Empfehlungen zu Ransomware und Datensicherung, bsi.bund.de
- CIS Critical Security Controls v8.1, Control 11 „Data Recovery“, cisecurity.org
- Microsoft: Shared-Responsibility-Modell und Aufbewahrungsrichtlinien in Microsoft 365, learn.microsoft.com
- KONTORIT Wissen: „IT-Notfallplan“ (kontorit.de/whitepaper)

Unterstützung gewünscht? KONTORIT begleitet kleine und mittlere Unternehmen in Hamburg bei Bestandsaufnahme, Umsetzung und Betrieb. Anfrage: **kontorit.de/kontakt** · E-Mail: **support@kontorit.de**

Dieses Dokument ist eine allgemeine, unverbindliche Orientierungshilfe. Es ersetzt keine individuelle Beratung, kein Sicherheitsaudit, keine Rechts- oder Steuerberatung und keinen Zertifizierungsnachweis. Produktfunktionen, Lizenzen und rechtliche Anforderungen ändern sich; prüfen Sie den aktuellen Stand anhand der genannten Quellen und Ihrer konkreten Umgebung. Genannte Marken gehören ihren jeweiligen Inhabern. © 2026 KONTORIT · Stand 16. November 2026 · Version 2.0