

CHECKLISTE · TOMORIS TOOLBOX

Backup-Checkliste: 3-2-1-1-0 mit Offline-Kopie und getesteter Wiederherstellung

Datensicherung zum Abhaken, belegt mit BSI IT-Grundschutz CON.3, dem BSI-Maßnahmenkatalog Ransomware und CISA

STAND

22.10.2026

UMFANG

PDF, 5 Seiten

ONLINE

tomoris.com/downloads/backup-checkliste-3-2-1-1-0

AUF EINEN BLICK

3-2-1-1-0

Regel mit Offline-Kopie und getesteter Wiederherstellung

19

Prüfpunkte zum Abhaken, je mit Beleg

1x im Jahr

Wiederherstellung mindestens prüfen (CISA CPG 2.0)

FÜR WEN

- Geschäftsführung und IT-Verantwortliche in kleinen und mittleren Unternehmen
- Administratoren, die Datensicherungen betreiben oder neu aufsetzen
- Wer die Datensicherung an einen Dienstleister ausgelagert hat und sie prüfen möchte

WURUM ES GEHT

Die meisten Ransomware-Angreifer versuchen laut der US-Behörde CISA, erreichbare Datensicherungen zu finden und zu löschen oder zu verschlüsseln. Diese Checkliste übersetzt die 3-2-1-Regel und ihre Erweiterung um eine Offline-Kopie und geprüfte Wiederherstellung in Punkte zum Abhaken. Grundlage sind der Baustein CON.3 Datensicherungskonzept des BSI IT-Grundschutz-Kompendiums, der Maßnahmenkatalog Ransomware des BSI und Empfehlungen der CISA.

Die Checkliste fasst Anforderungen und Empfehlungen der genannten Stellen zusammen und ersetzt kein Datensicherungskonzept. Welche Häufigkeit, Aufbewahrung und Wiederherstellungszeit für Ihre Systeme passt, hängt von Ihren Geschäftsprozessen ab.

INHALT

01	Die Regel: 3-2-1-1-0	2
02	Konzept und Pläne	3
03	Getrennt und geschützt aufbewahren	4
04	Wiederherstellung testen: null Fehler	4
05	Quellen	5

01

Die Regel: 3-2-1-1-0

Was die fünf Ziffern bedeuten und welche Stelle welchen Teil empfiehlt.

3

Kopien

Drei Kopien wichtiger Daten: das Original und zwei Sicherungen (BSI-Hilfsmittel zum Standard 200-4, ENISA, CISA).

2

Speichermedien

Auf zwei unterschiedlichen Speichermedien (BSI-Hilfsmittel zum Standard 200-4, ENISA, CISA).

1

Kopie an einem anderen Ort

Eine Kopie an einem anderen Ort, räumlich getrennt, möglichst in einem anderen Brandabschnitt (BSI CON.3.A12, ENISA, CISA).

1

Kopie offline

Eine Kopie offline: nach der Sicherung von den übrigen Systemen getrennt (BSI-Maßnahmenkatalog Ransomware, CISA #StopRansomware Guide).

0

Fehler bei der Wiederherstellung

Null Fehler: Die Wiederherstellung ist getestet, die Daten kommen einwandfrei und rechtzeitig zurück (BSI CON.3.A15, CISA CPG 2.0).

3-2-1 empfehlen das BSI (Hilfsmittel zum BCM-Standard 200-4), die EU-Agentur ENISA und die US-Behörde CISA. Die Erweiterung zu 3-2-1-1-0 ist keine Norm, sondern ein von Herstellern geprägter Begriff. Ihre beiden Zusätze, eine Offline-Kopie und eine geprüfte Wiederherstellung, empfehlen BSI und CISA aber ausdrücklich.

Datenspiegelungen über RAID gelten nicht als Datensicherung (BSI CON.3, Beschreibung). Für Einrichtungen unter NIS2 gehört Backup-Management ausdrücklich zu den Risikomanagementmaßnahmen (§ 32 Abs. 4 lit. c NISG 2026).

02

Konzept und Pläne

Was gesichert wird, wie oft, wie lange, und in welcher Reihenfolge es zurückkommt.

- ☐ Für jedes System sind die Rahmenbedingungen erhoben: zu sichernde Daten, Speicher- und Änderungsvolumen, Verfügbarkeit, Vertraulichkeit, rechtliche Anforderungen, Löschvorgaben und Zuständigkeiten (CON.3.A1).
- ☐ Art, Häufigkeit und Zeitpunkt der Sicherungen sind festgelegt, ebenso Speichermedien, Transport und Aufbewahrung (CON.3.A2).
- ☐ Je System oder Systemgruppe gibt es einen Datensicherungsplan: was gesichert wird, Reihenfolge der Wiederherstellung, Vorgehen, Aufbewahrungsdauer, Schutz vor Zugriff und Überschreiben, eingesetzte Hard- und Software (CON.3.A4).
- ☐ Für jedes System ist festgelegt, wie viel Datenverlust höchstens tragbar ist (Recovery Point Objective, CON.3.A6).
- ☐ Die Pläne zur Wiederherstellung sind auch dann greifbar, wenn das Datensicherungssystem selbst ausfällt, etwa zusätzlich auf Papier (CON.3.A6; Gefährdung 2.4 nennt Ransomware als Grund).
- ☐ Alle Mitarbeitenden kennen die Regeln zur Datensicherung und ihre eigenen Aufgaben dabei (CON.3.A5).
- ☐ Online-Speicher ist vertraglich geregelt: Speicherort, Verfügbarkeit, Anmeldung, Verschlüsselung gespeicherter und übertragener Daten (CON.3.A9).

03 —

Getrennt und geschützt aufbewahren

Eigene Medien, anderer Ort, eine Kopie offline und kein Überschreiben durch Unbefugte.

- ☐ Sicherungen liegen immer auf eigenen Speichermedien, nicht nur auf dem gesicherten System (CON.3.A2).
- ☐ Die Medien liegen räumlich getrennt von den gesicherten Systemen, möglichst in einem anderen Brandabschnitt (CON.3.A12).
- ☐ Mindestens eine Kopie ist offline und nach der Sicherung von den übrigen Systemen getrennt (BSI-Maßnahmenkatalog Ransomware; CON.3.A2 für besonders schützenswerte Medien).
- ☐ Probe der Trennung: Ein Domänen-Administrator versucht testweise, auf die getrennten Kopien zuzugreifen. Das darf nicht gelingen (BSI-Maßnahmenkatalog Ransomware).
- ☐ Sicherungen können weder absichtlich noch versehentlich überschrieben werden; Schreibzugriff haben nur autorisierte Sicherungs- und Administrationsvorgänge (CON.3.A14).
- ☐ Sicherungen sind verschlüsselt, die Schlüssel getrennt gesichert, und verschlüsselte Daten lassen sich auch nach längerer Zeit noch einspielen (CON.3.A13, bei erhöhtem Schutzbedarf).

Eine automatische Synchronisation in die Cloud ist allein kein ausreichendes Backup: Verschlüsselt ein Angreifer die lokalen Dateien, werden die verschlüsselten Fassungen mit synchronisiert (CISA #StopRansomware Guide).

04 —

Wiederherstellung testen: null Fehler

Regelmäßig, mindestens einmal im Jahr, vollständig und in angemessener Zeit.

- ☐ Es wird regelmäßig getestet, ob gesicherte Daten einwandfrei und in angemessener Zeit zurückgespielt werden können (CON.3.A15).
- ☐ Mindestens einmal im Jahr wird die Wiederherstellung geprüft (CISA CPG 2.0; WKO-Leitfaden zu technischen und organisatorischen Maßnahmen).
- ☐ Geübt wird die Wiederherstellung von Daten und ganzen Systemen, nicht nur das Sichern (BSI-Maßnahmenkatalog Ransomware).
- ☐ Die Reihenfolge der Wiederherstellung richtet sich nach der Wichtigkeit der Dienste (CON.3.A4; CISA #StopRansomware Guide).

- ☐ Regelmäßig wird kontrolliert, ob das Datensicherungskonzept so umgesetzt ist wie beschrieben (CON.3.A6).
- ☐ Ergebnis und Dauer jeder Probe sind dokumentiert; Fehler werden behoben und erneut getestet.

Der letzte Punkt ist eine Empfehlung von TOMORIS: Erst eine dokumentierte, erfolgreiche Probe zeigt, dass die Null in 3-2-1-1-0 erreicht ist.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

05

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **BSI IT-Grundschutz-Kompendium, Baustein CON.3 Datensicherungskonzept, Edition 2023**
Anforderungen A1, A2, A4, A5, A6, A9, A12 bis A15, Gefährdungen 2.4 und 2.10
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 2 **BSI: Maßnahmenkatalog Ransomware, Version 1.0 vom 23.02.2022**
Offline-Kopie, Probe der Trennung, Üben der Wiederherstellung
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Th...
- 3 **BSI: Vorschläge zu Business-Continuity-Strategien, Hilfsmittel zum BSI-Standard 200-4 (Community Draft 2.0)**
Kapitel 3.1, 3-2-1-Regel
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmi...
- 4 **ENISA: Threat Landscape for Ransomware Attacks (Juli 2022)**
Kapitel 6.1
www.enisa.europa.eu/sites/default/files/publications/ENISA%20Th...
- 5 **CISA: #StopRansomware Guide**
Offline- und verschlüsselte Backups, Cloud-Synchronisation, Wiederherstellung nach Priorität
www.cisa.gov/resources-tools/resources/stopransomware-guide
- 6 **CISA: Cross-Sector Cybersecurity Performance Goals 2.0**
Backups offline, Test mindestens einmal im Jahr
www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0
- 7 **CISA/US-CERT: Data Backup Options**
3-2-1-Regel
www.cisa.gov/sites/default/files/publications/data_backup_optio...
- 8 **WKO it-safe: Leitfaden technische und organisatorische Maßnahmen im Rahmen der DSGVO**
Abschnitt 3.7, jährliche Prüfung der Wiederherstellung
www.wko.at/oe/it-sicherheit/Leitfaden-massnahmen-dsgvo-1.pdf
- 9 **NISG 2026, BGBl. I Nr. 94/2025, § 32 Abs. 4 lit. c**
www.ris.bka.gv.at/eli/bgbl/i/2025/94
- 10 **Veeam: 3-2-1 Backup Rule (Herkunft des Begriffs 3-2-1-1-0)**
www.veeam.com/blog/321-backup-rule.html