Backup-Übersicht

Bei Ransomware entscheidet eine einzige Frage über Verhandeln oder Wiederherstellen: **Gibt es Backups, die der Angreifer nicht erreichen konnte – und wurden sie je erfolgreich zurückgespielt?** Das IR-Team braucht Speicherorte, Netztrennung und den letzten Restore-Test – nicht das Marketing-Datenblatt der Backup-Software.

Warum dieses Dokument?

Ob wiederhergestellt werden kann, hängt an drei Spalten: Offline-Trennung, Zugriffsweg, Restore-Test. Diese Übersicht macht die Lücken sichtbar – heute, nicht im Ernstfall.

Wann brauchen Sie es?

In Stunde 1 beim Schützen der Backups (IR-02, Punkt 4), danach bei der Entscheidung Wiederherstellen vs. Verhandeln und für die Wiederanlauf-Planung.

Wo aufbewahren?

Ausgedruckt im Notfallordner + zweiter Brandabschnitt. Praxisfall: Die Backups waren da – aber die Passwörter der Backup-Konsole lagen nur im verschlüsselten Passwortmanager.

Backups in der ersten Stunde

1. **Replikation stoppen** – Copy-Jobs und Sync sofort anhalten
2. **Ziele vom Netz** – Repository/NAS per Switchport oder Kabel trennen
3. **Sauberer Stand** – letzte intakte Sicherung identifizieren + notieren
4. **Restore mit Freigabe** – erst nach Forensik-Freigabe des IR-Teams

Grundregel: Nie in die Produktivumgebung zurücksichern, solange der Angreifer drin sein könnte – sonst wird auch das Backup verbrannt.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv)

Was	Methode	Ziel	Offline?	Letzter Restore-Test
Alle VMs RZ Augsburg	Veeam B&R	Repo-Server RZ (lokal)	**nur online (!)**	12.03.2026: 1 VM, ok, 40 min
Wochenstände	Veeam Copy-Job	LTO-9-Tapes, Bankschließfach	Air-Gap, wöchentl. Wechsel	12.03.2026: File-Restore ok
M365 (Mail, SharePoint)	SaaS-Backup-Dienst	Cloud EU, eigener Tenant	immutable 30 T.	**nie (!)**
ERP-DB	DB-Dump + Copy-Job	NAS Leipzig	online, eigenes Konto	20.05.2026: Voll-Restore Testumgebung, 6 h

⚠ **Backups mit Domänen-Anmeldung und Online-Erreichbarkeit gelten im Ransomware-Fall als verloren.** Prüfen Sie die Spalten „Offline/immutable“ und „Zugriff aus dem Produktivnetz“ heute – nicht im Ernstfall. Ein Restore, der nie getestet wurde, ist keine Wiederherstellung, sondern eine Hoffnung.

Halbjährliche Prüfung: ☐ Restore-Test aktuell ☐ Offline-Kette intakt ☐ Passwort offline
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

BACKUP-ZIELE & JOBS – EINE ZEILE PRO BACKUP-ZIEL/-JOB

Was wird gesichert (Systeme/Daten, Inventar-Nr. → IR-10)	Software / Methode	Ziel / Speicherort (Gerät + physischer Ort)	Offline / immutable?	Zugriff aus Produktivnetz?	Frequenz + Aufbewahrung
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	
			☐ Air-Gap/Tape ☐ Immutable Storage ☐ nur online (!)	☐ ja ☐ nein mit Domänen-Konto: ☐ ja ☐ nein	

„Nur online“ heißt: Der Angreifer kann das Backup im Ransomware-Fall erreichen – diese Zeile heute entschärfen.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

RESTORE-TESTS, ZUGÄNGE & SCHLÜSSEL – GLEICHE ZEILEN WIE BLATT 1

Was (wie Blatt 1)	Letzter erfolgreicher Restore-TEST (Datum, was, durch wen)	Geschätzte Dauer Vollrestore	Backup-Konsole: Wer hat Zugang – und wo liegt das Passwort AUSSERHALB des Netzes?	Verschlüsselungspasswort / Key des Backups: Verwahrort

Tipp aus der Einsatzpraxis: Konsolen-Passwort und Verschlüsselungs-Key gehören in den versiegelten Umschlag zu den Break-Glass-Konten (IR-12) – nicht in den Passwortmanager, der im Ernstfall mitverschlüsselt ist.

NOTIZEN