BR-Systems

BACKUP & RESILIENCE 2026

Ransomware-feste Backups

Wie 3-2-1, Proxmox Backup Server, Offline-Medien und Restore-Tests zu echter Wiederanlauffähigkeit werden

Dokument-ID	BR-WP-BCK-002
Version	1.0
Fachstand	12. Mai 2026
Veröffentlicht	26. Mai 2026
Klassifizierung	Öffentlich – kostenfreier Fachbeitrag
Autor	Benjamin Raulf, BR-Systems
Herausgeber	BR-Systems · IT-Systemhaus · Unterlüß
Standort zum Fachstand	Unterlüß
Kontakt	info@br-systems.eu · https://br-systems.eu · +49 179 1601700

Executive Summary

Dieses Whitepaper übersetzt aktuelle Anforderungen und technische Entwicklungen in einen umsetzbaren Betriebsansatz. Im Mittelpunkt stehen nicht einzelne Produkte, sondern Verantwortlichkeiten, überprüfbare Kontrollen und ein realistischer Weg vom heutigen Zustand zu einer belastbaren Zielarchitektur.

Die vier wichtigsten Aussagen

- Backup von Wiederherstellungsfähigkeit unterscheiden
- 3-2-1 um Unveränderbarkeit und Tests erweitern
- Proxmox Backup Server, Tape und RDX sinnvoll kombinieren
- RTO, RPO, Schlüssel und Notfallzugänge praktisch planen

Inhalt

1. Warum ein grüner Backup-Status nicht genügt

Ransomware-Angriffe zielen nicht nur auf Produktivdaten. Angreifer suchen nach erreichbaren Sicherungen, Administrationskonten, Hypervisoren und Fernwartungswerkzeugen. Sie versuchen, Backups zu löschen, Aufbewahrungsregeln zu verändern oder Wiederherstellungszugänge zu kompromittieren. Deshalb ist ein erfolgreich beendeter Sicherungsjob lediglich ein technisches Zwischenergebnis. Die geschäftlich relevante Frage lautet: Kann die Organisation ihre wichtigsten Prozesse innerhalb der benötigten Zeit aus vertrauenswürdigen Daten wiederherstellen?

CISA empfiehlt, kritische Daten häufig zu sichern, verschlüsselte Offline-Kopien vorzuhalten und Verfügbarkeit sowie Integrität regelmäßig in einem Disaster-Recovery-Szenario zu testen [1]. Diese Empfehlung enthält drei unterschiedliche Aufgaben: Daten kopieren, Kopien gegen denselben Angriff schützen und den Wiederanlauf beweisen. In der Praxis werden diese Aufgaben häufig vermischt. Ein zweites Volume im selben Storage ist eine Kopie, aber keine ausreichende Trennung. Eine Cloud-Sicherung kann wertvoll sein, bleibt aber gefährdet, wenn dasselbe kompromittierte Administratorkonto sie löschen kann.

Ransomware-Resilienz beginnt mit einer Annahme: Ein Teil der produktiven Umgebung könnte bereits kompromittiert sein. Backup-Systeme benötigen daher eigene Identitäten, restriktive Rechte, getrennte Managementpfade und möglichst eine Kopie, die vom Produktivsystem nicht verändert werden kann. Zusätzlich muss geklärt sein, welche Systeme nach einem Vorfall als sauber gelten. Eine schnelle Rücksicherung in eine weiterhin kompromittierte Umgebung stellt den Betrieb nicht zuverlässig wieder her.

2. Von 3-2-1 zu 3-2-1-1-0

Die klassische 3-2-1-Regel fordert drei Datenkopien auf zwei unterschiedlichen Medientypen, davon eine Kopie außerhalb des Standorts. Proxmox beschreibt dieses Prinzip ebenfalls als wirksame Grundlage gegen Brände, Naturereignisse und Angriffe [2]. Moderne Konzepte ergänzen häufig eine weitere "1" für eine offline oder unveränderbar gehaltene Kopie und eine "0" für null ungeklärte Fehler nach Verifikation und Restore-Test. Die Schreibweise ist weniger wichtig als die Architektur dahinter.

Drei Kopien bedeuten nicht drei Ordner auf demselben System. Produktivdaten, lokales Backup und externe Kopie müssen unterschiedliche Fehlerdomänen besitzen. Zwei Medientypen können beispielsweise Festplattenspeicher und Band sein. Die externe Kopie schützt gegen Standortschäden und lokale Kompromittierung. Offline-Medien wie ausgeworfene RDX-Kassetten oder exportierte LTO-Bänder entziehen sich nach dem Sicherungslauf dem direkten Netzwerkzugriff. Unveränderbarer Objektspeicher kann eine Alternative oder Ergänzung sein, wenn Aufbewahrung und Löschschutz unabhängig administriert werden.

Die Null steht für überprüfte Lesbarkeit. Prüfsummen und automatische Verifikationsjobs erkennen beschädigte Daten, ersetzen aber keinen vollständigen Anwendungs-Restore. Eine virtuelle Maschine kann technisch starten und trotzdem fachlich unbrauchbar sein, weil Datenbank, Lizenzserver, Identitätsdienst oder externe Abhängigkeit fehlen. Deshalb braucht es verschiedene Teststufen: Dateiwiederherstellung, VM-Start in isolierter Umgebung, Anwendungsprüfung und schließlich einen priorisierten Wiederanlauf mehrerer Systeme.

3. Proxmox Backup Server richtig einordnen

Proxmox Backup Server ist für virtuelle Maschinen, Container und physische Hosts ausgelegt und unterstützt Deduplizierung, Kompression, Verifikation, clientseitige Verschlüsselung, Remote-Synchronisation und

Tape-Integration [3]. Bestehende Blöcke werden im Datastore nicht durch einen kompromittierten Backup-Client umgeschrieben. Das erschwert die Manipulation vorhandener Sicherungsstände, ersetzt jedoch keine vollständige Sicherheitsarchitektur. Wer administrative Kontrolle über Backup-Server, Datastore und Aufbewahrung erlangt, kann weiterhin erheblichen Schaden verursachen.

Eine belastbare Rollenverteilung trennt Backup-Erstellung, Backup-Administration und Wiederherstellung soweit praktikabel. API-Tokens erhalten nur die benötigten Rechte. Interaktive Administratoren verwenden MFA. Der Managementzugang liegt nicht offen im normalen Benutzersegment. Synchronisationsziele werden so konfiguriert, dass ein kompromittierter Quellhost nicht automatisch alle Generationen am Ziel löschen kann. Verschlüsselungsschlüssel und Wiederherstellungsinformationen werden getrennt, nachvollziehbar und auch offline gesichert.

Verifikationsjobs sollten geplant und überwacht werden. Proxmox weist darauf hin, dass Prüfungen auch Hinweise auf Ransomware-Aktivität liefern können [2]. Das ist kein vollständiges Erkennungssystem, aber ein nützlicher Kontrollpunkt. Entscheidend ist die Reaktion auf Fehler: Wer erhält die Meldung? Wie schnell wird sie bewertet? Wird bei wiederholten Fehlern eine zusätzliche Kopie angelegt oder der Datastore gesperrt? Ein unbeachtetes Dashboard schafft keine Resilienz.

4. Tape, RDX und externe Speicher

Band ist kein Relikt, sondern ein anderes Betriebsmodell. Proxmox unterstützt Tape-Backups, um eine zusätzliche Kopie auf einem anderen Medium und an einem weiteren Ort zu speichern [4]. Exportierte Bänder sind physisch vom Netzwerk getrennt. Sie eignen sich für längere Aufbewahrung und große Datenmengen, erfordern aber Medienrotation, Inventar, sichere Lagerung, Schlüsselmanagement und realistische Wiederherstellungszeiten. Ein Restore von Band beginnt nicht mit einem Mausklick, wenn das Medium erst aus einem externen Tresor beschafft werden muss.

RDX kann für kleinere Umgebungen eine pragmatische Offline-Schicht bilden. Entscheidend ist, dass Medien nach dem Lauf tatsächlich ausgeworfen und räumlich getrennt werden. Bleibt die Kassette dauerhaft eingebunden, verliert sie einen wesentlichen Sicherheitsvorteil. Rotation und Beschriftung müssen so einfach sein, dass sie im Alltag durchgeführt werden. Ein klarer Kalender, Verantwortliche und dokumentierte Übergaben sind wirksamer als ein theoretisch perfektes Modell, das regelmäßig vergessen wird.

Externer Objektspeicher oder ein zweiter Backup-Server kann schnelle Offsite-Kopien ermöglichen. Dabei sind Mandantentrennung, Object Lock, Löschschutz, separate Konten, MFA, Datenstandort, Bandbreite und Kosten für Rückübertragung zu prüfen. Die Entscheidung ist kein Entweder-oder: Lokales Disk-Backup sorgt für schnelle Alltagsrestores, eine externe unveränderbare Kopie schützt gegen Standort- und Administrationsrisiken, Offline-Medien erweitern die Unabhängigkeit.

5. RTO, RPO und Wiederanlaufreihenfolge

RPO beschreibt den maximal tolerierbaren Datenverlust in Zeit, RTO die angestrebte Wiederherstellungsdauer. Beide Werte müssen aus Geschäftsprozessen abgeleitet werden. Wenn die Auftragsbearbeitung höchstens vier Stunden Daten verlieren darf, reicht eine nächtliche Sicherung nicht. Wenn ein System innerhalb von zwei Stunden verfügbar sein muss, kann ein ausschließlich extern gelagertes Band ungeeignet sein. Umgekehrt braucht nicht jedes Archiv eine teure Sofortwiederherstellung.

Die Wiederanlaufreihenfolge berücksichtigt Abhängigkeiten. Netzwerk, DNS, Identitäten, Virtualisierung, Storage, Datenbanken und Fachanwendungen bilden eine Kette. Zugangsdaten, Lizenzen, Installationsmedien und Konfigurationsdokumente müssen ebenfalls verfügbar sein. CISA empfiehlt, kritische Assets und ihre

Abhängigkeiten vorab zu inventarisieren und Wiederherstellung zu priorisieren [1]. Ein kompakter Wiederanlaufplan sollte pro System Verantwortliche, Quelle der Sicherung, benötigte Schlüssel, Zielplattform, Prüfschritte und Freigabekriterien nennen.

Tests müssen messbar sein. Wann begann der Restore, wann war die Anwendung technisch verfügbar, wann fachlich freigegeben? Welche Schritte waren unklar? Welche Zugangsdaten fehlten? Aus jedem Test entsteht eine Verbesserungsliste. So wächst Wiederanlauffähigkeit iterativ. Ein jährlicher Großtest kann sinnvoll sein, wird aber durch kleinere monatliche oder quartalsweise Stichproben wirksamer ergänzt.

6. Betriebsmodell und Sofortmaßnahmen

In den ersten vier Wochen sollten Unternehmen Backup-Quellen, Aufbewahrung, Administratoren und Löschrechte dokumentieren. Danach wird eine getrennte Kopie eingerichtet und mindestens eine kritische Anwendung testweise wiederhergestellt. Im zweiten Schritt folgen Rollenbereinigung, MFA, Monitoring, Schlüsselhinterlegung und eine schriftliche Medienrotation. Abschließend wird der Wiederanlauf gemeinsam mit Fachverantwortlichen geprobt.

Ein belastbares Backup-Konzept ist weder ein einzelnes Produkt noch eine einmalige Installation. Es ist ein wiederholbarer Prozess aus Sichern, Trennen, Prüfen, Wiederherstellen und Verbessern. Wer diese fünf Verben organisatorisch verankert, reduziert nicht nur Ransomware-Risiken. Er verbessert auch den Umgang mit Fehlbedienung, Hardwaredefekten, Softwarefehlern und Standortausfällen.

7. Vom Konzept zum belastbaren Betrieb

Technische Maßnahmen entfalten ihren Wert erst in einem geregelten Betrieb. Dazu gehören ein benannter Service Owner, eine aktuelle Systemdokumentation, ein Änderungsprozess und ein fester Kontrollrhythmus. Der Umfang darf zur Organisation passen. Ein kleiner Betrieb benötigt keine Sitzungsbürokratie wie ein Konzern. Er benötigt jedoch Klarheit darüber, wer entscheidet, wer umsetzt, wer prüft und wie Abweichungen behandelt werden.

Bei jeder Maßnahme sollten vier Fragen beantwortet werden: Welches konkrete Risiko wird reduziert? Woran erkennen wir, dass die Maßnahme aktiv ist? Wer reagiert auf Fehler oder Alarme? Wie verlassen oder ersetzen wir die Lösung später? Diese Fragen schützen vor Scheinsicherheit und unnötiger Herstellerbindung. Sie machen Angebote vergleichbarer und erleichtern die Übergabe zwischen internen und externen Verantwortlichen.

Dokumentation ist kein Selbstzweck. Sie verkürzt Störungen, macht Änderungen sicherer und verhindert, dass kritisches Wissen ausschließlich bei einer Person liegt. Gute Dokumentation ist knapp genug, um gepflegt zu werden, und konkret genug, um in einer Störung zu helfen. Dazu gehören Übersichten, Abhängigkeiten, Verantwortliche, Zugangsverfahren, Wiederanlaufhinweise und der Stand der letzten Prüfung.

Ein Management-Review sollte Risiken nicht in technischen Einzelmeldungen verstecken. Sinnvoll sind wenige verständliche Kennzahlen: ungeklärte kritische Schwachstellen, Abdeckung starker Authentisierung, erfolgreiche Restore-Tests, überfällige Offboardings, nicht unterstützte Systeme und offene Maßnahmen nach Priorität. Die Kennzahlen dienen Entscheidungen, nicht dem Schönrechnen eines Ampelstatus.

Die beste Roadmap ist umsetzbar. Maßnahmen werden in kleine, prüfbare Pakete geschnitten und mit Termin sowie Verantwortlichem versehen. Kritische Sofortmaßnahmen stehen vor Komfortprojekten. Nach jedem Abschnitt wird geprüft, ob das Risiko tatsächlich gesunken ist. So entsteht über Monate ein belastbarer Betrieb, ohne das Tagesgeschäft durch einen unrealistischen Komplettumbau zu blockieren.

Beschaffung und Betrieb sollten getrennt bewertet werden. Ein günstiger Einstieg kann durch aufwendige Administration, unklare Lizenzbedingungen, fehlende Exportmöglichkeiten oder schwachen Support später teuer werden. Umgekehrt ist eine umfangreiche Plattform nicht automatisch die bessere Wahl. Vor einer Entscheidung werden deshalb fünf Jahre Betrieb, interne Zeit, notwendige Kompetenzen, Ausfallfolgen, Datenmigration und Rückbau betrachtet. Diese Gesamtsicht verhindert, dass ein kurzfristiger Preisvergleich die langfristige Handlungsfähigkeit bestimmt.

Auch Kommunikation ist eine Sicherheits- und Qualitätskontrolle. Mitarbeitende müssen wissen, wo sie Störungen, verdächtige Nachrichten oder Fehlbedienungen ohne Angst vor Schuldzuweisung melden können. Führungskräfte benötigen eine verständliche Lage, keine Sammlung unbewerteter Warnungen. Dienstleister brauchen eindeutige Freigaben und erreichbare Ansprechpartner. Ein kurzer, regelmäßig geübter Kommunikationsweg reduziert im Ernstfall Verzögerungen und Fehlentscheidungen deutlich.

Vor dem Produktivstart gehört eine unabhängige Abnahme in den Plan. Dabei wird nicht nur geprüft, ob Funktionen vorhanden sind, sondern ob Berechtigungen, Protokollierung, Sicherung, Alarmierung, Dokumentation und Rückfallweg tatsächlich funktionieren. Festgestellte Abweichungen werden mit Risiko, Verantwortlichem und Zieltermin protokolliert. Eine bewusste Rest-Risikoentscheidung ist legitim; eine unbemerkte Lücke ist es nicht. Diese Abnahme schafft eine belastbare Ausgangslage für den späteren Regelbetrieb.

Technische Standards müssen außerdem mit dem Arbeitsalltag vereinbar sein. Eine Kontrolle, die regelmäßig umgangen wird, schützt schlechter als eine etwas einfachere Lösung, die zuverlässig genutzt und überwacht wird. Pilotgruppen helfen, Nebenwirkungen früh zu erkennen. Rückmeldungen aus Fachabteilungen werden dokumentiert, ohne die Schutzziele aus dem Blick zu verlieren. So entsteht Akzeptanz nicht durch Marketing, sondern durch nachvollziehbare Entscheidungen und funktionierende Abläufe.

Mindestens einmal jährlich sollte die Organisation ihre Annahmen neu prüfen. Geschäftsprozesse, Mitarbeiterzahl, Standorte, Anwendungen, Bedrohungen und gesetzliche Rahmenbedingungen verändern sich. Ein früher sinnvoller Schwellenwert oder Vertrag kann später unpassend sein. Das Review betrachtet neue Abhängigkeiten, abgeschaltete Systeme, offene Ausnahmen, Wirksamkeitsnachweise und geplante Veränderungen. Daraus entsteht die nächste überschaubare Roadmap statt eines jahrelang unveränderten Dokuments.

Praxis-Checkliste

- Drei echte Kopien in getrennten Fehlerdomänen vorhalten
- Mindestens eine externe sowie offline oder unveränderbare Kopie betreiben
- Backup-Administratoren und Produktivadministratoren sinnvoll trennen
- MFA, restriktive Tokens und getrennte Managementzugänge verwenden
- Verschlüsselungsschlüssel und Notfallzugänge offline sichern
- RPO, RTO und Wiederanlaufreihenfolge je kritischem Prozess festlegen
- Restore-Tests dokumentieren und festgestellte Lücken nachverfolgen

Fazit

Die Qualität einer IT-Entscheidung zeigt sich nicht am Prospekt, sondern im Betrieb: an klaren Rollen, nachvollziehbaren Änderungen, getesteter Wiederherstellung und einer realistischen Exit-Option. BR-Systems unterstützt bei Bestandsaufnahme, Konzeption, Migration, Umsetzung und laufendem Betrieb - herstellerbewusst, aber nicht verkaufsgetrieben.

Quellen und weiterführende Informationen

[1] CISA: #StopRansomware Guide
https://www.cisa.gov/stopransomware/ransomware-guide

[2] Proxmox Backup Server: Backup Storage und 3-2-1
https://pbs.proxmox.com/docs/storage.html

[3] Proxmox Backup Server: Dokumentation
https://pbs.proxmox.com/docs/

[4] Proxmox Backup Server: Tape Backup
https://pbs.proxmox.com/docs/tape-backup.html

Historischer bzw. fachlicher Bezugsstand: 12. Mai 2026. Veröffentlicht: 26. Mai 2026. Online-Quellen zuletzt geprüft: 12. Mai 2026. Der Fachstand ist kein vorgetäuschtes Veröffentlichungsdatum. Dokument-ID BR-WP-BCK-002, Version 1.0.

Über BR-Systems

- Herstellerunabhängige Beratung mit Blick auf Nutzen, Betrieb und Exit-Fähigkeit
- Umsetzung und Betreuung für Microsoft 365, Security, Proxmox, Backup, Netzwerk und Open Source
- Ein fester Ansprechpartner, nachvollziehbare Dokumentation und transparente Leistungsgrenzen

Nächster Schritt

Sie möchten das Thema auf Ihre Umgebung übertragen? BR-Systems beginnt mit einer Bestandsaufnahme und einem klar begrenzten Maßnahmenplan. Kontakt: info@br-systems.eu oder +49 179 1601700.