Cyber-resiliente Backups im Test: Profi Digital Recovery gibt Tipps

12.03.2026, 15:16 | IT, New Media & Software

Pressemitteilung von: *Benjamin Bansal, B.A., LL.M.*

Manipulationssichere Backups sind längst keine optionale IT-Komponente mehr, sondern ein strategischer Bestandteil der Unternehmensresilienz. Verschlüsselungstrojaner, gezielte Ransomware-Kampagnen und KI-gestützte Angriffe stellen besonders kleine und mittelständische Unternehmen (KMU) vor existenzielle Risiken. Entscheidend ist nicht nur, ob Daten gesichert werden, sondern wie. Ein technischer Blick von Profi Digital Recovery auf moderne Backup-Architekturen zeigt, welche Anforderungen erfüllt sein müssen, damit Sicherungen im Ernstfall tatsächlich funktionieren.

Was ein cyber-resilientes Backup wirklich ausmacht

Klassische Backup-Strategien, etwa tägliche Sicherungen auf NAS-Systemen oder externen Datenträgern, bieten heute keinen ausreichenden Schutz mehr. Moderne Angriffe zielen gezielt auf Backup-Strukturen ab, bevor die eigentliche Verschlüsselung beginnt. Ein cyber-resilientes Backup-System sollte mindestens folgende Eigenschaften erfüllen:

1. **Immutable Storage (Unveränderbarkeit):** Backups müssen technisch gegen Löschung und Überschreiben geschützt sein, selbst durch Administrator-Konten. WORM-Mechanismen (Write Once, Read Many) oder zeitbasierte Unveränderbarkeit sind hier essenziell.
2. **Physische oder logische Isolation:** Air-Gap-Strategien, physisch oder virtuell, verhindern, dass sich Schadsoftware lateral auf Backup-Systeme ausbreitet. Backups dürfen nicht dauerhaft in derselben Domäne wie Produktionssysteme betrieben werden.
3. **Mehrstufige Authentifizierung:** Backup-Management-Zugänge müssen mit Multi-Faktor-Authentifizierung (MFA) abgesichert sein. Administratorzugänge ohne MFA stellen eine massive Schwachstelle dar.
4. **Versionierung und Retention-Strategie:** Ein Backup ist nur so gut wie seine Historie. Mehrere Wiederherstellungspunkte verhindern, dass bereits kompromittierte oder latent infizierte Daten zurückgespielt werden.
5. **Automatisierte Wiederherstellungstests:** Regelmäßige Restore-Tests sind Pflicht. Ein Backup, das nie getestet wurde, ist ein theoretisches Sicherheitsversprechen, kein belastbares Notfallinstrument.

Profi Digital Recovery weist darauf hin, dass insbesondere Immutable-Architekturen mit Systemen wie Datto SIRIS, eine zusätzliche Verteidigungsschicht darstellen, da sie interne Manipulationsversuche technisch unterbinden.

Die Backup-Architektur als häufig unterschätztes Risiko

Viele Unternehmen erfüllen formal die Anforderung einer „regelmäßigen Datensicherung“, übersehen jedoch strukturelle Schwachstellen. Kritisch wird es vor allem dann, wenn Backup-Server in derselben Active-Directory-Umgebung laufen, identische Zugangsdaten für Produktiv- und Sicherungssysteme verwendet werden oder eine konsequente Netzwerksegmentierung fehlt. Auch unverschlüsselte Backup-Transporte und eine fehlende Überwachung von Anomalien erhöhen das Risiko erheblich. Ransomware-Gruppen wie LockBit oder BlackCat analysieren gezielt genau diese Konstellationen. Wird zuerst das Backup kompromittiert, folgt die Verschlüsselung der Produktivsysteme oft im zweiten Schritt mit maximalem Erpressungspotenzial. Ein resilientes Design folgt laut Digital Recovery daher dem Prinzip: Erkennen – Isolieren – Bewahren – Wiederherstellen.

Cyber-resiliente Backups für KMU: Eine Checkliste zur Selbstprüfung

Gerade kleinere Unternehmen ohne eigene IT-Sicherheitsabteilung sollten ihre Backup-Strategie regelmäßig kritisch prüfen. Zentral ist die Frage, ob Sicherungen technisch unveränderbar sind, also selbst durch Administratoren nicht gelöscht oder überschrieben werden können. Ebenso wichtig sind eine klare Trennung vom Produktionsnetz, mindestens ein externer oder cloudbasierter Speicherort, dokumentierte Wiederherstellungstests sowie abgesicherte Zugänge per Multi-Faktor-Authentifizierung. Auch ein definierter Incident-Response-Plan und die Überwachung von Backup-Logs gehören zu den Grundlagen moderner Resilienz. Bleibt eine dieser Fragen unbeantwortet oder unsicher, besteht konkreter Handlungsbedarf. Der kostenfreie SIRIS-Backup-Check von Digital Recovery setzt genau hier an und analysiert, ob bestehende Backup-Architekturen echten Schutz vor Ransomware bieten oder nur vermeintliche Sicherheit vermitteln.

Praxisbeispiel: Datenrettung trotz kompromittierter Sicherung

In der Praxis zeigt sich immer wieder, dass selbst vermeintlich zerstörte Backups nicht zwangsläufig endgültig verloren sind. Bei einem Angriff auf einen Automobilzulieferer konnten über 40 Terabyte geschäftskritischer Daten rekonstruiert werden, obwohl Produktionsserver und Sicherungen zeitgleich verschlüsselt worden waren. Möglich wurde dies durch forensische Analyse der Angriffskette, Identifikation verbliebener Datenfragmente, Rekonstruktion von Dateisystemstrukturen, gezielte Low-Level-Wiederherstellungsverfahren. Der Fall von Digital Recovery verdeutlicht, dass professionelle Incident Response und datenforensische Expertise oft die letzte Verteidigungslinie darstellen.

Digital Recovery gibt Handlungsempfehlung für Unternehmen

1. Führen Sie mindestens einmal jährlich einen externen Backup-Audit durch.
2. Implementieren Sie Immutable Storage als festen Bestandteil Ihrer Architektur.
3. Testen Sie Wiederherstellungen unter realistischen Bedingungen.
4. Schulen Sie IT-Administratoren regelmäßig im Bereich Ransomware-Mechanismen.
5. Dokumentieren Sie klar definierte Wiederanlaufzeiten (RTO) und Datenverlust-Toleranzen (RPO).

Nur wer diese Parameter kennt und überprüft, kann im Ernstfall schnell und strukturiert reagieren. Cyber-resiliente Backups sind heute keine rein technische Frage mehr, sondern ein wirtschaftlicher Überlebensfaktor. Unternehmen, die ihre Backup-Architektur regelmäßig überprüfen und technisch gegen Manipulation absichern, reduzieren das Risiko existenzbedrohender Ausfälle erheblich.

Weitere Informationen zum kostenfreien SIRIS-Backup-Check finden Interessierte unter www.digitalrecovery.com/de.

Impressum:
Digital Recovery PHD GmbH
W-Tec Haus 4
Heinz-Fangman-Str. 2-6
42287 Wuppertal

info@digitalrecovery.de
www.digitalrecovery.com/de

Digital Recovery PHD GmbH

Heinz-Fangman-Str. 2-6
42287 Wuppertal
Deutschland

www.digitalrecovery.com/de

Portrait

Digital Recovery ist ein international aktives Datenrettungs- und Cyber-Resilienz-Unternehmen, das sich seit über 25 Jahren auf die Wiederherstellung verlorener oder verschlüsselter Daten für Unternehmen spezialisiert hat – von einfachen Festplatten über RAID-, NAS- und Serversysteme bis hin zu komplexen Ransomware-Vorfällen. Mit proprietärer Technologie wie TRACER, 24/7-Notfall-Support und einem globalen Netzwerk von Experten bietet das Unternehmen schnelle, technisch fundierte Lösungen, um auch in kritischen IT-Notfällen Daten zu retten und Ausfallzeiten zu minimieren.

News-ID: 1306441 • Views: 331 (Stand: 13.05.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1306441/Cyber-resiliente-Backups-im-Test-Profi-Digital-Recovery-gibt-Tipps.html