groupios
Mare Cloud

ENTSCHEIDER-WHITEPAPER – Multi-Node-Backup

Datensicherheit für kleine und mittlere Unternehmen

Was nach DSGVO, NIS2, Cyberversicherung und Compliance wirklich zählt – und woran die meisten Backup-Konzepte scheitern.

MADE IN GERMANY

POST-QUANTUM

EU-VERTEILT

Drei Fragen, die jedes Unternehmen beantworten muss.

Kleine und mittlere Unternehmen stehen zunehmend unter Druck: Cyberangriffe, steigende Compliance-Anforderungen, Anforderungen von Cyberversicherungen und die wachsende Abhängigkeit von digitalen Geschäftsprozessen erhöhen die Bedeutung einer belastbaren Datensicherungsstrategie.

1. **Wann wurde zuletzt getestet wiederhergestellt?**

   Nicht: Wann wurde gesichert. Sondern: Wann wurde eine Wiederherstellung mit dokumentiertem Ergebnis durchgeführt — vorlagefähig gegenüber Auditoren, Kunden, Cyberversicherern oder Datenschutzbeauftragten?

2. **Liegt das Backup außerhalb der Angreifer-Reichweite?**

   Moderne Ransomware kompromittiert zuerst die Backup-Infrastruktur. Ein Backup im selben Active Directory ist eine zweite Kopie der zu verschlüsselnden Daten — kein Backup.

3. **Sind archivierte Daten über Jahrzehnte nachweisbar lesbar?**

   Archivfristen von 10–30 Jahren. Können Sie belegen, dass Kunden-, Projekt-, Vertrags- und Geschäftsdaten unverändert und maschinell auswertbar wiederherstellbar sind?

Wenn auch nur eine dieser Antworten unklar ist — dieses Whitepaper zeigt, was fehlt und was zu tun ist.

Warum Datenpannen heute mehr als ein IT-Problem sind

Datenpannen sind in jedem Unternehmen kritisch. Heute betreffen sie jedoch weit mehr als nur die IT-Abteilung. Ein Sicherheitsvorfall kann gleichzeitig Datenschutzpflichten auslösen, Betriebsabläufe unterbrechen, Kundenbeziehungen belasten und wirtschaftliche Schäden verursachen. Hinzu kommen Anforderungen von Cyberversicherungen, Auditoren und Geschäftspartnern, die zunehmend Nachweise über Wiederherstellbarkeit und Datensicherheit verlangen.

DSGVO & Compliance

Art. 32 DSGVO · Art. 83 Bußgeld
Stand der Technik als Pflicht. Bußgeldrahmen trifft Unternehmen jeder Größe. Datenschutzbeauftragte zeigen wachsende Intoleranz gegenüber vermeidbaren Datenpannen.

Kunden- & Geschäftsdaten

Art. 33 & 34 DSGVO
Kunden-, Vertrags-, Finanz- und Projektdaten gehören zu den wertvollsten Vermögenswerten eines Unternehmens. Bei einem Sicherheitsvorfall ist das Unternehmen zur Meldung verpflichtet.

Geschäftsrisiko & Haftung

Betriebsunterbrechung · Umsatzverlust · Haftungsrisiken
Datenverlust kann zu Betriebsunterbrechungen, Vertragsstrafen, Umsatzausfällen und Reputationsschäden führen.

NIS2 & Lieferketten

NIS2UmsuCG · seit 6.12.2025 in Kraft
Viele Unternehmen werden direkt oder indirekt von NIS2-Anforderungen betroffen sein. Kunden verlangen zunehmend Nachweise zur Cyberresilienz.

Fazit: Eine Datenpanne ist heute gleichzeitig ein Datenschutz-, Compliance-, Betriebs- und Geschäftsrisiko.

Was Standard-Setups leisten — und wo sie systematisch ausfallen

Der nachfolgende Vergleich basiert auf den Strukturen, die in kleinen und mittelgroßen Unternehmen anzutreffen sind. Er ist nicht als Kritik an einzelnen Anbietern oder externen Rechenzentren gemeint, sondern beschreibt eine strukturelle Lücke: Die meisten unternehmerischen IT-Setups sind für den Normalbetrieb dimensioniert. Datensicherung wird im Ernstfall jedoch unter Bedingungen gebraucht, die nicht der Normalbetrieb sind.

✗ Standard heute

ISOLATION
Backup im selben Active Directory. Bei Domain-Admin-Kompromittierung ebenfalls erreichbar.

WORM
Dateisystem-Sicherung mit denselben Rechten löschbar wie Quelldaten.

VERSCHLÜSSELUNG
Symmetrische Verfahren. Nicht geeignet für langfristig archivierte Bestände.

RESTORE-NACHWEIS
Restore-Tests ad hoc oder gar nicht. Dokumentiert werden Sicherungsläufe, nicht Wiederherstellungen.

✓ Tragfähig

ISOLATION
Getrennte Authentifizierung. Kein lateraler Zugriff aus der Produktiv-Domäne.

WORM
Storage-seitige Unveränderbarkeit. Auch Admins des Dienstleisters können nicht überschreiben.

VERSCHLÜSSELUNG
Post-Quantum: CRYSTALS-Kyber-1024 (NIST FIPS 203) + AES-256. Auch gegen Quantencomputer.

RESTORE-NACHWEIS
Automatisierte Tests. Auditierbarer Bericht — vorlagefähig für Audits, Compliance-Nachweise und Cyberversicherungen.

Die rechte Spalte beschreibt das, was DSGVO Art. 32 als „Stand der Technik" verlangt — in 2026.

Die Bedrohungslage hat sich grundlegend verändert

Drei Entwicklungen haben die Anforderungen an Datensicherung in den letzten Jahren grundlegend verschoben. Wer noch mit dem Sicherungskonzept von 2018 arbeitet, schützt sich gegen die Angriffe von 2018.

01

Unternehmen im Fadenkreuz

BSI: Steigende Angriffszahlen auf Unternehmen und kritische Infrastrukturen. Die Liste der Angriffe wächst jährlich. Moderne Ransomware kompromittiert zuerst die Backup-Infrastruktur, dann erst verschlüsselt sie.

02

„US-Cloud“ ist kein Datenstandort

US CLOUD Act: Gilt auch bei EU-Rechenzentren von US-Anbietern. US-Anbieter müssen Daten auf Anforderung der US-Behörden herausgeben — unabhängig vom RZ-Standort. Für Kunden-, Finanz- und Geschäftsdaten ist das eine Frage der digitalen Souveränität.

03

Verschlüsselung von morgen

„Harvest now, decrypt later“: Quantencomputer im 10–15-Jahres-Horizont. Archivfristen von 20+ Jahren. Angreifer sammeln heute verschlüsselte Daten, um sie später mit Quantencomputern zu entschlüsseln.

04

Heute post-quantum denken

Wer 2018er-Verschlüsselung nutzt, schützt gegen 2018er-Angriffe. Das bedeutet: Wer heute archiviert, muss heute mit Post-Quantum verschlüsseln — nicht erst, wenn Quantencomputer verfügbar sind.

Wenn auch nur eine dieser Antworten unklar ist — dieses Whitepaper zeigt, was fehlt und was zu tun ist.

groupios Multi-Node Backup — wie es funktioniert

Das Multi-Node Backup ist keine zusätzliche Schicht über einem klassischen Backup. Es ist eine eigenständige Architektur, die auf den oben beschriebenen Anforderungen aufbaut – fragmentiert, post-quantum-verschlüsselt, geografisch verteilt, unveränderbar. Die nachfolgende Beschreibung orientiert sich an den Anforderungen, die moderne Unternehmens-IT heute erfüllen muss.

Fragmentierung statt Replikation

Datei wird in tausende Segmente zerlegt. Kein Segment enthält rekonstruierbare Information. Kompromittierter Standort = wertlose Fragmente.

Post-Quantum + AES-256

CRYSTALS-Kyber-1024 + AES-256: NIST FIPS 203 (Kyber) für Schlüsselkapselung, AES-256 für Datenverschlüsselung.

Seit 2024 standardisiert

Der aktuelle NIST-Standard für quantensichere Verschlüsselung. Clientseitig vor Übertragung. Schutz für langfristig aufbewahrte Unternehmensdaten und Archive.

Geografische EU-Verteilung

Fragmente auf mehrere EU-Standorte mit unterschiedlichen Betreibern. Zugriff durch außereuropäische Behörden rechtlich und technisch ausgeschlossen.

Unveränderbarkeit (WORM)

Innerhalb der Aufbewahrungsfrist technisch nicht veränderbar — auch nicht durch groupios-Administratoren. Anforderungen an revisionssichere Datenspeicherung objektiv erfüllt.

Nachweisbare Wiederherstellbarkeit

Regelmäßige automatisierte Restore-Tests mit auditierbarem Bericht. Vorlagefähig für Auditoren, Datenschutzbeauftragte und Cyberversicherungen.

Was wir zusagen — konkret und vertraglich

Eine Datensicherungslösung muss in den internen IT-Alltag passen — auch unter den Rahmenbedingungen gewachsener IT- und Prozesslandschaften. Konkret heißt das:

Drei belastbare Zusagen für Planung und Betrieb

01 | PLANBAR

Kalkulierbare Kosten

Keine Lastspitzen bei Wiederherstellungen. Was Sie sichern, kostet im Ernstfall nicht mehr. Transparent kalkulierbar für Budgetplanung und Investitionsentscheidungen.

RPO 24 h · Datenverlust max. 24 h · optional bis 1 h

02 | UMSETZBAR

Implementierung in 4–6 Wochen

Kein Hardware-Invest. Kein Bruch mit bestehenden Strukturen. Einführung durch unser Team in Abstimmung mit Ihrer IT — ohne tiefe IT-Sicherheitskompetenz im Unternehmen erforderlich.

RTO < 4 h · Einzelpostfach/OneDrive · E-Mail/Datei < 30 Min.

03 | SKALIERBAR

Skaliert mit Ihrem Unternehmen

Von 500 GB bis 50 TB und mehr. Aufbewahrungsfristen individuell konfigurierbar – abgestimmt auf gesetzliche, vertragliche und unternehmensinterne Anforderungen. Keine versteckten Migrationskosten.

99,9 % SLA · Backup-Infrastruktur vertraglich zugesichert · DE RZ · kein US-Konzernzugriff

Vertrauen ist eine Konstruktion — hier sind die Bausteine

In einer Branche, die selbst von Vertrauen lebt, ist die Frage nach dem Anbieter genauso wichtig wie die Frage nach der Technik. Wir formulieren das offen:

Rechtssitz Deutschland

step3IT GmbH, Neumünster, gegr. 2015. Keine außereuropäische Mutter- oder Holdinggesellschaft. Gerichtsbarkeit: deutsch.

ISO 27001 & ISO 9001

Zertifiziert für Informationssicherheits-Management. Anerkannter Nachweis für Auditoren, Datenschutzbeauftragte und Compliance-Verantwortliche.

Schlüsselhoheit Kunde

Kryptografische Schlüssel verbleiben ausschließlich bei Ihrem Unternehmen. Datenzugriff durch step3IT technisch ausgeschlossen.

Erfahrung in regulierten Umgebungen

Backup-Lösungen für Unternehmen mit hohen Anforderungen an Datenschutz, Compliance und Informationssicherheit.

2015	ISO	100%	0
Gründungsjahr	27001 & 9001*	EU-Datenhaltung	US-Abhängigkeiten bei der Backup-Infrastruktur
	*(in Umsetzung • Ziel: Okt 2026)		

In 45 Minuten zeigen wir Ihnen live, ob Ihre Daten heute wirklich wiederherstellbar sind — anhand Ihrer eigenen Umgebung. Kein Verkaufsgespräch, sondern ein konkreter Nachweis.

Nachweisbar handlungsfähig — technisch, rechtlich und operativ:

- ✓ Geschäfts-, Kunden- und Projektdaten liegen fragmentiert auf mehreren EU-Standorten.
- ✓ CRYSTALS-Kyber-1024 + AES-256 — Stand der Technik inkl. Post-Quantum-Schutz.
- ✓ Wiederherstellungstests finden regelmäßig statt, Protokoll auditier- und nachweisbar.
- ✓ Dienstleister nach ISO 27001/9001 zertifiziert, Sitz im EU-Rechtsraum.
- ✓ Vollständiger Restore eines Postfachs — live, nicht als Screencast.
- ✓ Granulare Wiederherstellung einzelner E-Mails oder Dateien.
- ✓ Auditierbares Protokoll wird direkt mitgeliefert.
- ✓ Ihre Fragen an die Architektur — keine Sales-Präsentation.
- ✓ Prüfung des nachweisbaren Backup- und Restore-Konzeptes für Cyberversicherungen.

Diese Aussagen sind nicht Marketing — sie sind auditierbar. Aus Datenschutzgründen nennen wir keine Kundennamen. Das ist genau der Standard, den wir für Ihre Daten anwenden.

Sales & Beratung: +49 4321 539 942 0 · sales@groupios-mare.cloud · www.groupios-mare.cloud