

Souveräne Wiederherstellbarkeit

Warum Unternehmen jetzt prüfen sollten, ob ihre Microsoft 365®-Daten im Ernstfall wirklich wiederherstellbar sind.

MADE IN GERMANY

DSGVO-KONFORM

CLOUD-ACT-FREI

Drei Fragen, die Sie sich jetzt stellen sollten

Die Digitalisierung kleiner und mittlerer Unternehmen schreitet mit hoher Geschwindigkeit voran. KMU setzen zunehmend auf cloudbasierte Anwendungen wie Microsoft 365®, um Geschäftsprozesse zu digitalisieren, mobiles Arbeiten zu ermöglichen und ihre Wettbewerbsfähigkeit zu sichern.

1. Wissen wir, wo unsere Daten liegen?

Welche Microsoft 365®-Daten, Geschäftsdokumente, Kundeninformationen und Projektdaten liegen in welcher Cloud?

2. Können wir unabhängig wiederherstellen?

Die entscheidende Frage lautet nicht: „Microsoft 365 ist verfügbar“. Sondern: Können wir gelöschte, verschlüsselte oder manipulierte Daten aus einer getrennten Sicherung nachweisbar wiederherstellen?

3. Gibt es eine Backup- und Cyberresilienzstrategie?

Sind Schlüsselhoheit, EU-Datenhaltung, Exit-Fähigkeit, Restore-Tests und Anbieterabhängigkeiten dokumentiert und entscheidungsfähig bewertet?

Wenn auch nur eine dieser Antworten unklar ist, ist dieses Whitepaper für Sie geschrieben.

Warum jetzt: Ihre Cloud-Daten sind geschäftskritisch

Viele Unternehmen geraten zunehmend in eine technologische Abhängigkeit von wenigen Cloud-Anbietern. Gleichzeitig steigt die Bedrohung durch Ransomware, Kontoübernahmen und Datenmanipulationen. Gerade deshalb fordern Cyberversicherungen zunehmend dokumentierte Backup- und Wiederherstellungsprozesse als Voraussetzung für Versicherungsschutz. Zusätzlich erhöhen regulatorische Anforderungen wie NIS2 und DSGVO den Druck auf Unternehmen, ihre Wiederherstellungsfähigkeit nachweisbar sicherzustellen.

Cyberfälle treffen den Mittelstand unmittelbar

Laut BSI gehören Ransomware-Angriffe weiterhin zu den größten Risiken für Unternehmen. Besonders KMU sind betroffen, da Ausfälle unmittelbar zu Produktions-, Umsatz- und Reputationsschäden führen können. Das ist kein abstraktes Risiko.

Microsoft 365 ist Plattform — nicht Ihr vollständiger Recovery-Plan

Im Shared-Responsibility-Modell bleiben Kundendaten, Identitäten, Konfiguration, Aufbewahrung und Wiederherstellung in wesentlichen Teilen Aufgabe der Organisation.

EU-Speicherort allein löst nicht jedes Souveränitätsrisiko

US CLOUD Act: Selbst wenn Ihre M365-Daten in Frankfurt liegen, kann eine US-Behörde Microsoft zur Herausgabe verpflichten — ohne Ihr Wissen und ohne deutschen Gerichtsbeschluss.
EU-Speicherort schützt nicht vor US-Zugriff.

Nachweise werden wichtiger als Behauptungen

DSGVO Art. 32 fordert u. a. Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit. NIS2 erhöht den Druck auf Cyberresilienz, Lieferketten- und Dokumentationsfähigkeit.

Der kritische Irrtum: Plattformverfügbarkeit ist kein Backup

Viele Unternehmen setzen darauf, dass ein Hosting in europäischen Rechenzentren ausreicht. Ein norddeutsches Produktionsunternehmen mit 80 Mitarbeitern oder eine Steuerkanzlei mit 20 Berater*innen stellt sich dieselbe Frage: Sind unsere M365®-Daten wirklich unter unserer Kontrolle — oder nur unter der von Microsoft?

Was Microsoft®, Google® und AWS® zuverlässig adressiert

- Verfügbarkeit und Betrieb der Plattform
- Rechenzentrums-Redundanz
- Schutz der Cloud-Infrastruktur
- Service-Updates und Patches
- Grundlegende Sicherheitsfunktionen

Was bei Ihnen entscheidend bleibt

- Nachweisbare Wiederherstellung nach Löschung
- Schutz vor kompromittierten Accounts
- Granulares Restore einzelner Objekte
- Aufbewahrung außerhalb nativer Fristen
- Dokumentation für Datenschutzbeauftragte, Auditoren, Geschäftsführung und IT-Leitung

Kernfrage für Geschäftsführung und IT-Verantwortliche: Können wir einen Restore nicht nur behaupten, sondern demonstrieren und protokollieren?

Was im Vorfall wirklich zählt: Geprüfte Wiederherstellung

Praxisbeispiel: Ransomware-Angriff auf ein mittelständisches Unternehmen

Tag 0

Angriff: Konto kompromittiert

Kompromittiertes M365®-Konto. Angreifer verschlüsseln OneDrive® und SharePoint®-Bibliotheken innerhalb von 4 Stunden.

Tag 1-3

Ausfall: Fehler spät erkannt

Produktionsplanung, Projektunterlagen und Kundendokumente stehen nicht mehr zur Verfügung. Mitarbeiter können nicht auf zentrale Daten zugreifen.

Tag 4-21

Wiederherstellung: Betrieb unter Druck

Schaden: Forensik, Wiederaufbau und Betriebsunterbrechungen verursachen hohe Kosten. Ohne unabhängiges Backup sind wichtige Daten nur teilweise wiederherstellbar.

Ergebnis

Entscheidungspunkt

Je nach Unternehmensgröße können Ausfallkosten innerhalb weniger Tage sechs- bis siebenstelligen Beträge erreichen.

Mit Cloud2Cloud-Backup: vollständige Wiederherstellung in < 4 Stunden möglich.

Ein Cloud-Datenvorfall wird nicht durch gute Absichten beherrschbar, sondern durch einen vorab getesteten Restore-Pfad.

groupios Mare Cloud — Was die Cloud2Cloud-Backup-Lösung konkret leistet

Die Lösung ermöglicht die unabhängige Sicherung wichtiger Cloud-Daten aus Plattformen wie Microsoft 365®, Exchange Online®, OneDrive®, SharePoint® oder Teams®. Im Mittelpunkt steht dabei nicht nur die reine Datensicherung, sondern vor allem die Wiederherstellung digitaler Kontrolle und Souveränität.

Vollabdeckung M365®

Exchange Online®, SharePoint®, OneDrive®, Teams®-Chats, Kalender, Kontakte – granular pro Nutzer sicherbar.

RPO < 24h / RTO < 4h

Wiederherstellung einzelner E-Mails, Dateien oder ganzer Postfächer in definierten Zeitfenstern.

Schlüsselhoheit bei Ihnen

step3IT besitzt keinen Zugriff auf Ihre Daten. Wiederherstellung ohne Ihre Mitwirkung ist technisch unmöglich.

DSGVO-konform & EU-only

Datenspeicherung ausschließlich in deutschen Rechenzentren. Kein US-Mutterkonzern, keine CLOUD-Act-Exposition.

ISO 27001

Vollständig zertifiziertes ISMS. Auditberichte und Nachweise für Datenschutzbeauftragte, Auditoren, Kunden und Cyberversicherer.

Auditierbare Protokolle

Jede Backup- und Restore-Operation wird revisionssicher dokumentiert — für Audits, Compliance-Anforderungen und interne Governance.

Der pragmatische Prüfpfad: Von einem Verdacht zur Entscheidung

Eine Datensicherungslösung muss zum Unternehmen passen — auch unter den Rahmenbedingungen interner IT, externer Rechenzentren und langfristig gewachsener IT- und Prozesslandschaften. Deshalb empfehlen wir Ihnen:

Unser 3-Phasen-Aktionsplan zur unternehmerischen Cyberresilienz

step1 | 0–2 Wochen

Assessment

Cloud-Daten und kritische Workloads erfassen
Bestehende Retention/Backups bewerten
Risikoanalyse kritischer Geschäftsprozesse durchführen

Ergebnis:
Lückenbild + Angebotsumfang

step2 | 3–6 Wochen

Pilot / Nachweis

Tenant-Scope und Sicherungsziele festlegen
Beispiel-Backups und Restore-Demo durchführen
RPO/RTO, Protokolle und Rollenmodell prüfen

Ergebnis:
technische Entscheidungsgrundlage

step3 | 7–12 Wochen

Einführung

Produktivsetzung mit dokumentiertem Betriebsmodell
Restore-Testplan und Eskalationsweg vereinbaren
Compliance-, Versicherungs- und Audit-Anforderungen dokumentieren

Ergebnis:
handlungsfähige Recovery-Strategie

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. Gerichtsstand und anwendbares Recht: Deutschland.

ISO 27001 & ISO 9001

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

Schlüsselhoheit Kunde

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

Erfahrung in hochregulierten Umgebungen

Backup-Lösungen für Unternehmen mit hohen Anforderungen an Datenschutz, Compliance und Informationssicherheit. Aus Datenschutzgründen nennen wir keine Kundennamen — das ist genau der Standard, den wir für Ihre Daten anwenden.

2015

Gründungsjahr

ISO

27001 & 9001*
*(in Umsetzung • Ziel: Okt 2026)

100%

EU-Datenhaltung

0

US-Abhängigkeiten bei der
Backup-Infrastruktur

In 45 Minuten zeigen wir Ihnen live, ob Ihre M365®-Daten heute wirklich wiederherstellbar sind — anhand Ihrer eigenen Umgebung. Kein Verkaufsgespräch, sondern ein konkreter Nachweis.

So erfahren Sie, ob Ihr Unternehmen im Ernstfall handlungsfähig bleibt:

- ✓ Assessment Ihrer aktuellen M365®-Backup- und Restore-Fähigkeit
- ✓ Konkreter Leistungs- und Preisrahmen nach Workloads, Nutzern und Aufbewahrungsdauer
- ✓ Live-Restore-Demo mit dokumentiertem Ergebnis
- ✓ Nachweispaket: AVV/TOMs, Datenhaltung, Schlüssel, Rollen, Auditstatus
- ✓ RPO/RTO, Eskalationsweg und Betriebsmodell als Entscheidungsgrundlage
- ✓ Prüfung des nachweisbaren Backup- und Restore-Konzepts für Cyberversicherungen

Live-Nachweis einer vollständigen Wiederherstellung anhand realer Microsoft 365®-Daten

Sales & Beratung:

☎ +49 4321 539 942 0 ·

✉ sales@groupios-mare.cloud ·

🌐 www.groupios-mare.cloud