

Souveräne Wiederherstellbarkeit

Warum Städte und Kommunen jetzt prüfen sollten, ob ihre Microsoft 365®-Daten im Ernstfall unabhängig wiederherstellbar sind.

MADE IN GERMANY

DSGVO-KONFORM

CLOUD-ACT-FREI

Drei Fragen, die Sie sich jetzt stellen sollten

Städte und Kommunen nutzen zunehmend cloudbasierte Anwendungen wie Microsoft 365®, um Verwaltungsprozesse zu digitalisieren, mobiles Arbeiten zu ermöglichen und Bürgerdienste zu modernisieren.

1. Wissen wir, wo unsere Daten liegen?

Welche M365®-Daten und Verwaltungsdokumente liegen in welcher Cloud – und wer kann technisch, administrativ oder rechtlich darauf zugreifen?

2. Können wir unabhängig wiederherstellen?

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

3. Gibt es eine kommunale Souveränitätsstrategie?

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

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

Warum jetzt: Kommunale Cloud-Daten sind betriebsrelevant

Kommunen geraten zunehmend in technologische Abhängigkeit von wenigen Cloud-Anbietern. Gleichzeitig steigt die Bedrohung durch Ransomware, Kontoübernahmen und Datenmanipulationen. Regulatorische Anforderungen wie DSGVO, NIS2 und das BSI-Recht erhöhen zusätzlich den Druck, Wiederherstellungsfähigkeit, Lieferketten und Verantwortlichkeiten nachvollziehbar zu dokumentieren.

Cyberfälle treffen Verwaltungen unmittelbar

Der BSI-Lagebericht beschreibt einen Angriff auf einen kommunalen IT-Dienstleister mit 72 betroffenen Kommunen, rund 20.000 Arbeitsplätzen und etwa 1,7 Millionen Einwohnerinnen und Einwohnern. Das ist kein abstraktes Risiko.

EU-Speicherort allein löst nicht jedes Souveränitätsrisiko

US CLOUD Act: Auch bei EU-Speicherung können US-Behörden Anbieter wie Microsoft zur Herausgabe verpflichten. Der Speicherort allein verhindert keinen Zugriff nach US-Recht.

Microsoft 365 ist Plattform — nicht Ihr vollständiger Recovery-Plan

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

Nachweise werden wichtiger als Behauptungen

DSGVO Art. 32 fordert Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit. NIS2 und BSI-Recht erhöhen den Druck auf Cyberresilienz, Lieferketten und Dokumentationsfähigkeit.

Der kritische Irrtum: Plattformverfügbarkeit ist kein Backup

Viele Kommunen gehen davon aus, dass ein Hosting in europäischen Rechenzentren bereits vollständige Kontrolle garantiert. Entscheidend bleibt jedoch: Sind die M365®-Daten der Verwaltung wirklich unabhängig wiederherstellbar – oder nur innerhalb der Plattform verfügbar?

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 Datenschutz, Rechnungsprüfung, Verwaltungsspitze und IT-Leitung

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

Was im Vorfall wirklich zählt: geprüfte Wiederherstellung

Praxisbeispiel: Ransomware-Angriff auf eine Kreisverwaltung

Tag 0

Angriff: Konto kompromittiert

Ein kompromittiertes M365®-Konto ermöglicht die Verschlüsselung von OneDrive®- und SharePoint®-Daten innerhalb weniger Stunden.

Tag 1-3

Ausfall: Fehler spät erkannt

Bürgerdienste sind eingeschränkt. Standesamt, Kfz-Zulassung und Sozialleistungen können nicht zuverlässig auf zentrale Daten zugreifen.

Tag 4-21

Wiederherstellung: Betrieb unter Druck

Schaden: Forensik, Wiederaufbau und eingeschränkte Verwaltungsleistungen verursachen erheblichen Aufwand. Ohne unabhängiges Backup bleibt oft nur eine Teilwiederherstellung.

Ergebnis

Entscheidungspunkt

Bürgerdienste, interne Abläufe und Krisenkommunikation können über Tage oder Wochen beeinträchtigt bleiben.

Mit Cloud2Cloud Backup: Wiederherstellung innerhalb definierter RTO-Ziele.

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 sichert wichtige kommunale Cloud-Daten aus Microsoft 365®, Exchange Online®, OneDrive®, SharePoint® und Teams® unabhängig. Im Mittelpunkt stehen nicht nur Datensicherung, sondern nachweisbare Wiederherstellung, digitale Kontrolle und kommunale 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

Zertifiziertes ISMS mit Auditberichten und Nachweisen für Datenschutzbeauftragte, Rechnungsprüfung, Kommunalaufsicht und Cyberversicherer.

Auditierbare Protokolle

Backup- und Restore-Operationen werden nachvollziehbar dokumentiert – für Rechnungsprüfung, Datenschutzaufsicht, Audits und interne Governance.

Der pragmatische Prüfpfad: vom Verdacht zur Entscheidung

Eine Datensicherungslösung muss in den Verwaltungsalltag passen – unter den Rahmenbedingungen kommunaler IT, kommunaler Rechenzentren und langjährig gewachsener Fachverfahrens- und Prozesslandschaften. Deshalb empfehlen wir Ihnen:

Unser 3-Phasen-Aktionsplan zur kommunalen Cyberresilienz

step1 | 0–2 Wochen

Assessment

Cloud-Daten und kritische Workloads erfassen
Bestehende Aufbewahrung und Backups bewerten
Risiko- und Schutzbedarfsprofil erstellen

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
DSGVO-, NIS2- und Audit-Anforderungen dokumentieren

Ergebnis:
handlungsfähige Recovery-Strategie

Vertrauen ist eine Konstruktion — hier sind die Bausteine

Öffentliche Verwaltung lebt von Vertrauen. Deshalb 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 Datenschutzbeauftragte, Rechnungsprüfung und kommunale Compliance-Verantwortliche.

Schlüsselhoheit Kunde

Kryptografische Schlüssel verbleiben ausschließlich bei Ihrer Kommune. Datenzugriff durch step3IT ist technisch ausgeschlossen.

Erfahrung in hochregulierten Umgebungen

Backup-Lösungen für Organisationen mit Auditpflichten, Meldewegen und öffentlicher Verantwortung. Aus Datenschutzgründen nennen wir keine Kundennamen – derselbe Maßstab gilt für Ihre Daten.

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 wirklich wiederherstellbar sind — anhand Ihrer eigenen Umgebung. Kein Verkaufsgespräch, sondern ein konkreter Nachweis.

So erfahren Sie, ob Ihre Kommune 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/TOM, Datenhaltung, Schlüssel, Rollen und Auditstatus
- ✓ RPO/RTO, Eskalationsweg und Betriebsmodell als Entscheidungsgrundlage
- ✓ Einordnung des Backup- und Restore-Konzepts für Datenschutz, Audit und Cyberversicherung

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