groupios
Mare Cloud

ENTSCHEIDER-WHITEPAPER – Multi-Node-Backup

Datensicherheit für Städte & Kommunen

Was nach DSGVO, Sozialdatenschutz, NIS2 und Archivrecht wirklich zählt—und woran die meisten kommunalen Backup-Konzepte scheitern.

MADE IN GERMANY

POST-QUANTUM

EU-VERTEILT

AI

Drei Fragen, die jede Kommunalverwaltung Beantworten muss

Städte und Kommunen arbeiten unter einer Risikolage, die in kaum einem anderen Bereich deröffentlichen Hand so vollständig zusammenfällt: Pflicht zur Sicherstellung der Daseinsvorsorge, hochsensible Datenbestände aus Meldewesen, Sozial-, Jugend- und Gesundheitsverwaltung, langjährige Archivierungs- und Aufbewahrungspflichten — und in der Praxis IT-Strukturen, die diesen Anforderungen oft nicht standhalten.

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

   Nicht: Wann wurde gesichert. Sondern: Wann wurde eine Wiederherstellung mit dokumentiertem Ergebnis durchgeführt — vorlagefähig gegenüber Rechnungsprüfung und Aufsicht?

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 Bürger-, Sozial- und Verwaltungsdaten 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 eine Datenpanne in Kommunen rechtlich anders wirkt

Datenpannen sind in jeder Organisation unangenehm. In einer Kommunalverwaltung sind sie etwas anderes: ein gleichzeitiger Vorgang im Datenschutzrecht, im Sozialdatenrecht, im ITSicherheitsrecht, gegebenenfalls im Strafrecht — und in der politischen Verantwortung der Verwaltungsspitze gegenüber Rat, Aufsicht und Bürgerschaft. Die Verkettung dieser Ebenen ist es, was die Risikolage der kommunalen Ebene von der eines durchschnittlichen Mittelständlers unterscheidet.

DSGVO & Landesdatenschutz

Art. 32 DSGVO · Art. 83 Bußgeld
Stand der Technik als Pflicht. Bußgeldrahmen trifft formal auch die öffentliche Hand. Landesdatenschutzbeauftragte zeigen wachsende Intoleranz gegenüber vermeidbaren Datenpannen.

Sozialdatenschutz SGB

§ 78a SGB X · §§ 67 ff. SGB X · § 35 SGB I
Jugendamt, Sozialamt, Jobcenter, Gesundheitsamt: Schutzanforderungen über DSGVO-Niveau. Datenverlust = sozialrechtlicher Vorgang mit eigener Meldekette und Aufsicht.

NIS2 / Eigenbetriebe

NIS2UmsuG · seit 6.12.2025 in Kraft
Kommunale Eigenbetriebe (Wasser, Abfall, ÖPNV, Kliniken) direkt erfasst. Persönliche Geschäftsleiterhaftung. IT-Dienstleister gehört zur Lieferkette — Pflichten reichen in die Verwaltung.

Straf- & Dienstrecht

§ 203 StGB · § 353b StGB · Beamtenrecht
Verletzung von Privat-geheimnissen durch Amtsträger strafbewehrt. Fahrlässigkeit reicht. Vermeidbarer Datenverlust hat persönliche Konsequenzen für Verwaltungsleitung und Bürgermeister.

Fazit: Eine Datenpanne ist datenschutzrechtlicher, sozialdatenschutz-rechtlicher, strafrechtlicher und politischer Vorgang — in einem Ereignis.

Was kommunale Standard-Setups leisten — und wo sie systematisch ausfallen

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

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 Sicherungs-konzept von 2018 arbeitet, schützt sich gegen die Angriffe von 2018.

01

Städte und Kommunen sind ins Fadenkreuz gerückt

Sachsen-Anhalt, Bitterfeld 2021: Katastrophenfall · BSI: steigende Angriffszahlen
Rhein-Pfalz-Kreis, Kr. Düren, Schwerin, Witten, Potsdam — die Liste wächst. 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 Meldedaten, Sozialdaten und Gesundheitsdaten ist das eine Frage der digitalen Souveränität.

03

Daten müssen die Verschlüsselung von morgen aushalten

„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

Wer 2018er-Verschlüsselung nutzt, schützt gegen 2018er-Angriffe.

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 ordnet sich exakt an den Anforderungen, was kommunales Standard-Setup heute leisten müsste.

Fragmentierung statt Replikation

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

Post-Quantum: CRYSTALS-Kyber-1024 + AES-256

NIST FIPS 203 (Kyber) für Schlüsselkapselung, AES-256 für Datenverschlüsselung.

Clientseitig vor Übertragung

Schutz über kommunale Archivhorizonte von 20+ Jahren.

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. Archivrechtliche Anforderung objektiv erfüllt.

Nachweisbare Wiederherstellbarkeit

Regelmäßige automatisierte Restore-Tests mit auditierbarem Bericht. Vorlagefähig für Rechnungsprüfung und Landesdatenschutzbeauftragte.

Was wir zusagen – konkret und vertraglich

Eine Datensicherungslösung muss in den Verwaltungsalltag passen — auch unter den Rahmenbedingungen kommunaler IT, kommunaler Rechenzentren und langjährig gewachsener Fachverfahrensstrukturen. 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 Haushaltsplan und Gemeinderatsbeschluss.

RPO 24h · Wiederherstellungspunkt · Datenverlust maximal 24 Stunden · konfigurierbar bis 1h (Option)

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 in der Verwaltung erforderlich.

RTO < 4h · Einzelpostfach / OneDrive · Einzelne E-Mail oder Datei in unter 30 Minuten

03 | SKALIERBAR

Skaliert mit Ihrer Verwaltung

Von 500 GB bis 50 TB und mehr. Aufbewahrungsfristen individuell konfigurierbar: 7 Jahre für Haushalt, 30 Jahre für Personenstandsdaten. Keine versteckten Migrationskosten.

99,9% · Verfügbarkeits-SLA · Backup-Infrastruktur vertraglich zugesichert · DE RZ · Datenstandort · Ausschließlich Deutschland · 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 Kommunalaufsicht und Landesbeauftragte.

Schlüsselhoheit Kunde

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

Erfahrung hochreguliert

Jede Backup- und Restore-Operation protokolliert. Vorlagefähig für Rechnungs-prüfung und Datenschutzaufsicht

2015
Gründungsjahr

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

100%
EU-Datenhaltung

0
US-Abhängigkeiten bei der Backup-Infrastruktur

Fordern Sie jetzt eine Produktvorführung an - Kein Verkaufsgespräch, sondern ein konkreter Nachweis.

Gegenüber Aufsicht, Rat und Bürgerschaft nachweisbar handlungsfähig.

- ✓ Verwaltungs-, Melde- und Sozialdaten liegen fragmentiert auf mehreren EU-Standorten
- ✓ CRYSTALS-Kyber-1024 + AES-256 — Stand der Technik inkl. Post-Quantum-Schutz
- ✓ Wiederherstellungstests finden regelmäßig statt, Protokoll vorlagefähig
- ✓ Dienstleister nach ISO 27001/9001 zertifiziert, Sitz im EU-Rechtsraum
- ✓ Vollständiger Restore eines Postfachs — live, nicht als Screencast
- ✓ Granulare Wiederherstellung einzelner E-Mail oder Dateien
- ✓ Auditierbares Protokoll wird direkt mitgeliefert
- ✓ Ihre Fragen an die Architektur — keine Sales-Präsentation

Diese Aussagen sind nicht Marketing — sie sind auditierbar

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