Empalis CONSULTING

WebKonferenz IT-Sicherheit aus Deutschland für die öffentliche Verwaltung

Datensouveränität as a Service: Made in Germany

Cyberresiliente, souveräne Backups für die öffentliche Verwaltung – wenn der Ernstfall zählt

DATUM
16. Juli 2026

SPRECHER
Philip Röder · Head of Business Development & Consulting

Empalis CONSULTING

Ihr Referent

Philip Röder

Head of Business Development & Consulting, Empalis Consulting

Sommer 2021, eine deutsche Kreisverwaltung

Als die Verwaltung stillstand

02.06.2021
Der Angriff beginnt. Still. Niemand bemerkt ihn.

06.07.2021
Entdeckung: Ransomware „Grief". Rund 900 Rechner verschlüsselt, 159 Fachverfahren in 20 Ämtern stehen still.

09.07.2021
Erster Cyber-Katastrophenfall Deutschlands. Sozialleistungen nicht auszahlbar.

Dann stellt sich die Frage, die alles entscheidet: die Backups.

Was die Sichtung der Backups ergab – und was sie hätte ergeben können – klären wir heute.

Quelle: KommunalWiki (Böll), heise

Derselbe Fall, nüchtern betrachtet

Was den Ernstfall zur Katastrophe machte

Ein Monat unbemerkt

Angreifer bewegen sich still durchs Netz und bereiten den Schlag in Ruhe vor.

Keine Logs

Forensik blind: nicht einmal der Anmeldezeitpunkt war rekonstruierbar, das Einfallstor ist bis heute unbekannt.

Ein Schlag traf alles

Rund 900 Rechner, 159 Fachverfahren, alle drei Standorte gleichzeitig verschlüsselt.

Nie geprobt

Kein vollständiges Verzeichnis der Fachverfahren, zwei parallele Führungsstäbe in der Krise (BSI-Abschlussbericht).

Hilfe nicht gesichert

Externer Forensik-Dienstleister steigt nach neun Tagen im Finanzierungsstreit aus.

? Und die Backups?

dazu später

Alle Befunde öffentlich dokumentiert.

Quellen: Landkreistag (Vortrag Griebsch) · BSI-Abschlussbericht (via heise) · KommunalWiki (Böll)

Empalis CONSULTING

Unsere Erfahrung zeigt

„Die meisten Backup-Strategien in der Verwaltung erfüllen NIS2 nicht – auch wenn die Compliance-Tabellen grün sind.“

NIS2 = EU-Richtlinie 2022/2555 zur Netz- und Informationssicherheit („Network and Information Security 2“)

Fakten zum Status Quo

Fälle in der öffentlichen Verwaltung

1.041

angezeigte Ransomware-Angriffe 2025 (+10 %) – öffentliche Einrichtungen besonders betroffen

~80 %

der gemeldeten Ransomware-Angriffe treffen KMU und öffentliche Stellen

36.706

DDoS-Angriffe 2025 (+25 %) – Behörden und Verwaltungen im Fokus

10

dokumentierte kommunale IT-Notbetriebe (Mai–Juli 2026)

Quelle: BKA (Bundeskriminalamt) Bundeslagebild Cybercrime 2025 · BSI-Lagebericht 2025 · kommunaler-notbetrieb.de

Neue Pflichten. Ohne Übergangsfrist.

NIS2UmsuCG – seit 06.12.2025 in Kraft

- NIS2UmsuCG (NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) setzt die EU-Richtlinie in deutsches Recht um
- Erweiterter Kreis betroffener Einrichtungen
- §30 BSIG (BSI-Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) verlangt Risikomanagement inkl. Backup-Management
- Melde- und Nachweispflichten
- Keine Übergangsfrist

Souveränität endet nicht am Serverstandort

- Der US CLOUD Act („Clarifying Lawful Overseas Use of Data Act", 2018) erlaubt US-Behörden Zugriff auf Daten US-amerikanischer Anbieter – weltweit
- Auch EU-Rechenzentren von US-Konzernen sind betroffen
- Die Verwaltung trägt die Verantwortung für Bürgerdaten
- Lösung: Betreiber und Infrastruktur ohne US-Rechtsbindung

Quelle: Security-Insider 2025

Europäischer Maßstab

SEAL-Levels – der neue Beschaffungsmaßstab

- EU-Kommission, DG Digital Services, v1.2.1, Oktober 2025
- 8 Sovereignty Objectives („Souveränitätsziele", SOV-1–SOV-8)
- 5 SEAL-Levels (SEAL = „Sovereignty Effectiveness Assurance Level", Souveränitätsstufen 0–4)
- Minimum-SEAL als Ausschluss-, Score als Zuschlagskriterium

Einordnung
Empalis Sovereign Vault (ESV): SEAL-3 bis 4 in den relevanten Objectives.

Quelle: EU-Kommission 2025

EU, Bund, Praxis

Wo Empalis Sovereign Vault die Verwaltung abholt

01

EU-Ebene

Cloud Sovereignty Framework / SEAL

02

Nationale Ebene

DVS – Deutsche Verwaltungscloud-Strategie

03

Praktische Ebene

BSI C5 / IT-Grundschutz

Empalis Sovereign Vault adressiert alle drei Ebenen.

C5 = „Cloud Computing Compliance Criteria Catalogue" – BSI-Anforderungskatalog für Cloud-Dienste · Quelle: BMI – DVS

3-2-1-1-0 – Backup-Architektur für Ernstfälle

3
Kopien

2
Medientypen

1
Offsite

1
Offline
air-gapped / immutable

0
Ungetestete Backups
Recovery-Tests als Pflicht

Unveränderlich. Auch für Admins.

„Object Lock“ – warum Immutability alles ändert

- Einmal geschrieben, nicht löschbar oder veränderbar
- Weder Ransomware noch ein kompromittierter Admin kommen daran vorbei
- WORM-Prinzip („Write Once, Read Many" – einmal schreiben, nie mehr verändern)
- Grundlage für NIS2- und Versicherungsbelege

Das übersehene Prinzip

„Separation of Duties“ – der entscheidende Unterschied

- Backup mit eigenem Zugangsmanagement, getrennt vom Produktionsnetz
- Kein Produktions-Admin hat Schreibzugriff auf das Backup
- Ein kompromittierter Domain-Admin kann das Backup nicht löschen
- Genau an diesem Punkt entscheidet sich die Geschichte vom Anfang

Kein Tape mehr nötig

„Modern Airgap“ – Offsiting ohne Logistik

- Traditionell: Tape-Transport und -Lagerung
- Modern Airgap = logische Trennung + Immutability
- Keine Lieferketten, kein physischer Transport, kein Menschenfehler
- Automatisiert, skalierbar, auditierbar

Empalis Sovereign Vault – souveräner Offsite-Speicher

- Empalis Sovereign Vault (ESV) = Empalis-managed Offsite-Backup auf Basis Impossible Cloud
- Deutsches Unternehmen, deutsches Rechenzentrum, kein CLOUD-Act-Risiko
- Laufende Betriebsausgabe ab 12 €/TB/Monat
- S3-kompatibel (S3 = „Simple Storage Service", der De-facto-Schnittstellenstandard für Objektspeicher) – integriert in bestehende Backup-Software

Für Ihre Daten. Nicht für irgendjemanden.

Was die Verwaltung sichern muss

Fachverfahren
Meldewesen, Steuer, SGB-Verfahren (Sozialgesetzbuch), Wahlsysteme

Bürgerdaten
personenbezogene Daten („PII"), Sozialdaten

Bildungs-IT
Schul- und Hochschulserver

Kommunale Versorgung
Stadtwerke, Energie, Wasser – KRITIS-relevant (Kritische Infrastrukturen)

Verwaltungsleistung
Online-Antragstrecken, E-Akte

Kernmerkmale

Fünf Eigenschaften, die im Ernstfall zählen

01

Datenhoheit

Betreiber, Infrastruktur und Support liegen vollständig in Deutschland.

02

Object Lock

Einmal geschrieben, ist das Backup unveränderlich und nicht löschbar.

03

Separation of Duties

Das Backup ist vom Produktionsnetz und dessen Admins getrennt.

04

Maximale Kontrolle

Zugriff und Wiederherstellung bleiben in Ihrer Hand.

05

Active Recovery Support

Wiederherstellung wird begleitet, getestet und dokumentiert.

Betreiber, Infrastruktur und Support aus Deutschland

- Deutsche Betreibergesellschaft
- Deutsches Rechenzentrum
- Kein CLOUD-Act-Zugriff
- Prozesse konform zu ISO 27001 (internationale Norm für Informationssicherheits-Management) und BSI C5

Active Recovery Support – das Werkzeug für CISOs

- NIS2-konforme Vorfalls-Dokumentation mit Audit-Trail
- Reporting-Vorlagen für BSI-Meldepflichten (24/72 h)
- Belege für Cyber-Versicherer
- Wiederkehrende Recovery-Tests (NIS2-DVO Annex 4.2.6; DVO = Durchführungsverordnung der EU, konkretisiert die technischen Anforderungen)

CISO = Chief Information Security Officer (IT-Sicherheitsverantwortliche:r)

Empalis Sovereign Vault integriert sich in Ihre bestehende Backup-Infrastruktur

Veeam	IBM Storage Protect	Commvault	Cohesity	Rubrik

Kein Austausch der bestehenden Backup-Software nötig.

Planbar. Transparent.

Ab 12 €/TB/Monat – Festpreis

- Inkl. Infrastruktur, Betrieb, Monitoring
- Inkl. Active Recovery Support
- Keine versteckten Egress-Gebühren (Gebühren für ausgehenden Datentransfer)
- Skalierung in Minuten

Marktkontext 2026

Warum jetzt der richtige Zeitpunkt ist

CAPEX = Investitionsausgaben (eigene Hardware kaufen) · OPEX = Betriebsausgaben (als laufender Dienst beziehen)

Eigene Backup-Hardware (CAPEX)

- DRAM-Preise (Arbeitsspeicher) Q1 2026: +50–55 %
- Lieferzeiten 6–12 Wochen
- HDD-Kapazitäten (Festplatten) knapp
- HPE: Preisanpassung nach Bestellung
- NIS2 sofort erfüllen – aber Hardware nicht da

Empalis Sovereign Vault (OPEX)

- Planbare Kosten
- Compliance sofort nachweisbar
- Skalierung in Minuten
- Kein Beschaffungsrisiko
- Als Betriebsausgabe budgetierbar

Quelle: Bitkom / HPE 2026

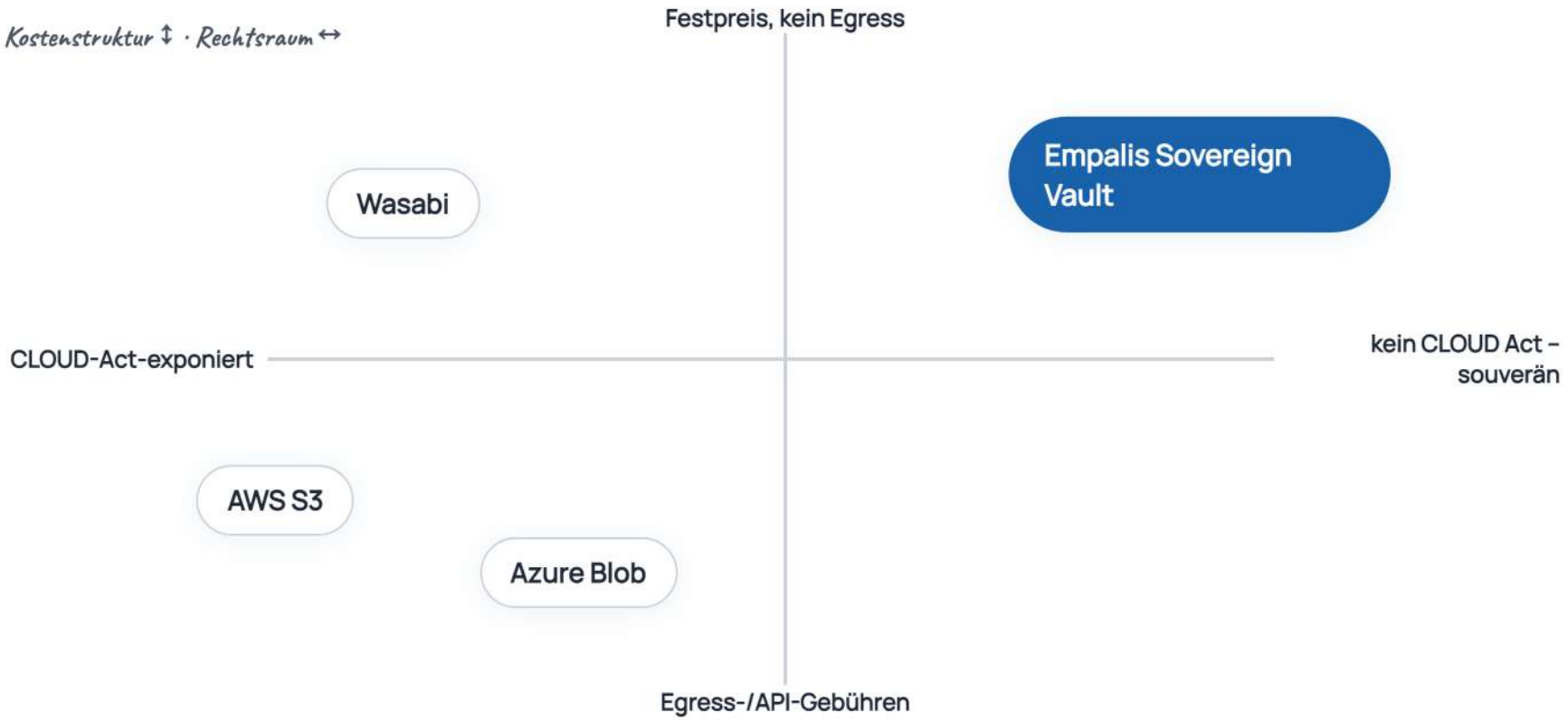
Empalis Sovereign Vault im EU Cloud Sovereignty Framework

SOV	Bezeichnung	ESV-Level	Begründung
SOV-2	Legal & Jurisdictional	SEAL-4	Dt. Betreiber, kein CLOUD Act
SOV-3	Data & AI	SEAL-3	DE/EU-Daten, Object Lock
SOV-4	Operational	SEAL-3 bis 4	Dt. Betrieb, S3-kompatibel
SOV-7	Security & Compliance	SEAL-3	ISO 27001, NIS2-Ready

Selbsteinschätzung. Offizielle Bewertung nur im Beschaffungsverfahren.

Sachlicher Vergleich

Was den Unterschied macht



AWS S3 · Azure Blob · Wasabi · Empalis Sovereign Vault

	AWS S3	Azure Blob	Wasabi	Empalis Sovereign Vault
Rechtsraum	CLOUD Act	CLOUD Act	CLOUD Act	kein CLOUD Act
Betreiber-Nationalität	USA	USA	USA	Deutschland
Egress-Gebühren	ja	ja	nein	nein
Object Lock	ja	ja	ja	ja
Deutscher Support	nein	nein	nein	ja
Active Recovery Support	nein	nein	nein	ja

Zurück zur Geschichte vom Anfang

Von einem Angriff – zwei mögliche Wege

Wendepunkt: Die Frage nach den Backups

Was wäre wenn – mit Empalis Sovereign Vault

RTO: Tage · RPO: nahe Null

Kein Datenverlust, kein Lösegeld

Realer Fall

Keine saubere, vollständige Kopie – Komplett-Neuaufbau statt Restore

Katastrophenfall 207 Tage · Sozialleistungen gestoppt

Nur 80–90 % rekonstruiert, Umweltdatenbank dauerhaft verloren

~2,5 Mio. €

RTO = Recovery Time Objective (Zeit bis zur Wiederherstellung) · RPO = Recovery Point Objective (maximal tolerierter Datenverlust)

Quelle: KommunalWiki (Böll), heise

Ab dem Wendepunkt – mit einer Architektur wie Empalis Sovereign Vault

- Die immutable Offsite-Kopie bliebe unangetastet
- „Separation of Duties“: erbeutete Produktions-Zugänge reichen nicht an die Kopie heran
- Active Recovery Support + Cleanroom-Recovery – vorbereitet statt improvisiert, als Vertragsbestandteil
- RTO in Tagen statt Monaten
- Kein Datenverlust, kein Lösegeld

Empalis CONSULTING

Die Lehre

„Der Unterschied waren nicht Stunden mehr Arbeit – es war eine Architektur-Entscheidung, die Jahre vorher getroffen wird.“

Ihr nächster Schritt

Von heute bis zur Resilienz – drei Stationen

1

Discovery Call

30 Minuten – aktueller Stand, erste Analyse

2

Technical Assessment

Schwachstellenanalyse Ihrer Backup-Architektur

3

PoC

„Proof of Concept" – Testinstallation mit eigenen Daten: Empalis Sovereign Vault in Ihrer Umgebung, ohne Risiko

Lernen Sie uns und Empalis Sovereign Vault (ESV) persönlich kennen

- Vereinbaren Sie gern mit uns einen unverbindlichen Termin:
- https://www.empalis.de/kontakt/termin-vereinbaren/

Vorschau 2. Halbjahr 2026

Empalis Events

20.08.2026 · 10:00–10:30	**Datensouveränität-as-a-Service für KRITIS – made in Germany** WebKonferenz IT-Sicherheit „KRITIS"
28.–30.09.2026 · Track 02 (29.09., 14:15–15:00)	**How to boost resiliency in Storage Protect/Defender in a world of cloud and AI** GSE ISP Symposium · The Westin Leipzig
29.09.2026	**Empalis & Guests – IT.CON 2026** Saarbrücken
20.10.2026	**Empalis Live Experten Talk (ELET): Nachlese GSE ISP Symposium 2026** Empalis Live Experten Talk (ELET)
19.11.2026 · 9:30–10:00	**KI & IT-Sicherheit** WebKonferenz IT-Sicherheit

Bleiben Sie auf dem Laufenden: https://www.empalis.de/wissen/events/

Sprechen wir

Ihr Kontakt zu Empalis

Ansprechpartner

Philip Röder

Rolle

Head of Business Development & Consulting

E-Mail

philip.roeder@empalis.com

Meine Kontaktdaten

Zum Mitnehmen

Die fünf wichtigsten Kernbotschaften

1. Die Prüffrage entscheidet: Kann ein kompromittierter Admin Ihre Backups löschen? Ihre Antwort muss ein belegbares „Nein“ sein.
2. Im Ernstfall zählt die Kopie, nicht die Verschlüsselung – nur eine unveränderliche, getrennte Offsite-Sicherung (Object Lock, Separation of Duties) übersteht den Angriff.
3. NIS2 gilt seit dem 6.12.2025 – ohne Übergangsfrist. Grüne Compliance-Tabellen sind kein Nachweis von Wiederherstellbarkeit.
4. Souveränität ist Beschaffungskriterium: SEAL-Level, deutscher Betreiber und Rechenzentrum, kein CLOUD-Act-Risiko.
5. Empalis Sovereign Vault liefert die souveräne, unveränderliche Offsite-Kopie als Service – inkl. Active Recovery Support. Erster Schritt: Discovery Call, 30 Minuten.

Denn Perfektion geht nur gemeinsam.

Ihre Fragen – wir haben Zeit.

Empalis CONSULTING