Physische Datenhoheit als Pfeiler für Resilienz und Beweissicherung

Warum reine Cloud-Strategien bei Produkthaftung, Bauakten und Gerichtsakten an Grenzen stoßen – und wie physische (WORM)-Speicher Haftungs- und Beweisrisiken fälschungssicher eliminieren.

1. Executive Summary

Die veränderte globale Risikolage fordert eine grundlegende Neuausrichtung: Die Transformation von reiner Prozesseffizienz hin zu unanfechtbarer **operativer und digitaler Resilienz**.

Eine ausschließliche Fokussierung auf hochgradig vernetzte Cloud-Infrastrukturen erzeugt systemische Klumpenrisiken. Politisches Eingreifen, kaskadierende Ausfälle bei internationalen Hyperscalern, automatisierte Ransomware-Angriffe sowie geopolitische Störungen der digitalen Lieferketten zeigen: **Wer im Notfall keinen direkten, netzunabhängigen Zugriff auf seine kritischsten Daten und Backup-Sets hat, riskiert den Stillstand der Organisation und physikalischen Wertschöpfung.**

Eine zukunftsfähige Datenstrategie basiert daher auf **vier komplementären Säulen**:

1. **Cloud-Infrastrukturen als Leistungsträger im Regelbetrieb:** Optimiert für dynamische Prozesse, globale Kollaboration und skalierbare Smart-Workflows.
2. **Physische Datenhoheit zur Absicherung des Kerns:** Gezielte Entkopplung (*Air-Gapping*) für organisationskritische Daten und fälschungssichere Nachweise.
3. **Erweiterte 3-2-1-1-0 Backup-Governance:** Erfüllung der gesetzlichen Pflichten zur Krisenfrüherkennung (§ 1 StaRUG) und Cybersicherheit (EU NIS-2 / Art. 21) durch mindestens eine physisch getrennte, hardware-schreibgeschützte Offline-Kopie.
4. **Herstellergestützte Resilienz für den Standort:** Garantierte Verfügbarkeit von Ersatzkomponenten, Notfall-Data-Sets und Service-Dokumentationen direkt am Standort der Organisation – für den Erhalt der physischen Lauffähigkeit.

Im Ergebnis: Sie kombinieren die Geschwindigkeit der digitalen Cloud mit der unerschütterlichen Autarkie der physischen Datenhoheit.

2. Die 4 praktischen Risikofaktoren reiner Cloud-Strategien im B2B-Umfeld

- **Beweisverlust bei Produkthaftung & Gewährleistung (Industrie):**

Tritt bei einer Maschine oder Anlage nach Jahren ein Schadensfall ein, fordert die Versicherung den lückenlosen Nachweis der CE-Konformität und Wartung. Liegen diese Daten nur auf dynamischen Cloud-Servern, drohen Compliance-Risiken, Beweisverluste durch Systemwechsel, gelöschte Konten oder Datenkorruption.

- **Ablaufende Links & Bauverzögerungen (Baugewerbe):**

Ausführungspläne und Revisionszeichnungen müssen viele Jahre abrufbar bleiben. Werden Baugenehmigungen oder Übergabeprotokolle per Cloud-Link übermittelt, führt der Ablauf des Links oder ein Serverausfall auf der Baustelle zu teuren Stillständen und Rechtsstreitigkeiten.

- **Angreifbarkeit digitaler Beweismittel (Polizei & Justiz):**

Beweismittel und Ermittlungsakten müssen im Straf- und Zivilprozess unanfechtbar sein. Jede Online-Schnittstelle erhöht das Risiko eines Leaks, von Manipulation oder einer Fern-Löschung.

- **Haftung bei Datenverlust (§ 1 StaRUG & NIS-2):**

Entscheidungsträger haften persönlich dafür, dass geschäftskritische Unterlagen vor Verlust und Manipulation geschützt sind. Die alleinige Verwahrung in Dritten-Cloud-Systemen erfüllt bei Kern-Dokumenten nicht die Anforderungen an eine vorsorgliche Risiko-Governance.

3. Physische Datenhoheit für die Praxis

Die 4 Kern-Einsatzfelder in der Praxis:

- **Produkthaftung & Maschinenakten (Industrie):** Unveränderbarer, BSI-konformer Nachweis von Bauanleitungen, Konformitätserklärungen und Prüfberichten über die gesamte Maschinen-Lebensdauer.
- **Bauzeichnungen & Gebäude-Dokumentationen:** Fälschungssichere Archivierung von Plänen, Statikberechnungen und Revisionsakten direkt im Bauordner vor Ort.
- **Beweismittel & Ermittlungsakten (Polizei & Justiz):** Manipulationssichere Verwahrung von digitalen Spuren, Videodateien und Asservaten – physikalisch getrennt vom Internet.

- **Mandanten- & Audit-Akten (Kanzleien & Notare):** Revisionssichere Übergabe vertraulicher Testamente, Verträge und Jahresabschlüsse ohne Abhängigkeit von externen Cloud-Servern.

Höchste Sicherheitsstandards für die Inhouse-Anwendung

Um das Risiko von Schadsoftware beim Einstecken von USB-Medien auszuschließen, setzt das FiLEREX®-System auf industrielle Sicherheitsarchitekturen:

- **ISO 9001 zertifizierte Speicher:** Verwendung geprüfter Chip-on-Board (COB) Bausteine.
- **Hardware-WORM-Schreibschutz (auditSafe©):** Einmal beschrieben, können die Daten auf dem Datenträger weder gelöscht, überschrieben noch von Ransomware verschlüsselt werden.
- **Inhouse-Bespielung an Ihrem Standort:** Absolute Datensouveränität durch die Bespielung kritischer Daten direkt in Ihren Räumen durch Ihr eigenes Personal – ohne Datenabfluss an externe Dienstleister oder Drittländer.

Weiterführende Quellen & Referenzen zur Nachverfolgung

1. **Bundesamt für Sicherheit in der Informationstechnik (BSI):** *Anforderungen an die Revisionssicherheit und Unveränderbarkeit digitaler Archivmedien.*
2. **Deutscher Bundestag / StaRUG & EU NIS-2 Directive:** *Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen (StaRUG § 1)* sowie EU-Richtlinie NIS-2 (Art. 21) zur Pflicht von Führungskräften bezüglich Krisenfrüherkennung und Risikomanagement.
3. **Financial Stability Board (FSB) & Allianz Risk Barometer:** *Analysen zu systemischen Klumpenrisiken von Cloud-Hyperscalern und Betriebsunterbrechungen durch Cyber-Incidents.*