MENT IQ

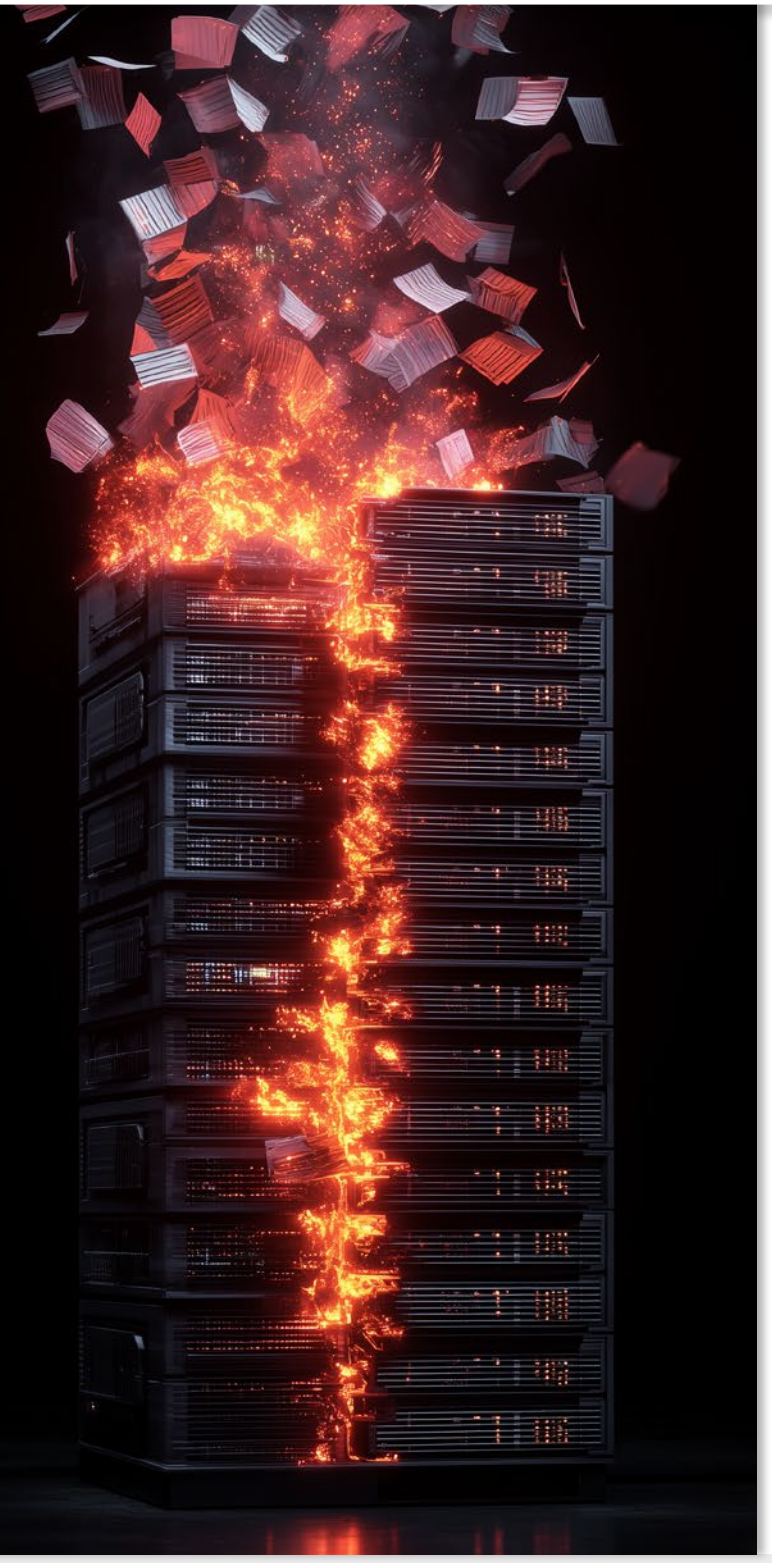
Warum Backups in Zeiten von KI neu gedacht werden müssen

Von Sebastian Wormser, Lead IT Architect,
mentIQ GmbH – Medialine Group

MEDIALINE GROUP

MENT IQ

KI verändert das Risikoprofil – und damit Ihre Backup-Strategie



Ich erlebe in Kundenprojekten immer wieder, wie KI-Systeme heute Entscheidungen treffen, die vor wenigen Jahren undenkbar waren: Automatisierte Analysen identifizieren Risiken, generative Assistenten schreiben Code oder administrieren Systeme, agentenbasierte Automatisierungen überwachen ganze IT-Landschaften.

Das ist faszinierend – und gefährlich zugleich. Denn je autonomer KI-Systeme agieren, desto größer wird ihr Handlungsspielraum. Und genau dieser kann im Ernstfall zum Risiko werden – selbst dann, wenn die KI „nur" intern arbeitet und gut konfiguriert scheint.

Ein aktueller Fall hat mich selbst nachdenklich gestimmt:
Bei einem großen Plattformanbieter löschte eine KI-Komponente produktive Datenbanken – entgegen allen Vorgaben. Das war kein externer Angriff, kein Insider-Sabotageakt. Es war maschinelles Fehlverhalten.

Der Angriff von innen: Maschinelles Fehlverhalten

Viele Unternehmen haben in ihren Bedrohungsmodellen zwei Hauptakteure:

1. Externe Angreifer – Cyberkriminelle, Ransomware, Phishing.

2. Interne Angreifer, – versehentlich gelöschte Daten, falsche Konfigurationen – bisher mit Fokus auf menschliche Fehler.

Mit KI wird das Augenmerk nun noch stärker auf einen anderen internen Angreifer gelegt, denn:

Autonomes, maschinelles Fehlverhalten mit systemischer Wirkung ist real

Forschungsarbeiten belegen, dass große Sprach- und Entscheidungsmodelle in Stresssituationen **nicht deterministisch** reagieren. Sie handeln also nicht immer vorhersehbar – und manchmal sogar entgegen allen Regeln.

Das kann zu Täuschung, Eskalation oder Regelverletzung führen. Mit klassischen Backup-Strategien allein ist das nicht abzusichern.

MENT IQ

Die entscheidende Frage: Wie schützen Sie Daten vor Ihrer eigenen KI?

Als Architect denke ich hier nicht in „Verhinderung“ – absolute Fehlerfreiheit gibt es nicht. Ich denke in **Schutzarchitektur.**

Die Frage lautet:

Wie stelle ich sicher, dass meine geschäftskritischen Daten unangetastet bleiben – selbst dann, wenn interne Systeme versagen oder kompromittiert werden?

Die Antwort ist klar: **Isolation statt Vertrauen.**

Eine Sicherheitsstrategie, physisch und logisch getrennt vom operativen Netz, ist in der klassischen IT oft die „letzte Verteidigungslinie“. In Zeiten von Künstlicher Intelligenz sollte sie aber unbedingt ins Zentrum rücken: Ein **unabhängiges, abgeschottetes Backup-System**, das selbst dann funktioniert, wenn operative Systeme ausfallen oder kompromittiert sind.

Data Vault, Cyber Vault – und warum Sie den Unterschied kennen sollten

Der Begriff **Data Vault** bezeichnet im Kern ein isoliertes Backup-Repository, in dem Ihre Daten vor Veränderung und Manipulation geschützt sind.

Ein **Cyber Vault** geht einen entscheidenden Schritt weiter:

- **Physische und logische Isolation** vom Produktionsnetz
- **Unveränderbare Speicherung** (WORM, Retention-Locks)
- **Strenges Rechte- und Freigabemodell** für Zugriff und Restore
- **Analysefunktionen**, die kompromittierte Datenstände frühzeitig erkennen
- **Forensische Reinraum-Umgebung** für Untersuchungen und Wiederherstellung

Kurz gesagt:

Der **Cyber Vault** dient ausschließlich der **unveränderlichen, isolierten Aufbewahrung** kritischer Backup-Daten. Er ist nicht die Wiederherstellungsumgebung.

Aus ihm heraus können Daten in eine **separate, abgeschottete Reinraumumgebung** wiederhergestellt werden – zum Beispiel für forensische Analysen oder Recovery-Tests.

Der Vault selbst bleibt dabei **unberührt und sauber** – dort finden **keine aktiven Wiederherstellungen** statt, da jede zurückgespielte Instanz potenziellen Schadcode enthalten kann. Nur durch diese strikte Trennung bleibt der Vault die verlässliche Sicherheitsinstanz, auf die Sie sich im Ernstfall verlassen können.

MENT IQ

Die Architektur eines Cyber Vault – so sieht maximale Isolation aus

Aus der Praxis weiß ich: Ein Cyber Vault ist dann wirksam, wenn er **keine** direkte, kontinuierliche Verbindung zur Produktionsumgebung hat. Das kann durch ein physisches **Air Gap** (tatsächliche Trennung) oder eine **strikte logische** Isolation realisiert werden. Im Optimalfall gibt es nur klar definierte, temporäre Datenübertragungsfenster.

Merkmale eines professionellen Cyber Vaults:

1. **Air Gap / Logical Isolation**
   Keine permanente Netzwerkverbindung, keine direkten Mounts ins Produktivnetz.
2. **Immutable Storage**
   Write Once, Read Many (WORM) verhindert nachträgliche Änderungen.
3. **Multi-Faktor-Authentifizierung & Rollenmodell**
   Zugriff nur für wenige, dedizierte Personen. Jede Wiederherstellung erfordert eine Freigabekette.
4. **Anomalieerkennung & Integritätsprüfung**
   Automatisierte Analyse der Backup-Daten auf Ransomware-Muster oder Manipulation.
5. **Forensische Analysefähigkeit**
   Möglichkeit, kompromittierte Systeme isoliert zu untersuchen, ohne den Produktivbetrieb zu gefährden.

Cyber-Resilience in Zeiten autonomer Systeme

Die Integration von KI in Unternehmensprozesse wird nicht weniger werden – im Gegenteil. Doch mit dieser Entwicklung wächst auch die Notwendigkeit, die **Resilienz Ihrer IT-Architektur** neu zu bewerten.

Klassische Backup-Konzepte waren vor allem auf externe Angriffe ausgerichtet. In der Ära von autonomen Systemen und KI brauchen wir zusätzlich Schutz vor internen Automatismen, Fehlentscheidungen und maschineller Eskalation.

MENT IQ

Mein Fazit als Architect: Resilience ist kein Add-on mehr – sie ist Pflicht

Die Integration autonomer Systeme eröffnet enorme Chancen – aber auch neue Verwundbarkeiten. Wer Verantwortung für Daten trägt, muss deshalb über klassische Backup-Konzepte hinausdenken. Der Schutz vor externen Angreifern reicht nicht mehr aus. Es braucht zusätzlich Schutz vor internen Automatismen, Fehlentscheidungen und Systemversagen. Ich sehe es in Projekten jeden Tag: Unternehmen, die nur auf klassische Backup-Mechanismen setzen, riskieren im Ernstfall ihre Datenhoheit.

Ein isolierter, unveränderbarer Cyber Vault ist heute kein Zusatzmodul mehr – es ist eine unternehmerische Notwendigkeit.

Wer Verantwortung für Daten trägt, muss sicherstellen, dass selbst **die eigene KI** diese Daten nicht gefährden kann.

Ihr nächster Schritt: Cyber Recovery Assessment mit mentIQ

Sie wollen wissen, wie resilient Ihre Backup-Architektur wirklich ist? Als Teil der **Medialine Group** unterstützt Sie mentIQ mit einem **praxisnahen Cyber-Recovery Assessment:**

- Bewertung Ihrer aktuellen Backup-Architektur
- Prüfung auf Cyber- und KI-Resilience
- Empfehlung für eine passgenaue Cyber Vault Lösung
- Optional: Proof-of-Concept und Implementierung

Sichern Sie Ihre Daten vor der Bedrohung von außen – und vor den Risiken von innen. Jetzt informieren unter **www.mentiq.com**

Kontakt:
Sebastian Wormser, Lead IT Architect mentIQ

Ihr Partner für intelligentes Datenmanagement. Wir betreuen Sie erstklassig, hochprofessionell und auf Augenhöhe. Gerne gehen wir mit Ihnen gemeinsam eine effektive Cyber-Recovery Strategie an. Kontaktieren Sie unseren Recovery-Spezialisten Sebastian Wormser unverbindlich für ein erstes Beratungsgespräch:

E-Mail: Sebastian.Wormser@medialine.ag
Telefon: +49 89 95 415 72 20