“Game-Changer Cyber-Recovery”: Threat Hunting und Monitoring mit Empalis und der Rubrik Security Cloud

Cyber Resilience mit Plan: Lücken erkennen, Widerstandsfähigkeit stärken.

25.09.2025



Philip Röder, Key Account Manager & Business Development, Empalis Consulting GmbH
Gürkan Ars, Channel Development Manager, Rubrik

07.05.2025

Ihre Experten heute



Philip Röder

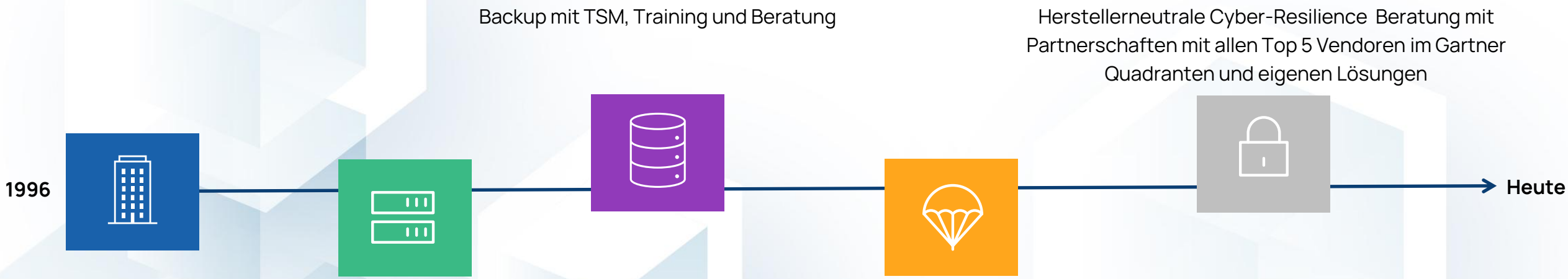
Key Account Manager &
Business Development



Gürkan Ars

Channel Development
Manager

30 Jahre Empalis: Vom Mainframe zur Cyber-Resilience



Erfolgreiche Cyber-Angriffe verursachen einen **schaden von 260 Mrd. €** in der Deutschen Wirtschaft. **52% der Angriffe** sind für das betroffene Unternehmen **Existenzgefährdend**.

Quellen:

- Luendedonk 2023
- BSI-Lagebericht

Ein Kundenbeispiel: Das passiert nach einem Angriff

Ausgangslage

- Spezialmaschinenhersteller
- 1500 Mitarbeiter
- 70 TB Primärdaten + Gleichgroßer Spiegel im 2 RZ
- Natürliches AirGap durch Tape Anbindung für Backup
- Kunde von Empalis im Bereich ISP (für zum Beispiel Updates der Umgebung)
- Alles läuft normal, doch der Angreifer plant seinen nächsten Schritt bereits seit 7 Monaten

Angriff

- Anruf beim IT-Leiter
- Alle Primärdaten sind verschlüsselt in beiden Rechenzentren
- Login auf die Konsole nicht möglich
- Geschäftsführung und LKA werden eingeschaltet
- Ermittlungen starten
- Wiederherstellungsprozess wir eingeleitet
- Öffentlichkeit muss informiert werden

Woche 1

Shutdown

Tapes mit Daten sind glücklicherweise vorhanden, aber:

- Was ist die letzte saubere Backup Kopie?
- Wohin kann wiederhergestellt werden? Welche Hardware benötigen wir? Wo kriegen wir diese her?
- Produktion steht weiterhin still
- Mitarbeiter müssen in Kurzarbeit geschickt werden

Woche 1

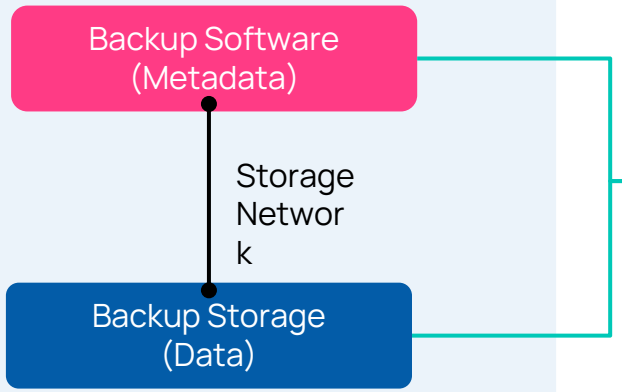
Wiederaufnahme

- **Nach 2 Wochen** konnte erst die **nötige proprietäre Hardware** beschafft werden (unter anderem über Ebay)
- Tapes werden einzeln in Sandbox Umgebung wiederhergestellt und nach Viren durchsucht
- **Nach >4 Wochen** manueller Wiederherstellungsarbeit kann die **Produktion wieder anlaufen**
- Mitarbeiter kehren an die Arbeit zurück

Woche 2-5

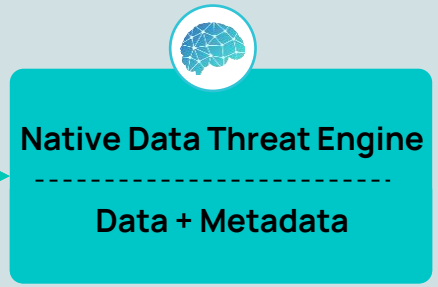
Rubrik Built a Radically Different Architecture

LEGACY BACKUP & RECOVERY



FULL TRUST ARCHITECTURE

RUBRIK WAY



ZERO TRUST ARCHITECTURE I IMMUTABLE

Combining Backup & Cyber Security → Cyber-RTO

1. Determine scope of attack
What data was compromised? What was encrypted?

+

2. Determine point of infection
At what point was the server compromised? Can we quickly identify clean recovery points?

+

3. Assess sensitive data impact
What sensitive data was on the network and likely exfiltrated?

+

4. Find malware and quarantine
Can we find all locations of malware? Can we isolate malware to prevent re-infection?

+

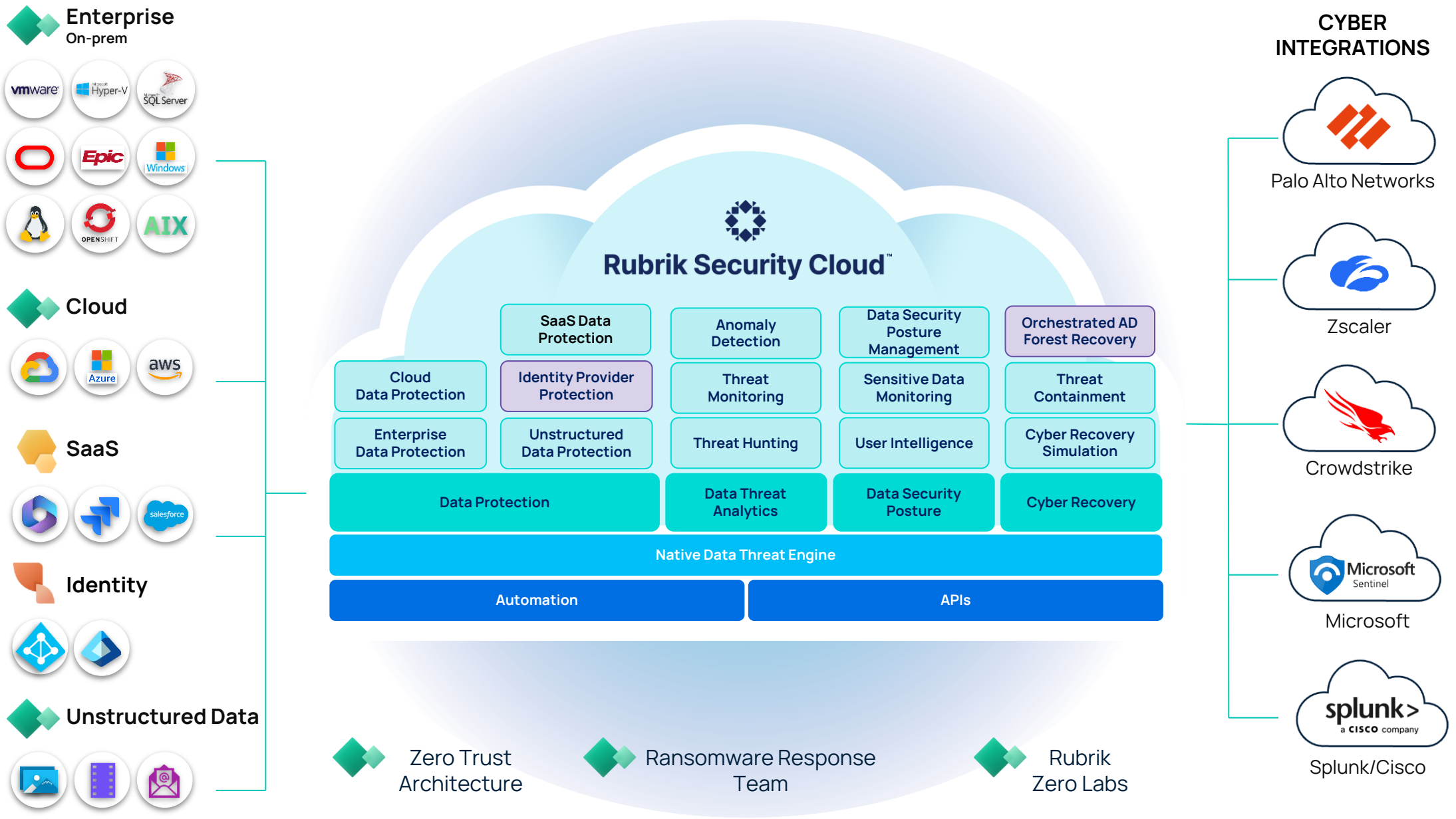
5. Restore from backup
How do we automate, test, and document a recovery in line with regulatory requirements?

Traditional Backups have worked great for traditional Disaster Recovery (RTO),

but are not architected & designed for Cyber-Recovery (Cyber-RTO)

Trusted by >7000 leading institutions to enhance Cyber Resilience

Cyber Resilience across Data & Identity



Jetzt individuellen Gesprächs- und / oder Demo-Termin buchen



https://www.empalis.de/kontakt/termin-vereinbaren/

Weitere Termine in 2025 – 2.Hbj.

07. Oktober 2025, 14:00 – 15:00 Uhr

Empalis Live Experten Talk „ELET - Cyber Resilience Assessment – Kennen Unternehmen den Cyber Resilience Reifegrad ihres Unternehmens?“ Panel-Diskussion

In Kürze zur Anmeldung auf unserer Website verfügbar:

04. November 2025, 14:00 - 15:00 Uhr

Empalis Live Experten Talk „ELET - Hypervisor: Proxmox, AWS und Co. – To migrate or not to migrate?“

27. November 2025, 9:30 - 10:00 Uhr

Empalis bei der WebKonferenz der IT-Sicherheit „Cyber Security Update“ zum Thema Cloud Resilience – EntraID-Backup: Der Tenant wird angegriffen? – Wie man darauf reagiert.

11. Dezember 2025, 10:00- 10:30 Uhr

Empalis bei der WebKonferenz der IT-Sicherheit „KRITIS“ zum Thema „Backup mit Strategie – Gesichertes Business Continuity Management“

Bleiben Sie auf dem Laufenden: https://www.empalis.de/competence-center/events/

Empalis CONSULTING



Perfektion geht nur gemeinsam.

Wir freuen uns, von Ihnen zu hören.

Philip Röder

Key Account Manager & Business Development

Mobil: +49 162 4196789

Mail: philip.roeder@empalis.com

Philip Röder