Business Continuity Management

Business Impact Analyse

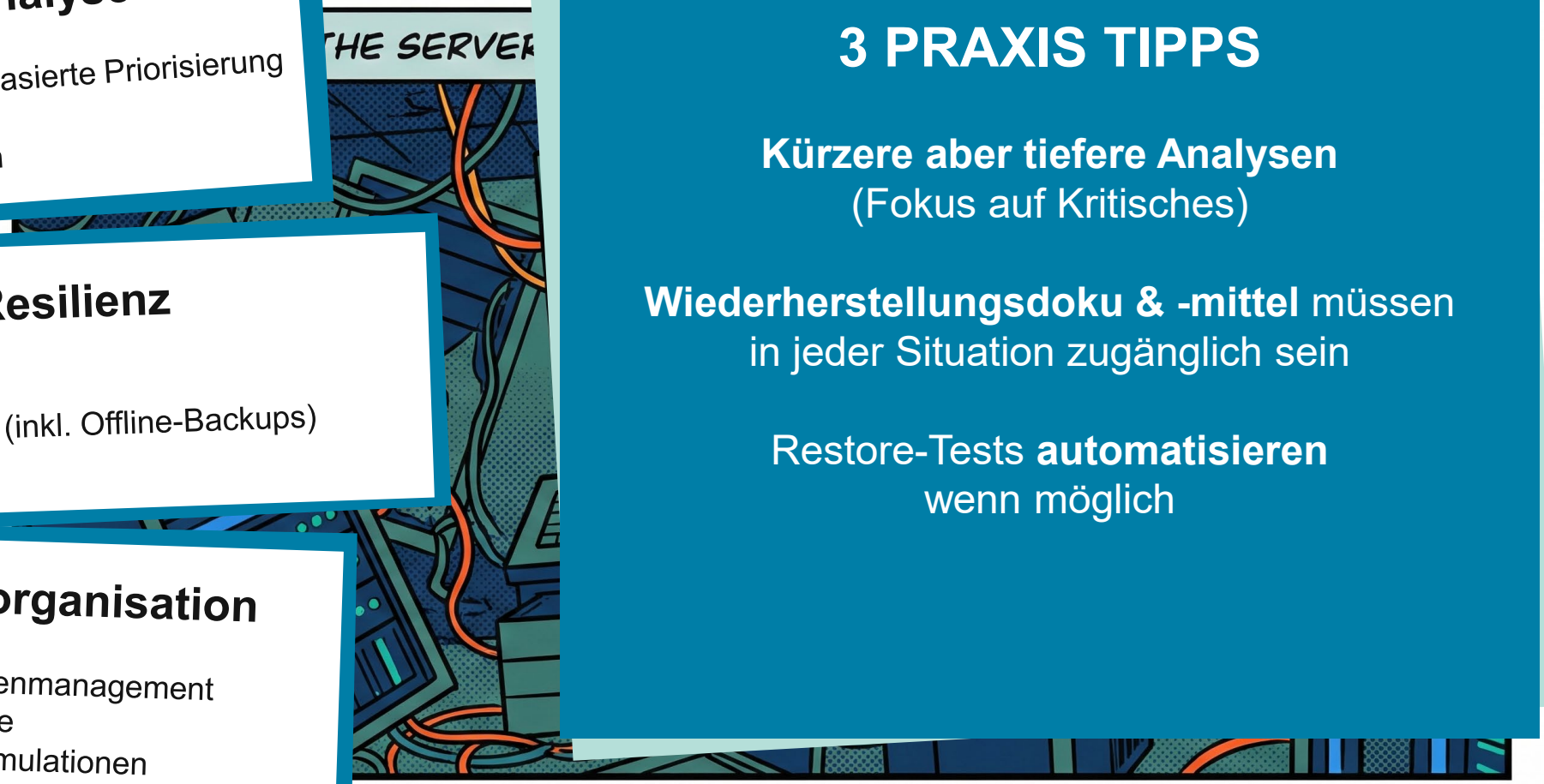
- Kennzahlen (RPO, RTO) basierte Priorisierung
- Kritikalität von Prozessen
- Analyse d. Abhängigkeiten

Technische Resilienz

- Redundanzen
- Backupstrategien (inkl. Offline-Backups)
- Restore Tests

Krisen- & Notfallorganisation

- Notfall-, Incident- & Krisenmanagement
- Kommunikationsstrategie
- Tabletop-Exercises & Simulationen



3 PRAXIS TIPPS

Kürzere aber tiefere Analysen
(Fokus auf Kritisches)

Wiederherstellungsdoku & -mittel müssen
in jeder Situation zugänglich sein

Restore-Tests **automatisieren**
wenn möglich

Human Risk / Security Awareness

Risikobasiert

- Hochrisiko-Rollen (Finance, IT-Admins, …)
- Rollenspezifische Trainings
- Zusatztrainings bei riskantem Verhalten

Kontinuierlich

- Weniger aber öfter (Micro-Learnings)
- Realistische Simulationen
- Management Awareness

KPIs & Kultur

- Wirksamkeit messen (KPIs, Assessments)
- Risikobewusste-Kultur – keine Angstkultur!
- Vorbildfunktionen fördern

3 PRAXIS TIPPS

Geschichten (aus dem eigenen Unternehmen) **erzählen**

mit **Security Champions** in den Fachbereichen arbeiten

Aufwände durch **Automatisierung** klein halten

Endpoint Security

Intelligent & Multifunktional

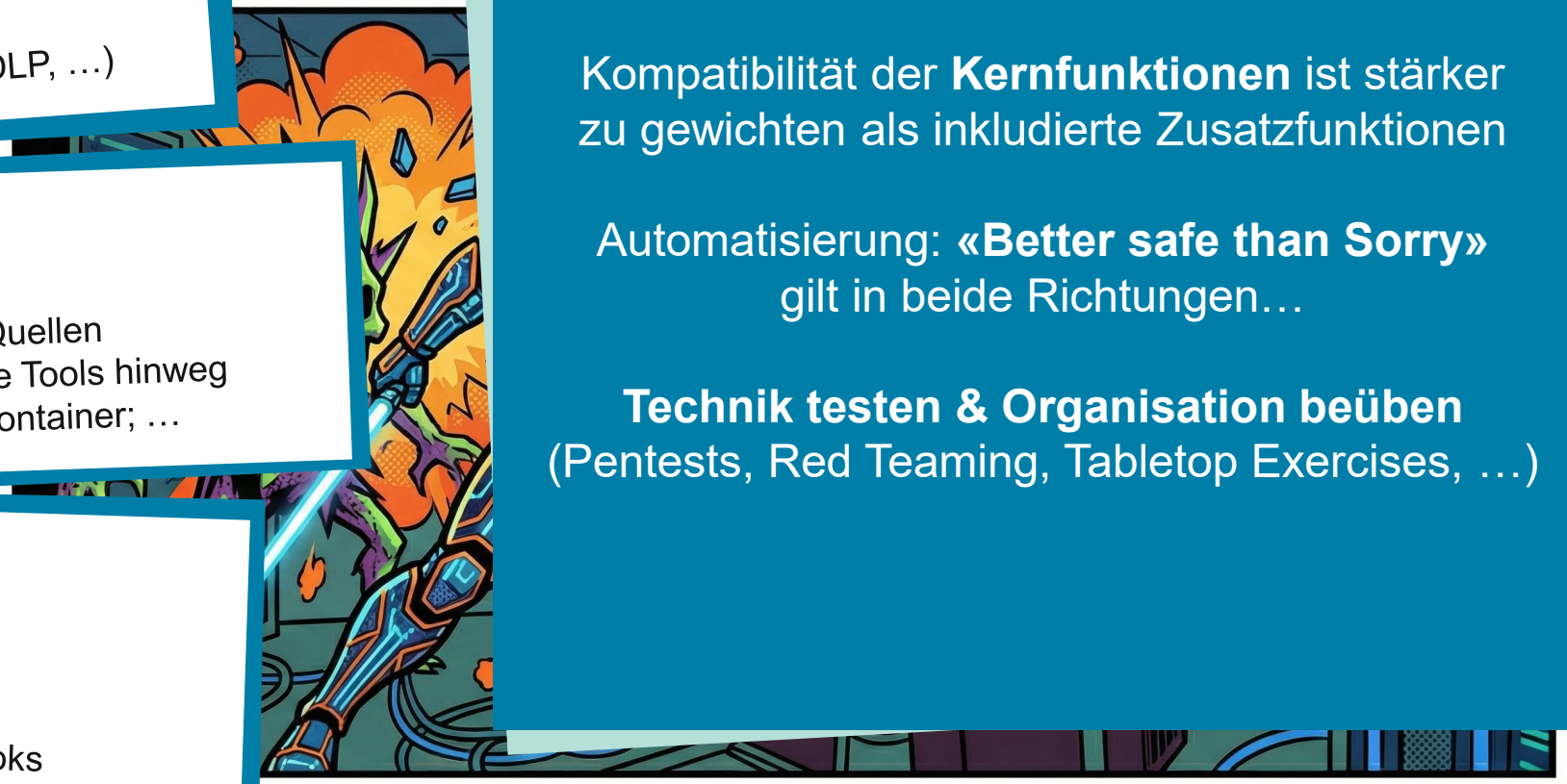
- Moderne EDR/XDR Lösungen
- AI/ML basierte Threat Detection
- Zusatzfunktionen (Vulnerabilities, DLP, …)

Intergiert

- Korrelation mehrere Log-Quellen
- Orchestrierung über mehre Tools hinweg
- Cloud & on-prem; OS & Container; …

Schnelle Reaktion

- Automatische Isolation
- 24/7 Incident Response via SOC
- Vordefinierte & getestete Playbooks



3 PRAXIS TIPPS

Kompatibilität der **Kernfunktionen** ist stärker zu gewichten als inkludierte Zusatzfunktionen

Automatisierung: **«Better safe than Sorry»** gilt in beide Richtungen…

Technik testen & Organisation beüben (Pentests, Red Teaming, Tabletop Exercises, …)

KI & Unternehmenssicherheit

Angreifer nutzen KI

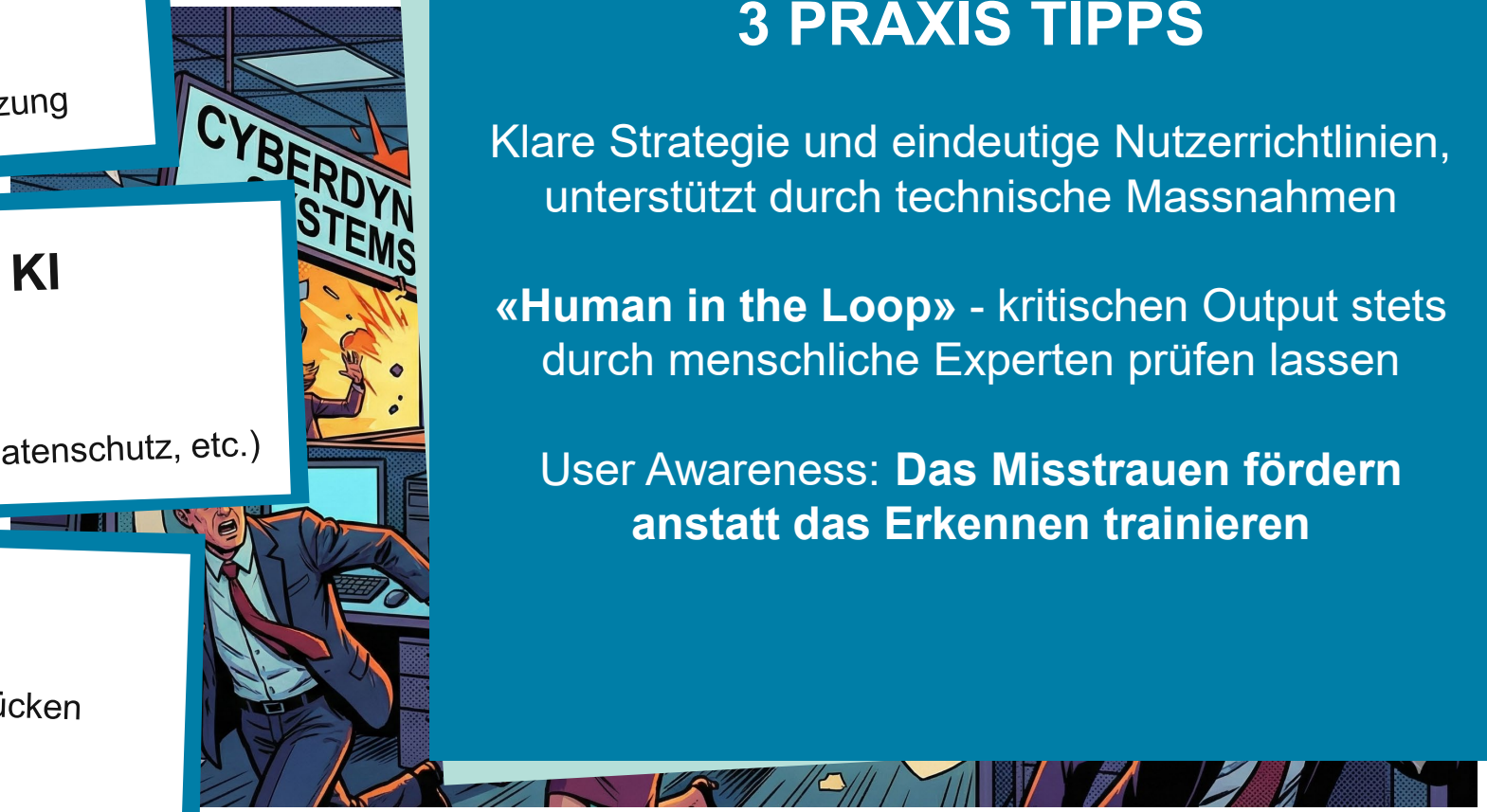
- Bessere Phishing Mails, automatisiert
- Deepfakes, Voice-Cloning, etc.
- Exploit-Entwicklung & Angriffsunterstüzung

Mitarbeitende nutzen KI

- Shadow IT
- Datenabfluss
- Rechtliche Kopfschmerzen (Datenschutz, etc.)

Entwickler nutzen KI

- KI generierter Code mit Sicherheitslücken
- Nachvollziehbarkeit & Wartbarkeit
- Prompt Injection und weitere Risiken



3 PRAXIS TIPPS

Klare Strategie und eindeutige Nutzerrichtlinien, unterstützt durch technische Massnahmen

«Human in the Loop» - kritischen Output stets durch menschliche Experten prüfen lassen

User Awareness: **Das Misstrauen fördern anstatt das Erkennen trainieren**