Whitepaper & Notfall-Checkliste

Ransomware-Angriff

ANGRIFF

✓ Richtig vorbeugen

- Regelmäßige, getestete Backups nach der 3-2-1-Regel (3 Kopien, 2 Medien, 1 offsite).
- Zeitnahes Patch-Management für Betriebssysteme und Software.
- Endpoint-Schutz mit verhaltensbasierter Erkennung einsetzen.
- Netzwerksegmentierung, um Ausbreitung zu begrenzen.
- Mitarbeitende regelmäßig zu Phishing schulen (Haupteinfallstor).

■ Im Ernstfall – Schritt für Schritt

Vorfall-Protokoll (bitte ausfüllen)

Datum:	
Uhrzeit:	
Betroffenes System / Gerät:	
Gemeldet durch:	
Gemeldet an (IT-Verantwortlicher):	

- ■ **1.** Betroffene Systeme sofort vom Netzwerk trennen (Kabel ziehen / WLAN aus).
- ■ **2.** Keinesfalls das Lösegeld zahlen oder eigenmächtig mit Angreifern kommunizieren.
- ■ **3.** IT-Dienstleister / IT-Notfall-Hotline umgehend kontaktieren.
- ■ **4.** Betroffene Systeme NICHT herunterfahren (forensische Spuren erhalten).
- ■ **5.** Verschlüsselte Dateien und Erpresserbotschaft sichern/fotografieren.
- ■ **6.** Strafanzeige bei der Polizei erwägen.
- ■ **7.** Betroffenheit prüfen: welche Systeme, welche Daten, welche Nutzer.
- ■ **8.** Wiederherstellung ausschließlich aus sauberen, geprüften Backups.