Checkliste: Sicherheitsparameter zum Schutz vor Ransomware

Prävention:

- ☐ regelmäßige Mitarbeiterschulungen, um insbesondere gegen Social Engineering und das Öffnen von bösartigen Links gewappnet zu sein
- ☐ Emailschutz (Malwareschutz, Spamschutz, Ransomware Schutz, Verschlüsselung, URL Scanner)
- ☐ Patch Management Policy für Virenschutz, Firewall und Betriebssystem
- ☐ Backup von Ordnern, Adressbüchern, Lesezeichen, Emails und Kalender
- ☐ Ad-Blocker im Browser installieren, Hovern über Links zur Analyse
- ☐ Cyber-Insurance
- ☐ DLP (Data Loss Prevention)
- ☐ Partner/Lieferketten – Schutz der eigenen Infrastruktur vor Kettenreaktionen
- ☐ Firewalls und Phishing-resistente (für kritische Schnittstellen) MFA, Starke Passwort Policy
- ☐ Zero Downtime Emailserver sicherstellen
- ☐ Zero-Trust-Policy
- ☐ Homeoffice Infrastruktur absichern, kein BYOD
- ☐ Kollaborationstools wie Teams, Zoom und Slack absichern
- ☐ Endpoint Schutz (EDR: Endpoint Detection and Response)
- ☐ Passwortmanager nutzen (z.B. kostenlose Software „Bitwarden“)
- ☐ SOC (Security Operations Center) und SIEM (Security Information and Event Management)
- ☐ Ransomware Playbook

Während eines Angriffs:

- ☐ Geräte nicht wie gewöhnlich ausschalten sondern direkt vom Strom trennen
- ☐ Falls professionelle Intervention erforderlich wird, ist es notwendig externe Firmen zu konsultieren, Report an Strafverfolgungsbehörden ist in jedem Fall unerlässlich
- ☐ Entschärfung und Behebung, nicht auf Erpressungen eingehen
- ☐ Malware Scan

Post-Angriff:

- ☐ Entschlüsselung der eigenen Daten
- ☐ Hohe Geschwindigkeit bei Wiederherstellung von Daten: Backup Anbieter sinnvoll wählen
- ☐ Infrastruktur analysieren, Scans, affektierte Systeme in Quarantäne verschieben
- ☐ Passwörter zurücksetzen