Checkliste Cyber-Angriff

Präventionsmaßnahmen & Maßnahmen für den Ernstfall

VEREIN NETZWERK LOGISTIK

PRÄVENTIONSMAßNAHMEN

- Bereitstellung der Organisationsstruktur → Informationssicherheit auf Top Management Ebene, Managementsysteme (z.B. ISO/IEC 27001 / CISIS 12)
- Optimierung der (IT-) Prozesse
- Risikomanagement (Matrix)
- „Last Line of Defence“: Faktor Mensch und Sensibilisierung der Mitarbeiter:innen in ALLEN Fachbereichen
- Bereitstellung der Kommunikationsmittel und -kanäle
- Offene und regelmäßige Kommunikation / Information intern und extern
- Transparenz der Systeme
- Separieren von Systemen
- Segmentieren der Netzwerke (Mikrosegmentierung)
- Notfallplan (vgl. Brandfall)
    - Checkliste für Mitarbeiter:innen inkl. wichtiger Telefonnummern
    - Meldesystem
    - Krisenstab einrichten (im Rahmen vorhandener Prozesse und Personen)
    - Kommunikationsplan und -regeln
    - Simulationen
- Versicherungsschutz
- Back-ups nach der 3-2-1-Regel
- Patch
- Verwendung von E-Mail-Zertifikaten
- Passwortmanagement
- „Least-Privilege-Prinzip“: Nur für das eigene Aufgabenfeld benötigte Zugriffsrechte
- Multi-Faktor-Authentifizierung
- „4-Augen-Prinzip“
- Berücksichtigung der IT-Dienstleister (Bsp.: TeamViewer und Zugänge)
- Standard-Malware darf nicht zu Mitarbeiter:innen durchdringen
- Vermeidung von leichten Angriffsstellen

MAßNAHMEN im ERNSTFALL

- RUHE bewahren
- Erstes Lagebild erzeugen und Entscheidung über Ersthandlung treffen
- Welche Prioritäten müssen gesetzt werden? (Schadensbegrenzung)
- Rechtzeitige Meldung und angemessene Dokumentation (Polizei / IT-Ermittler LKA/ Staatsanwaltschaft)
- Ursachenforschung, evtl. Kontaktaufnahme mit Spezialisten
- Zeitnahe Kommunikation (Mitarbeiter:innen/ extern – Kunde & Lieferanten & Partner) – auf Wording achten!

STAND: JUNI 2022