CyberWehr
RISK MANAGEMENT SOLUTIONS GMBH
Monika Wehr ▪ +41 79 348 55 63 ▪ 8803 Rüschlikon, Alte Landstrasse 109

Checkliste Cybersicherheit

Die Datenschutz-Grundverordnung ist im revidierte Datenschutzgesetz der Schweiz verankert. Gefordert wird die Gewährleistung eines dem Risiko angemessenen Schutzniveaus für personenbezogene Daten hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit der Systeme (Netzwerk, Betriebssysteme, Rechenzentren, Datenverarbeitungssprozesse etc.). Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

Welche IT Strategie verfolgen Sie?

Ist eine Übersicht des internen/externen Netzwerkverkehr/IoT gegeben?
Beschreiben Sie Ihren Stand der Umsetzung der Digitalisierung /Ziele/Deadlines/ Applikationen/Abhängigkeiten von weiteren Systemen, Netzen, Diensten

Wie überprüfen und bewerten Sie Ihre technischen Ressourcen? bestehende Verschlüsselungs- und Sicherheitsmechanismen auf mögliche Schwachstellen. Prüfung evtl. Datenlecks? Nehmen Sie eine Datenlöschung vor?

Wie sichern sie Ihre Geschäftsprozesse in Bezug auf Cyberbedrohungen?

1. Ist ein Incident Response Plan vorhanden?
2. Sind die Sofortmassnahmen im Falle eines IT-Vorfalls definiert?
2. Ist eine redundante Festplatte vorhanden?
3. Beinhaltet das Antivirus auch eine Abwehr gegen Cyberattacken? - Sind Spamlisten aufgeführt?
4. Arbeiten Sie mit KI Softwarelösungen? Eine cloudbasierte Erkennung und Analyse sowie eine immer besser werdende heuristische Erkennung von Schadsoftware.
5. Führen Sie die Prävention eines Angriffs mittels eines Verschlüsselungstrojaners durch?

Wie schnell muss eine Wieder-Inbetriebnahme nach einem Cyberangriff erfolgen? Wie lange darf maximal eine Betriebsunterbrechung dauern?

Ist das Mindestmass an Cyber-Widerstandsfähigkeit gegeben?
- **Data Breach & Phishing** – Datendiebstahl, Ausspionieren von Daten ausserhalb der Organisation. Webhacking: anormale HTTP-Anfragen an ungewöhnliche externe Domains.

- **Data Leackage** - Datendiebstahl innerhalb der Organisation (Unternehmen, Verwaltung etc.)

- **(Distributed) Denial of Service Attack (DoS/DDoS)** - Überlasten und damit blockieren einer Internetschnittstelle oder eines anderen Services durch ein automatisch generiertes Übermass an Service-Anfragen.

- **Ransomeware:** böswillige Verschlüsselung von Daten, um Erpressungsgeld zu fordern.

Welche adäquaten, technischen und organisatorischen Massnahmen treffen Sie zur angemessenen Sicherung personenbezogener Daten vor Missbrauch und Verlust?

Welche Massnahmen haben Sie in der Datenverarbeitung verankert, um **Vertraulichkeit, Integrität, Verfügbarkeit und Daten-Zuverlässigkeit** zu gewährleisten?