Cyber Security Preparedness: Eine Checkliste, um Ihr Unternehmen auf Cyber-Attacken vorzubereiten

Systeme & Team

Welche Systeme sind wichtig?

Auf welche Systeme sind die Kernprozesse angewiesen?

☐

Wo sind die Daten?

- In welchen Systemen sind welche Daten?
- Wie fliessen diese Daten zwischen den unterschiedlichen Systemen?

☐

Wer ist verantwortlich?

Kontaktdaten für jedes wichtige System hinterlegen:

- Verantwortlicher
- Stellvertreter

☐

Intern oder extern?

- Entweder: Aufbau eines Incident Response Teams
- Oder: Vertrag mit einem Incident-Reponse-Anbieter

☐

Abläufe

Definition eines Sicherheitsvorfalls

- Welche Systeme sind relevant?
- Welche Vorfallarten sind kritisch?

☐

Durch Logs Basis schaffen

- Werden für alle wichtigen Systeme Logs erstellt?
- Werden diese Logs zeitnah auf potenzielle Vorfälle analysiert?

☐

Erkennung & Benachrichtigung

- Wie werden die relevanten Vorfälle erkannt?
- Wie werden die Verantwortlichen benachrichtigt?

☐

Priorisierung der Aktivitäten

Abwägung Priorisierung:

- Schadensbegrenzung
- Schadensbehebung
- Wiederherstellung des normalen Geschäftsbetriebs

☐

Zuständigkeiten festlegen

Wer hat im Notfall welche Zuständigkeiten?

☐

Kommunikation

Welche Stakeholder benachrichtigen?

Wer muss benachrichtigt und auf dem Laufenden gehalten werden?

- Kunden
- Partner
- Mitarbeitende
- Anfragende Presse

☐

Meldestellen kennen

In welchem Fall muss welche Stelle wie benachrichtigt werden?

- NCSC
- Zuständige Polizeibehörde
- Aufsichtsbehörden (z. B. EDÖB)

☐

Kommunikationsteam festlegen

- Wer kommuniziert intern?
- Wer kommuniziert extern mit wem?
- Welche Kanäle werden genutzt?

☐

Sie haben einen Cyber-Security-Vorfall?

Unser Incident Response Team steht Ihnen 24/7 zur Verfügung.
Garantierte Verfügbarkeit mit vorgängiger Vereinbarung.

Tel: +41 31 511 37 51 E-Mail: incident@redguard.ch

REDGUARD
SECURING YOUR ASSETS