Cyber Incident Response: Eine Checkliste, um auf eine Cyber Attacke zu reagieren

Fakten sammeln

Entdeckung

- Welche Systeme/ Netzwerke sind gefährdet?
- Welche Daten sind betroffen und wie?
- Welche Logfiles können bei der Analyse helfen?

☐

Analyse

- Wann, von wem, wie und wo entdeckt?
- Wann mit Analyse gestartet?
- Geschätzter Zeitpunkt der Problemlösung?

☐

Gesicherte Erkenntnisse

- Was ist zweifelsfrei über den Ablauf der Sicherheitsverletzung bekannt?
- Was ist über den Angreifer bekannt?

☐

Reaktion

Verantwortlichkeiten

- Wer hat die Leitung für die Behebung des Vorfalls?
- Wer nimmt die unterstützenden Rollen wahr?

☐

Expertise sichern

- Welche Expertise ist für die Behebung erforderlich?
- Wer stellt diese Expertise bereit?
- Wird externe Expertise benötigt?

☐

Stoppen & Absichern

- Netzwerk und Systeme vor weiterem Befall bewahren
- Daten absichern

☐

Wiederherstellung

Abwägung Priorisierung:

- Schadensbegrenzung
- Schadensbehebung
- Wiederherstellung des normalen Geschäfts-betriebs

☐

Rechtliches

- Was fordern Verträge, Regulatorien und relevante Gesetze?
- Wie sind die weiteren rechtlichen Implikationen des Vorfalls?

☐

Kommunikation

Transparenz

- Es geht nicht nur um ein IT-Risiko sondern auch um ein Unternehmensrisiko.
- Verstehen der Auswirkungen der Kommunikation

☐

Kommunikations-Team

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

☐

Zielgruppen informieren

- NCSC
- Polizei
- Aufsichtsbehörden (z. B. EDÖB)
- Betroffene Personen
- Presse

☐

Überlegt informieren

- Reaktiv oder proaktiv?
- Eine zeitnahe Kommunikation ist wichtig, aber auch deren Richtigkeit
- Situation nicht noch verschlimmern durch später notwendige Korrekturen

☐

Situation und Zukunft erklären

- Was ist geschehen?
- Wie ist es dazu gekommen und warum war das überhaupt möglich?
- Wie wird so ein Vorfall zukünftig verhindert?

☐

Update-Frequenz etablieren

Stündliches Update, selbst wenn nichts geschehen ist, statt ständig Anfragen beantworten zu müssen

☐

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