

INCIDENT RESPONSE MANAGEMENT

FALLS DER WORST-CASE ZUR REALITÄT WIRD

Security Incidents, ausgelöst durch Cyberattacken, nehmen drastisch zu und werden immer teurer für Unternehmen. Wenn der Worst-Case zur Realität wird, stehen wir Ihnen als erfahrener Incident Response Manager zur Seite. Ob Datendiebstahl, Malware oder Verschlüsselungsattacken: Wir übernehmen – und das zu gesicherter Reaktionszeit.

» IHR LEISTUNGSANSPRUCH

» AUF MANAGEMENT-EBENE

- Vertraglich zugesicherte Reaktionszeit von 2 Stunden
- 24x7 Service
- Daily Calls
- Interne Kommunikationsmatrix
- Juristische Beratung und Behördenkommunikation
- Abschlusspräsentation & Lessons Learned Präsentation für Managementebene

» AUS TECHNISCHER SICHT

- Unser Computer Security Incident Response Team
 - Incident Manager
 - Security-Consultants
 - Data & Malware Analyst
- Analytische & forensische Dokumentation
- Prozesssicherheit durch SOPs

Bei unserem vollumfänglichen Service übernehmen wir bei Ihnen die Vorbereitung, Identifikation, Eindämmung, Bereinigung, Wiederherstellung und Nachbereitung des gesamten Vorfalls mit den klaren Zielen der Schadensbegrenzung und schnellstmöglichen Wiederaufnahme Ihres Regelbetriebs.

» UNSER INCIDENT HANDLING

- 01 Vorbereitung** Bevor wir uns Ihren Systemen nähern, erarbeiten wir folgende Punkte mit Ihnen: Access Control, Dokumentation, Backups, Richtlinien, Priorisierung und Kommunikationsplan.
- 02 Identifikation** Wir sammeln und identifizieren alle Events, um den Schaden zu bewerten und eine Vorfalsthese zu evaluieren.
- 03 Eindämmung** Um den Schaden einzugrenzen und weitere Systeminfizierungen zu vermeiden, isolieren wir die betroffenen Systeme vom Netzwerk.
- 04 Bereinigung** Wir zerstören die Schadprogramme nachhaltig und treffen umfassende Schutzvorkehrungen wie die Sicherung aller Festplatten, um Neuinfektionen auszuschließen.
- 05 Wiederherstellung** Alle betroffenen Systeme werden von uns wiederhergestellt und in die Produktionsumgebung überführt, sodass der Regelbetrieb wieder anlaufen kann.
- 06 Nachbereitung** Wir stellen Ihnen die umfangreichen Dokumentationen des Incidents zur Verfügung und besprechen mit Ihnen die notwendigen Maßnahmen, um einen erneuten Angriff präventiv abwehren zu können.

» UNSER VERSPRECHEN

- IR Management aller Angriffsarten
- Vorfallsbewältigung nach internationalen Standards (SANS)
- Fokus auf Schadensbegrenzung & Wiederaufnahme des Regelbetriebs
- Vergünstigung des IR-Tagessatzes
- Umfassendes Know-how von Major Incidents
- 24x7 Erreichbarkeit
- Nachhaltige Verbesserung der IT-Infrastruktur
- Diskretion