Incident Response Quickstart – Handlungsfähig im Ernstfall

Ein Service Ihrer Cybersecurity-Partner – SilentSec

Wichtiger Hinweis vorab

Dieser Quickstart-Guide dient dazu, in einer kritischen Situation handlungsfähig zu bleiben und erste, sinnvolle Maßnahmen zu koordinieren. Er ersetzt keine professionelle digitale Forensik, langfristige Sicherheitsanalyse oder rechtliche Beratung. Sein Ziel ist es, den Schaden zu begrenzen und die Grundlage für eine spätere, professionelle Aufarbeitung zu schaffen.

Im Zweifel: Holen Sie sich frühzeitig externe Hilfe. Kapitel 4 definiert, wann dies unbedingt notwendig ist.

Kapitel 1: Vorbereitung ist alles – Das Team

• **Incident Lead:** Treibt den Prozess an, trifft finale Entscheidungen, ist zentrale Anlaufstelle.

• **IT-Admin / Technischer Ansprechpartner:** Führt technische Maßnahmen durch (Isolieren, Sichern).

• **Kommunikationsverantwortlicher:** Steuert interne und externe Kommunikation.

• **Rechtlicher Ansprechpartner:** Beurteilt Melde- und Benachrichtigungspflichten (z. B. DSGVO).

Kritische Kontaktliste (24/7)

Rolle	Name	Telefon	E-Mail	Stellvertretung
Incident Lead				
IT-Admin				
Kommunikation				
Rechtlicher Ansprechpartner				
Externer IR-Dienstleister				
Lokal zuständige Polizei (Cyber)				
BSI / CERT-Bund		+49 22899 9582-0		

Kapitel 2: Die ersten 60 Minuten – Eskalation & Erstmaßnahmen

Bewahren Sie Ruhe. Handeln Sie besonnen. Dokumentieren Sie jede Aktion (Wer, Was, Wann).

Checkliste Erstmaßnahmen (DO / DON’T)

Maßnahme	DO (Tun)	DON’T (Nicht tun)
Isolieren	System vom Netzwerk trennen	System herunterfahren
Beweise sichern	Screenshots & Logs sichern	Dateien verändern
Zugang sperren	Passwörter von sauberem System ändern	Lokal ändern
Dokumentieren	Ereignisprotokoll führen	Nur mündlich anweisen

Kapitel 3: Kommunikationsplan

Schweigen ist keine Strategie. Gesteuerte Kommunikation schützt den Ruf und verhindert Fehlinformationen.

Muster: Interne Erstmeldung

Betreff: WICHTIG – Interne Information zu einem technischen Vorfall

Liebe Kolleginnen und Kollegen,

unsere Systeme haben einen sicherheitsrelevanten Vorfall erkannt. Unser Incident Response Team hat die Untersuchung aufgenommen. Bitte folgen Sie den vorläufigen Anweisungen des Incident Leads. Weitere Informationen folgen.

Mit freundlichen Grüßen
Incident Lead

Kapitel 4: Wann Sie uns brauchen

Ziehen Sie externe Incident-Response-Spezialisten sofort hinzu, wenn eines oder mehrere der folgenden Kriterien erfüllt sind:

• Ransomware aktiv Systeme verschlüsselt

• Erheblicher Datenabfluss vermutet oder bestätigt

• Persistenter Zugriff des Angreifers

• Kritische Produktions- oder OT-Systeme betroffen

• Interne Kapazität oder Expertise überfordert

• Meldepflicht wahrscheinlich

Handlungsfähig bleiben beginnt mit Vorbereitung.
✔ Team benennen ✔ Kontaktliste pflegen ✔ Guide regelmäßig prüfen