# **Playbook: Reaktion auf einen Ransomware-Angriff**

## **Zweck:**

Dieses Playbook beschreibt die Schritte, die das Security Operations Center (SOC) durchführen muss, um auf einen Ransomware-Angriff zu reagieren. Ziel ist es, die Auswirkungen zu minimieren, die Bedrohung einzudämmen und die Systeme sicher wiederherzustellen.

## **1. Vorfallbeschreibung**

**Definition:**

Ein Ransomware-Angriff ist ein Vorfall, bei dem bösartige Software Daten oder Systeme verschlüsselt, um ein Lösegeld zu fordern.

**Symptome:**

• Unerwartete Verschlüsselung von Dateien.

• Popup-Fenster mit Lösegeldforderungen.

• ungewöhnlich hohe CPU-Auslastung oder Netzwerkaktivitäten.

• Verbindungsprobleme mit kritischen Systemen.

## **2. Rollen und Verantwortlichkeiten**

1. **Tier-1 SOC-Analyst:**

• Überwachung und Analyse der Alarmmeldungen.

• Initiale Eskalation an Tier-2 Analysten.

2. **Tier-2 SOC-Analyst:**

• Validierung des Vorfalls und Einleitung der Eindämmungsmaßnahmen.

• Zusammenarbeit mit Systemadministratoren.

3. **Incident Response Manager:**

• Koordination der Maßnahmen und Eskalation an externe Partner (z. B. Forensiker).

• Kommunikation mit der Geschäftsführung.

4. **Systemadministrator:**

• Durchführung der technischen Maßnahmen wie Isolierung und Wiederherstellung.

## **3. Schritt-für-Schritt-Anleitung**

**Phase 1: Erkennung und Validierung**

1. **Alarmanalyse:**

* SIEM-Alarme überprüfen, die auf ungewöhnliche Dateizugriffe oder hohe Netzwerkaktivitäten hinweisen.
* Identifikation betroffener Systeme und Benutzerkonten.

2. **Initiale Validierung:**

* Prüfung von Logs und Endgeräten, ob typische Ransomware-Indikatoren vorhanden sind (z. B. .locked-Dateiendungen).
* Kontaktaufnahme mit dem Benutzer, der den Vorfall gemeldet hat.

3. **Eskalation:**

• Weiterleitung an Tier-2 Analysten mit allen relevanten Informationen.

**Phase 2: Eindämmung (Containment)**

1. **Systemisolierung:**

* Trennen betroffener Systeme vom Netzwerk (z. B. durch VLAN-Änderungen oder physische Trennung).
* Sperrung kompromittierter Benutzerkonten.

2. **Verhinderung der Ausbreitung:**

* Blockieren von verdächtigen IP-Adressen und Domains auf der Firewall.
* Deaktivieren von Netzwerkfreigaben und File Shares.

**Phase 3: Eradication und Recovery**

1. **Beseitigung der Bedrohung:**

* Analyse und Entfernung der Malware mit Forensik-Tools wie Volatility oder Autopsy.
* Untersuchung von Logs auf weitere Spuren der Bedrohung.

2. **Wiederherstellung:**

* Wiederherstellen betroffener Systeme aus sauberen Backups.
* Durchführung von Sicherheitstests, um sicherzustellen, dass die Bedrohung vollständig beseitigt wurde.

**Phase 4: Nachbereitung**

1. **Post Mortem Report:**

• Detaillierte Dokumentation des Vorfalls, der Maßnahmen und Lessons Learned.

2. **Playbook-Optimierung:**

• Überprüfung und Anpassung dieses Playbooks basierend auf den Erkenntnissen.

3. **Mitarbeiterschulungen:**

• Schulung der betroffenen Abteilungen zu Phishing- und Ransomware-Prävention.

## **4. Tools und Technologien**

• **SIEM:** Elastic Security, Splunk oder Wazuh.

• **EDR:** CrowdStrike, SentinelOne.

• **Threat Intelligence Plattform:** MISP, openCTI.

• **Forensik Tools:** Volatility, Autopsy, Wireshark.

## **5. Kommunikation**

1. **Interne Kommunikation:**

• Tägliche Updates an das Management während des Vorfalls.

• Abschlussbericht nach der Wiederherstellung.

2. **Externe Kommunikation:**

• Meldung an Behörden, falls personenbezogene Daten betroffen sind (DSGVO, NIS2).

• Zusammenarbeit mit externen Incident Response Dienstleistern.

## **6. KPIs zur Erfolgsmessung**

• Zeit bis zur Erkennung des Vorfalls (Detection Time).

• Zeit bis zur Isolierung betroffener Systeme (Containment Time).

• Gesamtzeit bis zur vollständigen Wiederherstellung (Recovery Time).

• Anzahl der betroffenen Systeme oder Daten.

## **7. Lessons Learned**

• **Stärken:** Schnelle Isolierung betroffener Systeme.

• **Verbesserungspotenziale:** Verbesserung der Phishing-Filter und Endpoint Protection.