# **Prozessbeschreibung: Incident Response Prozess**

## **1. Zweck und Ziel des Prozesses**

Der Incident Response Prozess definiert strukturierte und standardisierte Schritte zur Erkennung, Analyse, Eindämmung, Behebung und Nachbereitung von Sicherheitsvorfällen. Ziel ist es, die Auswirkungen von Vorfällen zu minimieren, die IT-Systeme schnellstmöglich wiederherzustellen und zukünftige Vorfälle durch kontinuierliche Verbesserung zu verhindern.

## **2. Geltungsbereich**

Dieser Prozess gilt für alle Sicherheitsvorfälle, die IT-Systeme, Netzwerke, Anwendungen, Daten oder Benutzerkonten betreffen. Er ist verbindlich für alle Mitglieder des Security Operations Centers (SOC), das Incident Response Team (IRT) sowie für alle relevanten Stakeholder des Unternehmens.

## **3. Rollen und Verantwortlichkeiten**

|  |  |
| --- | --- |
| **Rolle** | **Verantwortlichkeiten** |
| **SOC Analyst (Tier-1)** | Überwachung und erste Analyse von Vorfällen; Eskalation an Tier-2 Analysten. |
| **SOC Analyst (Tier-2)** | Validierung und weitere Analyse; Einleitung von Eindämmungsmaßnahmen. |
| **Incident Response Manager** | Koordination der Maßnahmen; Kommunikation mit Stakeholdern und Eskalation an Führungsebene. |
| **Systemadministratoren** | Unterstützung bei der Eindämmung, Behebung und Wiederherstellung betroffener Systeme. |
| **Compliance Officer** | Sicherstellung, dass alle Maßnahmen regulatorische Anforderungen erfüllen |
| **Geschäftsführung** | Entscheidungsträger für Eskalationen und strategische Maßnahmen. |

## **4. Phasen des Incident Response Prozesses**

**4.1. Vorbereitung (Preparation)**

**Ziel:** Sicherstellen, dass alle notwendigen Ressourcen, Prozesse und Dokumentationen verfügbar sind.

* Erstellung und Pflege von Playbooks für häufige Vorfälle (z. B. Phishing, Malware, Ransomware).
* Durchführung von Schulungen und Übungen für das SOC- und IRT-Team.
* Implementierung und Konfiguration von Sicherheitswerkzeugen (SIEM, EDR, SOAR, etc.).
* Sicherstellen, dass alle Mitarbeiter wissen, wie Vorfälle gemeldet werden.

**4.2. Erkennung und Analyse (Detection and Analysis)**

**Ziel:** Identifizieren und analysieren eines Sicherheitsvorfalls.

**Schritte:**

1. Überwachung von Logs, Alarmen und Anomalien mit Tools wie SIEM und EDR.
2. Identifikation von Indikatoren für Kompromittierungen (IoCs).
3. Durchführung von Netzwerkanalysen (z. B. mit Wireshark) und Endpunkt-Überprüfungen.
4. Bewertung des Vorfalls basierend auf Kritikalität, betroffenen Systemen und potenziellen Auswirkungen.
5. Erstellung eines ersten Incident Reports zur Dokumentation aller Analysen.

**4.3. Eindämmung (Containment)**

**Ziel:** Verhindern, dass sich der Vorfall weiter ausbreitet.

**Schritte:**

1. Isolierung betroffener Systeme vom Netzwerk (z. B. VLAN-Änderungen, physische Trennung).
2. Sperrung kompromittierter Benutzerkonten oder Berechtigungen.
3. Blockierung von bösartigen IPs, Domains oder Anwendungen auf Firewalls und Proxies.
4. Kommunikation mit betroffenen Teams über die ergriffenen Maßnahmen.

**4.4. Beseitigung und Wiederherstellung (Eradication and Recovery)**

**Ziel:** Vollständige Entfernung der Bedrohung und Wiederherstellung des Normalzustands.

**Schritte:**

1. Identifikation und Entfernung der Ursache des Vorfalls (z. B. Malware, Schwachstellen).
2. Aktualisierung betroffener Systeme durch Patches oder Konfigurationsänderungen.
3. Wiederherstellung betroffener Daten und Systeme aus sicheren Backups.
4. Durchführung von Sicherheitstests, um sicherzustellen, dass die Bedrohung vollständig beseitigt wurde.

**4.5. Nachbereitung (Post-Incident Activity)**

**Ziel:** Lernen aus dem Vorfall, um zukünftige Angriffe besser zu verhindern.

**Schritte:**

1. Erstellung eines **Post Mortem Reports** mit einer detaillierten Analyse des Vorfalls.
2. Durchführung eines Nachbereitungstreffens, um Lessons Learned zu identifizieren.
3. Aktualisierung von Playbooks, Richtlinien und Prozessen basierend auf den Erkenntnissen.
4. Kommunikation der Ergebnisse an Stakeholder und, falls erforderlich, an Behörden (Compliance-Bericht).

## **5. Kommunikationsplan**

• **Interne Kommunikation:**

• Regelmäßige Updates an das Management und betroffene Abteilungen.

• Eskalation kritischer Vorfälle an die Geschäftsführung.

• **Externe Kommunikation:**

• Meldung von Vorfällen an Regulierungsbehörden (z. B. bei GDPR- oder NIS2-Verstößen).

• Zusammenarbeit mit externen Forensik-Dienstleistern oder Incident Response Experten.

## **6. Tools und Technologien**

|  |  |
| --- | --- |
| **Tool** | **Funktion** |
| **SIEM (z. B. Elastic)** | Erkennung und Analyse von Vorfällen durch Log-Daten. |
| **EDR/XDR** | Schutz und Überwachung von Endgeräten. |
| **SOAR** | Automatisierung von Sicherheitsprozessen. |
| **Threat Intelligence** | Identifikation neuer Bedrohungen und IoCs. |
| **Forensik-Tools** | Untersuchung kompromittierter Systeme. |

## **7. KPIs zur Erfolgsmessung**

* **Mean Time to Detect (MTTD):** Durchschnittliche Zeit bis zur Erkennung eines Vorfalls.
* **Mean Time to Contain (MTTC):** Durchschnittliche Zeit bis zur Eindämmung eines Vorfalls.
* **Mean Time to Recover (MTTR):** Durchschnittliche Zeit bis zur vollständigen Wiederherstellung.
* **Anzahl der Vorfälle pro Monat:** Messung der Sicherheitslage.

## **8. Lessons Learned**

Nach jedem Vorfall wird evaluiert, wie der Prozess optimiert werden kann:

• **Was lief gut?**

• Schnelle Identifikation und Isolierung betroffener Systeme.

• **Was kann verbessert werden?**

• Frühere Erkennung durch verbesserte Alarmregeln.

• Bessere Kommunikation während der Eindämmungsphase.

Dieser Incident Response Prozess stellt sicher, dass Sicherheitsvorfälle effizient bearbeitet werden und das Unternehmen resilient gegen zukünftige Angriffe wird.