# **Communication Plan**

**Version:** 1.0

**Datum:** [Einfügedatum]

**Verantwortlich:** SOC Manager

**Genehmigt durch:** [Name des Sicherheitsbeauftragten]

## **1. Zweck des Communication Plans**

Dieser Communication Plan legt fest, wie das Security Operations Center (SOC) während eines Sicherheitsvorfalls sowie im normalen Betrieb effektiv kommuniziert. Ziel ist es, klare Kommunikationswege und -verfahren zu definieren, um Verwirrung zu vermeiden, die Reaktionszeit zu minimieren und Vertrauen bei internen und externen Stakeholdern aufzubauen.

## **2. Geltungsbereich**

Dieser Plan gilt für:

• Alle SOC-Mitarbeiter (Tier 1–3).

• Incident Response Teams (IRT).

• Externe Partner und Drittanbieter.

• Management und andere interne Abteilungen.

## **3. Kommunikationsziele**

1. Sicherstellung klarer und konsistenter Kommunikation zwischen allen Beteiligten während eines Vorfalls.

2. Minimierung von Informationsverlust und Missverständnissen.

3. Schnelle Eskalation von Vorfällen an die zuständigen Stellen.

4. Aufbau und Erhalt des Vertrauens von Kunden, Behörden und der Öffentlichkeit.

## **4. Kommunikationswege**

|  |  |  |
| --- | --- | --- |
| **Stakeholder** | **Kommunikationsmittel** | **Zweck** |
| SOC-Mitarbeiter | Microsoft Teams, Slack | Interne Echtzeitkommunikation während Vorfällen und im täglichen Betrieb. |
| Incident Response Team | E-Mail, Teams, Telefon | Telefon Eskalation und detaillierte Vorfallkommunikation. |
| Management | Berichte, E-Mail, Meetings | Status-Updates und strategische Entscheidungen. |
| Externe Partner | E-Mail, verschlüsselte Kommunikation | Austausch von Bedrohungsinformationen und Koordination externer Maßnahmen. |
| Öffentlichkeit/Kunden | E-Mail, verschlüsselte Kommunikation | Krisenkommunikation bei Vorfällen mit externer Wirkung. |

## **5. Kommunikationsphasen**

**5.1 Normalbetrieb**

• **Tägliche Berichterstattung:**

• Tägliche oder wöchentliche Updates zu SOC-Aktivitäten und identifizierten Bedrohungen.

• **Regelmäßige Meetings:**

• Monatliche Meetings mit Management und anderen Abteilungen.

**5.2 Sicherheitsvorfall**

• **Erkennung:**

• SOC-Mitarbeiter melden Vorfälle sofort an das Incident Response Team (IRT).

• **Eskalation:**

• Kritische Vorfälle werden direkt an den SOC Manager und das Management eskaliert.

• **Reaktion:**

* Kommunikation zwischen betroffenen Teams über festgelegte Kanäle (z. B. Teams, Telefon).

**5.3 Nachbearbeitung**

• **Debriefing:**

• Detaillierte Besprechung der Vorfallreaktion mit allen Beteiligten.

• **Reporting:**

• Erstellung eines Abschlussberichts für das Management und externe Stakeholder.

## **6. Eskalationsrichtlinien**

|  |  |  |
| --- | --- | --- |
| Vorfallstyp | Eskalationsstufe | Verantwortlicher |
| Niedriger Vorfall (z. B. Spam) | Lokales SOC-Team | Tier 1 Analyst |
| Mittlerer Vorfall (z. B. Malware) | SOC Manager | Tier 2 Analyst, Incident Responder |
| Kritischer Vorfall (z. B. Ransomware) | Unternehmensleitung und externe Partner | SOC Manager, Incident Response Team |

## **7. Kommunikationsinhalte**

|  |  |
| --- | --- |
| **Stakeholder** | **Inhalt** |
| **SOC-Team** | Details zum Vorfall, betroffene Systeme, laufende Maßnahmen. |
| **Management** | Zusammenfassung des Vorfalls, potenzielle Auswirkungen, empfohlene Maßnahmen. |
| **Externe Partner** | IoCs (Indicators of Compromise), technische Details zur Koordination. |
| **Kunden/Öffentlichkeit** | Bestätigung des Vorfalls, Maßnahmen zur Begrenzung der Auswirkungen, zukünftige Präventionsstrategien. |

## **8. Tools und Vorlagen**

• **Kommunikationstools:**

• Microsoft Teams, Slack, E-Mail, Telefon.

• **Vorlagen:**

• Incident-Update-Bericht.

• Abschlussbericht.

• Pressemitteilung für Vorfälle mit externer Wirkung.

## **9. Erfolgskennzahlen (KPIs)**

1. **Reaktionszeit:** Zeit zwischen Vorfallmeldung und Eskalation.

2. **Kommunikationsgeschwindigkeit:** Zeit, bis Stakeholder informiert wurden.

3. **Zufriedenheit der Stakeholder:** Feedback der Beteiligten nach der Vorfallbearbeitung.

## **10. Überprüfung und Aktualisierung**

Dieser Plan wird mindestens jährlich überprüft und nach Bedarf aktualisiert, um sicherzustellen, dass er mit den aktuellen Anforderungen und Bedrohungslandschaften übereinstimmt.