# **Regelmäßiger SOC-Bericht (Monatlicher SOC-Report)**

## **SOC-Bericht: [Monat, Jahr]**

*Erstellt von: [Name des SOC-Managers]*

*Datum: [Erstellungsdatum]*

## **1. Einleitung**

**Berichtszweck:**

Dieser Bericht bietet eine Übersicht über die Sicherheitslage des Unternehmens für den Monat [Monat, Jahr]. Er umfasst erkannte Vorfälle, umgesetzte Maßnahmen, aktuelle Trends und Empfehlungen zur Verbesserung der Sicherheitsinfrastruktur.

## **2. Zusammenfassung der Sicherheitslage**

|  |  |
| --- | --- |
| **Parameter** | **Wert** |
| **Anzahl der Sicherheitsvorfälle:** | [Anzahl der Vorfälle] |
| **Eskalierte Vorfälle:** | [Anzahl eskalierter Fälle] |
| **Anzahl geschlossener Vorfälle:** | [Anzahl geschlossener Fälle] |
| **Mean Time to Detect (MTTD):** | [Zeit in Minuten/Stunden] |
| **Mean Time to Respond (MTTR):** | [Zeit in Minuten/Stunden] |

## **3. Sicherheitsvorfälle im Detail**

**3.1 Zusammenfassung der Vorfälle**

|  |  |  |  |
| --- | --- | --- | --- |
| **Vorfalltyp** | **Anzahl** | **Eskalationen** | **Geschlossen** |
| Malware-Angriffe | [Anzahl] | [Anzahl] | [Anzahl] |
| Phishing-Vorfälle | [Anzahl] | [Anzahl] | [Anzahl] |
| Ransomware-Versuche | [Anzahl] | [Anzahl] | [Anzahl] |
| Insider Threats | [Anzahl] | [Anzahl] | [Anzahl] |
| Andere Vorfälle | [Anzahl] | [Anzahl] | [Anzahl] |

**3.2 Kritische Vorfälle**

**Beispiel: Malware-Angriff am [Datum]**

* **Beschreibung:** Ein Endpoint-System wurde durch eine Malware infiziert, die durch einen unsicheren Anhang in einer E-Mail installiert wurde.

• **Maßnahmen:**

• System wurde isoliert und gesäubert.

• Benutzerkonto wurde gesperrt.

• Awareness-Schulungen für betroffene Abteilung durchgeführt.

• **Status:** Geschlossen.

**Beispiel: Phishing-Angriff am [Datum]**

* **Beschreibung:** Mehrere Mitarbeiter erhielten E-Mails mit gefälschten Login-Links zu internen Systemen.

• **Maßnahmen:**

• Blockierung der Phishing-Domains in der Firewall.

• Keine Benutzerzugänge kompromittiert.

• Phishing-Simulation für die gesamte Belegschaft geplant.

• **Status:** Offen (Awareness-Schulung ausstehend).

## **4. Schwachstellen und Empfehlungen**

**4.1 Ergebnisse der Schwachstellen-Scans**

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset** | **Schwachstelle** | **Kritikalität** | **Status** |
| Webserver | Veraltete Softwareversion | Hoch | Behoben |
| Datenbankserver | Fehlende Zugangsbeschränkungen | Mittel | Offen |
| Endpoint-Systeme | Unsichere Browser-Plug-ins | Niedrig | Behoben |

**4.2 Empfehlungen**

1. **Regelmäßige Patches und Updates:**

* Implementierung eines automatisierten Patch-Management-Systems zur Minimierung von Schwachstellen.

2. **Mitarbeiter-Schulungen:**

* Durchführen regelmäßiger Awareness-Trainings zur Erkennung von Phishing-Angriffen.

3. **Endpoint-Security:**

* Einführung von EDR/XDR-Lösungen zur besseren Erkennung und Eindämmung von Bedrohungen auf Endpunkten.

4. **Zugangskontrolle:**

* Striktere Durchsetzung von Zugangsbeschränkungen auf kritischen Servern.

## **5. Bedrohungstrends**

**Aktuelle Trends:**

• **Zunahme von Phishing-Angriffen:** Ein Anstieg um [X]% im Vergleich zum Vormonat.

• **Vermehrte Brute-Force-Angriffe:** Häufiger auf Remote Desktop Protokoll (RDP).

• **Neue Schwachstellen:** Veröffentlichung kritischer Schwachstellen in [Produkt].

**Empfohlene Maßnahmen:**

• Verbesserung der Mailfilter und Sensibilisierung für Phishing.

* Einschränkung von RDP-Zugängen und Einführung von Multi-Faktor-Authentifizierung (MFA).

## **6. Compliance-Status**

|  |  |  |
| --- | --- | --- |
| **Anforderung** | **Status** | **Bemerkung** |
| ISO 27001 | Erfüllt | Regelmäßige interne Audits laufen. |
| NIS2 | Teilweise erfüllt | Verbesserungen bei Schwachstellen-Management erforderlich. |
| DORA | In Bearbeitung | Implementierung eines SIEM-Systems. |
| GDPR (DSGVO) | Erfüllt | Keine Verstöße gemeldet. |

## **7. Lessons Learned**

1. **Proaktive Erkennung:** Früherkennung durch verfeinerte SIEM-Regeln hat zu schnelleren Reaktionszeiten geführt.
2. **Kommunikation:** Eskalationsprozesse müssen klarer definiert und trainiert werden.
3. **Awareness:** Phishing bleibt die häufigste Bedrohung; weitere Sensibilisierungsmaßnahmen notwendig.

## **8. Fazit und nächster Schritt**

**Zusammenfassung:**

Der Monat [Monat, Jahr] zeigte Fortschritte bei der Eindämmung von Malware und Schwachstellenmanagement. Phishing bleibt jedoch ein wiederkehrendes Problem, das durch verstärkte Schulungen angegangen werden muss.

**Nächste Schritte:**

• Implementierung neuer SIEM-Regeln zur besseren Erkennung von Insider Threats.

• Einführung einer internen Phishing-Simulation bis [Datum].

• Abschluss der Patches für [kritische Schwachstelle] bis [Datum].

**Bericht erstellt von:**

[Name des SOC-Managers]

[Position]

[Datum]