# **Sicherheitsstrategie**

## **1. Einleitung**

**1.1 Ziel der Sicherheitsstrategie**

Diese Sicherheitsstrategie dient als Leitlinie, um die IT-Sicherheitslage des Unternehmens ganzheitlich zu verbessern. Ziel ist es, eine sichere, widerstandsfähige und zukunftsfähige IT-Umgebung zu schaffen, die sowohl aktuelle als auch zukünftige Bedrohungen proaktiv adressiert. Ein zentrales Element dieser Strategie ist der Aufbau und Betrieb eines Security Operations Centers (SOC).

**1.2 Grundprinzipien**

1. **Proaktivität:** Bedrohungen frühzeitig erkennen und abwehren.
2. **Ganzheitlichkeit:** Schutz aller digitalen und physischen Assets des Unternehmens.
3. **Regelkonformität:** Einhaltung regulatorischer Anforderungen (ISO 27001, NIS2, DORA, DSGVO, etc.).
4. **Kollaboration:** Enge Zusammenarbeit zwischen IT, Compliance und Geschäftsführung.
5. **Kontinuierliche Verbesserung:** Regelmäßige Überprüfung und Optimierung der Sicherheitsmaßnahmen.

## **2. Status Quo**

**2.1 Bedrohungslandschaft**

Das Unternehmen sieht sich folgenden Bedrohungen gegenübergestellt:

• Zunehmende Phishing-Angriffe und Social-Engineering-Vorfälle.

• Schwachstellen in veralteten Softwarelösungen.

• Erhöhte Risiken durch Remote-Arbeit und BYOD (Bring Your Own Device).

• Steigende Zahl von Ransomware-Angriffen.

**2.2 Bestehende Sicherheitsmaßnahmen**

• Firewall- und Netzwerksegmentierung.

• Grundlegendes Schwachstellenmanagement (Patch-Management).

• Awareness-Programme für Mitarbeiter.

• Antivirus- und Endpoint Protection-Lösungen.

**2.3 Identifizierte Lücken**

1. Fehlendes Security Operations Center (SOC) zur proaktiven Überwachung.

2. Unzureichende Incident Response-Prozesse und Playbooks.

3. Keine umfassende Threat Intelligence Integration.

4. Schwächen im Schwachstellenmanagement.

## **3. Sicherheitsstrategie**

**3.1 Strategische Ziele**

1. Aufbau eines zentralisierten SOC, das Bedrohungen in Echtzeit überwacht und reagiert.
2. Einführung eines robusten Incident Response Frameworks.
3. Verbesserung des Schwachstellenmanagements.
4. Umsetzung eines Zero-Trust-Ansatzes zur Minimierung von Zugriffsrisiken.
5. Integration moderner Sicherheitslösungen wie SIEM, SOAR und Threat Intelligence Plattformen.

## **4. Sicherheitsmaßnahmen**

**4.1 Aufbau eines SOC**

**4.1.1 Zielsetzung**

Das SOC dient als zentrale Einheit zur Überwachung, Erkennung und Behebung von Sicherheitsvorfällen.

**4.1.2 Bestandteile des SOC**

1. **SIEM (Security Information and Event Management):** Elastic Security, Splunk oder Wazuh zur Sammlung und Analyse von Log-Daten.
2. **SOAR (Security Orchestration, Automation, and Response):** Automatisierung und Orchestrierung von Sicherheitsprozessen.
3. **Threat Intelligence:** Plattformen wie MISP oder openCTI zur Erkennung neuer Bedrohungen.
4. **Case Management:** Tools wie TheHive oder DFIR-IRIS zur Verwaltung von Sicherheitsvorfällen.

**4.1.3 Betriebsmodelle**

• **24/7 SOC:** Rund-um-die-Uhr-Überwachung.

• **9-5 SOC:** Tagesbetrieb mit Eskalation an ein externes Team außerhalb der Arbeitszeiten.

• **Hybrid SOC:** Kombination aus internem Team und externer Unterstützung.

**4.2 Incident Response Framework**

**4.2.1 Phasen des Frameworks**

1. **Preparation:** Entwicklung von Playbooks, Schulungen und Eskalationsrichtlinien.
2. **Detection and Analysis:** Überwachung von Logs, Alarmsystemen und IoCs (Indicators of Compromise).
3. **Containment:** Isolierung kompromittierter Systeme.
4. **Eradication and Recovery:** Entfernung der Bedrohung und Wiederherstellung betroffener Systeme.
5. **Post-Incident Activity:** Erstellung eines Post Mortem Reports und Optimierung der Playbooks.

**4.3 Verbesserung des Schwachstellenmanagements**

**4.3.1 Maßnahmen**

• Einführung eines automatisierten Schwachstellen-Scanners.

• Regelmäßige Schwachstellen- und Patch-Management-Routinen.

• Priorisierung basierend auf Risikobewertungen.

**4.4 Zero-Trust-Ansatz**

**4.4.1 Prinzipien**

• Zugang auf Basis des **Need-to-Know**-Prinzips.

• Implementierung von Multi-Faktor-Authentifizierung (MFA).

• Mikrosegmentierung zur Verhinderung von Lateral Movement.

## **5. Rollen und Verantwortlichkeiten**

|  |  |
| --- | --- |
| **Rolle** | **Verantwortlichkeiten** |
| **SOC Manager** | Strategische Leitung und Berichterstattung. |
| **Tier-1 Analysten** | Überwachung und erste Analyse von Sicherheitsvorfällen. |
| **Tier-2 Analysten** | Tiefere Analysen und Einleitung von Eindämmungsmaßnahmen. |
| **Incident Response Manager** | Koordination und Eskalation von Sicherheitsvorfällen. |
| **Systemadministratoren** | Unterstützung bei Patching und Wiederherstellung. |
| **Compliance Officer** | Sicherstellung der Einhaltung regulatorischer Anforderungen. |

## **6. Metriken und KPIs**

* **Mean Time to Detect (MTTD):** Durchschnittliche Zeit bis zur Erkennung eines Vorfalls.
* **Mean Time to Respond (MTTR):** Durchschnittliche Zeit bis zur Eindämmung eines Vorfalls.
* **Anzahl geschlossener Schwachstellen:** Monatliche Reduzierung von Sicherheitslücken.
* **Awareness-Level:** Ergebnisse regelmäßiger Phishing-Tests.

## **7. Budgetplanung**

• **Initialer Aufbau des SOC:** 120.000 € (Einrichtung von Tools, Hardware, Lizenzen).

• **Laufende Betriebskosten:** 60.000 €/Jahr (Personal, Wartung, Lizenzen).

• **Awareness-Programme und Schulungen:** 15.000 €/Jahr.

## **8. Zeitplan**

|  |  |  |
| --- | --- | --- |
| **Phase** | **Zeitraum** | **Meilenstein** |
| Aufbau des SOC | Q1–Q2 [Jahr] | SOC vollständig einsatzbereit |
| Einführung des Incident Response Frameworks | Q2–Q3 [Jahr] | Framework implementiert und getestet |
| Verbesserung des Schwachstellenmanagements | Q2 [Jahr] | Automatisierte Prozesse implementiert |
| Einführung Zero-Trust-Ansatz | Q3 [Jahr] | Zero-Trust-Richtlinien aktiv |

## **9. Risiken**

|  |  |
| --- | --- |
| **Risiko** | **Mitigation** |
| Verzögerung bei der SOC-Implementierung | Externe Berater einbeziehen, um Expertise zu sichern. |
| Hohe Schulungskosten | Nutzung interner Ressourcen für Schulungen. |
| Widerstand der Mitarbeiter gegen neue Prozesse | Awareness-Kampagnen und klare Kommunikation starten. |

## **10. Fazit**

Diese Sicherheitsstrategie mit der Integration eines SOC legt den Grundstein für eine sichere und widerstandsfähige IT-Umgebung. Durch den proaktiven Ansatz, die Implementierung moderner Technologien und die enge Zusammenarbeit aller Abteilungen wird das Unternehmen in der Lage sein, Bedrohungen frühzeitig zu erkennen, effektiv darauf zu reagieren und seine regulatorischen Anforderungen zu erfüllen.

**Genehmigt durch:**

[Name der Führungskraft]

[Position]

[Datum]