# **Risk Register**

## **Übersicht: Risk Register**

Ein Risk Register ist ein zentralisiertes Dokument, das alle identifizierten Risiken eines Unternehmens erfasst, bewertet und priorisiert. Es enthält die Maßnahmen zur Minderung der Risiken sowie den Status ihrer Bearbeitung.

## **Risk Register**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risiko-ID** | **Risiko** | **Kategorie** | **Auswirkungen** | **Wahrscheinlichkeit** | **Risiko-bewertung** | **Maßnahmen zur Risikominderung** | **Verantwortlicher** | **Status** |
| R001 | Ransomware-Angriff durch Phishing-Mails | Cyber-security | Verlust von Daten, Betriebsunterbrechung | Hoch | Kritisch | - Einführung von E-Mail-Filtern- Schulung der Mitarbeiter zu Phishing-Erkennung- regelmäßige Backups | IT-Sicherheitsabteilung | Offen |
| R002 | Veraltete Software auf kritischen Systemen | IT-Infrastruktur | Schwachstellen führen zu potenziellen Angriffen | Mittel | Hoch | - Regelmäßige Updates und Patches- Einführung eines Schwachstellen-Management-Tools | Systemadministrator | In Bearbeitung |
| R003 | Nicht autorisierte Zugriffe auf sensible Kundendaten | Daten-schutz | Verletzung der DSGVO, potenzielle Geldstrafen | Mittel | Hoch | - Einführung von Multi-Faktor-Authentifizierung (MFA)- Zugriffskontrollen überprüfen | Compliance Officer | Offen |
| R004 | Fehlende Incident Response Dokumentation | Operatives Risiko | Verzögerte Reaktion bei Sicherheitsvorfällen | Niedrig | Mittel | - Erstellung von Playbooks und einem Incident Response Framework- Schulungen für das SOC-Team | Incident Response Manager | In Bearbeitung |
| R005 | Insider-Bedrohungen (z. B. unzufriedene Mitarbeiter) | Human Resources | Datendiebstahl, Sabotage | Niedrig | Mittel | - Einführung von Monitoring-Tools- Awareness-Trainings für Mitarbeiter | HR-Abteilung | Überprüft |
| R006 | Schwache Netzwerksegmentierung | Netzwerk-Architektur | Lateral Movement bei Cyberangriffen | Hoch | Kritisch | - Einführung einer Zero-Trust-Architektur- Segmentierung kritischer Netzwerkbereiche | Netzwerkadministrator | Offen |
| R007 | Fehlende Business Continuity und Disaster Recovery Pläne | Unternehmensstrategie | Lange Ausfallzeiten bei Vorfällen | Mittel | Hoch | - Entwicklung eines BCDR-Plans- Durchführung von Tabletop-Übungen | Geschäftsführung | Offen |

## **Risikobewertungsskala**

**Wahrscheinlichkeit:**

• **Niedrig:** <20% Eintrittswahrscheinlichkeit.

• **Mittel:** 20-50% Eintrittswahrscheinlichkeit.

• **Hoch:** >50% Eintrittswahrscheinlichkeit.

**Auswirkungen:**

• **Gering:** Keine nennenswerten Auswirkungen auf den Betrieb.

• **Mittel:** Betrieb wird beeinträchtigt, jedoch keine langfristigen Schäden.

* **Kritisch:** Schwere Beeinträchtigung des Betriebs, langfristige Schäden oder regulatorische Konsequenzen.

**Risikobewertung:**

Kombination aus Wahrscheinlichkeit und Auswirkungen:

• **Gering:** Keine sofortigen Maßnahmen erforderlich.

• **Mittel:** Maßnahmen innerhalb von 3 Monaten einleiten.

• **Hoch/Kritisch:** Sofortige Maßnahmen erforderlich.

## **Zusammenfassung**

Das Risk Register dient als Werkzeug zur systematischen Erfassung, Bewertung und Verfolgung von Risiken im Unternehmen. Es ermöglicht der Organisation, präventiv Maßnahmen zu ergreifen und die Sicherheitslage kontinuierlich zu verbessern. Alle offenen Risiken sollten regelmäßig überprüft und aktualisiert werden, um Veränderungen in der Risikolandschaft zu berücksichtigen.