# **Eskalationsmatrix**

## **Einleitung**

Die Eskalationsmatrix definiert klare Richtlinien und Verantwortlichkeiten für die Handhabung von Vorfällen in einem Unternehmen. Sie legt fest, welche Schritte und Ansprechpartner bei unterschiedlichen Vorfallstypen und -schweregraden einzuhalten sind, um eine effektive und schnelle Reaktion sicherzustellen.

## **1. Eskalationsstufen**

|  |  |  |
| --- | --- | --- |
| **Stufe** | **Beschreibung** | **Beispiele** |
| **Stufe 1 Niedrig:** | Routineprobleme, die durch den operativen Betrieb gelöst werden können. | Fehlgeschlagene Backups, Benutzerfehler, kleinere Softwarefehler. |
| **Stufe 2 Mittel:** | Probleme, die mehrere Abteilungen betreffen, aber den Geschäftsbetrieb nicht kritisch stören. | Lange Reaktionszeiten des ERP-Systems, kleinere Malware-Erkennung ohne Auswirkungen. |
| **Stufe 3 Hoch:** | Kritische Vorfälle mit potenziellen Auswirkungen auf die Geschäftskontinuität. | Datenlecks, Ransomware-Angriffe, Netzwerkausfälle in Kernsystemen. |
| **Stufe 4 Kritisch:** | Sicherheitsvorfälle, die den Betrieb vollständig lahmlegen oder rechtliche Konsequenzen haben. | Domänen-Controller-Kompromittierung, umfassender Datenverlust, DDoS-Angriffe. |

## **2. Eskalationsmatrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vorfallstyp** | **Stufe 1** | **Stufe 2** | **Stufe 3** | **Stufe 4** |
| **Netzwerkprobleme** | Lokale Verbindungs-probleme | Langsamer Netzwerk-verkehr, keine Kernsysteme betroffen | Netzwerkaus-fall bei einem Standort | Kompletter Netzausfall im Unternehmen |
| **Malware/Bedroh ungserkennung** | Einzelner Endpoint betroffen, ohne Ausbreitung | Malware auf mehreren Endpoints erkannt | Malware auf kritischen Systemen (z. B. Server) | Ransomware-Angriff mit Datenver-schlüsselung |
| **Datenverlust** | Einzelne Dateien verloren | Datenverlust auf Abteilungs-ebene | Datenverlust in Kernsystemen | Umfassender Verlust geschäftskritischer Daten |
| **Physische Sicherheit** | Unbefugte Nutzung von Arbeitsstationen | Gestohlene Geräte | Einbruch in kritische Räumlichkeiten | Totalausfall durch Sabotage |

## **3. Eskalationswege**

**Stufe 1 – Niedrig**

**Ansprechpartner:**

• Erstes IT-Support-Level

• Abteilungsleiter

**Maßnahmen:**

• Sofortige Problembehebung durch IT-Support.

• Dokumentation im internen Ticketsystem.

**Stufe 2 – Mittel**

**Ansprechpartner:**

• IT-Leiter

• Abteilungsleiter der betroffenen Abteilung

**Maßnahmen:**

• Analyse des Problems durch IT-Leiter.

• Einbindung betroffener Abteilungen.

• Regelmäßige Status-Updates an alle Beteiligten.

**Stufe 3 – Hoch**

**Ansprechpartner:**

• SOC Manager

• IT-Sicherheitsbeauftragter

• Compliance Officer

**Maßnahmen:**

• Aktivierung des Incident Response Teams.

• Umgehende Eskalation an die Geschäftsführung.

• Sicherung betroffener Systeme und Durchführung von Forensik.

**Stufe 4 – Kritisch**

**Ansprechpartner:**

• Geschäftsführung

• Externe Experten (Forensik, Recht)

• Behörden (z. B. Datenschutzbeauftragter, Polizei)

**Maßnahmen:**

• Aktivierung des Notfallplans.

• Benachrichtigung aller relevanten internen und externen Stakeholder.

• Einleitung von Maßnahmen zur Schadensbegrenzung (z. B. Abschaltung des Netzwerks).

## **4. Verantwortlichkeiten nach Stufe**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rolle** | **Stufe 1** | **Stufe 2** | **Stufe 3** | **Stufe 4** |
| **IT-Support** | Problemlösung | Unterstützung | Eskalation | Unterstützung |
| **IT-Leiter** | Überwachung | Leitung der Analyse | Koordination | Unterstützung |
| **SOC Manager** | N/A | Überwachung | Leitung | Leitung |
| **Compliance Officer** | N/A | Beratung | Unterstützung | Leitung der rechtlichen Aspekte |
| **Geschäfts-führung** | N/A | N/A | Entscheidungsfindung | Strategische Entscheidungen |
| **Externe Berater/Experten** | N/A | N/A | Unterstützung | Leitung spezifischer Maßnahmen |

## **5. Kommunikationsplan**

|  |  |  |
| --- | --- | --- |
| **Eskalationsstufe** | **Kommunikationsebene** | **Frequenz** |
| **Stufe 1** | E-Mail an Abteilungsleiter und IT-Support | Nach Abschluss der Problembehebung |
| **Stufe 2** | Status-Update an IT-Leiter und betroffene Abteilungen | Wöchentlich oder nach Bedarf |
| **Stufe 3** | Berichte an Geschäftsführung und SOC Manager | Wöchentlich oder nach Bedarf |
| **Stufe 4** | Direkte Kommunikation mit Behörden und Geschäftsführung | Jede Stunde oder bei kritischen Fortschritten |

## **6. Fazit**

Eine klare Eskalationsmatrix sorgt für schnelle, strukturierte und effektive Reaktionen auf Vorfälle. Sie minimiert Schäden, fördert die Zusammenarbeit und gewährleistet, dass alle Verantwortlichen genau wissen, was zu tun ist.