Incident Response Plan

April 14, 2022

# Änderungsnachweis

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Änderung** | **Name** | **Datum** |
| V0.1 | Erstellung des Dokumentes | Editor | 14.04.2022 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Inhaltsverzeichnis

[1. Änderungsnachweis 0](#_Toc100848707)

[2. Inhaltsverzeichnis 1](#_Toc100848708)

[3. Organisation 2](#_Toc100848709)

[3.1. Erklärung der Geschäftsleitung 2](#_Toc100848710)

[3.2. Zweck und Ziele 2](#_Toc100848711)

[3.3. Umfang 2](#_Toc100848712)

[3.4. Definitionen 2](#_Toc100848713)

[3.5. Rollen und Zuständigkeiten 2](#_Toc100848714)

[3.6. Priorisierung von Vorfällen 2](#_Toc100848715)

[3.7. Leistungskriterien 2](#_Toc100848716)

[3.8. Kontaktdaten 2](#_Toc100848717)

[3.8.1. Notfall-Kontakt 2](#_Toc100848718)

[3.8.2. Externes Incident Response Team 2](#_Toc100848719)

[3.8.3. Internet Service Provider 2](#_Toc100848720)

[3.8.4. Software Hersteller 2](#_Toc100848721)

[3.8.5. Behörden 2](#_Toc100848722)

[4. Response Plan 3](#_Toc100848723)

[4.1. Mission 3](#_Toc100848724)

[4.2. Strategien und Ziele 3](#_Toc100848725)

[4.3. Reaktion auf Vorfälle 3](#_Toc100848726)

[4.4. Kommunikation 3](#_Toc100848727)

[4.4.1. Intern 3](#_Toc100848728)

[4.4.2. Extern 3](#_Toc100848729)

[5. Genehmigung durch die Geschäftsleitung 4](#_Toc100848730)

# Organisation

*Dieses Dokument ist eine Vorlage und nicht für die 1:1 Übernahme gedacht. Abhängig von der Firmenstruktur, sollten Teile dieses Dokumentes angepasst werden.*

## Erklärung der Geschäftsleitung

Ein definiertes Sicherheitsvorfall-Konzept im Unternehmen ist eine Voraussetzung für die Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der IT-Infrastruktur. Durch eine schnelle Reaktion können Schäden minimiert und mittels Dokumentation die Wiederholung eines Vorfalls protokolliert werden.

Dieser Leitfaden beschreibt, wie Vorfälle unterschiedlicher Art priorisiert, kategorisiert, behandelt und kommuniziert werden. Als Grundlage zur Ergreifung der richtigen Massnahmen.

## Umfang

Dieses Dokument beinhaltet den Umgang und die Vorgehensweise mit Sicherheitsereignissen- und Vorfällen im Zusammenhang mit der IT-Infrastruktur. Sicherheitsvorfälle werden anhand einer vorgegebenen Priorisierung kategorisiert.

## Definitionen

### Sicherheitsereignis

Ein Sicherheitsereignis ist eine Anomalie in einem IT-System, welche durch Mitarbeitende oder Sicherheitssystem entdeckt wird.

Beispiele für Sicherheitsereignisse sind:

* Logins von fragwürdigen Orten
* Ein Laptop ging verloren / wurde gestohlen.
* Verdächtiger Netzwerkverkehr

### Sicherheitsvorfall

Ein Sicherheitsvorfall ist ein Sicherheitsereignis, bei welchem ein grosser Verdacht besteht, dass Unternehmensressourcen komprimiert wurden. Jeder Sicherheitsvorfall ist ein Sicherheitsereignis. Nicht jedes Sicherheitsereignis ist ein Sicherheitsvorfall.

Beispiele für Sicherheitsereignisse sind:

* Ein Benutzer hat sein Passwort auf einer Phishing-Webseite eingegeben
* Ransomware wurde ausgeführt

## Rollen und Zuständigkeiten

### IT Support

Der IT Support ist die erste Anlaufstelle für Mitarbeitende, überwacht die Systeme und ist für Supportangelegenheiten bei Sicherheitsevents und Sicherheitsvorfällen zuständig. Ab einem Sicherheitsereignis ist der IT Support für die Registrierung und Protokollierung zuständig.

Ab einem kritischen Sicherheitsvorfall eskaliert der IT Support den Vorfall an den Vorfallmanager.

#### Befugnisse

* Benutzer bei falschem Umgang mit IT-Ressourcen benachrichtigen
* Die Vorgesetzten eines Mitarbeitenden bei Verstössen gegen die IT-Richtlinien informieren.
* Bei Verdacht auf Komprimierung von Benutzeraccounts den Zugang und Berechtigungen von Mitarbeitenden sperren
* Jegliche Systeme und Clients mit Malware sofort herunterzufahren.
* Eskalation von Sicherheitsvorfällen an den Vorfallmanager

### Vorfallmanager

Eine oder mehrere Personen, die während des Zeitraumes eines Sicherheitsvorfalls für den Incident-Response Prozess verantwortlich sind und die Koordination übernehmen.

#### Befugnisse

* Einleiten von Managementmassnahmen bei schwerwiegenden Sicherheitsvorfällen.
* Informieren aller betroffenen Parteien.
* Eskalation an das Management, den Sicherheitsverantwortlichen und das Incident Response Team.

### Sicherheitsverantwortlicher

Eine Person, die die Gesamtverantwortung für die Informationssicherheit der IT-Infrastruktur trägt. Der Sicherheitsverantwortliche ist der Ansprechpartner für alle Sicherheitsmassnahmen, welche in der IT-Infrastruktur eingesetzt werden.

#### Befugnisse

* Systematische Sicherheitschecks durchführen.
* Die Zusammenarbeit mit den Behörden sicherstellen.
* Definieren von IT-Richtlinien und deren Durchsetzung.
* Berichte an die Geschäftsleitung.

### Kommunikationsverantwortlicher

Eine oder mehrere Personen, die während des Zeitraumes eines Sicherheitsvorfalls für die Kommunikation zuständig sind. Dies beinhaltet die interne Kommunikation zu Mitarbeitenden und, wenn nötig, die Kommunikation extern mit Medien und Behörden.

### Incident Response Team

Ein definiertes Team von internen und/oder externen IT-Spezialisten, die im Falle eines Sicherheitsvorfalls die Incident Response übernehmen. Das Incident Response Team ist zuständig für die Bestimmung der Auswirkungen, des Umfangs und der Art des Vorfalls. Zusätzlich reagiert das Incident Response Team auf den Vorfall und führt die Bereinigung durch.

## Kontaktdaten

Die Kontaktdaten befinden sich in der Datei “Incident Response Kontaktformular.docx”.

# Response Plan

## Mission

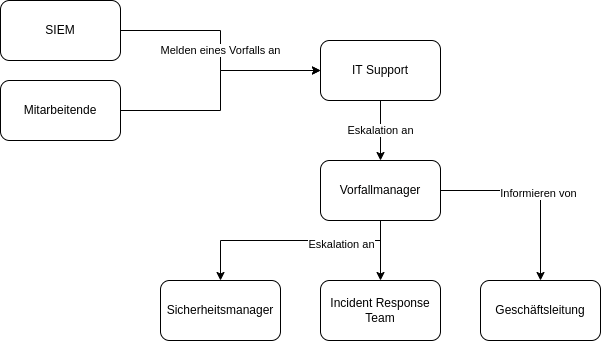
Bei einem Sicherheitsvorfall gilt es schnell zu reagieren, um Schäden möglichst minimal zu halten. Dies soll mit einem definierten Ablauf erreicht werden. Dadurch wissen alle Mitarbeitende wie Sie bei einem Vorfall reagieren müssen und wen es zu kontaktieren gilt.

## Strategien und Ziele

Durch die Priorisierung kann schneller entschieden werden, wann ein Vorfall eskaliert werden muss. Dies minimiert die Zeit bei Entscheidungen und gewährleistet ein einheitliches Vorgehen.

Ziel ist es, dass Vorfälle möglichst schnell reagiert wird und die richtigen Personen informiert werden.

## Kommunikationsablauf



## Priorisierung von Vorfällen

Die Priorisierung wird anhand nachfolgender Tabelle gemacht. Falls mehrere Prioritätsstufen auf ein Ereignis zutreffen, gilt es die höchste Priorität zu wählen.

### Priorisierungsmatrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Auswirkung** | | | |
| **Betroffene Entität** | **Kritisch** | **Hoch** | **Mittel** | **Klein** |
| **Unternehmenskritische Systeme:**   * **AD** * **Datenbanken** * **VIP-User Accounts** | 1 | 1 | 2 | 3 |
| **Reguläre Systeme:**   * **DHCP-Server** * **Applikationsserver** | 1 | 2 | 3 | 4 |
| **Computer** | 2 | 3 | 3 | 4 |
| **Benutzeraccounts** | 2 | 3 | 4 | 4 |

## Reaktion auf Vorfälle

### Kommunikation

Beim Umgang mit einem Sicherheitsvorfall muss mit einer gewissen Diskretion umgegangen werden. Wenn möglich sollte die Anzahl involvierter Personen auf einem Minimum beschränkt werden, bis sich der Vorfall geklärt hat. Personen im definierten Ablauf müssen immer informiert werden.

### Eskalation

Ab Priorität 3 eskaliert der IT Support den Vorfall an den Vorfallmanager. Dieser trifft weitere Entscheidungen über den Verlauf des Vorfalls und informiert nötige Parteien. Er entscheidet mit Absprache mit dem IT Support, ob der Vorfall weiter eskaliert werden muss oder nicht.

Ab Priorität 2 informiert der Vorfallmanager die Geschäftsleitung über den Vorfall. Zusätzlich muss das Incident Response Team informiert werden.

### Dokumentation

Alle Schritte während der Bewältigung eines Incidents werden dokumentiert und abgelegt.

Dies beinhaltet:

* Betroffene Systeme
* Betroffene Benutzer
* Gefundene Anomalien
* Eintrittsort
* Verbreitungsweg

### Nacharbeiten

Nach der Bewältigung eines Vorfalls werden, wenn möglich, neue Sicherheitsmassnahmen definiert, um ein erneutes Eintreten eines solchen Vorfalls zu minimieren.

# Genehmigung durch die Geschäftsleitung

Hiermit bestätigt die Geschäftsleitung, dass folgendes Dokument per XX.XX.XXXX in Kraft tritt.

Datum, Ort Name, Vorname

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_