# **Notfallplan**

## **1. Einleitung**

**1.1 Zweck des Notfallplans**

Der Notfallplan legt Verfahren und Richtlinien fest, um sicherzustellen, dass das Unternehmen auf unerwartete Ereignisse vorbereitet ist und die Geschäftskontinuität gewahrt bleibt. Ziel ist es, die Auswirkungen von Vorfällen auf ein Minimum zu reduzieren und die betroffenen Geschäftsprozesse so schnell wie möglich wiederherzustellen.

## **2. Geltungsbereich**

Der Plan gilt für:

• Alle Geschäftsprozesse und IT-Systeme, die als geschäftskritisch eingestuft wurden.

• Alle internen und externen Mitarbeiter, die in Notfallsituationen eingebunden sind.

* Szenarien wie Cyberangriffe, Naturkatastrophen, Stromausfälle, Hardwareausfälle oder Datenverluste.

## **3. Ziele**

1. Sicherstellung der Geschäftskontinuität durch ein funktionierendes BCM.

2. Minimierung der Auswirkungen von Ausfällen auf Geschäftsprozesse.

3. Schnelle Wiederherstellung der IT-Systeme und Daten durch Disaster Recovery.

4. Schutz der Reputation und Einhaltung regulatorischer Anforderungen.

## **4. Szenarien und Risiken**

**4.1 Typische Notfallszenarien**

• Cyberangriffe (z. B. Ransomware, DDoS).

• Naturkatastrophen (z. B. Überschwemmungen, Erdbeben).

• Technische Störungen (z. B. Serverausfälle, Stromausfall).

• Menschliches Versagen (z. B. versehentliches Löschen von Daten).

**4.2 Risikobewertung**

|  |  |  |  |
| --- | --- | --- | --- |
| **Szenario** | **Wahrscheinlichkeit** | **Auswirkung** | **Risikobewertung** |
| Cyberangriff (Ransomware) | Hoch | Kritisch | Hoch |
| Hardwareausfall | Mittel | Mittel | Mittel |
| Naturkatastrophe | Niedrig | Hoch | Mittel |

## **5. Aufbau des Notfallplans**

**5.1 Aktivierung des Notfallplans**

1. **Erkennung:** Der Vorfall wird durch das SOC, einen Mitarbeiter oder ein Alarmsystem gemeldet.
2. **Eskalation:** Der Notfallkoordinator wird informiert und entscheidet über die Aktivierung des Notfallplans.
3. **Kommunikation:** Das Notfallteam wird benachrichtigt, und die betroffenen Abteilungen werden informiert.

**5.2 Rollen und Verantwortlichkeiten**

|  |  |
| --- | --- |
| **Rolle** | **Verantwortlichkeiten** |
| **Notfallkoordinator** | Gesamtverantwortung für die Umsetzung des Notfallplans |
| **IT-Leiter** | Leitung des Disaster Recovery Teams, Wiederherstellung der IT-Systeme. |
| **Kommunikationsteam** | Informiert Mitarbeiter, Kunden und externe Partner. |
| **Mitarbeiter** | Befolgung der Anweisungen und Unterstützung bei der Wiederherstellung. |

**5.3 Priorisierte Geschäftsprozesse**

|  |  |  |  |
| --- | --- | --- | --- |
| **Prozess** | **Priorität** | **Maximale Ausfallzeit** | **Wiederherstellungsplan** |
| ERP-System | Hoch | 4 Stunden | Wiederherstellung aus Backups. |
| E-Mail-Kommunikation | Hoch | 2 Stunden | Failover auf Cloud-basierte Lösung. |
| Produktion | Mittel | 8 Stunden | Nutzung von Ausweichsystemen. |

## **6. Business Continuity Management (BCM)**

**6.1 BCM-Strategie**

1. **Analyse der Geschäftsprozesse:** Bewertung der kritischen Abhängigkeiten und der maximal tolerierbaren Ausfallzeiten (Maximum Tolerable Downtime, MTD).

2. **Alternativlösungen:**

• Nutzung von Ausweicharbeitsplätzen für betroffene Mitarbeiter.

• Umleitung von Geschäftsprozessen auf weniger betroffene Standorte.

**6.2 Kontinuitätspläne**

**6.2.1 IT-Services**

• **Regelmäßige Backups:** Tägliche Backups aller kritischen Systeme und Daten.

• **Failover-Systeme:** Automatische Umschaltung auf redundante Server.

* **Cloud-Lösungen:** Nutzung von SaaS für kritische Anwendungen wie E-Mail und Dokumentenmanagement.

**6.2.2 Kommunikation**

* **Notfallkommunikation:** Einrichtung eines separaten Kommunikationskanals (z. B. WhatsApp-Gruppe).
* **Mitarbeiterschulungen:** Regelmäßige Schulungen zur Nutzung der Notfallkommunikationswege.

## **7. Disaster Recovery (DR)**

**7.1 Disaster Recovery Plan**

**Ziel:** Wiederherstellung der IT-Systeme und Daten nach einem Ausfall.

**7.1.1 Vorbereitung**

• Implementierung von Disaster Recovery Sites (z. B. Hot-Site, Cold-Site).

• Dokumentation aller IT-Systeme, Abhängigkeiten und Wiederherstellungspläne.

**7.1.2 Wiederherstellungsphasen**

1. **Initiale Bewertung:** Analyse des Schadensumfangs durch das IT-Team.

2. **Priorisierung:** Kritische Systeme (z. B. ERP, E-Mail) werden zuerst wiederhergestellt.

3. **Wiederherstellung:** Nutzung von Backups oder Failover-Systemen.

4. **Validierung:** Überprüfung der wiederhergestellten Systeme durch Tests.

**7.2 Wiederherstellungsziele**

|  |  |  |
| --- | --- | --- |
| System | Recovery Time Objective (RTO) | Recovery Point Objective (RPO) |
| ERP-System | 4 Stunden | 1 Stunden |
| E-Mail | 2 Stunden | 15 Minuten |
| File-Server | 6 Stunden | 30 Minuten |

## **8. Test- und Wartungsplan**

**8.1 Tests**

• **Tabletop-Übungen:** Quartalsweise Simulation von Notfallszenarien.

• **Live-Tests:** Jährliche Wiederherstellungstests für kritische Systeme.

**8.2 Wartung**

• **Überprüfung des Notfallplans:** Halbjährliche Aktualisierung der Dokumentation.

* **Technologie-Aktualisierungen:** Regelmäßige Updates der IT-Infrastruktur und Sicherheitslösungen.

## **9. Kommunikationsplan**

**9.1 Interne Kommunikation**

• **Mitarbeiter:** Regelmäßige Updates über E-Mail oder ein Intranet-Portal.

• **Führungskräfte:** Direkte Kommunikation über dedizierte Kanäle.

**9.2 Externe Kommunikation**

• **Kunden und Partner:** Information über den Vorfall und die ergriffenen Maßnahmen.

• **Behörden:** Meldung gemäß regulatorischen Anforderungen (z. B. DSGVO).

## **10. Lessons Learned**

Nach jedem Notfall wird eine Nachbesprechung durchgeführt, um Folgendes zu bewerten:

• Was lief gut?

• Was muss verbessert werden?

• Aktualisierung des Notfallplans basierend auf den Ergebnissen.

## **11. Genehmigung**

**Name:** [Name des Verantwortlichen]

**Position:** [Position]

**Datum:** [Datum]

**Unterschrift:** [Unterschrift]