# Incident Response Plan

**Letzte Aktualisierung**: März 2025

## 1. Einleitung und Zweck

Dieser Incident Response Plan definiert strukturierte Prozesse und Verantwortlichkeiten zur Erkennung, Bewertung, Eindämmung, Behebung und Nachbereitung von Sicherheitsvorfällen in cloudbasierter IT-Umgebung. Der Plan dient als Leitfaden für ein schnelles und koordiniertes Vorgehen bei Sicherheitsvorfällen, um Auswirkungen zu minimieren und die Wiederherstellung zu beschleunigen. Aber zuerst: **Atmen Sie ein paarmal tief ein und aus und konzentrieren Sie sich!** Panik ist jetzt keine Hilfe.

## 2. Anwendungsbereich

Dieser Plan gilt für alle Systeme und Daten in unserer Cloud-Infrastruktur, einschließlich:

- Infrastructure-as-a-Service (IaaS) Ressourcen
- Platform-as-a-Service (PaaS) Komponenten
- Software-as-a-Service (SaaS) Anwendungen
- Hybride Umgebungen mit On-Premises-Komponenten
- Alle Daten, die in diesen Umgebungen verarbeitet oder gespeichert werden

## 3. Incident Response Team

### 3.1 Zusammensetzung des Teams

- **Incident Response Manager**: Koordination und Leitung des Gesamtprozesses
- **Cloud-Sicherheitsspezialist**: Technische Analyse und Reaktion in Cloud-Umgebungen
- **Systemadministrator**: Technische Unterstützung und Systemkonfiguration
- **Datenschutzbeauftragter**: Beratung zu datenschutzrechtlichen Anforderungen
- **Kommunikationsverantwortlicher**: Interne und externe Kommunikation
- **Rechtsberater**: Rechtliche Beratung (bei Bedarf hinzuzuziehen)

### 3.2 Kontaktinformationen und Erreichbarkeit

- Primärer Kontakt: incident-response@unternehmen.de
- Notfall-Hotline: +49 (0) 123 456789 (24/7 erreichbar)
- On-Call-Plan: [Verweis auf aktuellen Bereitschaftsplan]

## 4. Klassifizierung von Vorfällen

### 4.1 Schweregradbestimmung

| Schweregrad | Beschreibung | Beispiele | Reaktionszeit |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Kritisch** | Erhebliche Auswirkungen auf Geschäftsbetrieb oder sensible Daten; erfordert sofortige Aufmerksamkeit | Ransomware-Befall, Datenexfiltration, unbefugter Admin-Zugriff | Sofort (< 1 Std.) |
| **Hoch** | Signifikante Auswirkungen auf einzelne Systeme oder bestimmte Daten | Kompromittierung einzelner Systeme, Ausfall kritischer Cloud-Dienste | < 4 Std. |
| **Mittel** | Begrenzte Auswirkungen auf nicht-kritische Systeme oder Daten | Verdächtige Zugriffsversuche, Fehlkonfigurationen mit Sicherheitsrelevanz | < 24 Std. |
| **Niedrig** | Minimale oder keine unmittelbaren Auswirkungen | Einzelne fehlgeschlagene Login-Versuche, Policy-Verstöße ohne direkte Sicherheitsrelevanz | < 48 Std. |

### 4.2 Kategorien von Vorfällen

- **Datenschutzverletzungen**: Unbefugter Zugriff auf personenbezogene Daten
- **Systemintrusion**: Unbefugter Zugriff auf Systeme oder Konten
- **Malware-Infektionen**: Ransomware, Trojaner, Backdoors
- **Denial-of-Service (DoS)**: Beeinträchtigung der Verfügbarkeit von Diensten
- **Cloud-Ressourcen-Missbrauch**: Kryptomining, unbefugte Nutzung
- **Fehlkonfiguration**: Sicherheitsrelevante Fehlkonfigurationen in Cloud-Diensten
- **Zugriffsanomalien**: Ungewöhnliche Nutzungsmuster oder Zugriffsversuche

## 5. Incident Response Prozess

### 5.1 Vorbereitung

- Sicherstellung ausreichender Logging- und Monitoring-Konfiguration für alle Cloud-Dienste
- Implementierung automatisierter Warnmeldungen für verdächtige Aktivitäten
- Regelmäßige Schulung des Incident Response Teams
- Dokumentation aller Cloud-Ressourcen und Zugriffsberechtigungen
- Bereitstellung und Test dedizierter Forensik-Tools für Cloud-Umgebungen
- Einrichtung isolierter Forensik-Umgebungen in der Cloud

### 5.2 Erkennung und Analyse

1. **Erkennung**:
    a. Monitoring-Warnungen (SIEM, CSPM (Cloud-Security-Posture-Management))
    b. Meldungen von Mitarbeitern oder externen Parteien
    c. Automatisierte Sicherheitsscans und Audits
2. **Erste Bewertung**:
    a. Verifizieren des Vorfalls, um Fehlalarme auszuschließen
    b. Bestimmen des Schweregrads und der Kategorie

c. Dokumentieren der ersten Beobachtungen und betroffenen Systeme
d. Eskalation an das entsprechende Team basierend auf dem Schweregrad

3. **Detaillierte Analyse**:
    a. Sammeln von Cloud-Logs und Ereignisdaten
    b. Identifizieren des Angriffswegs und betroffene Ressourcen
    c. Bestimmen der potenziellen Auswirkungen und des Schadens
    d. Dokumentation aller Analyseschritte und Ergebnisse

## 5.3 Eindämmung

1. **Kurzfristige Eindämmung**:
    a. Isolieren betroffener Cloud-Instanzen durch Sicherheitsgruppen/Firewall-Regeln
    b. Temporäre Deaktivierung kompromittierter Benutzerkonten
    c. Blockieren verdächtiger IP-Adressen
    d. Sichern betroffener Ressourcen durch Snapshots/Backups für forensische Zwecke
2. **Langfristige Eindämmung**:
    a. Implementieren strengerer Sicherheitskontrollen
    b. Überprüfen und Anpassen von IAM-Berechtigungen
    c. Aktualisieren von Cloud-Sicherheitsrichtlinien
    d. Überprüfen ähnlicher Systeme auf Kompromittierung

## 5.4 Beseitigung

1. **Entfernen der Bedrohung**:
    a. Bereinigen infizierter Systeme oder Neuaufbau aus vertrauenswürdigen Images
    b. Entfernen von Malware und unbefugten Zugängen
    c. Zurücksetzen kompromittierter Anmeldeinformationen
2. **Systemwiederherstellung**:
    a. Wiederherstellen von Daten aus vertrauenswürdigen Backups
    b. Stufenweise Wiederinbetriebnahme von Diensten nach Sicherheitsüberprüfung
    c. Überprüfen der wiederhergestellten Umgebung auf Anzeichen fortbestehender Kompromittierung

## 5.5 Wiederherstellung

1. **Betriebswiederaufnahme**:
    a. Stufenweise Rückführung in den Normalbetrieb
    b. Überwachung auf ungewöhnliche Aktivitäten
    c. Implementierung zusätzlicher Sicherheitskontrollen
2. **Bestätigung der Wiederherstellung**:
    a. Validierung der Funktionalität aller betroffenen Dienste
    b. Überprüfung der Datenintegrität

c. Bestätigung der vollständigen Bereinigung

### 5.6 Nachbereitung

1. **Dokumentation und Berichterstattung**:
    a. Erstellung eines detaillierten Vorfallsberichts
    b. Dokumentation aller ergriffenen Maßnahmen und Erkenntnisse
    c. Aufzeichnung des Zeitplans des Vorfalls und der Reaktion
2. **Lessons Learned**:
    a. Durchführung einer Post-Incident-Analyse
    b. Identifizierung von Verbesserungspotentialen
    c. Aktualisierung von Sicherheitsrichtlinien und -kontrollen
3. **Prozessverbesserung**:
    a. Aktualisierung des Incident Response Plans basierend auf Erkenntnissen
    b. Behebung identifizierter Sicherheitslücken
    c. Durchführung zusätzlicher Schulungen bei Bedarf

## 6. Cloud-spezifische Reaktionsmaßnahmen

### 6.1 AWS-spezifische Maßnahmen

- Isolation von EC2-Instanzen durch Sicherheitsgruppen
- Temporäre Deaktivierung von IAM-Rollen und Zugriffsschlüsseln
- Aktivierung von AWS GuardDuty für erweiterte Bedrohungserkennung
- Überprüfung von CloudTrail-Logs auf unbefugte Aktivitäten
- Erstellen von Snapshots kompromittierter EC2-Instanzen und EBS-Volumes

### 6.2 Azure-spezifische Maßnahmen

- Isolation von VMs durch Netzwerksicherheitsgruppen
- Überprüfung von Azure AD Sign-in-Logs auf verdächtige Aktivitäten
- Nutzung von Azure Security Center für Bedrohungsanalyse
- Temporäre Deaktivierung von App Registrations und Service Principals
- Sicherung von Forensik-Artefakten mit Azure Forensics-Tools

### 6.3 Google Cloud-spezifische Maßnahmen

- Isolation von Compute Engine-Instanzen durch Firewall-Regeln
- Überprüfung von Cloud Audit Logs auf unbefugte Aktivitäten
- Nutzung von Security Command Center für Bedrohungsanalyse
- Rotation kompromittierter Service Account-Schlüssel
- Snapshots von Compute Engine-Instanzen für forensische Untersuchungen

## 7. Kommunikationsplan

### 7.1 Interne Kommunikation

- **Erste Benachrichtigung**: Innerhalb von 1 Stunde nach Bestätigung eines Vorfalls

- **Regelmäßige Updates**: Alle 2-4 Stunden je nach Schweregrad des Vorfalls
- **Eskalationspfad**: Technisches Team → Abteilungsleiter → Geschäftsführung
- **Kommunikationskanal**: Primär E-Mail und MS Teams; Telefonkonferenzen für kritische Vorfälle

### 7.2 Externe Kommunikation

- **Kundenkommunikation**: Nach Genehmigung durch Geschäftsführung und Rechtsberatung
- **Behördenmeldungen**: Nach rechtlichen Vorgaben (z.B. DSGVO-Meldung innerhalb von 72 Stunden)
- **Medienkommunikation**: Ausschließlich durch autorisierte Kommunikationsverantwortliche

## 8. Compliance und regulatorische Anforderungen

### 8.1 DSGVO-Compliance

- Meldung an Aufsichtsbehörde innerhalb von 72 Stunden bei Datenschutzverletzungen
- Dokumentation aller Vorfälle gemäß Art. 33 DSGVO
- Benachrichtigung betroffener Personen/Stakeholder, wenn erforderlich

### 8.2 Branchenspezifische Anforderungen

- [Ergänzen Sie hier branchenspezifische Compliance-Anforderungen]

## 9. Ressourcen und Tools

### 9.1 Tools für Incident Response

- Cloud-native Sicherheitstools: AWS Security Hub, Azure Security Center, Google Security Command Center
- SIEM-Lösung: [Name der SIEM-Lösung des Unternehmens]
- Forensik-Tools: Spezialisierte Cloud-Forensik-Tools wie AWS Forensics Framework
- Kommunikationstools: [Namen der im Unternehmen genutzten Tools]

### 9.2 Dokumentationsvorlagen

- Incident Response Formular
- Vorfalls-Logbuchvorlage
- Kommunikationsvorlagen für verschiedene Stakeholder
- Post-Incident-Analyse-Fragebogen

## 10. Schulung und Übungen

### 10.1 Schulungsplan

- Jährliche Auffrischung für alle Incident Response Team-Mitglieder
- Vierteljährliche Updates zu neuen Bedrohungen und Cloud-spezifischen Risiken
- Spezifische Schulungen für neue Cloud-Dienste oder -Features

### 10.2 Übungen

- Jährliche Tabletop-Übungen für verschiedene Vorfallsszenarien
- Halbjährliche technische Übungen zur Simulation realer Vorfälle

- Nachbesprechungen und Verbesserungsmaßnahmen nach jeder Übung

## Anhang A: Kontaktliste

| Rolle | Name | E-Mail | Telefon | Bereitschaft |
|---|---|---|---|---|
| Incident Response Manager | [Name] | [E-Mail] | [Telefon] | Primär |
| Cloud-Sicherheitsspezialist | [Name] | [E-Mail] | [Telefon] | Primär |
| Systemadministrator | [Name] | [E-Mail] | [Telefon] | Backup |
| Datenschutzbeauftragter | [Name] | [E-Mail] | [Telefon] | Nach Bedarf |
| Kommunikationsverantwortliche r | [Name] | [E-Mail] | [Telefon] | Nach Bedarf |
| Externe Forensik-Firma | [Firma] | [E-Mail] | [Telefon] | 24/7 Vertrag |

## Anhang B: Checklisten für häufige Vorfallsarten

### B.1 Ransomware-Vorfall

1. Isolieren infizierter Systeme
2. Snapshot der betroffenen Cloud-Ressourcen erstellen
3. Lösegeldanforderungen dokumentieren (nicht bezahlen ohne Genehmigung)
4. Backups auf Integrität prüfen
5. Infektionsquelle identifizieren
6. Wiederherstellungsplan entwickeln
7. Systeme aus sauberen Backups wiederherstellen
8. Rechtliche Meldepflichten prüfen

### B.2 Unbefugter Zugriff

1. Betroffene Konten identifizieren und sperren
2. Zugriffsprotokollierung für alle Cloud-Dienste aktivieren
3. Zugriffsverlauf auf verdächtige Aktivitäten prüfen
4. Sicherheitseinstellungen für ähnliche Konten überprüfen
5. Multi-Faktor-Authentifizierung einrichten/erzwingen
6. Passwörter und Zugriffsschlüssel rotieren
7. IAM-Berechtigungen überprüfen und unnötige Rechte entfernen

### B.3 Datenleck

1. Betroffene Datenspeicher identifizieren
2. Zugriffskontrollen für alle betroffenen Ressourcen überprüfen
3. Öffentliche Zugänglichkeit von Datenspeichern überprüfen
4. Umfang und Art der exponierten Daten ermitteln

5. Datenschutzbeauftragten einbeziehen
6. Rechtliche Meldepflichten prüfen und einhalten
7. Betroffene informieren (falls erforderlich)
8. Sicherheitskontrollen für alle ähnlichen Datenspeicher überprüfen

## Anhang C: Forensik-Leitfaden für Cloud-Umgebungen

### C.1 Grundlegende Forensik-Schritte

1. Snapshots/Backups der betroffenen Ressourcen erstellen
2. Logging-Daten der Cloud-Plattform sichern
3. Zugriffshistorie und API-Aufrufe analysieren
4. Netzwerkdaten und Verbindungsinformationen sammeln
5. Forensische Images von virtuellen Maschinen erstellen
6. Forensische Analysetools in isolierter Umgebung anwenden
7. Beweiskette dokumentieren und aufrechterhalten

Es wird empfohlen, den Incident Response Plan in ausgedruckter Form an einem für die Verantwortlichen leicht zugänglichen Ort aufzubewahren. Dies gewährleistet, dass auch bei vorübergehenden Stromausfällen oder wenn elektronische Geräte nicht verfügbar sind, die notwendigen Maßnahmen zur Incident Response ohne Verzögerung eingeleitet und die einzelnen Handlungsschritte systematisch abgearbeitet werden können.