# **Backup- und Ausfallsicherheitskonzept für das SOC**

## **1. Einleitung**

Ein Security Operations Center (SOC) ist das Herzstück der IT-Sicherheitsüberwachung. Um den reibungslosen Betrieb und die Kontinuität zu gewährleisten, ist ein umfassendes Backup- und Ausfallsicherheitskonzept erforderlich. Dieses Konzept schützt vor Datenverlust, Ausfällen und Angriffen, die die Effektivität des SOC beeinträchtigen könnten.

## **2. Ziele des Konzepts**

1. Sicherstellung der Verfügbarkeit von SOC-Diensten, auch bei ungeplanten Ausfällen.
2. Schutz vor Datenverlust und schneller Wiederherstellung von kritischen Daten.
3. Minimierung der Ausfallzeiten durch redundante Systeme und automatisierte Prozesse.
4. Einhaltung regulatorischer Vorgaben (z. B. ISO 27001, NIS2, DORA).
5. Maximierung der Effizienz und Zuverlässigkeit des SOC durch regelmäßige Tests und Updates.

## **3. Bestandteile des SOC und Backup-Bedarf**

|  |  |  |  |
| --- | --- | --- | --- |
| **Komponente** | **Beschreibung** | **Backup-Frequenz** | **Recovery-Zeit** |
| **SIEM-Systeme** | Speicherung und Analyse von Logs und IoCs | Stündlich (Transaktionen) | 1 Stunde |
| **SOAR-Plattform** | Automatisierung und Orchestrierung. | Täglich (Konfigurationen) | 2 Stunden |
| **Threat Intelligence Feeds** | Aktuelle Bedrohungsdaten und IoCs. | Täglich (aktuelle Feeds) | 30 Minuten |
| **Case Management Systeme** | Verwaltung von Vorfällen und Reports. | Täglich (Vorfall-Daten) | 2 Stunden |
| **Datenbanken** | Speicherung historischer Daten und Analysen. | Täglich (vollständig) | 4 Stunden |
| **Netzwerk-Logs** | Überwachung der Netzwerkaktivität. | 1 Stunde (inkrementell) | 1 Stunde |

## **4. Backup-Strategie**

**4.1 Backup-Typen**

* **Full Backup:** Komplette Kopie aller Daten, z. B. wöchentlich.
* **Inkrementelles Backup:** Speichert nur Änderungen seit dem letzten Backup, z. B. stündlich.
* **Differentielles Backup:** Speichert Änderungen seit dem letzten vollständigen Backup, z. B. täglich.

**4.2 Standortstrategie**

* **On-Premise:** Lokale Backups für schnelle Wiederherstellung.
* **Offsite:** Backups in entfernten Rechenzentren zur Absicherung gegen physische Schäden.
* **Cloud-Backups:** Nutzung von Cloud-Anbietern wie AWS, Azure oder Google Cloud für Flexibilität und Skalierbarkeit.

**4.3 Redundanzstrategie**

• Mindestens drei Kopien aller Daten:

• **Primäre Daten:** Produktionsumgebung.

• **Sekundäre Kopie:** Lokales Backup.

• **Tertiäre Kopie:** Offsite oder Cloud-Backup.

## **5. Ausfallsicherheitskonzept**

**5.1 Redundante Infrastruktur**

• **Server:** Cluster mit automatischem Failover.

• **Netzwerk:** Redundante Switches, Firewalls und Internetverbindungen.

• **Stromversorgung:** USV und Dieselgeneratoren.

**5.2 Disaster Recovery**

1. **Hot Site:** Vollständig ausgestatteter Standort, der sofort einsatzbereit ist.
2. **Warm Site:** Teilweise vorbereiteter Standort, der innerhalb weniger Stunden aktiviert werden kann.
3. **Cold Site:** Nur physische Infrastruktur, Aktivierung dauert mehrere Tage.

**5.3 Automatisierte Failover-Systeme**

• Automatische Umschaltung auf redundante Systeme bei Ausfällen.

* Beispiel: Cluster für SIEM und SOAR, um kontinuierliche Datenverarbeitung sicherzustellen.

## **6. Monitoring und Tests**

|  |  |  |
| --- | --- | --- |
| **Maßnahme** | **Frequenz** | **Ziel** |
| **Backup-Überprüfung** | Wöchentlich | Sicherstellen, dass Backups vollständig und fehlerfrei sind. |
| **Wiederherstellungstests** | Quartalsweise | Überprüfung der Recovery-Zeit und -Integrität. |
| **Failover-Tests** | Halbjährlich | Sicherstellen, dass redundante Systeme nahtlos funktionieren. |
| **Netzwerkbelastungstests** | Jährlich | Testen der Infrastruktur unter extremen Bedingungen. |

## **7. Dokumentation und Prozesse**

**7.1 Backup-Prozesse**

1. Backup-Zeitplan erstellen und einhalten.

2. Protokollierung aller Backups.

3. Benachrichtigungen bei fehlgeschlagenen Backups.

**7.2 Wiederherstellungsprozesse**

1. Notfall-Team benachrichtigen.

2. Backup-Daten auf redundante Systeme wiederherstellen.

3. Testen der wiederhergestellten Systeme vor Live-Betrieb.

**7.3 Eskalation im Notfall**

• **Stufe 1:** Kleinere Vorfälle, Wiederherstellung innerhalb von Stunden.

• **Stufe 2:** Größere Ausfälle, Einbeziehung von externen Beratern.

• **Stufe 3:** Katastrophenfall, Aktivierung des Disaster Recovery Plans.

## **8. Sicherheitsmaßnahmen für Backups**

|  |  |
| --- | --- |
| **Risikofaktor** | **Maßnahme** |
| **Datenverlust** | Verschlüsselung aller Backups (z. B. AES-256). |
| **Unbefugter Zugriff** | Zugriffskontrolle und MFA für Backup-Systeme. |
| **Fehlende Integrität** | Hashing zur Verifizierung der Backups. |
| **Ransomware-Angriffe** | Air-gapped Backups (physisch getrennt). |

## **9. Compliance**

|  |  |
| --- | --- |
| **Anforderung** | **Umsetzung** |
| **ISO 27001** | Implementierung eines ISMS mit dokumentierten Backups. |
| **NIS2** | Sicherstellung von Wiederherstellbarkeit kritischer Systeme. |
| **DORA** | Resilienz durch redundante Systeme und Tests. |