DGI® Deutsche Gesellschaft für Informationssicherheit AG

Security Information and Event Management (SIEM)

- Konzept -

Inhaltsverzeichnis

1 Ziel und Zweck

Diese Regelung bestimmt die einzuhaltenden Vorgaben für das Security Information and Event Management.

Durch die Einhaltung der Vorgaben dieser Regelung soll insbesondere Folgendes sichergestellt werden

- Die Einhaltung gesetzlicher und vertraglicher Anforderungen zur Risikofrüherkennung sowie der Umsetzung von technischen und organisatorischen Maßnahmen (Compliance)
- Die Erfüllung der Anforderungen bezüglich der vereinbarten Steuerung, des Monitorings, der Protokollierung, der Detektion und der Reaktion von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen des Betriebs der IT
- Die Umsetzung von Maßnahmen für die Vermeidung von unerwünschten Beeinträchtigungen der Betriebsfähigkeit der IT
- Die Unterstützung bei der
    - Erfüllung der Anforderungen an die vereinbarte Überwachung, Messung, Analyse und Auswertung des IT-Betriebs
    - Erbringung von Nachweisen wie Protokollen und Berichten, um die vereinbarten und geforderten Nachweispflichten zu erfüllen
    - Umsetzung von Maßnahmen für die frühzeitige Detektion und frühestmögliche Reaktion, insbesondere in Folge von sicherheitskritischen Vorfällen, zur Vermeidung von Schäden
    - Auswertung und forensischen Analyse von sicherheitsrelevanten Ereignissen
    - Identifikation von Bedrohungen (Threat Detection) für den ordnungsgemäßen, sicheren und konformen Betrieb der IT
    - Zentralisierung der Informationsbeschaffung und der angemessenen Darstellung von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen des Betriebs der IT

2 Geltungsbereich

Die Vorgaben dieser Regelung gelten für

- Geltungsbereich benennen, wie „*die gesamte Organisation, die Abteilung IT oder den Standort Berlin*“

3 Verantwortlichkeiten für das Management dieser Regelung

Verantwortlich für die Planung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.
Verantwortlich für die Umsetzung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.
Verantwortlich für die Überwachung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.
Verantwortlich für die Aufrechterhaltung und Verbesserung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.

5.3.3 Verantwortungsbereiche für das Monitoring und die Behandlung von Events

Die Vorgaben für das Management der Aktivitäten für die Durchführung der Identifikation und Detektion von sicherheitsrelevanten sowie der Reaktion auf sicherheitsrelevante Informationen, Ereignissen und Vorfällen sowie für den Betrieb eines SIEM-Tools muss durch den Informationssicherheitsbeauftragten initiiert, gesteuert sowie angemessen dokumentiert werden, um die Erfüllung der Anforderungen an den sicheren, konformen und ordnungsgemäßen Geschäftsbetrieb zu gewährleisten.

Die Verantwortung für die Planung, die Umsetzung, den Betrieb sowie die fortlaufende Aufrechterhaltung und Verbesserung der SIEM-Lösung sowie der Festlegung der Verantwortlichkeiten und Befugnisse für den Betrieb des SIEM-Tools liegt beim Informationssicherheitsbeauftragten.

Zudem müssen sämtliche Erkenntnisse aus qualifizierten sicherheitsrelevanten Informationen

5.3.3.2 Content Engineer

Es sollten verantwortliche Personen, für die Implementierung von Regeln zur Detektion von Verdachtsmomenten, für die fortlaufende Verbesserung und Optimierung bestehender und implementierter Regeln, um insbesondere den Use Cases gerecht zu werden sowie Fehlmeldungen zu reduzieren und zu vermeiden sowie für die Entwicklung, Festlegung und Implementierung von Messwerten, Log-Datenaufzeichnungen, Protokollen und Berichten, bestimmt und benannt werden (Content Engineer).

5.3.3.3 Security Incident Manager

Es sollten verantwortliche Personen, für die Behandlung von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen, insbesondere für die qualifizierte Risikobewertung und die Umsetzung der reaktiven Maßnahmen bei der Detektion von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen (Security Incidents), für die Koordination mit dem Business Continuity Management oder dem CERT und Cyber Security Incident Response Team (CSIRT) sowie für das Berichtswesen von Security Incidents gegenüber den relevanten Stakeholdern bestimmt, und benannt werden (Security Incident Manager).

5.3.3.4 Security Analyst

Es sollten verantwortliche Personen, für die differenzierte Analyse und Bewertung der Informationen aus

- Meldungen des CERT oder CSIRT
- Hinweise sämtlicher Stakeholder
- Meldungen und Berichte des SIEM-Tools

Zudem müssen verantwortliche Personen, für

- die Installation und den Aufbau der SIEM-Infrastruktur,
- den Betrieb und die Wartung der SIEM-Infrastruktur,
- die Anbindung von Datenquellen an das Monitoring des SIEM-Tools sowie
- die Entwicklung und Implementierung der Prozesse und Aktivitäten für den Betrieb der SIEM-Lösung, insbesondere des SIEM-Tools,

bestimmt und benannt werden.

Eignung dahingehend bewertet werden, ob die Überwachung, die Messung und das Monitoring sowie die Analyse und Bewertung der spezifischen Anwendungsfälle realistisch umsetzbar sind.

Die Use Cases sowie die herangezogenen Indikatoren und Parameter für die Festlegung der Überwachungs- und Verhaltensregeln müssen anforderungsgerecht dokumentiert, bereitgestellt und aufbewahrt werden.

5.3.5.1 Identifikation und Festlegung der Datenquellen für das Monitoring

Um die geforderte und vereinbarte Überwachung, Messung und das Monitoring von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen zu gewährleisten, muss bei der Auswahl der Datenquellen für die Überwachung und das Monitoring sowie die Bereitstellung der Daten insbesondere Folgendes beachtet werden:

- Informationsquellen Dritter, wie Hersteller oder Betreiber von IT-Systemen
- CERT- und CSIRT-Meldungen
- Informationen und Log-Daten
    - aus Betriebssystemen
    - aus Hardware-Komponenten
    - aus Software und Anwendungen
    - des Netzwerkverkehrs wie Flow-Daten oder Traffic
    - aus Datenbanken
    - des Datenverkehrs wie Web-Traffic oder Netzwerk-Traffic
    - zur Nutzung von Zutritts-, Zugangs- und Zugriffsberechtigungen (Access)
    - aus IT-Infrastrukturkomponenten wie Domain-Controller, Router, Switches, Bridges, Wireless Access Points, Modems und Hubs

- aus IT-Systemen wie Servern, ICS-Systemen, Videoüberwachungssystemen, Peripheriegeräten, netzwerkfähigen Geräten, Clients und Storage-Systemen
- aus Cloud-Systemen
- aus Security Devices wie IDP, IPS, PKI, Proxy-Servern, Firewalls, Antivirus-Software und Content-Filter, Web-Filter

Sämtliche Informationen der als relevant zu berücksichtigenden Datenquellen für die Detektion von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen müssen anforderungsgerecht dokumentiert, bereitgestellt und aufbewahrt werden.

5.3.6 Kategorisierung und Klassifizierung von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen

- Ableitung von Maßnahmen der Informationssicherheit aus der Kategorisierung und Klassifizierung
- Harmonisierung der Kategorisierung und Klassifizierung von Configuration Items sowie Events, Incidents und Problems
- sicherheitsrelevante Informationen müssen zeitgerecht wie vereinbart sowie eindeutig kategorisiert und klassifiziert werden

Die Kategorien und Klassen sowie die Prozesse für die Festlegung der Kategorisierung und Klassifizierung müssen anforderungsgerecht dokumentiert, bereitgestellt und aufbewahrt werden.

5.3.7 Priorisierung der Reaktion auf sicherheitsrelevante Ereignisse und Vorfälle

Die identifizierten, analysierten und bewerteten Informationssicherheitsrisiken und die Auswirkungen auf den ordnungsgemäßen, sicheren und konformen Geschäftsbetrieb sowie auf die Betriebsfähigkeit der IT dienen der Priorisierung für die Durchführung der Aktivitäten und Aufgaben einer Reaktion auf ein sicherheitsrelevantes Ereignis oder einen sicherheitsrelevanten Vorfall.

Die Analyse, Abschätzung und Bewertung der spezifischen Auswirkungen auf den sicheren Geschäftsbetrieb sowie auf die Betriebsfähigkeit der IT muss gemäß der Vorgaben aus den Bereichen Risikomanagement, IT-Risikomanagement, Business Continuity Management und Informationssicherheit erfolgen.

Insbesondere muss die geforderte und vereinbarte Umsetzung von Maßnahmen für die Sicherstellung der

bei der Priorisierung der Durchführung der Aktivitäten und Aufgaben einer Reaktion auf sicherheitsrelevante Ereignisse und Vorfälle muss insbesondere Folgendes einbezogen und berücksichtigt werden

- die spezifische Sicherheitsrelevanz und Kritikalität der IT-Systeme für den Geschäftsbetrieb
- das Ausmaß der Beeinträchtigungen der Betriebsfähigkeit der IT
- die Optionen für die Wiederaufnahme von Aufgaben, Aktivitäten und Tätigkeiten des Geschäftsbetriebs
- die Optionen der Risikobehandlung und Risikoakzeptanz im Zuge der Risikopriorisierung
- die Erfüllung der Anforderungen an die Informationssicherheit
- die Erfüllung der Anforderungen an die Business Continuity
- die Erfüllung der Vorgaben aus dem Risikomanagement insbesondere dem IT-Risikomanagement

Die Herleitung der Festlegung der Durchführung der Aktivitäten und Aufgaben für die Priorisierung einer Reaktion muss anforderungsgerecht dokumentiert, bereitgestellt und aufbewahrt werden.

5.3.8 Detektion von sicherheitsrelevanten Ereignissen und Vorfällen

5.3.8.1 Besonderheiten der Protokollierung beim Betrieb einer SIEM-Lösung

Neben den Anforderungen an eine angemessene Protokollierung des IT-gestützten Geschäftsbetriebs, muss für die Sicherstellung der vereinbarten Detektion von sowie die Reaktion auf sicherheitsrelevante Informationen, Ereignisse und Vorfälle die Protokollierung einer SIEM-Lösung insbesondere Folgendes gewährleisten

- Umsetzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Informationen, Ereignisse und Vorfälle

sowie von Angriffsszenarien müssen insbesondere die folgenden Anforderungen durch die SIEM-Lösung erfüllt werden

- Durchführung der Verhaltensanalyse sowie Identifikation von IT-Nutzern, sämtlicher IT-Entitäten, wie IT-Systeme, Anwendungen, Hardware, Software, IT-Infrastrukturkomponenten und Security Devices (User and Entity Behavior Analytics)
- Identifikation von Bedrohungen und Angriffen auf der Grundlage von Anomalien
- Kontinuierliche Verbesserung der Begrenzung der False Positive-Meldungen und Verkürzung der Reaktionszeiten durch Optimierung und Anpassung der hinterlegten Grenzwerte und Entwicklung der Use Cases
- Identifikation und Filterung von Anomalien in Echtzeit sowie von sicherheitsrelevanten Informationen, Ereignissen und Vorfällen
- Frühestmögliche Meldung von Sicherheitsbedrohungen (Warning oder Alert)
- Frühestmögliche Reaktion und automatisierte Behandlung von unerwünschten Beeinträchtigungen