DGI® Deutsche Gesellschaft für Informationssicherheit AG

Monitoring und Event Management

Prüfung und Freigabe

Geprüft am	Durch	Unterschrift
TT.MM.JJJJ		

Freigabe am	Durch	Unterschrift
TT.MM.JJJJ		

Änderungshistorie

Version	Geändert am	Durch	Änderungen
	TT.MM.JJJJ		
	TT.MM.JJJJ		
	TT.MM.JJJJ		

Dokumentensteuerung und Verteilerkreis

A accountable - rechenschaftspflichtig
R responsible - verantwortlich
C consulted - beratend einzubeziehen
I informed - zu informieren

	Erstellung	Prüfung	Freigabe	Verteilung
Arbeitssicherheit				
Aufsichtsrat				
Betriebsrat / Personalrat				
Buchhaltung / Rechnungswesen				
Business Continuity Management				
Compliance				
Datenschutz				
Einkauf				
Fertigung / Produktion				
Finanzen				
Forschung und Entwicklung				
Geschäftsführung				
Gesellschafter				
Hausverwaltung / Facility Management				
Informationssicherheit				
IT				
IT-Sicherheit				
Kundenbetreuung				
Logistik / Materialwirtschaft				
Marketing				
Personal				
Public Relations				
Qualitätssicherung				
Qualitätsmanagement				
Recht				
Risikomanagement				
Verkauf / Vertrieb				
Sonstige				

Inhaltsverzeichnis

5.3 Umsetzung

5.3.1 Allgemeines

Die Prozesssteuerung sowie das Management für die Umsetzung dieser Regelung müssen dokumentiert und sollten in die bestehende Aufbau- und Ablauforganisation integriert werden.

Die Maßnahmen für die Umsetzung müssen kontinuierlich sowie anlassbezogen aktualisiert, angepasst und verbessert werden.

5.3.2 Anforderungen an das Management des Monitoring und von Events

Die Anforderungen an das Management des Monitoring und von Events müssen regelmäßig durch die

zuständigen Informationen bei der Bestimmung, Erhebung, Verarbeitung sowie der Reaktion und Maßnahmenumsetzung

- Angaben zum Umfang der zu erhebenden Informationen
- Angaben zum Umfang der zu archivierenden Informationen
- Angaben zu Risiken und potenziellen Schadensauswirkungen für den Geschäftsbetrieb bei der Beeinträchtigung des definierten Sicherheitsniveaus
- Verfahren für den Zugang und den Zugriff auf die Informationen
- Verfahren für die Kontrolle, Wartung und den Test von Monitoring-Tools, Geräten und Systemen
- Eine einheitliche und harmonisierte Kategorisierung von Events, Incidents, Problems und den relevanten Configuration Items
- Anforderungen an die Schutzziele der zu verarbeitenden Informationen insbesondere der Verfügbarkeit, der Integrität und der Vertraulichkeit

- Anforderungen an Datenquellen
- Anforderungen an Formate der Informationen
- Anforderungen an Schnittstellen
- Anforderungen an die Monitoring-Systeme
- Anforderungen an die Übermittlung von Informationen
- Anforderungen an die Archivierung von Informationen
- Anforderungen für den Einsatz kryptographischer Verfahren bei der Übermittlung, dem Zugang und Zugriff sowie der Wiederherstellung von Informationen

Um die definierten Anforderungen für das Management des Monitoring und von Events zu erfüllen, sollten relevante Abhängigkeiten insbesondere zu den folgenden Regelungen berücksichtigt werden

- Das Passwortkonzept

- Dem Servicekatalog Management
- Dem Incident Management
- Dem Problem Management
- Dem Change Management
- Dem Release and Deployment Management
- Dem Information Security Management
- Dem Service Asset and Configuration Management (SACM)
- Dem Service Continuity Management
- Dem Prozess Service Reporting und Measurement

Sämtliche Dokumentationen müssen angemessen vorgehalten und aufbewahrt werden.

5.3.3 Identifikation der zu überwachenden Informationen

Sämtliche Configuration Items sollten auf die Möglichkeit hin bewertet werden, ob Logdaten sowie eine automatisierte Benachrichtigung erzeugt werden können.

Grundsätzlich sollten sämtliche betriebsrelevanten und sicherheitsrelevanten Aktivitäten von Configuration Items, die für die Sicherstellung eines ordnungsgemäßen, sicheren und konformen Geschäftsbetriebs erforderlich sind, überwacht werden. Hierzu zählen insbesondere

- Details zur Identifikation des Configuration Item, wie zur Funktionsweise sowie dem Zweck des Einsatzes, zu zeitlichen Korrelationen, zu Überlastung der erforderlichen Ressourcen für den Betrieb, zu Einschränkungen, zu unzureichender Performance, zum Status, Angaben zu Entwicklungs- und Testphasen, für
  - Sämtliche betriebsrelevanten und sicherheitsrelevanten Applikationen
  - Art bzw. Typ der ausgeübten Berechtigung
  - Status der Ausübung der Berechtigung, wie erfolgreich / nicht erfolgreich
  - Anzahl der Versuche zur Ausübung der Berechtigung
- Die technischen Schnittstellen, mit Details zu
  - Art der Schnittstelle
  - Status der Schnittstelle
  - Möglichkeit der Überwachung und Protokollierung der Schnittstelle
  - Fehlermeldungen, wie Laufzeitfehler oder unerwartete Programmfehler
  - Laufzeitinformationen wie Start und Beendigung einer Anwendung sowie durchgeführte Datentransaktionen

Des Weiteren sollte eruiert werden, ob die Festlegung von ober- oder unterschwelligen Grenzwerten oder einer unerwünschten Statusänderung erfolgen kann und korrelierend eine automatisierte Benachrichtigung über eine Statusänderungen generiert werden kann.

Die identifizierten Configuration Items sowie deren betriebsrelevanten und sicherheitsrelevanten Aktivitäten inklusive der erforderlichen Details müssen anforderungsgerecht dokumentiert werden.

5.3.4 Festlegung der Grenzwerte für Benachrichtigungen

Für sämtliche Configuration Items sollten Grenzwerte für das Über- oder Unterschreiten oder die Werte für eine unerwünschte Statusänderung festgelegt werden.

Die festzulegenden Grenzwerte sollten auf Basis der Vorgaben insbesondere aus dem

- Anforderungen an interne und externe Datenquellen
- Anforderungen an Formate der Informationen
- Anforderungen an Schnittstellen
- Einbeziehung wirtschaftlicher Faktoren bei der Erhebung und Vorhaltung der Logdaten und Protokolldateien
- Möglichkeiten der Parametrisierung der zu erhebenden Logdaten und Protokolldateien
- Sicherstellung der Transparenz und Nachvollziehbarkeit bei der Bestimmung, Erkennung, Erhebung und Bewertung der Logdaten und von Protokolldateien
- Einhaltung der Prinzipien der Informationssicherheit bei der Erhebung und Vorhaltung der Logdaten und Protokolldateien, insbesondere der Einhaltung der
    - Datensparsamkeit
    - Datenminimierung

- Anonymisierung und Pseudonymisierung
- Zweckbindung
- Rechtmäßigkeit

Die Protokollierungsinfrastruktur sollte ausreichend dimensioniert und skalierbar, im Sinne der Strukturierung und Erweiterbarkeit, sein.

Die Erfüllung der Anforderungen an die Erzeugung, die Erhebung und die Vorhaltung von Logdaten und von Protokolldateien muss anforderungsgerecht dokumentiert werden.