DGI® Deutsche Gesellschaft für Informationssicherheit AG

Monitoring und Event Management

- Konzept -

Inhaltsverzeichnis

Prüfung und Freigabe 2
Änderungshistorie 3
Dokumentensteuerung und Verteilerkreis 4
1 Ziel und Zweck 7
2 Geltungsbereich 7
3 Verantwortlichkeiten für das Management dieser Regelung 7
4 Begriffe 8
5 Management des Monitoring und der Behandlung von Events 8
5.1 Änderungsmanagement 8
5.2 Planung 9
5.2.1 Allgemeines 9
5.2.2 Risikomanagement 10
5.2.3 Ressourcen 11
5.2.4 Beschaffung 11
5.2.5 Datenschutz und Arbeitnehmerrechte 12
5.2.6 Informationssicherheitsvorfall 12
5.2.7 Schulung und Unterweisung 13
5.3 Umsetzung 14
5.3.1 Allgemeines 14
5.3.2 Anforderungen an das Management des Monitoring und der Behandlung von Events 14
5.3.3 Identifikation der zu überwachenden Informationen 15
5.3.4 Festlegung der Grenzwerte für Benachrichtigungen 16
5.3.5 Anforderungen an die Protokollierung 17
5.3.6 Monitoring 18
5.3.6.1 Anforderungen an Benachrichtigungen aus dem Monitoring 18
5.3.6.2 Kategorisierung und Klassifizierung 18
5.3.7 1st Level-Korrelation 19
5.3.7.1 Hinterlegung der Grenzwerte in Monitoring-Tools 19
5.3.7.2 Event-Filterung 20
5.3.7.3 Bereitstellung von Informationen für die Auswertung und Bewertung von Events 20
5.3.8 2nd Level-Korrelation 21
5.3.8.1 Erkennen, Interpretieren und Einordnen von Korrelationen 21
5.3.8.2 Reaktion auf Events 21
5.3.9 Event-Review 22
5.3.10 Reporting des Monitoring 22
5.3.11 Archivierung von Logdaten und Protokolldateien 23
5.3.12 Löschung von digitalen Logdaten und digitalen Protokolldateien 23
5.3.13 Entsorgung von analogen Logdaten und Datenträgern 23
5.4 Überwachung 25

5.4.1 Allgemeines 25
5.4.2 Maßnahmen der Überwachung 25
5.5 Aufrechterhaltung und Verbesserung 26
5.5.1 Allgemeines 26
5.5.2 Maßnahmen der Aufrechterhaltung und Verbesserung 26
6 Sanktionen 27
7 Referenzierte Dokumente 27