

Management der Prozesse sowie des Betriebs eines CERT

- 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
4.1 Anmerkung zur Abgrenzung der Begriffe Ereignis, Informationssicherheitsereignis und Informationssicherheitsvorfall	8
5 Management der Prozesse sowie des Betriebs eines CERT	10
5.1 Änderungsmanagement.....	10
5.2 Planung	10
5.2.1 Allgemeines	10
5.2.2 Risikomanagement.....	11
5.2.3 Ressourcen	13
5.2.4 Beschaffung	13
5.2.5 Datenschutz und Arbeitnehmerrechte.....	13
5.2.6 Informationssicherheitsvorfall.....	14
5.2.7 Schulung und Unterweisung	14
5.3 Umsetzung.....	15
5.3.1 Allgemeines	15
5.3.2 Anforderungen an Aktivitäten für das Management der Prozesse sowie den Betrieb des CERT	15
5.3.3 Erfüllung der Anforderungen an die Prozesse sowie den Betrieb des CERT.....	17
5.3.4 Aufgaben des CERT	18
5.3.5 Verantwortlichkeiten, Befugnisse und Rollen.....	19
5.3.6 Korrelierende Konzepte für das Management der Prozesse sowie den Betrieb des CERT	21
5.3.6.1 Allgemeines	21
5.3.6.2 Einbindung des Monitoring und Event Management.....	21
5.3.6.3 Einbindung des Incident Management	22
5.3.6.4 Einbindung des Security Information and Event Management	23
5.3.6.5 Einbindung der Lenkung eines Informationssicherheitsvorfalls	24
5.3.6.6 Einbindung des Business Continuity Management / Business Continuity Planning	24
5.3.7 Kommunikation im Zuge der Durchführung der Prozesse sowie des Betriebs des CERT	26
5.3.7.1 Allgemeines	26
5.3.7.2 Anforderungen an die Kommunikation	27
5.3.7.3 Erfüllung der Anforderungen an die Kommunikation.....	29
5.3.8 Auswahl und Evaluierung geeigneter Quellen für die Informations- und Datenbeschaffung	30
5.3.8.1 Allgemeines	30

5.3.8.2 Identifizierung und Verifizierung der Quellen für die Meldung von Informationssicherheitsereignissen	31
5.3.9 Meldung von Informationssicherheitsereignissen an das CERT	33
5.3.9.1 Allgemeines	33
5.3.9.2 Meldung eines relevanten Informationssicherheitsereignisses an das CERT	35
5.3.9.3 Risikobeurteilung eines als relevant erkannten Informationssicherheitsereignisses	37
5.3.9.4 Klassifizierung eines als relevant erkannten Informationssicherheitsereignisses.....	38
5.3.9.5 Priorisierung der Behandlung eines relevanten Informationssicherheitsereignisses.....	39
5.3.10 Reaktion auf ein gemeldetes Informationssicherheitsereignis.....	40
5.3.11 Behandlung eines CERT-relevanten Informationssicherheitsereignisses	42
5.3.11.1 Allgemeines	42
5.3.11.2 Maßnahmenevaluierung und Umsetzung der Maßnahmen	43
5.3.12 Schließen eines an das CERT gemeldeten Informationssicherheitsereignisses	44
5.3.13 Archivierung von Informationen und Daten des CERT	45
5.3.14 Löschung von Informationen und Daten des CERT	46
5.3.15 Berichterstellung und Reporting.....	48
5.4 Überwachung.....	49
5.4.1 Allgemeines.....	49
5.4.2 Maßnahmen der Überwachung.....	49
5.5 Aufrechterhaltung und Verbesserung.....	50
5.5.1 Allgemeines.....	50
5.5.2 Maßnahmen der Aufrechterhaltung und Verbesserung.....	50
6 Sanktionen.....	51
7 Referenzierte Dokumente.....	51