

Management der Festlegung der Schutzbedarfsklassen und der Durchführung einer Schutzbedarfsfeststellung

- Konzept -

Inhaltsverzeichnis

Prüfung und Freigabe	2
Änderungshistorie	3
Dokumentensteuerung und Verteilerkreis	4
Abbildungsverzeichnis	8
1 Ziel und Zweck	9
2 Geltungsbereich	9
3 Verantwortlichkeiten für das Management dieser Regelung	9
4 Begriffe	10
5 Management der Festlegung der Schutzbedarfsklassen und der Durchführung einer Schutzbedarfsfeststellung	11
5.1 Änderungsmanagement	11
5.2 Planung	11
5.2.1 Allgemeines	11
5.2.2 Risikomanagement	12
5.2.3 Ressourcen	13
5.2.4 Beschaffung	14
5.2.5 Datenschutz und Arbeitnehmerrechte	14
5.2.6 Informationssicherheitsvorfall	14
5.2.7 Schulung und Unterweisung	15
5.3 Umsetzung	16
5.3.1 Allgemeines	16
5.3.2 Anforderungen an die Festlegung der Schutzbedarfsklassen sowie die Durchführung einer Schutzbedarfsfeststellung	16
5.3.3 Verantwortungsbereiche für die Festlegung der Schutzbedarfsklassen und die Durchführung einer Schutzbedarfsfeststellung	18
5.3.3.1 Initiierung durch die oberste Leitung	18
5.3.3.2 Grundlegende Aufgaben des Informationssicherheitsbeauftragten	18
5.3.4 Rollen, Verantwortlichkeiten und Befugnisse für die Festlegung der Schutzbedarfsklassen und die Durchführung einer Schutzbedarfsfeststellung	19
5.3.4.1 Grundlegende Aufgaben der verantwortlichen Personen	19
5.3.4.2 Grundlegende Aufgaben der Prozesseigner	20
5.3.5 Prozessablauf für die Durchführung einer Schutzbedarfsfeststellung	22
5.3.6 Vorbereitende Aktivitäten für die Durchführung einer Schutzbedarfsfeststellung	24
5.3.6.1 Übernahme der relevanten Informationen aus der IT-Strukturanalyse	24
5.3.6.2 Übernahme der relevanten Informationen aus der Business Impact Analyse	26
5.3.6.3 Zusammenführung der Informationen von vorgelagerten Analysen	27
5.3.6.4 Reihenfolge für die Durchführung der Schutzbedarfsfeststellung	28
5.3.6.5 Verkürzung der vorbereitenden Aktivitäten für die Durchführung einer Schutzbedarfsfeststellung	28

5.3.6.6 Erstellung des Katalogs von Maßnahmen für die Gewährleistung der Schutzziele (Sicherheitsmaßnahmen)	29
5.3.6.7 Festlegung der Schutzstufen für die Bestimmung und Bewertung der Wirksamkeit der Sicherheitsmaßnahmen	30
5.3.7 Festlegung von Schutzbedarfsklassen	31
5.3.7.1 Allgemeines	31
5.3.7.2 Die Spezifizierung der Schutzbedarfsklassen	32
5.3.8 Durchführung der Schutzbedarfsfeststellung	34
5.3.8.1 Befragungen für die Feststellung des Schutzbedarfs	34
5.3.8.1.1 Allgemeines	34
5.3.8.1.2 Durchführung der Befragungen der Prozesseigner sowie der verantwortlichen Personen	34
5.3.8.2 Eruiierung der IT-Unterstützung für die Durchführung des ordnungsgemäßen, sicheren und konformen Geschäftsbetriebs	36
5.3.8.2.1 Allgemeines	36
5.3.8.2.2 Feststellung der Graduierung der IT-Unterstützung	37
5.3.8.2.3 Feststellung der Priorisierung der einzelnen durchzuführenden Schutzbedarfsfeststellungen	37
5.3.8.3 Anforderungen für die Bestimmung der einzeln umzusetzenden Schutzziele	38
5.3.8.3.1 Allgemeines	38
5.3.8.3.2 Bestimmung des Schutzziels „Vertraulichkeit“	39
5.3.8.3.3 Bestimmung des Schutzziels „Integrität“	39
5.3.8.3.4 Bestimmung des Schutzziels „Verfügbarkeit“	40
5.3.8.3.5 Bestimmung des Schutzziels „Authentizität“	41
5.3.8.4 Umsetzung der Durchführung einer Schadensanalyse für die Feststellung des Schutzbedarfs	42
5.3.8.4.1 Allgemeines	42
5.3.8.4.2 Durchführung einer Schadensanalyse	42
5.3.8.5 Bewertung der Ergebnisse aus den durchgeführten Schadensanalysen	44
5.3.8.6 Ableitung und Bewertung des Schutzbedarfs der zu betrachtenden Assets	45
5.3.8.7 Bewertung des Schutzbedarfs der Anwendungen	46
5.3.8.8 Ableitung und Bewertung des Schutzbedarfs für IT-Systeme	46
5.3.8.9 Ableitung und Bewertung des Schutzbedarfs für Räume, Gebäude und Gebäudeteile	47
5.3.8.10 Ableitung und Bewertung des Schutzbedarfs für Kommunikationsverbindungen	48
5.3.8.11 Auswahl und Festlegung der Sicherheitsmaßnahmen	48
5.3.9 Nachbereitung der Durchführung einer Schutzbedarfsfeststellung	50
5.3.9.1 Eruiierung der Durchführung von ergänzenden IT-Risikobeurteilungen	50
5.3.9.2 Eruiierung der Durchführung von ergänzenden Business Impact Analysen	50
5.4 Überwachung	51
5.4.1 Allgemeines	51
5.4.2 Maßnahmen der Überwachung	51
5.5 Aufrechterhaltung und Verbesserung	52

5.5.1 Allgemeines	52
5.5.2 Maßnahmen der Aufrechterhaltung und Verbesserung	52
6 Sanktionen	53
7 Referenzierte Dokumente	53

Bitte dieses Dokument an Ihre Organisation anpassen