Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 6. Übung im SoSe 2013:

Konzepte zur IT-Sicherheit

6.1 Aufgaben des IT-Sicherheits-beauftragten

Aufgabe:

- Ein Unternehmen möchte einen **IT-Sicherheitsbeauftragten** einsetzen. Dessen Aufgaben sollen in der information security policy festgeschrieben werden. Dabei sollen insbesondere die Maßnahmen M 2.193, M 2.199, M 2.201, M 2.337 und M 6.58 aus den IT-Grundschutzkatalogen sinnvoll integriert werden. Formulieren Sie den entsprechenden Part zum IT-Sicherheitsbeauftragten zur information security policy!

6.1 Aufgaben des IT-Sicherheits-beauftragten (1)

Aufgaben nach M 2.193 (Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit):

- Steuerung und Koordination des Informationssicherheitsprozesses
  → Prozessverantwortung bei ITSB
- Unterstützung der Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit
  → Verantwortung für Informationssicherheit bleibt bei Leitung
- Koordination der Erstellung von
  ° IT-Sicherheitskonzept
  ° Notfallvorsorgekonzept
  ° und anderer Teilkonzepte und System-Sicherheitsrichtlinien
  → Konzeption der IT-Sicherheit (= Prozessdefinition)
- Erlass weiterer Richtlinien und Regelungen zur Informationssicherheit
  → Genehmigungsinstanz für Richtlinien und Regelungen

6.1 Aufgaben des IT-Sicherheits-beauftragten (2)

Aufgaben nach M 2.193 (Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit): 1. Fortsetzung

- Erstellung des Realisierungsplans für die IT-Sicherheitsmaßnahmen, Initiierung und Prüfung von deren Realisierung
  → Maßnahmenverantwortung (erfordert entsprechendes Budget!)
- Bericht über den Status Quo der Informationssicherheit an Leitungs-ebene und dem Informationssicherheits-Management-Team
  → Rechenschaftsbericht gegenüber Leitungsebene
  → Vorsitz im Informationssicherheits-Management-Team
- Koordination sicherheitsrelevanter Projekte
  → alle Projekte mit Bezug zur IT-Sicherheit bedürfen der aktiven Be-teiligung des ITSB
- Sicherstellen des Informationsflusses zwischen Bereichs-IT, Projekt- sowie IT-System-Sicherheitsbeauftragten

6.1 Aufgaben des IT-Sicherheits-beauftragten (3)

Aufgaben nach M 2.193 (Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit): 2. Fortsetzung

- Untersuchen sicherheitsrelevanter Zwischenfälle
  → Verantwortung für Sicherheitsvorfall-Management
- Initiieren und Steuern von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit
  → Planung von Awareness-Maßnahmen
- Beteiligung bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben
- Beteiligung bei der Einführung neuer Anwendungen und IT-Systeme
- Beteiligung bei der Beschaffung von IT-Systemen
- Beteiligung bei der Gestaltung von IT-gestützten Geschäftsprozessen
- Ausübung der Funktion als Stabsstelle unterhalb der Leitungsebene

6.1 Aufgaben des IT-Sicherheits-beauftragten (4)

Aufgaben nach M 2.199 (Aufrechterhaltung der Informationssicherheit):

- Regelmäßige Überprüfung aller Sicherheitsmaßnahmen (i.d.R. jährlich, teilweise auch unangemeldet)
- Regelmäßige Überprüfung der korrekten Umsetzung als auch der Umsetzbarkeit eines Sicherheitskonzepts mit
  - ° Prüfung von Eignung und Effizienz der Maßnahmen im Hinblick auf die gesteckten IT-Sicherheitsziele (Vollständigkeit & Aktualität)
  - ° Kontrolle der Umsetzung der IT-Sicherheitsmaßnahmen in den einzelnen Bereichen (Revision)
- Umsetzung der im Sicherheitskonzept geplanten Sicherheitsmaßnahmen gemäß dem Realisierungsplan
- Dokumentation des Umsetzungsstandes
- Überwachung und Steuerung der Zieltermine und des Ressourceneinsatzes

6.1 Aufgaben des IT-Sicherheits-beauftragten (5)

Aufgaben nach M 2.199 (Aufrechterhaltung der Informationssicherheit):
1. Fortsetzung

- Anpassung der bestehenden Sicherheitsmaßnahmen aufgrund der Erkenntnisse aus
  - ° sicherheitsrelevanten Zwischenfällen
  - ° Veränderungen im technischen oder technisch-organisatorischen Umfeld
  - ° Änderungen von Sicherheitsanforderungen
  - ° Änderungen von Bedrohungen
- Dokumentation zu den Ergebnissen der einzelnen Überprüfungen
- Einleitung der erforderlichen Korrekturmaßnahmen

6.1 Aufgaben des IT-Sicherheits-beauftragten (6)

Aufgaben nach M 2.199 (Aufrechterhaltung der Informationssicherheit):
2. Fortsetzung

- Unterjährige Prüfungen bei
  - ° Aufbau neuer Geschäftsprozesse, Anwendungen oder IT-Komponenten
  - ° Vornahme größerer Änderungen der Infrastruktur (z.B. Umzug)
  - ° Anstehen größerer organisatorischer Änderungen (z.B. Outsourcing)
  - ° Änderung der Gefährdungslage
  - ° Bekanntwerden gravierender Schwachstellen oder Schadensfälle
- Prüfung der Durchführung aller vorgesehenen Detektionsmaßnahmen (z.B. Auswertung von Protokolldaten)
- Vorschlag einer Korrekturmaßnahme für jede Abweichung
- Information des jeweiligen Vorgesetzten bei Entdecken unzulässiger Aktivitäten von Mitarbeitern

6.1 Aufgaben des IT-Sicherheits-beauftragten (7)

Aufgaben nach M 2.199 (Aufrechterhaltung der Informationssicherheit):
3. Fortsetzung

- Auswertung externer Wissensquellen, wie Standards oder Fachpublikationen
- Kontakte zu Gremien und Interessengruppen, die sich mit Sicherheitsaspekten beschäftigen (Praxisaustausch)
- Dokumentation des Sicherheitsprozesses
- Sicherstellen, dass Auditoren, die Prüfungen vornehmen, nicht an der Konzeption beteiligt waren
- Sicherstellen, dass nur Befugte Zugriff auf Audit- oder Diagnosewerkzeuge und die dokumentierten Prüfungsergebnisse haben

6.1 Aufgaben des IT-Sicherheits-beauftragten (8)

Aufgaben nach M 2.201 (Dokumentation des Sicherheitsprozesses):

- Dokumentation zum Ablauf des IT-Sicherheitsprozesses
- Dokumentation zu wichtigen Entscheidungen im IT-Sicherheitsprozess
- Dokumentation zu den Arbeitsergebnissen der einzelnen Phasen des IT-Sicherheitsprozesses
- Archivierung der Vorgängerversionen der Dokumentationen zum IT-Sicherheitsprozess (→ Nachvollziehbarkeit der Entwicklung)
- Dokumentation der Berichte zum Status der Informationssicherheit an die Leitungsebene
- Beachten, dass die **Leitlinie zur Informationssicherheit** die Sicherheitsziele und Sicherheitsstrategie festlegt und von der obersten Leitungsebene festgelegt und veröffentlicht wurde
- Beschreiben der erforderlichen Sicherheitsmaßnahmen und deren Umsetzung im **Sicherheitskonzept**

6.1 Aufgaben des IT-Sicherheits-beauftragten (9)

Aufgaben nach M 2.201 (Dokumentation des Sicherheitsprozesses):
1. Fortsetzung

- Beachten, dass die bereichs- und systemspezifischen Sicherheitsrichtlinien und die Regelungen für den ordnungsgemäßen und sicheren IT-Einsatz auf der Sicherheitsleitlinie aufbauen
- Dokumentation der Sitzungsprotokolle und Beschlüsse des Informationssicherheits-Management-Teams
- Dokumentation der Ergebnisse von Audits und Überprüfungen (inkl. Prüflisten und Befragungsprotokollen)
- Dokumentation von Sicherheitsvorfällen zur Nachvollziehbarkeit aller damit verbundenen Vorgänge und Entscheidungen (inkl. Protokolle und vorfallsbezogener System-Meldungen)
- Dokumentation zu Installations- und Konfigurationsanleitungen

6.1 Aufgaben des IT-Sicherheits-beauftragten (10)

Aufgaben nach M 2.201 (Dokumentation des Sicherheitsprozesses):
2. Fortsetzung

- Dokumentation der Anleitungen für den Wiederanlauf nach einem Sicherheitsvorfall
- Dokumentation von Test- und Freigabeverfahren (Belegfunktion)
- Dokumentation der Anweisungen für das Verhalten bei Störungen und Sicherheitsvorfällen
- Bereitstellen der geltenden Sicherheitsrichtlinien für Mitarbeiter
- Bereitstellen übersichtlicher Merkblätter für den verantwortungsvollen Umgang mit internen Informationen, für die sichere Nutzung von IT-Systemen und Anwendungen sowie zum Verhalten bei Sicherheits-vorfällen für Mitarbeiter
- Bereitstellen von Handbüchern und Anleitungen für die eingesetzten IT-Systeme und Anwendungen

6.1 Aufgaben des IT-Sicherheits-beauftragten (11)

Aufgaben nach M 2.201 (Dokumentation des Sicherheitsprozesses):
3. Fortsetzung

- Beschreibung und zeitnahe Aktualisierung der Meldewege und der Vorgehensweise für den Informationsfluss zum Sicherheitsprozess

6.1 Aufgaben des IT-Sicherheits-beauftragten (12)

Aufgaben nach M 2.337 (Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse):

- Abstimmen der Methoden zum Risikomanagement aus dem Bereich der Informationssicherheit mit bereits etablierten Methoden der gesamten Einrichtung (→ Einbinden der IT-Risiken in allgemeine Risiken)
- Beitragen zur Widerspruchsfreiheit in Arbeitsanweisungen oder Dienstvereinbarungen aus unterschiedlichen Bereichen
- Beitragen zur klaren Definition von Zuständigkeiten und Kompetenzen unter Berücksichtigung von Vertretungsregeln
- Beitragen zur Planung, Beschreibung, Einrichtung und Bekanntgabe der Kommunikationswege mit Festlegung der Aufgaben, Rollen und des Umfangs der zu kommunizierenden Informationen
- Unterstützt werden durch Fachverantwortliche bei der Erarbeitung und Umsetzung der Sicherheitsstrategie

6.1 Aufgaben des IT-Sicherheits-beauftragten (13)

Aufgaben nach M 2.337 (Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse): Fortsetzung

- Beteiligung an der Einweisung der Mitarbeiter in die erforderlichen Sicherheitsmaßnahmen
- Beteiligung an der Sensibilisierung für Risiken und Schutzvorkehrungen im alltäglichen Umgang mit Informationen
- Überblick über alle Arten von Dienstleistern (sowohl für die Verarbeitung geschäftsrelevanter Informationen als auch für allgemeine Unterstützungsleistungen) und Einschätzung, welche Sicherheitsvorkehrungen diese Dienstleister zu treffen haben

6.1 Aufgaben des IT-Sicherheits-beauftragten (14)

Aufgaben nach M 6.58 (Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen):

- Vorbereitung der Einrichtung auf den angemessenen Umgang mit Sicherheitsvorfällen aller Art
- Etablierung einer geeigneten Vorgehensweise zur Behandlung von Sicherheitsvorfällen
- Klare Definition der Abläufe und Regeln für die verschiedenen Arten von Sicherheitsvorfällen
- Abstimmung mit dem Notfallmanagement
- Entgegennahme von Meldungen über Sicherheitsvorfälle
- Entscheidung über die Einstufung als Sicherheitsproblem oder Sicherheitsvorfall
- Einschaltung des Eskalationswegs bei Sicherheitsvorfällen
- Einleitung notwendiger Maßnahmen zu Sicherheitsvorfällen

6.1 Aufgaben des IT-Sicherheits-beauftragten (15)

Text für information security policy:

Es wird die Funktion eines IT-Sicherheitsbeauftragter eingerichtet, die als Stabstelle der Leitung folgende Aufgaben wahrnimmt:

1. Konzeption der Leitlinie zur Informationssicherheit, die von der Leitung verabschiedet wird
2. Konzeption des Informationssicherheitsprozesses, das von der Leitung verabschiedet wird
3. Regelmäßige Berichterstattung an die Leitung zur aktuellen Sicherheitslage und Vortragsrecht gegenüber der Leitung zu Fragen der Informationssicherheit
4. Information von Fachverantwortlichen über von Beschäftigten verursachte IT-Sicherheitsvorfälle
5. Erlass aller sicherheitsspezifischen Richtlinien und Regelungen im Einklang mit der Leitlinie und dem Sicherheitsprozess

6.1 Aufgaben des IT-Sicherheits-beauftragten (16)

Text für information security policy: 1. Fortsetzung

Es wird die Funktion eines IT-Sicherheitsbeauftragter eingerichtet, die als Stabstelle der Leitung folgende Aufgaben wahrnimmt:

6. Festlegung und regelmäßige Überprüfung der Maßnahmen zur Gewährleistung von Informationssicherheit
7. Abwicklung von IT-Sicherheitsvorfällen
8. Planung von Awarenessmaßnahmen zur Informationssicherheit
9. Einweisung der Beschäftigten zur Informationssicherheit
10. Erstellung von Merkblättern und Anleitungen zur Informationssicherheit
11. Dokumentation aller gültigen Regelungen zur Informationssicherheit und vorgefallener IT-Sicherheitsvorfälle
12. Dokumentation zu durchgeführten Sicherheitsaudits
13. Konsultation zur Informationssicherheit bei allen IT-Projekten

6.1 Aufgaben des IT-Sicherheits-beauftragten (17)

Text für information security policy: 2. Fortsetzung

Es wird die Funktion eines IT-Sicherheitsbeauftragter eingerichtet, die als Stabstelle der Leitung folgende Aufgaben wahrnimmt:

14. Konsultation bei wesentlichen Änderungen beim Ablauf der Geschäftsprozesse und beim Outsourcing, der mit einem Zugriff auf Informationen verbunden ist
15. Konsultation bei der Gestaltung des allgemeinen Risikomanagements zur adäquaten Einbeziehung festgestellter IT-Risiken

6.2 Notfall-Vorsorge-Konzept

Aufgabe:

- Welche Bestandteile sollte ein **Notfall-Vorsorge-Konzept** bei einem Unternehmen, das lediglich mittleren Schutzbedarf und nur eine geringe Komplexität aufweist, Ihrer Ansicht nach auf alle Fälle beinhalten? Sehen Sie sich hierzu die entsprechenden Ausführungen in den BSI-Grundschutzkatalogen bzw. den BSI-Standards an und wählen Sie begründet aus.

6.2 Notfall-Vorsorge-Konzept (1)

Ein Notfallvorsorgekonzept beschreibt, wie das Eintreten eines Notfalls vorzugsweise verhindert werden kann/soll → **präventiver Schutz**

→ Komplettes Notfallmanagement ist auf den BSI-Seiten beschrieben im **BSI-Standard 100-4** (abrufbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/31045/standard_1004.pdf)

→ Darin **Kapitel 5.5 Notfallvorsorgekonzept** auswerten

→ **Bestandteile** (Inhalt des Notfallvorsorgekonzepts):
- ° Verantwortlichkeiten, Geltungsbereich, Inhaltsangabe
- ° Abgrenzungen, Ziele, Zuständigkeiten, Ablauforganisation
- ° betrachtete Notfallszenarien, Wiederanlauf-Anforderungen, Priorisierungen
- ° Alarmierungsverfahren, Beschreibung vorbeugender Maßnahmen
- ° Einbinden des Notfallmanagements in Unternehmenskultur
- ° Aufrechterhaltung & Kontrolle

6.2 Notfall-Vorsorge-Konzept (2)

Ein mittelständisches Unternehmen wird sich auf Kernfragen konzentrieren

→ In Grundschutzkatalogen nach Notfallmanagement suchen

→ **Baustein 1.3 zum Notfallmanagement** wählen (abrufbar unter: https://www.bsi.bund.de/cln_183/sid_AB2A5EAB735FF0FE0D1D3C525AB43C3D/ContentBSI/grundschutz/kataloge/baust/b01/b01003.html)

→ Im Baustein 1.3 lediglich Maßnahmen der Kategorie A (Einstieg in Grundschutz) auswählen (M 6.111 zur Leitlinie, M 6.112 zur Organisationsstruktur, **M 6.114 Notfallkonzept** & M 6.118 Aufrechterhaltung des Notfallmanagements)

Bestandteile eines Notfallvorsorgekonzepts nach M 6.114:

- Übersicht zu Verfügbarkeitsanforderungen (maximal tolerierbare Ausfallzeiten, Wiederanlaufparameter, Prioritäten für Wiederanlauf)
- Vorgehen zur Durchführung einer Business Impact Analyse (BIA) & einer Risikoanalyse
- Auflistung der Maßnahmen zur Risikobehandlung

6.3 Notfallplan

Aufgabe:

- Welche Bestandteile sollte dagegen ein **Notfallplan** aufweisen? Begründen Sie Ihre Antwort!

6.3 Notfallplan

Ein Notfallplan beschreibt, was bei Eintritt eines Notfalls zu tun ist!

→ **reaktiver Schutz**

→ Notwendige **Bestandteile** eines Notfallplans:

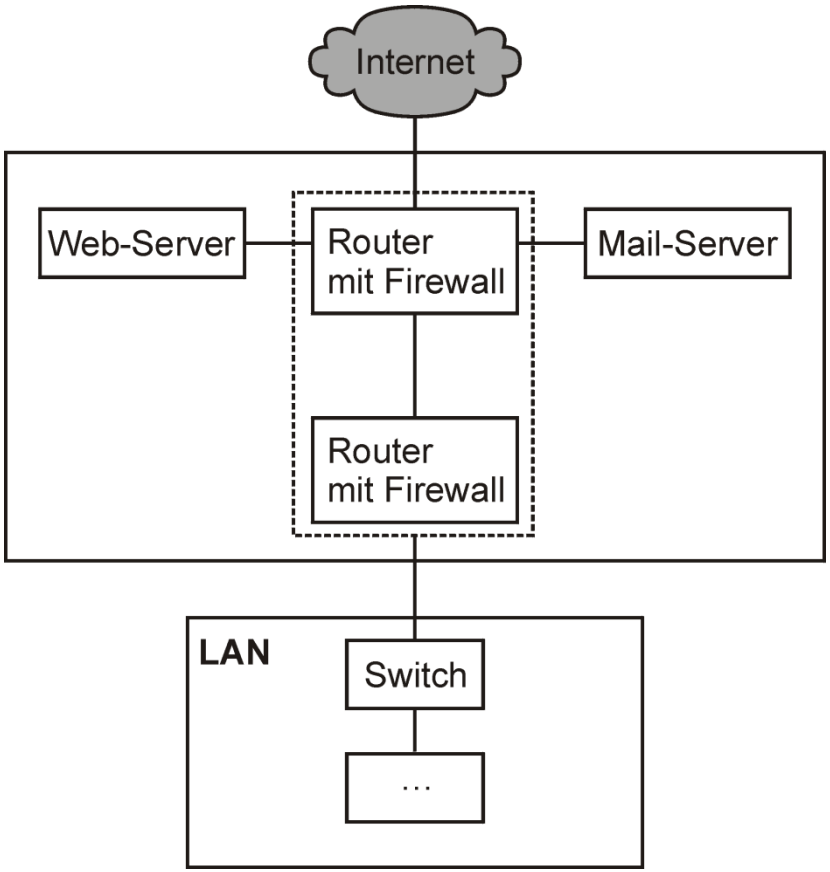
- Zielsetzung des Notfallplans und ggf. geltende Abgrenzungen (hinsichtlich des Scope)
- Festlegung der Verantwortlichkeiten (wer macht was?)
- Aufstellung des Alarmierungsplans (wer ist wann anzurufen?)
- Ablaufpläne für entsprechende Notfallszenarien (im Sinne von Checklisten)
- Dokumentationen zur eingesetzten IT-Infrastruktur und den Maßnahmen zur Notfall-Vorsorge
- Bereitstellung aller wesentlichen Unterlagen und Nachweise (z.B. zu durchgeführten Notfall-Übungen)

6.4 DMZ

Aufgabe:

- Ein Unternehmen möchte sensible Daten im LAN vor Angriffen aus dem Internet schützen. Das Unternehmen betreibt zur Kommunikation mit dem Internet zwei Dienste: Web (Zugriff auf Internet-Seiten und Bereitstellung von Web-Seiten-Content) und E-Mail. Skizzieren Sie die zugehörige **DMZ** mit zwei Routern!

6.4 DMZ


Internet
Web-Server
Router
mit Firewall
Mail-Server
Router
mit Firewall
LAN
Switch
…

6.5 Sicherheitsziele & Kontrollbereiche

Aufgabe:

- Ordnen Sie die im BDSG genannten **Kontrollbereiche** inhaltlich den **Sicherheitszielen** der mehrseitigen IT-Sicherheit zu (Mehrfach-Zuordnungen sind erlaubt)!

6.5 Sicherheitsziele & Kontrollbereiche

	Verfügbarkeit	Integrität	Vertraulichkeit	Zurechenbarkeit	Rechtsverbindlichkeit
Organisationskontrolle	X	X	X	X	X
Zutrittskontrolle	X		X		
Zugangskontrolle	X	X	X		
Zugriffskontrolle	X	X	X	X	X
Weitergabekontrolle	X	X	X	X	X
Eingabekontrolle		X		X	
Auftragskontrolle					X
Verfügbarkeitskontrolle	X				
Datentrennungskontrolle		X	X	X	X