Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 7. Übung im SoSe 2018:

Business Continuity Management & ISMS

7.1 ISMS Einrichtungsfehler

Aufgabe:

- Nennen Sie fünf grundlegende Fehler, die beim Aufbau eines **Informations-Sicherheits-Management-Systems (ISMS)** besser vermieden werden sollten!

7.1 ISMS Einrichtungsfehler (1)

- **ISMS falsch ausrichten**:
  - Nicht alle relevanten Anforderungen (rechtlich, vertraglich, eigene Vorgaben, Stand der Technik) ermitteln vor Einrichtung des ISMS
  - Sich mit der Einrichtung selbst „zufrieden geben“
  - Methodologien wählen, die nicht adäquat zum Kontext sind

- **ISMS falsch steuern**:
  - Risikomanagement nicht auf Kontext ausrichten
  - Methoden einsetzen, die einfach oder billig erwerbbar sind
  - Einsatz lediglich vordefinierter Gefährdungskataloge
  - Risikoanalyse als „lästige“ Pflicht ansehen

7.1 ISMS Einrichtungsfehler (2)

- **Zentrale ISMS-Funktionen falsch besetzen**:
  - Den falschen Beauftragten für Informationssicherheit einsetzen – nötig ist ein erfahrener Funktionsträger, der frei von operativen Interessenkonflikten ist und den nötigen Gesamtüberblick hat
  - Falsche Auditoren einsetzen, welche nicht beide Bereiche, Technik und Organisation/Prozesse, ausreichend tief abdecken können
  - Die falschen Mitglieder ins CSIRT einsetzen – zunächst werden solche Personen benötigt, die über ausgeprägte Analysefähigkeiten verfügen, um Ursachen für Information Security Incidents zutreffend ermitteln zu können

7.1 ISMS Einrichtungsfehler (3)

- **Beim ISMS die falschen Dinge regeln**:
  - In den Policies oder Sicherheitskonzepten die Zielvorstellungen angeben und dabei die Realität nicht berücksichtigen – in den Sicherheitskonzepten ist in erster Linie der IST-Stand zu dokumentieren und nur dann ein SOLL-Ziel aufzunehmen, wenn die zugehörige Maßnahme bereits geplant ist und bisher nur noch nicht vollständig umgesetzt wurde
  - Dinge regeln, die zu abstrakt oder hinsichtlich ihrer Wirksamkeit nicht mit vertretbarem Aufwand überprüfbar sind
  - Dinge unabhängig von Risikoanalysen zu regeln
  - Muster-Policies ohne Berücksichtigung des Kontextes übernehmen

7.1 ISMS Einrichtungsfehler (4)

- **Beim ISMS Sicherheitsvorfälle falsch adressieren**:
  - Aufbau eines Information Security Incident Managements ohne ausreichende Implementierung der Erhebung von Sicherheitsvorfällen – Solche müssen erst mal von betroffenen Stellen „erkannt“ bzw. technisch geeignet aufgezeichnet werden
    → Awareness über Sicherheitslücken und Sicherheitsvorfälle
    → Security Incident Response Readiness via Protokolle, IDS, etc.
    → klar definierte Meldeketten
  - Bei der Behebung von Sicherheitsvorfällen nicht berücksichtigen, ob ggf. Schritte zur Verfolgung der Verursacher eingeleitet werden sollen (hat sonst beweisvernichtende Vorgehensweisen zur Folge, die eine straf- oder zivilrechtliche Verfolgung unmöglich machen)
  - Auswirkung von Sicherheitsvorfällen falsch einschätzen
  - Kein (zeitlich begrenztes) Exception Handling für Ausnahmen zur Beseitigung von Sicherheitsvorfällen vorsehen

7.2 Business Impact Analyse I

Aufgabe:

- In einem Unternehmen, das ein hochwertiges und hochpreisiges Gut produziert, welches für jeden Kundenauftrag individuell entworfen und produziert wird und daher nach Abschluss der Herstellung möglichst rasch an den Kunden geliefert und diesem in Rechnung zu stellen ist, ergab eine durchgeführt Befragung der jeweiligen Fachverantwortlichen im Rahmen einer **Business Impact Analyse** folgende, stark vereinfachten Ergebnisse (bei den **maximal tolerablen Ausfallzeiten** [MTPD] konnte gewählt werden zwischen 2, 4, 8, 12, 24, 48, 72, 96 und 120 h):

  <u>Kernprozesse</u>:

  Vertrieb des Produkts (V): 24 h
  Entwurf des Produkts (E): 72 h
  Herstellung des Produkts (H): 12 h
  Buchhaltung (B): 48 h

  <u>Supportprozesse</u>:

  Präzisionsmaschinenverwaltung (P; Support für H): 24 h
  Lagerverwaltung (L; Support für H): 48 h
  IT-Verwaltung (I; Support für E, H, V, B, P und L): 2 h

  <u>Führungsprozesse</u>:

  Qualitätssicherung (Q; Abnahme des Produktes in H): 8 h

7.2 Business Impact Analyse II

Aufgabe:

- IT-Systeme:

  Vertriebssystem (IV; Ressource für V, Datenimport aus IB, Datenexport in IW und IK): 8 h

  Konstruktionssystem (IK; Ressource für E, Datenimport aus IV, Datenexport in IS): 8 h

  Steuerungssystem (IS; Ressource für H, Wartung über P, Steuerung für IF): 2 h

  Fertigungsstraßensystem (IF; Ressource für H, Datenimport aus IS, Datenexport in IW): 4 h

  Warenwirtschaftssystem (IW; Ressource für H, V und B, Datenimport aus IF, IL, IB und IV): 4 h

  Lagerverwaltungssystem (IL; Ressource für L, V und B, Datenexport in IB und IW): 8 h

  Buchhaltungssystem (IB; Ressource für B, Datenexport in IW und IV): 24 h

7.2 Business Impact Analyse III

Aufgabe:

- A) Welche **Wiederanlaufzeiten** (RTO; maximale Dauer bis zur Wiederherstellung der vollen Funktionsfähigkeit der Ressource bzw. des Prozesses) resultieren daraus im jeweiligen Wort Case Fall (maximaler Ausfall des Prozesses bzw. der Ressource unter Berücksichtigung vorhandener Abhängigkeiten) anhand der von den Verantwortlichen benannten MTPD?
- B) Welche Ausfallzeiten sind wofür tatsächlich tolerabel, wenn MTPD für den Kernprozess H zur Aufrechterhaltung der Geschäftskontinuität zwingend eingehalten werden muss? Für welche Ressourcen bzw. IT-Systeme ist dann ein Cold Stand-By (Reserve steht nach Ausfall innerhalb von 2 h zur Verfügung) oder ein Hot Stand-By (Reserve steht für Parallelbetrieb zur Verfügung mit 0 h Ausfallzeit)?

Lösungshinweis:

- *Damit ein Kernprozess erfolgreich abgeschlossen werden kann, muss nicht nur der Kernprozess selbst ausgeführt werden, sondern auch zugeordnete Support- und Führungsprozesse sowie eingesetzte IT-Systeme. Die zu beachtenden Abhängigkeiten sind oben ausdrücklich angegeben. Wird ein Prozess oder IT-System für mehrere Prozesse eingesetzt, muss dieser dort jeweils erfolgreich abgeschlossen werden. Eine Reduzierung von Ausfallzeiten solcher Ressourcen wirkt sich damit besonders stark aus.*

7.2 Business Impact Analyse (1)

A) Maximale Wiederanlaufzeiten für die jeweiligen Prozesse

- Im worst case wird jeder Subprozess und jedes IT-System unabhängig voneinander benötigt → jeweilige MTPD aufaddieren!
- Benötigt ein Prozess oder ein IT-System einen Datenimport aus einem IT-System, muss auch dieses IT-System zur Verfügung stehen → MTPD der Import-IT-Systeme miteinbeziehen!

Vertrieb (V)				Entwurf (E)		Herstellung (H)					Buchhaltung (B)				
24 h				72 h		12 h					48 h				
I				I		P		L	I	Q	I				
2 h				2 h		24 h		48 h	2 h	8 h	2 h				
						I		I							
						2 h		2 h							
IB	IV	IW	IL	IV	IK	IS	IF	IW	IL		IF	IL	IB	IV	IW
24 h	8 h	4 h	8 h	8 h	8 h	2 h	4 h	4 h	8 h		4 h	8 h	24 h	8 h	4 h
max. Ausfall: 44 h für IT-Systeme + 26 h für Prozess (V + I)				max. Ausfall: 16 h für IT-Systeme + 74 h für Prozess (E + I)		max. Ausfall: 18 h für IT-Systeme + 98 h für Prozess (H + P + L + 3*I + Q)					max. Ausfall: 48 h für IT-Systeme + 50 h für Prozess (B + I)				

7.2 Business Impact Analyse (2)

B) Tolerable Ausfallzeiten für Prozess H durch Cold bzw. Hot Stand-By:

- IW & IL werden für drei Prozesse benötigt und sollten daher im Hot Stand-By betrieben werden (→ Reduzierung der MTPD auf 0 h)
- IF wird für zwei Prozesse benötigt und sollte daher im Cold Stand-By betrieben werden (→ Reduzierung der MTPD auf 2 h)
- Die Support-Prozesse P, L & Q sollten im Cold Stand-By betrieben werden (→ Reduzierung der MTPD auf 2 h)
- Der dreifach auftauchende Support-Prozess I sollte dagegen im Hot Stand-By betrieben werden (→ Reduzierung der MTPD auf 0 h)

→ **Maximale Ausfallzeit wird rechnerisch auf 10 h reduziert → Puffer von 2 h !**

Herstellung (H)					
12 h					
P			L	I	Q
24 h → 2 h			48 h → 2 h	2 h → 0 h	8 h → 2 h
I			I		
2 h → 0 h			2 h → 0 h		
IS	IF	IW	IL		
2 h	4 h → 2 h	4 h → 0 h	8 h → 0 h		

7.3 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 im BSI-Standard 100-4 an und wählen Sie begründet aus (siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html).

7.3 Notfall-Vorsorge-Konzept

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

→ Komplettes Notfallmanagement ist auf den BSI-Seiten beschrieben im **BSI-Standard 100-4** (abrufbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html)

→ 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

7.4 Notfallplan

Aufgabe:

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

7.4 Notfallplan

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

→ **<u>reaktiver</u> 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)

7.5 Verfügbarkeitsberechnung

Aufgabe:

- Die **Verfügbarkeit** eines IT-Systems kann als das Produkt der Verfügbarkeiten ihrer jeweiligen Komponenten verstanden werden, sofern diese Komponenten <u>seriell</u> miteinander verbunden sind. Diese werden unter Berücksichtigung etwaiger Ausfallzeiten in % gegenüber der vereinbarten Servicezeit berechnet:
  $$\text{Verfügbarkeit einer IT-Komponente} = \frac{(\text{vereinbarte Servicezeit} - \text{Ausfallzeit})}{\text{vereinbarte Servicezeit}} \text{ [in \%]}$$
- Wenn hingegen Komponenten eines IT-Systems <u>parallel</u> betrieben werden, erhöht sich die Verfügbarkeit für diesen technisch redundanten Cluster in Abhängigkeit zur Anzahl der technisch redundant ausgelegten IT-Komponenten auf:
  $$\text{Redundanz-Verfügbarkeit} = 1 - (1 - \text{Verfügbarkeit}_{\text{normal}})^{\text{Anzahl}}$$
- A) Das zu betrachtende IT-System bestehe aus einem Server, der während der Betriebszeit zu 8 Stunden pro Jahr ausfällt, einem Client, der dabei zu 16 Stunden pro Jahr ausfällt, und einer Vernetzungskomponente, die während des Betriebs zu 24 Stunden pro Jahr ausfällt. Als Servicezeit sei ein 12-Stunden-Betrieb von Montag bis Freitag vereinbart worden. Wie hoch ist die Verfügbarkeit jeder einzelnen Komponente und des gesamten IT-Systems?
- B) Wie wirkt sich es sich auf die Verfügbarkeit des gesamten IT-Systems aus, wenn die Vernetzungskomponente mit einer identisch konfigurierten weiteren geclustert wird? Die Prozentangaben sind dabei auf drei Nachkommastellen anzugeben (also 12,345%).

7.5 Verfügbarkeitsberechnung

Teil A)

V_{server} = (12*5*52 – 8)/(12*5*52) = 3112/3120 = 99,744%

V_{client} = (12*5*52 – 16)/(12*5*52) = 3104/3120 = 99,487%

V_{netz} = (12*5*52 – 24)/(12*5*52) = 3096/3120 = 99,231%

$V_{gesamt} = V_{server} * V_{client} * V_{netz}$ = 99,744%*99,487%*99,231% = 98,469%

Teil B)

$V_{netzcluster} = 1 - (1 - V_{netz})^2 = 1 - (1 - 0{,}99231)^2$ = 99,994%

$V_{gesamt_neu} = V_{server} * V_{client} * V_{netzcluster}$ = 99,744%*99,487%*99,994%
= 99,226%