Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 6. Übung im SoSe 2014:
Business Continuity Management

6.1 Datensicherung

Aufgabe:

- Welche Regelungen sollte eine **Richtlinie zur Datensicherung** beinhalten?

6.1 Datensicherung (1)

Aus den IT-Grundschatzkatalogen (Baustein 1.4 Datensicherungskonzept & Maßnahme 6.33 Entwicklung eines Datensicherungskonzepts) lassen sich folgende **Regelungen zur Datensicherung** ableiten:

- Unterscheidung in Anwendungsdaten, Systemdaten, Applikationsdaten („Software“; Entwicklungsdaten & Installationsdaten) und Protokolldaten (s.a. M 6.36)
- Verfügbarkeitsanforderungen & Fristen (Vollsicherung, inkrementelle Datensicherung) → Regelmäßige Datensicherung (s.a. M 6.32)
- Datensicherungsplan je IT-System (s.a. M 6.35):
 - Art der Datensicherung
 - Häufigkeit und Zeitpunkt der Datensicherung
 - Anzahl der Generationen
 - Datensicherungsmedium
 - Verantwortlichkeit für die Datensicherung
 - Aufbewahrungsort der Backup-Datenträger
 - Anforderungen an das Datensicherungsarchiv
 - Transportmodalitäten
 - Rekonstruktionszeiten bei vorhandener Datensicherung
- Sporadische Restaurierungsübungen (s.a. M 6.22 & M 6.41)

6.1 Datensicherung (2)

Im Rahmen der Rechtsprechung lassen sich wiederum folgende **Regelungen zur Datensicherung** ableiten:

- täglich hat wenigstens eine Differenzsicherung zu erfolgen und wöchentlich eine Vollsicherung (nach dem Urteil des OLG Hamm vom 01.12.2003; Az.: 13 U 133/03)
- der Erfolg einer Datensicherung ist zu überprüfen (nach dem Urteil des OLG Karlsruhe vom 07.11.1995; Az.: 3 U 15/95)
- bei einer Datensicherung muss die Wiederherstellbarkeit der gesicherten Daten auch bei einem Hardwaretausch überprüft werden (nach dem Urteil des LG Stuttgart vom 30.01.2002; Az.: 38 O 149/00 KfH)
- selbst bei manuellen Datensicherungen sind Vorkehrungen zur Vermeidung von Bedienfehlern zu treffen (nach dem Urteil des OLG Oldenburg vom 03.06.2003; Az.: 9 U 10/03)
- wurde für einen Nutzer dauerhaft für Nebenpflichten ein Mail-Account angelegt, müssen die auf diesem Account abgelegten Daten so lange vorgehalten werden, bis der Nutzer keine Verwendung für diese Daten mehr hat (nach dem Beschluss des OLG Dresden vom 05.09.2012; Az.: 4 W 961/12)

6.2 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 durchgeführte 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):

Kernprozesse:

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

Supportprozesse:

- 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

Führungsprozesse:

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

6.2 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

6.2 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 Worst 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)?

6.2 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+i)☐					max. Ausfall: 48-h für IT-Systeme + 50-h für Prozess (B+i)☐					

6.2 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		

6.3 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 in den BSI-Grundschutzkatalogen bzw. den BSI-Standards an und wählen Sie begründet aus.

6.3 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

6.3 Notfall-Vorsorge-Konzept (2)

Ein mittelständisches Unternehmen wird sich auf Kernfragen konzentrieren

- In Grundschatzkatalogen nach Notfallmanagement suchen
- **Baustein 1.3 zum Notfallmanagement** wählen (abrufbar unter:
https://www.bsi.bund.de/cln_183/sid_AB2A5EAB735FF0FE0D1D3C525AB43C3D/ContentBSI/grundschatz/kataloge/baust/b01/b01003.html)
- Im Baustein 1.3 lediglich Maßnahmen der Kategorie A (Einstieg in Grundschatz) 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

6.4 Notfallplan

Aufgabe:

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

6.4 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)

6.5 Verfügbarkeitsberechnung

Aufgabe:

- Die **Verfügbarkeit** eines IT-Systems kann als das Produkt der Verfügbarkeiten ihrer jeweiligen Komponenten verstanden werden, sofern diese Komponenten seriell 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 parallel 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%).

6.5 Verfügbarkeitsberechnung

Teil A)

$$V_{\text{server}} = (12 \cdot 5 \cdot 52 - 8) / (12 \cdot 5 \cdot 52) = 3112 / 3120 = 99,744\%$$

$$V_{\text{client}} = (12 \cdot 5 \cdot 52 - 16) / (12 \cdot 5 \cdot 52) = 3104 / 3120 = 99,487\%$$

$$V_{\text{netz}} = (12 \cdot 5 \cdot 52 - 24) / (12 \cdot 5 \cdot 52) = 3096 / 3120 = 99,231\%$$

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

Teil B)

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

$$\begin{aligned} V_{\text{gesamt_neu}} &= V_{\text{server}} \cdot V_{\text{client}} \cdot V_{\text{netzcluster}} = 99,744\% \cdot 99,487\% \cdot 99,994\% \\ &= 99,226\% \end{aligned}$$