7. Übungsblatt zum 18. Juni 2018 zu "Grundlagen des Datenschutzes und der IT-Sicherheit":

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

7.2 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):

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

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

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.

7.3 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).

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

7.5 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%)

Allgemeine Hinweise zur Übung:
Die Übung zur LV erfolgt in Form einer Präsenzübung. Für den Notenbonus werden mind. 50 % der max. möglichen Votierpunkte und das Präsentieren von voraussichtlich 3 Lösungen benötigt (abhängig vom Beteiligungsgrad). Jede Aufgabe auf einem Übungsblatt erbringt gleich viele Punkte. **Es gibt verm. 10 Übungsblätter**.
Für das Votieren gilt folgende Regelung:

- Kann die Aufgabenlösung präsentiert werden → voller Punkt
- Existiert für die Aufgabenlösung nur eine Lösungsidee → halber Punkt
- Teilaufgaben werden anteilig gerechnet (d.h. A- bzw. B-Teil jeweils hälftig → insoweit zählt eine Lösungsidee z.B. für den A-Teil nur als ¼-Punkt)
- Zur Lösungspräsentation darf das eigene Lösungsblatt verwendet werden.

Die Einstufung erfolgt durch den Eintragenden und ist entsprechend in die zu Beginn der Übung ausgeteilte Liste einzutragen. Aufgaben, die bereits präsentiert wurden, sind nachträglich nicht mehr votierbar.
Wer Votierpunkte angegeben hat, kann vom Dozenten zur Präsentation seiner Lösung bzw. Lösungsidee aufgerufen werden. Nachweisbar unkorrektes Votieren wird mit 0 Punkten für das gesamte Übungsblatt gewertet.

Gutes Gelingen!