7. Übungsblatt zum 13. Juli 2015 zu "Grundlagen des Datenschutzes und der IT-Sicherheit":

- 7.1 Lesen Sie auf den Web-Seiten des BSI, abrufbar unter www.bsi.de, die Ausführungen in den BSI-Grundschutzkatalogen bzw. den BSI-Standards zum Notfallmanagement durch.
- A) 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? Begründen Sie Ihre Antwort!
- B) Welche Bestandteile sollte dagegen ein **Notfallplan** aufweisen? Begründen Sie Ihre Antwort!
- 7.2 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%)
- 7.3 Gegeben seien folgende Werte einer Sicherheitsanalyse eines IT-Systems hinsichtlich der Gefährdungen der Vertraulichkeit (C), Integrität (I) und Verfügbarkeit (A):

Nr.	Bedrohung	Verwundbarkeit	Auftreten	Schaden		
				C	I	A
1	Datenverlust	fehlende Clusterung	3	1	1	3
2	Datenverlust	Ermüdung Backupmedien	2	1	4	4
3	unbefugter Zugriff	fehlende Schutzzonen	3	5	1	5
4	unbefugter Zugriff	schlechte Passwörter	4	4	3	2
5	unbefugter Zugriff	fehlende Systemhärtung	3	4	4	4
6	unbefugter Zugriff	fehlende Timeoutfunktion	2	3	3	3
7	unbefugter Zugriff	Missbrauch Adminrechte	1	2	5	5
8	Vireninfection	fehlende Schutzzonen	3	3	4	4
9	Vireninfection	schlechter Virenschanner	2	3	3	3
10	DoS-Attacke	fehlende Schutzzonen	4	1	1	5
11	DoS-Attacke	fehlende Timeoutfunktion	2	1	1	4

Die Angaben lägen dabei zwischen 1 (sehr gering) und 5 (sehr hoch).

A) Erstellen Sie auf der Grundlage obiger Werte das zugehörige **Risikoportfolio!**

Betrachten Sie hierzu lediglich die Vertraulichkeitswerte, da der verantwortlichen Stelle die Vertraulichkeit besonders wichtig sei. Beim Risikoportfolio gilt:

- ° Felder, die ein Risiko bis max. den Wert 4 aufweisen, gelten dabei als akzeptabel.
- ° Felder, die ein Risiko ab dem Wert 5 aufweisen, gelten dabei als inakzeptabel.

° Felder, die ein Risiko zwischen diesen Werten aufweisen, bedürfen einer Prüfung. Für welche Risiken empfehlen Sie auf Grundlage des Risikoportfolios welche Gegenmaßnahmen?

B) Erstellen Sie auf der Grundlage obiger Werte die zugehörige **Risikomatrix** in Form einer Risikotabelle! Betrachten Sie hierzu lediglich die Verfügbarkeitswerte, da der verantwortlichen Stelle die Verfügbarkeit besonders wichtig sei.

Für die zu verwendende Risikotabelle verwenden Sie folgendes Schema:

Rg.	Gefährdung	Auftreten	Schaden	Risiko
-----	------------	-----------	---------	--------

Das Risiko ergibt sich aus dem Produkt von Auftreten und Schaden. Die Liste ist entsprechend dem sich rechnerisch ergebenden Rang aufzuführen.

- 7.4 A) Erstellen Sie eine **Fehlerbaum** (Fault Tree Analysis) zu dem Fehlerereignis "mangelnde Verfügbarkeit eines Mail-Servers".
B) Welche Gründe (= Basisereignisse) sind der **Safety** (unbeabsichtigte Ereignisse) zuzuordnen und welche der **Security** (beabsichtigte Angriffe)?
- 7.5 Erstellen Sie einen **Angriffsbaum** (Attack Tree Analysis) für das Angriffsziel "Beeinträchtigung der Verfügbarkeit eines Mail-Servers".

Lösungshinweis zu 7.4 & 7.5:

Recherchieren Sie im Web zu diesen beiden Analyse-Methoden, wie entsprechende Darstellungen von Fehlerbaum bzw. Angriffsbaum aussehen.

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 einer Lösung benötigt. Jede Aufgabe auf einem Übungsblatt erbringt gleich viele Punkte. **Es gibt insgesamt 7**

Übungsblätter.

Beim Votieren gilt folgende Regelung:

- Kann die Aufgabenlösung präsentiert werden → voller Punkt
- Existiert für die Aufgabenlösung nur eine Lösungsidee → halber 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!