

5. Übungsblatt zum 1. Juli 2024 zu "Grundlagen des Datenschutzes und der IT-Sicherheit":

- 5.1 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 Virens Scanner	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).

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 15 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?

- 5.2 Welche Maßnahmen sollten aus Gründen der Informationssicherheit bei der **Entwicklung von Software** ergriffen werden?
- 5.3 Erstellen Sie einen **Fehlerbaum** (Fault Tree Analysis) zu dem Fehlerereignis "mangelnde Verfügbarkeit eines Mail-Servers".
Welche Gründe (= Basisereignisse) sind der **Safety** (unbeabsichtigte Ereignisse) zuzuordnen und welche der **Security** (beabsichtigte Angriffe)?
- 5.4 Erstellen Sie einen **Angriffsbaum** (Attack Tree Analysis) für das Angriffsziel "Beeinträchtigung der Verfügbarkeit eines Mail-Servers".

Lösungshinweis zu 5.3 & 5.4:

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

- 5.5 Welche **Unterschiede** stellen Sie bei diesen beiden Analyse-Methoden fest?
Welche **Schwachstellen** lassen sich anhand dieser beiden Analyse-Methoden ermitteln?
Welche **Konsequenzen** würden Sie als verantwortlicher IT-Leiter daraus ziehen?

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 4 Lösungen benötigt (abhängig vom Beteiligungsgrad). Jede Aufgabe auf einem Übungsblatt erbringt gleich viele Punkte. **Es gibt verm. 6 Übungsblätter.**

Für das Votieren gilt folgende Regelung:

- Kann die Aufgabenlösung präsentiert werden [P] → voller Punkt
- Existiert für die Aufgabenlösung nur eine Lösungsidee [I] → 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 1/4-Punkt)

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!