4. Übungsblatt zum 17. Juni 2024 zu "Grundlagen des Datenschutzes und der IT-Sicherheit":

4.1 Bei einem Unternehmen ist unter Verwendung des **RACI-Modells** festzulegen, welche Stelle welche Aufgabe im Rahmen der Gewährleistung von Informationssicherheit zu erfüllen hat. Erstellen Sie eine Übersicht, in der Sie typische Aufgaben zur Gewährleistung von Informationssicherheit folgenden Stellen zuweisen:
° Geschäftsführer (in der Funktion als Chief Information Officer)
° IT-Leiter (als Verantwortlicher für alle Aufgaben mit IT-Bezug)
° IT-Sicherheitsbeauftragter (Manager von Informationssicherheit)
° Systemadministrator (ausführender IT-Mitarbeiter)
Berücksichtigen Sie in Ihrer Lösung nur die wesentlichen Prozesse zur Gewährleistung von Informationssicherheit, bestehend aus:
° **Einrichtung eines Informationssicherheitsmanagements** (und dessen generelle Funktionsweise)
° **Umgang mit Sicherheitsvorfällen** (Störungsmeldung und –beseitigung)
Konzentrieren Sie sich dabei auf das Wesentliche und gehen Sie bei Ihrer Lösung von einer einfachen IT-Infrastruktur aus, weisen Sie also nur grundlegende Aufgaben zu. Beachten Sie bei Ihrer Lösung, dass niemand eine Aufgabe umzusetzen hat, der diese Aufgabe zugleich zu genehmigen hat.
Hinweis:
*Beim **RACI-Modell** gibt es vier Rollen, nämlich*
***R = Responsible** → Umsetzung einer Aufgabe*
***A = Accountable** → Genehmigung einer Aufgabe*
***C = Consulted** → Anhörungsinstanz bei einer Aufgabe*
***I = Informed** → Mitteilungsempfangsinstanz bei einer Aufgabe*

4.2 Die mehrseitige IT-Sicherheit bestimmt sich anhand der Einhaltung der Sicherheitsziele:
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Zurechenbarkeit (im Sinne von Authentizität)
- Rechtsverbindlichkeit (im Sinne von Nachweisbarkeit)

Konstruieren Sie je ein Beispiel für eine **Bedrohung** der einzelnen Sicherheitsziele und begründen Sie, warum die von Ihnen angegebene Bedrohung für die Gewährleistung des betreffenden Sicherheitszieles gefährlich ist!
Geben Sie für ein frei gewähltes IT-System eine potentielle **Verwundbarkeit** an, über die die angegebene Bedrohung jeweils zu einer erfolgreichen Schädigung des IT-Systems bzw. der dort gespeicherten Daten führen kann!
Hinweis:
*Ein Vermögenswert (**asset**), hierzu zählen u.a. IT-Systeme als Supporting Assets (primary assets stellen dagegen die zu schützenden Informationen dar), kann von einer Bedrohung (**threat**) erfolgreich geschädigt werden, wenn die Bedrohung eine bestehende Verwundbarkeit (**vulnerability**) des Vermögenswertes ausnutzen kann; dies stellt dann eine Gefahr dar. Sicherheitsmaßnahmen (**safeguards**) verhindern die Ausnutzbarkeit entsprechender Verwundbarkeiten. Als Verwundbarkeit kann insoweit auch eine unterlassene Schutzmaßnahme angesehen werden.*

4.3 Geben Sie zu einem frei gewählten IT-System aufgrund der ermittelten Bedrohung und potenziellen Verwundbarkeit (zusammen stellt das eine Gefährdung dar) aus Aufgabe 4.2 geeignete **Maßnahmen** an, die dazu führen, dass das IT-System nicht mehr dieser Gefährdung ausgesetzt ist.

4.4 Welche Aspekte sollten in einem **Sicherheitskonzept**, das den laufenden Betrieb der eingesetzten IT-Infrastruktur gewährleisten soll, auf jeden Fall geregelt werden, um die gängigsten Schwachstellen abzudecken? Begründen Sie Ihre Antwort!

4.5 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:

$$\text{Redundanz-Verfügbarkeit} = 1 - (1 - \text{Verfügbarkeit}_{\text{normal}})^{\text{Anzahl}}$$

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?
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 eine Nachkommastelle anzugeben (also 12,3%)

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 ¼-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!