5. Übungsblatt zum 16. Juni 2014 zu "Grundlagen des Datenschutzes und der IT-Sicherheit":

5.1 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 Kernprozesse zur Gewährleistung von Informationssicherheit, bestehend aus:
° Einrichtung eines Informationssicherheitsmanagements (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*

5.2 Die mehrseitige IT-Sicherheit bestimmt sich anhand der Einhaltung der Sicherheitsziele:

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Zurechenbarkeit (im Sinne von Authentizität)
- Rechtsverbindlichkeit (im Sinne von Nachweisbarkeit)

a) 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!
b) Geben Sie für ein frei gewähltes IT-System eine potentielle **Verwundbarkeit** an, über die die unter a) angegebene Bedrohung jeweils zu einer erfolgreichen Schädigung des IT-Systems bzw. der dort gespeicherten Daten führen kann!
c) Welche **Maßnahme(n)** würden Sie dem IT-Leiter empfehlen, der den von Ihnen unter a) angegebenen Bedrohungen unter Beachtung der von Ihnen angegebenen Verwundbarkeit aus b) angemessen zu begegnen hat?

Hinweis zu 5.2:
*Ein Vermögenswert (**asset**), hierzu zählen u.a. IT-Systeme als Support 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. Sicherheitsmaßnahmen (**safeguards**) verhindern die Ausnutzbarkeit entsprechender Verwundbarkeiten. Als Verwundbarkeit kann insoweit auch eine unterlassene Schutzmaßnahme angesehen werden.*

5.3 Zu welchen Themenbereichen sollte ein Unternehmen **Richtlinien** erlassen, um **Informationssicherheit** adressieren zu können?
Gehen Sie bei Ihrer Lösung davon aus, dass das Unternehmen Mails und Webaccess nur zu dienstlichen Zwecken gestattet und keinerlei Tätigkeiten im Home-Office erbracht werden. In den Richtlinien sollen verbindliche Vorgaben festgeschrieben werden, die die Beschäftigten zu beachten haben.

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

5.5 Welche Maßnahmen nach den **IT-Grundschutzkatalogen** des BSI (siehe **www.bsi.de**) sind unmittelbar für den Betrieb eines Web-Servers beim Einstieg in IT-Grundschutz (= Siegelstufe A) zu adressieren? Der zugehörige IT-Verbund bestehe aus 1 allgemeinen Web-Server, 1 allgemeinen Client, 1 tertiäre IT-Verkabelung, 1 heterogenes Netzwerk, 1 Firewall; Server & Sicherungsbänder befänden sich jeweils in einem Schutzschrank und beide Schutzschränke seien im gleichen Büroraum untergebracht. Wählen Sie die relevanten Maßnahmen anhand der Bausteine unter Beachtung der im Baustein zum Web-Server genannten Bausteine aus den übergreifenden Aspekten aus. Geben Sie in Ihrer Lösung die jeweilige Nummer von Baustein (mit Angabe der zugehörigen Schicht) und Maßnahme an! Ignorieren Sie bei der Aufgabenlösung weitere Bestandteile eines in Praxis vergleichbaren IT-Verbundes.

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 wenigstens zwei (!) Lösungen benötigt (nach aktuellem Beteiligungsgrad). Jede Aufgabe auf einem Übungsblatt erbringt gleich viele Punkte.
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!