4. Übungsblatt zum 18. Juni 2012 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 den Stellen Geschäftsführer (Chief Information Officer), IT-Leiter, IT-Sicherheitsbeauftragter und Systemadministratoren zuweisen! Dabei sollen nur die Prozesse berücksichtigt werden zur Planung des Aufbaus eines Informationssicherheitsmanagements und zum Umgang mit Sicherheitsvorfällen. 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.
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!

4.3 Geben Sie für ein frei gewähltes IT-System eine potentielle **Verwundbarkeit** an, über die die unter 4.2 angegebene Bedrohung jeweils zu einer erfolgreichen Schädigung des IT-Systems bzw. der dort gespeicherten Daten führen kann!

4.4 Welche **Maßnahme(n)** würden Sie dem IT-Leiter empfehlen, der den von Ihnen unter 4.2 angegebenen Bedrohungen unter Beachtung der von Ihnen angegebenen Verwundbarkeit aus 4.3 angemessen zu begegnen hat?

4.5 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.

Hinweis zur Aufgabenstellung:
*Ein Vermögenswert (**asset**), zu den eben auch IT-Systeme zählen, 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.*

Allgemeine Hinweise:
Jede Aufgabe hat gleich viele Punkte. Beim Votieren gilt folgende Regelung:

- die Aufgabenlösung kann jederzeit präsentiert werden (→ voller Punkt)
- für die Aufgabenlösung existiert nur eine Lösungsidee (→ halber Punkt)
- zur Lösungspräsentation darf das eigene Lösungsblatt verwendet werden.

In die zu Beginn der Übung ausgeteilten Liste der Votierwilligen kann entweder das mit dem Dozenten vereinbarte Pseudonym oder der Name eingetragen werden. Sofern sich kein "Freiwilliger" zum Präsentieren meldet, wird einer vom Dozenten ernannt, der Votierpunkte angegeben hat. Nachweisbar unkorrektes Votieren wird mit 0 Punkten für das gesamte Übungsblatt gewertet.

Gutes Gelingen!