

IT-Sicherheit im Wintersemester 2019/2020

Übungsblatt 2

Termin: 05.11.2019 um 12:00 Uhr

Aufgabe 3: (K) Kategorisierung von Sicherheits-Maßnahmen

Wie im Vorlesungsskript (**Kap.2, Folie 13**) dargestellt, lassen sich grundsätzlich technische und organisatorische Sicherheitsmaßnahmen unterscheiden. Darüber hinaus lässt sich jede Maßnahme **mindestens** einer weiteren Kategorie (präventiv, detektierend, reaktiv) zuordnen.

- Beschreiben Sie den Unterschied von *technischen und organisatorische Maßnahmen* sowie zwischen *präventiven, detektiven und reaktiven Maßnahmen*.
- Ordnen Sie folgende Sicherheitsmaßnahmen mindestens einer dieser Kategorien zu, z.B. *technisch-präventiv* oder *organisatorisch-reaktiv* und begründen Sie ihre Zuordnung knapp.
 - Patchmanagementworkflow
 - Host Intrusion Detection System
 - Access Control Lists
 - Richtlinie zur Entsorgung von Datenträgern
 - Zutrittskontrolle
 - Backup
- Welche Schutzziele der Informationssicherheit (CIA) werden durch die folgenden Maßnahmen geschützt?
 - E-Mail Signatur
 - E-Mail Verschlüsselung
 - Dokumenten Backup
 - Dokumenten Archivierung

Aufgabe 4: (K) ISO/IEC 27000

In der Vorlesung wurde Ihnen die Normenreihe ISO/IEC 27000 im Überblick vorgestellt.

- Erläutern Sie in eigenen Worten die Begriffe *Informationssicherheits-Managementsystem (ISMS)*, *Leitlinie*, *Asset* und *Risiko*.
- Erklären Sie den Unterschied zwischen einer *Richtlinie*, einem *Prozess* und einem *Verfahren*.
- Beschreiben Sie die kontinuierliche Verbesserung des ISMS auf Basis des Deming-Zyklus. Welche konkreten Aktionen können zur Überprüfung (Check) durchgeführt werden?
- Beschreiben Sie den grundsätzlichen Ablauf des Risikomanagement gemäß ISO/IEC 27000. Gehen Sie dabei auf die Teilschritte der Risikoanalyse, Risikobewertung und Risikobehandlung ein.
- Nennen und erläutern Sie kurz mindestens drei Möglichkeiten zur *Risikobehandlung*. Sieht ISO/IEC 27001 das *Ignorieren existierender Risiken* **explizit** als Behandlungsoption vor? Begründen Sie ihre Entscheidung!