Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2021/2022
Übungsblatt 2

Besprechung: Di, 09.11.2021

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Aufgabe 4: (K) Kategorisierung von Sicherheits-Maßnahmen

Wie im Vorlesungsskript (**Kap.2, Folie 14**) dargestellt, lassen sich grundsätzlich technische und organisatorische Sicherheitsmaßnahmen unterscheiden. Darüber hinaus lässt sich jede Maßnahme **mindestens** einer weiteren Kategorie (präventiv, detektierend, reaktiv) zuordnen.

a. Beschreiben Sie den Unterschied von *technischen und organisatorische Maßnahmen* sowie zwischen *präventiven, detektiven und reaktiven Maßnahmen*.

b. 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

c. Welche Schutzziele der Informationssicherheit (CIA) werden durch die folgenden Maßnahmen geschützt?

- E-Mail Signatur
- E-Mail Verschlüsselung
- Dokumenten Backup
- Dokumenten Archivierung

Aufgabe 5: (K) ISO/IEC 27000

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

a. Erläutern Sie in eigenen Worten die Begriffe *Informationsicherheits-Managementsystem (ISMS)*, *Leitlinie*, *Asset* und *Risiko*.

b. Erklären Sie den Unterschied zwischen einer *Richtlinie*, einem *Prozess* und einem *Verfahren*.

c. Beschreiben Sie die kontinuierliche Verbesserung des ISMS auf Basis des Deming-Zyklus. Welche konkreten Aktionen können zur Überprüfung (Check) durchgeführt werden?

d. Beschreiben Sie den grundsätzlichen Ablauf des Risikomanagement gemäß ISO/IEC 27000. Gehen Sie dabei auf die Teilschritte der Risikoanalyse, Risikobewertung und Risikobehandlung ein.

e. 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!

Aufgabe 6: (H) Assets, Bedrohungen und Risiken

Sie sind verantwortlich für das Risiko Management (RM) in einem mittelständischen Unternehmen. Bisher standen meist die technischen Bereiche im Fokus des RM, doch nun sollen auch nichttechnische Prozesse genauer betrachtet werden. Sie starten das Onboarding der Geschäftsbereiche Accounting und Human Resources in das RM. Eine Hilfestellung und ergänzende Informationen für diese Aufgabe liefert das BSI-Grundschutz Kompendium (`https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf`).

a. Welche Assets identifizieren Sie in den betrachteten Geschäftsbereichen? Unterteilen Sie diese in primäre und unterstützende Assets.

b. Zwei potentielle Assets sind *Personaldaten* (primär), welche auf einem dedizierten *Server* (unterstützend) gespeichert werden. Von welchen Bedrohungen könnten diese Assets betroffen sein?
Hinweis: Das BSI-Grundschutz Kompendium liefert eine Liste mit Gefährdungen, die Sie als Hilfestellung nutzen können.

c. Wählen Sie ein Asset und eine Bedrohung aus und beschreiben Sie ein mögliches Risiko, das sich aus der Kombination ergeben könnte.

d. Sie wollen das Risiko vollständig eleminieren. Wie könnte das von Ihnen identifizierte Risiko vermieden werden?
Hinweis: Das BSI-Grundschutz Kompendium liefert einige Beispiele für Maßnahmen

e. Sie entscheiden sich stattdessen für eine Modifikation des Risikos. Überlegen Sie sich eine Maßnahme, welche das beschriebene Risiko verringern würde.

f. Verringert Ihre Maßnahme die Eintrittswahrscheinlichkeit oder Auswirkung des Risikos?