Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
PD Dr. Helmut Reiser, PD Dr. Wolfgang Hommel

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2012/2013
Übungsblatt 1

Abgabetermin: 07.11.2012 bis 14:00 Uhr

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

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 1: (H) Ziele der Informationssicherheit & wichtige Begriffe

In der Vorlesung wurden bereits einige Grundlagen und wichtige Begriffe im Bereich der Informationssicherheit erläutert.

a. Erläutern Sie die Sicherheitsziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* mit eigenen Worten und geben ein Beispiel für eine Maßnahme an, um das jeweilige Ziel zu erreichen.

b. Neben den drei, oben genannten wichtigsten Sicherheitszielen existieren noch weitere. Erläutern Sie die Begriffe *Authentizität*, *Nachvollziehbarkeit (Accountability)* und *Privacy*. Geben Sie für das jeweilige Ziel auch mindestens ein Beispiel für eine Maßnahme an, durch die das Ziel erreicht werden kann.

c. Wie Sie in der Vorlesung (Kap. 2, Folie 8) kennengelernt haben, lassen sich Sicherheitsmaßnahmen in verschiedene Kategorien einteilen. Ordnen Sie die folgenden Maßnahmen der jeweiligen Kategorie zu:

- Patchmanagement	- Host Intrusion Detection System	- Beleuchtung
- Router Access Control List	- Smartcard	- Zutrittskontrolle
- CPTED	- Umzäunung	- Passwort-Policy

Wie könnte die Kategorisierung sinnvoll erweitert werden?

Aufgabe 2: (H) ISO/IEC 27000

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

a. Wichtig für die Bestimmung des Risikos ist der Wert eines *Assets* für eine Organisation. Neben den Anschaffungskosten für ein IT-System oder Entwicklungskosten für ein Programm spielen bei der Beurteilung eines Asset-Values weitere Faktoren eine Rolle. Nennen Sie mindestens 4 solche Faktoren und erläutern diese knapp.

b. Ein Managementsystem ist per Definition ein System aus Leitlinien (Policies), Prozessen und Anleitungen (Procedures), die zur Erreichung der Ziele einer Organisation erforderlich sind. Gegeben sei exemplarisch ein organisationsweites Logfile-Management. In der zugehörigen Leitlinie finden sich die folgenden zwei Aussagen:

   – Logdaten sollen nur zu definierten Zwecken erhoben, gespeichert und verarbeitet werden.
   – Logdaten sollen regelmäßig ausgewertet werden.

   Formulieren Sie in Anlehnung daran jeweils **zwei** Beispiel-Statements aus

   – einer Prozessbeschreibung
   – einer Anleitung

c. Gerade der Aufbau einer neuen Webpräsenz auf Basis eines Apache Webservers erfordert die regelmäßige Auswertung der Protokolldateien *access.log* und *error.log*. Benennen und erläutern Sie die Felder, die Sie in einer typischen Zeile im Fehlerprotokoll vorfinden. Wie beurteilen Sie diese Informationen im Hinblick auf datenschutzrechtliche Rahmenbedingungen. Was schlagen Sie als mögliche Lösung vor?

Aufgabe 3: (T) Risikomanagement

Basis für ein ISO/IEC-27001-konformes ISMS ist ein Risikomanagement. Grundsätzlich lassen sich hierzu quantitative und qualitative Vorgehensweisen unterscheiden.

a. Eine Variante für eine qualitative Risikobewertung ist die *Delphi-Methode*.

b. Die quantitative Risikobewertung basiert hingegen auf monetären Werten. Wichtig für die Berechnungen sind dabei

   – die Single Loss Expectancy (SLE)
   – die Annual Loss Expectancy (ALE)
   – die Bestimmung des Wertes einer Maßnahme

c. Bestimmen Sie die SLE für eine Datenbank (1.000.000 Euro), in der wichtige Kundendaten gespeichert sind, die bei Eintritt eines bestimmten Ereignisses zu 45% zerstört wird.

d. Berücksichtigen Sie, dass das betrachtete Schadenereignis nur alle 20 Jahre auftritt.

e. Ein von Ihnen beauftragter Sicherheitsexperte schlägt eine technische Gegenmaßnahme vor, die Sie in 2 Jahren nur 19000 Euro kostet, jedoch nur 60% des möglichen Schadens abdeckt. Ist der Einsatz einer solchen Maßnahme unter Berücksichtigung von Kosten-Nutzen sinnvoll?