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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2011/2012
Übungsblatt 2

Abgabetermin: 09.11.2011 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikums Infrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungs Webseite zum Übungsberieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email, in der Vorlesung oder 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 4: (H) Kategorisierung von Security-Maßnahmen

Die technisch-orientierte OSI Security Architecture bietet eine Reihe von Sicherheitsdiensten und -mechanismen.

a. Sicherheitsmaßnahmen lassen sich grundsätzlich in die Kategorien

   – organisatorisch oder technisch und
   – präventiv, detektierend oder reaktiv

   einteilen. Ordnen Sie die folgenden Maßnahmen der jeweils passenden Kategorie zu.

   - Patchmanagement
   - Host Intrusion Detection System
   - Passwort-Policy
   - Router Access Control List
   - Security Incident Response Prozess
   - Zutrittskontrolle

b. Erläutern Sie den Unterschied zwischen präventiven und detektierenden Maßnahmen.

Aufgabe 5: (H) ISO/IEC 27001

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

a. Erläutern Sie in eigenen Worten die Begriffe *Informationsicherheits-Managementsystem*, *Asset*, *Leitlinie*, *Prozess* und *Verfahren*.

b. ISO/IEC 27000 basiert auf einer Risiko-getriebenes Vorgehensweise. Grenzen Sie die Begriffe Risikoidentifikation, Risikoanalyse, Risikobewertung und Risikobehandlung voneinander ab. Welche Möglichkeiten gibt es, Risiken zu behandeln? Nennen und erläutern Sie mindestens 3.

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 6: (T) Log-Management am LRZ

Am Leibniz-Rechenzentrum wurde ein zu ISO/IEC 27001-konformes Log-Management umgesetzt. In dieser Aufgabe wird ein kurzer Einblick in die rechtlichen, technischen und organisatorischen Themen gegeben, die es an dieser Stelle zu berücksichtigen galt.