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 2016/2017
Übungsblatt 1

Termin: Di, 08.11.2016 um 12:00 Uhr

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

Aufgabe 1: (K) SQL-Slammer & Grundlagen

In der Vorlesung wurden Ihnen einleitend berühmt gewordene Angriffe, z.B. Internet Worm und SQL Slammer vorgestellt.

a. Skizzieren Sie anhand der in der Vorlesung genannten Eckdaten die statistische Ausbreitung von SQL-Slammer innerhalb der ersten Minute. Wie viele Instanzen von SQL-Slammer existieren nach 60 Sekunden?

b. Wie ist die maximal beobachtete Probing Rate von 26.000 Hz begründbar?

c. Warum verlangsamte sich die Ausbreitungsgeschwindigkeit nach ca. 60 Sekunden?

d. Wie viele Infektionsversuche pro Sekunde werden nach 60 Sekunden von allen infizierten Systemen in Summe durchgeführt?

Aufgabe 2: (K) Allgemeine Grundlagen der Informationssicherheit

In der Vorlesung wurden Ihnen erste allgemeine Grundlagen der Informationssicherheit vermittelt.

a. Erläutern Sie den Unterschied zwischen *Security* und *Safety* in eigenen Worten und geben Sie mindestens zwei Beispiele für das jeweilige Themengebiet an.

b. Das bekannte Bell LaPadula Modell dient zur Sicherstellung der Vertraulichkeit klassifizierter Informationen. Beschreiben Sie kurz Eckpunkte dieses Modells, insb. die hier geltenden Regeln für Zugriffe auf diese Informationen und das hier angewendete Prinzip der sog. *dominance relation*.

c. Während das in der vorherigen Aufgabe behandelte Bell LaPadula Modell zur Sicherung der Vertraulichkeit dient, zielt das *Biba-Sicherheitsmodell* auf die Sicherung der Integrität von Informationen ab. Erläutern Sie die hier geltenden Zugriffsregeln. Begründen Sie anschließend, warum ein lesender Zugriff auf Informationen tieferer Schichten ein Problem darstellt.

Aufgabe 3: (K) Kategorisierung von Sicherheits-Maßnahmen & ISO/IEC 27000

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.

a. Ordnen Sie folgende Sicherheitsmaßnahmen mindestens einer dieser Kategorien zu, z.B. technisch-präventiv oder organisatorisch-reaktiv und begründen Sie ihre Zuordnung knapp.

- Patchmanagementworkflow
- Access Control Lists
- Zutrittskontrolle
- Security Information u. Event Management System
- Richtlinie zur Entsorgung von Datenträgern
- Backup

b. Was legt die Norm ISO/IEC 27001 genau fest? Wie ist der Begriff Informationssicherheitsmanagementsystem (ISMS) definiert und aus welchen Kernelementen setzt es sich zusammen?

c. Der Aufbau eines ISMS stützt sich normalerweise auf das Management von (Geschäfts-)Risiken. Erläutern Sie die in diesem Zusammenhang oftmals anzutreffende *Delphi-Methode*. In welcher Phase des Risikomanagementprozesses ist diese angesiedelt?

d. 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!