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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2014/2015
Übungsblatt 1

Abgabetermin: 28.10.2014 bis 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.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (über Uniworx als Einzelabgabe). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) 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)** SQL-Slammer & Grundlagen (6 Punkte)

In der Vorlesung wurden Ihnen einleitend berühmt gewordene Angriffe, z.B. Internet Worm und SQL Slammer vorgestellt und einige wichtige Grundlagen und Begriffe im Bereich der Informationssicherheit erläutert.

a. Skizzieren Sie anhand der in der Vorlesung genannten Eckwerten 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 verlangsamt sich das Wachstum der Ausbreitungsgeschwindigkeit nach ca. 60 Sekunden?

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

e. Erläutern Sie die Sicherheitsziele *Integrität* und *Nicht-Abstreitbarkeit* mit eigenen Worten und geben mindestens zwei Beispiele für Maßnahmen an, um das jeweilige Ziel zu erreichen.

f. Während das bekannte Bell LaPadula Modell zur Sicherung der Vertraulichkeit klassifizierter Information dient, zielt das *Biba-Sicherheitsmodell* auf die Sicherung der Integrität von Informationen ab. Erläutern Sie die zwei Zugriffsregeln dieses Modells. Begründen Sie, dass der lesende Zugriff auf Informationen tieferer Schichten ein Problem darstellt.

Aufgabe 2: (H) Kategorisierung von Sicherheits-Maßnahmen & ISO/IEC 27000 (8 Punkte)

Wie im Vorlesungsskript, Kap.2 Folie 12, dargestellt, lassen sich grundsätzlich technische und organisatorische Sicherheitsmaßnahmen unterscheiden. Darüber hinaus lässt sich jede Maßnahme mindestens einer weiteren Kategrorie (präventiv, detektierend, reaktiv) zuordnen.

a. Ordnen Sie folgende Sicherheitsmaßnahmen mindestens einer Kategorie zu, z.B. technisch-präventiv 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 Geschäftsrisiken. 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* als Behandlungsoption vor? Begründen Sie ihre Entscheidung!