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 2015/2016
Übungsblatt 1

Abgabetermin: 27.10.2015 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 (4 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 Eckdaten die statistische Ausbreitung von SQL-Slammer innerhalb der ersten Minute. Wie viele Instanzen von SQL-Slammer existieren nach 60 Sekunden?

b. Die maximal beobachtete Probing Rate wurde in der Vorlesung mit 26.000Hz angegeben. Diese ist durch die zur Verfügung stehende Bandbreite begrenzt. Wie viele Probes würde ein mit 1 GBit-Anschluss ausgestatteter infizierter PC heutzutage schaffen?

c. Der Internet-Knoten DE-CIX hat erst kürzlich einen Spitzendurchsatz von 4TBit/s vermeldet. Wie viele SQLSlammer-Instanzen wären notwendig um dieses Backend voll auszulasten?

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

Aufgabe 2: (H) Allgemeine Grundlagen (7 Punkte)

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 die jeweiligen Themengebiete 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: (H) Kategorisierung von Sicherheits-Maßnahmen & ISO/IEC 27000 (8 Punkte)

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 Kategorie zu, z.B. technisch-präventiv und begründen Sie ihre Zuordnung knapp.

- Patchmanagementworkflow	- Security Information u. Event Management System
- Access Control Lists	- Richtlinie zur Entsorgung von Datenträgern
- Zutrittskontrolle	- 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* **explizit** als Behandlungsoption vor? Begründen Sie ihre Entscheidung!