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 2

Abgabetermin: 04.11.2014 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 3: (H) Security Engineering (6 Punkte)

Das Security Engineering ist eines der zentralen Themen in der IT-Sicherheit. Das Ziel, das dabei grundsätzlich verfolgt wird, ist die Konstruktion sicherer IT-Systeme und -Infrastrukturen.

a. Nennen und erläutern Sie mindestens 4 Gründe, warum sich die Methoden für die Konstruktion sicherer Systeme kaum entwickelt haben.

b. Das Thema *Sicherheit* sollte von Anfang an in dem Entwicklungsprozess eines Systems berücksichtigt werden. Dazu existieren eine Reihe von Prinzipien:

   - Prinzip der minimalen Rechte (Least privileges)
   - Verbote sind Standard (Fail-Safe default)
   - Sicherheit hängt nicht von Geheimhaltung ab (Open design)
   - Trennung von Rechten (Separation of duties)

   Erläutern Sie diese vier hier genannten Prinzipien und geben Sie jeweils ein Beispiel aus der Praxis an.

Aufgabe 4: (H) Security Engineering in der Praxis (8 Punkte)

Sie sind Sicherheitsverantwortlicher in einem Unternehmen und werden von der Leitung gebeten, eine HTTP-basierte Portal-Lösung für Ihre Lieferanten abzusichern. Der Login erfolgt auf der aus dem Internet frei zugänglichen Portalseite über eine Kombination aus Username und Passwort. Das Management der Anwendung erfolgt aus ihrem internen Mitarbeiternetz heraus über einen TELNET-Client und damit unverschlüsselt.

a. Bei Erledigung ihrer Aufgabe orientieren sich an der in der Vorlesung vorgestellten Vorgehensweise (Kap. 3, Folie 4), wobei Sie sich auf die folgenden Phasen beschränken:

   (i) Bestandsaufnahme
   (ii) Bedrohungsanalyse
   (iii) Ableitung von Sicherheitsanforderungen
   (iv) Erstellung einer Sicherheitspolicy
   (v) Auswahl geeigneter Mechanismen zur Durchsetzung der Sicherheitsanforderungen

   Geben Sie exemplarisch für diese Phasen mögliche Inhalte an. Dazu zählen etwa, welche Tätigkeiten in der jeweiligen Phase durchzuführen sind, welche Komponenten Sie abzusichern haben, welche Sicherheitsanforderungen sie identifizieren konnten und mit welchen Mechnismen sie versuchen würden, das Web-Portal abzusichern? Berücksichtigen Sie dabei, dass neben dem Portal-System auch die für das Anwendungsmanagement eingesetzten Mitarbeiter-PCs einer adäquaten Absicherung bedürfen.

b. In der Vorlesung wurde das Vorgehensmodell in Anlehnung an das Wasserfallmodell dargestellt. Welchen Vorteil demgegenüber hätte eine am Spiralmodell orientierte Vorgehensweise?

c. Erläutern Sie kurz (in eigenen Worten) das Angreifermodell. In welchem Risikomanagement-Schritt spielt das Angreifermodell eine zentrale Rolle? Erläutern und begründen Sie ihre Antwort.