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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2012/2013
Übungsblatt 2

Abgabetermin: 14.11.2012 bis 14:00 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 (per Email an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich 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) Security Engineering

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. 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 einem Mitarbeiternetz heraus, unverschlüsselt über TELNET. Sie orientieren sich dabei an dem in der Vorlesung vorgestellten Vorgehensmodell (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 die angegebenen Phasen mögliche Inhalte an. Gehen Sie davon aus, dass neben dem Portal-System auch die Managementsysteme einer adäquaten Absicherung bedürfen.

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

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

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

Aufgabe 5: (H) Malicious Code

Tagtäglich gibt es Meldungen über die Ausbreitung von Malicious Code. Unter diesem Sammelbegriff werden im Allgemeinen Schadprogramme wie Computerviren, -würmer und Trojanische Pferde verstanden.

a. Zur Erkennung von Malicious Code auf einem System werden in der Regel Anti-Virus-Programme eingesetzt, die eine Reihe von Erkennungstechniken kombiniert verwenden. Erläutern Sie *Signatur-basierte*, *Heuristische/Anomalie-basierte* und *Emulations-basierte Erkennung*.

b. Welche Stärken bzw. Schwächen weisen die in der vorherigen Teilaufgabe beschriebenen Erkennungstechniken auf?

c. Um der Erkennung durch aktuelle Anti-Viren-Programme zu entgehen, werden bei der Programmierung von polymorphen Viren verschiedene Techniken eingesetzt. Erläutern Sie die Methoden

   - Garbage instructions
   - Instruction reordering
   - Interchangeable instructions

Aufgabe 6: (T) Der Wirtschaftssektor Malware-Verbreitung

Anfangs standen alleinig die Beschäftigung mit der Technik und das Kennenlernen und Ausreizen von Möglichkeiten, welche Computersysteme zum damaligen Zeitpunkt boten, im Vordergrund. Im Laufe der Zeit spielten aber eher auch Anerkennung in Hackerkreisen eine Rolle. Seit einigen Jahren ist jedoch eine Kriminalisierung dieser Szene beobachtbar, so dass finanzielle Interessen in den Vordergrund gerückt sind. In dieser Aufgabe soll ein kurzer Einblick in diesen Wandel gegeben werden. U.a. geht es hierbei um um heutige Verbreitungswege der Malware.