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 2021/2022
Übungsblatt 1

Abgabetermin: Di, 26.10.2021 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: (T) 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: (T) SolarWinds

Einer der größten Angriffe der letzten Jahre wird unter dem Titel „SolarWinds“ zusammengefasst.

a. Recherchieren und beschreiben Sie den Ablauf der SolarWinds-Angriffsreihe.

b. Welche Schwachstellen wurden vom Angreifer ausgenutzt? Warum verbreitete sich der Angriff und blieb so lange unentdeckt?

c. Wie kann ein vom Angriff betroffenes Unternehmen, seinen regulären IT-Betrieb wiederherstellen (recover)?

d. Was versteht man unter einem Supply-Chain-Angriff?

e. Mit welchen Präventions- oder Detektionsmaßnahmen könnte ein solcher Angriff in Zukunft erschwert werden?

Aufgabe 3: (H) Allgemeine Grundlagen der Informationssicherheit

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

a. Erläutern Sie die Sicherheitsziele *Vertraulichkeit*, *Integrität*, *Verfügbarkeit* und *Authentizität* in eigenen Worten und geben ein Beispiel für eine Massnahme an, um das jeweilige Ziel zu erreichen.

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

c. 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*.