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 2024/2025
Übungsblatt 3

Besprechung: Do, 14.11.2024

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) Malicious Code & SPAM-Protection

a. Zur Erkennung von Malicious Code auf einem System werden in der Regel Antiviren-Programme eingesetzt, die eine Reihe verschiedener Erkennungstechniken kombiniert verwenden. Erläutern Sie *Signatur-basierte*, *Heuristische/Anomalie-basierte* und *Emulations-basierte Erkennung* und beschreiben sie jeweils die Stärken und Schwächen des jeweiligen Ansatzes.

b. Um der Erkennung durch aktuelle Antiviren-Programme zu entgehen, werden bei der Erstellung und Programmierung polymorpher Viren verschiedene Techniken eingesetzt. Erläutern Sie die folgenden Techniken

   - Garbage instructions
   - Instruction reordering
   - Interchangeable instructions

c. Es existieren verschiedene Maßnahmen, SPAM zu erkennen und diesen herauszufiltern bzw. zu blocken. Erläutern Sie folgende Verfahren: *DNS-basierte Blacklists*, *RHSBLs* und *naive Bayes-Klassifizierung*. Gehen Sie hier zusätzlich auf rechtliche Probleme ein, die Ihnen bei Einsatz dieser Verfahren begegnen.

Aufgabe 2: (T) Endpoint Security & EDR

Die Endgeräte der Nutzer sind häufig Einstiegspunkt von Cyberangriffen auf Unternehmensnetze. Die Strategie der Endpoint Security zielt darauf ab, das zentrale Netz bereits an den einzelnen Endgeräten zu schützen, die sich am Rand des Netzes und oftmals außerhalb der Firmenfirewall befinden.

a. Welche Ansätze von Virenscannern gibt es? Welche Nachteile haben sie?

b. Welchen Ansatz verfolgen *Endpoint Security*-Systeme? Wo liegt hier der Unterschied zu Antivirenprogrammen?

c. Aus welchen Komponenten können Endpoint Security bzw. *Endpoint Protection* Systeme bestehen?

d. Welche Ziele verfolgt *Endpoint Detection und Response* (EDR)? Wie spielt EDR mit Endpoint Security zusammen?

e. Mit welchem Ansatz versucht *Extended EDR* (XDR) noch einen Schritt weiterzugehen?

Aufgabe 3: (T) Security Information and Event Management

SIEM stellt eine Kombination aus dem *Security Information Management* (SIM) und dem *Security Event Management* (SEM) dar. Grundidee ist es hierbei viele/alle sicherheitsrelevanten Informationen an einer zentralen Stelle zu sammeln und in Echtzeit auszuwerten.

a. Beschreiben Sie Aufgaben und Funktionsprinzip eines SIEM.

b. Welche Herausforderungen stellen sich dabei?

c. Welche Informationsquellen lassen sich an das SIEM anbinden?

d. Lassen sich durch den Einsatz eines SIEM mehr Bedrohungen erkennen als ohne?

e. Welche Vor- und Nachteile ergeben sich beim Einsatz eines SIEMs?

f. Wie unterscheidet sich ein SIEM von einem *Intrusion Detection System* (IDS) oder *Intrusion Prevention System* (IPS)?

Aufgabe 4: (T) Tactics, Techniques and Procedures

TTP ist ein etabliertes Konzept zur Beschreibung von Cyberangriffen bzw. -angriffsmustern.

a. Beschreiben Sie die drei Bestandteile des TTP-Konzepts und instanziieren Sie es durch ein geeignetes Beispiel. Für welche Einsatzzwecke sind TTPs geeignet?

b. Der folgende Artikel berichtet von einem Cyberangriff.
`https://www.golem.de/news/trickbot-us-militaer-greift-botnetzwerk-an-2010-151452.html`
Beschreiben Sie diesen Angriff im TTP-Schema.

c. Was ist die *MITRE ATT&CK*-Matrix (`https://attack.mitre.org/`)? Wie ist sie aufgebaut? Wozu kann sie eingesetzt werden?

d. *Access Token Manipulation* ist eine Technik zur *Privilege Escalation*.

   (i) Wie funktionieren derartige Angriffe?

   (ii) Welche Formen sind bekannt?

   (iii) Wie können sie detektiert und verhindert werden?

e. Angenommen ein Angreifer möchte auf möglichst vielen Maschinen in einem fremden Netzwerk einen Krypto-Miner installieren. Welche Zwischenschritte muss der Angreifer verfolgen, um zu diesem Ziel zu gelangen? Welche Techniken könnte er dazu jeweils einsetzen? Nutzen Sie die *MITRE ATT&CK*-Matrix.