Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Security

Sommersemester 2022
(LV 4120 und 7240)

1. Aufgabenblatt

Ziel dieser Übung ist es, die Begrifflichkeiten der Informationssicherheit sowie deren Abgrenzungen herauszustellen. Ferner diskutieren wir die potenzielle Gefährdungslage im IT-Umfeld sowie das grundsätzliche Anliegen nach Informationssicherheit. Im Hinblick auf die Gefährdungslage wird insbesondere zwischen den Begrifflichkeiten Angriff, Bedrohung, Schwachstelle, Sicherheitslücke und dem daraus ableitbaren Risiko unterschieden.

Aufgabe 1.1

a) Welches sind die drei Grundziele der Informationssicherheit?

b) Nehmen Sie eine Abgrenzung zwischen den Begrifflichkeiten IT-, Cyber- und Informationssicherheit vor.

c) Welche bewährte Methodik führt für ein IT-System auf eine dem individuellen Schutzbedarf angepasste und angemessene Informationssicherheit.

Aufgabe 1.2

a) Worin unterscheidet sich eine Schwachstelle von einer Sicherheitslücke? Was ist ein Exploit?

b) Wann führt eine Sicherheitslücke in einem IT-System zu einer Gefährdung?

c) Was verstehen wir unter einem Sicherheitsrisiko?

Aufgabe 1.3

a) Recherchieren Sie den Anteil der von Sicherheitsverstößen in Deutschland betroffenen Unternehmen sowie die am stärksten betroffenen Branchen.

b) Was sind die im Bereich der Computer-Kriminalität die am häufigsten zu verzeichnenden Missbrauchs-Delikte?

c) In welcher Größenordnung liegt die durchschnittliche Schadenshöhe bei Cybergefährdungen in Deutschland?

Aufgabe 1.4

a) Kreuzen Sie an, welche Sicherheitsmaßnahmen beim Erreichen welcher Schutzziele dominant sind:

	Heiße Reserve	**Verschlüsselung**	**CRC-Prüfsumme**	**Zwei-Faktor-Authentifizierung**
Integrität				
Vertraulichkeit				
Verfügbarkeit				
Zurechenbarkeit				

b) Kreuzen Sie in der folgenden Tabelle ferner an, welche Themen eher mit Safety und welche eher mit Security zu tun haben:

	Safety	**Security**
Malware Attacke		
Erdbeben		
Stromausfall		
Datendiebstahl		
Lichtschranke		

c) Kreuzen Sie in der folgenden Tabelle ferner an, welche Bestandteile vornehmlich in einem IT-Sicherheitskonzept enthalten sind:

	Ja	**Nein**
Programmieranleitung		
Bestandsanalyse		
Nutzungsbedingungen		
Schutzbedarfsfeststellung		
Schadensszenarien		

Aufgabe 1.5

Ein Online-Banking Kunde erhält von seiner Bank eine E-Mail mit der Aufforderung, seine persönlichen Bankdaten zu aktualisieren. Gleichzeitig wird der Kunde darüber informiert, dass ein System-Update seitens der Bank erfolgt ist und er nunmehr seine Online-Daten auf Korrektheit prüfen solle. In der E-Mail ist ein Hyperlink enthalten, der offensichtlich ohne großen Aufwand ein Kunden-Login auf dem Portal der Bank ermöglicht. Diesen Link klickt der Kunde an. Über den Browser erscheint ein Login-Formular, in welches der Kunde seine persönliche Online-Daten eingibt und welches er abschließend mit dem Login-Button abschließt. Im Anschluss an diese Aktion erscheint eine Fehlermeldung mit dem Hinweis, dass der Login-Versuch fehlgeschlagen sei und wiederholt werden müsse. Der Kunde folgt dieser Aufforderung. Einige Sekunden später wird der Browser automatisch auf das Bankportal geleitet, wonach der Kunde den Login-Vorgang erneut durchführt. Diesmal allerdings mit Erfolg!

a) Welcher Art des Angriffs ist der Kunde mit hoher Wahrscheinlichkeit zum Opfer gefallen?

b) Was sind die Schwachstellen eines solchen Online-Anmeldeformulars, mit dessen Hilfe der Kunde seine Benutzer-Authentifikation durch Eintippen von Benutzername und Kennwort in aller Regel mittels eines Standard-Browser bewerkstelligt?

c) Benennen und beschreiben Sie zwei Gegenmaßnahmen, die den Kunden vor dieser Art von Angriffsszenarium schützen.

d) Auf welche möglichen Motive der Angreifer lässt dieses Beispiel schließen? Nennen Sie mindestens vier.