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

Security

Sommersemester 2021
(LV 4121 und 4241)

1. Aufgabenblatt

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

Aufgabe 1.1

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

b) Versetzen Sie sich kurz in die Rolle eines Angreifers und beschreiben Sie generisch einen potenziellen Angriffsversuch. Welche prinzipiellen Schritte sind für einen IT-Angriff erforderlich? Welche Aktionen sind seitens des Angegriffenen zu erwarten? Wann ergibt sich aus einem Angriff eine Gefährdung?

Aufgabe 1.2

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.

Aufgabe 1.3

Warum sollen Passwörter auch dann nicht für Benutzer zugänglich abgespeichert sein, wenn die Passwörter beispielsweise durch eine Einwegfunktion verschlüsselt sind?

Aufgabe 1.4

a) Erklären Sie kurz folgende 5 Begriffe aus der IT-Security Vorlesung:

Funktionssicherheit, asymmetrische Verschlüsselung, Spoofing, HMAC und Verfügbarkeit.

b) Kreuzen Sie bitte an, welche Sicherheitsmaßnahmen beim Erreichen welcher Schutzziele sinnvoll sind:

	Redundanz	**Firewall**	**Kryptographie**	**Virenschutz**
Integrität				
Vertraulichkeit				
Verfügbarkeit				
Zurechenbarkeit				
Verbindlichkeit				

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

	Safety	**Security**
Höhere Gewalt		
Sniffing		
Malware		
HW-Defekt		
DDoS		