1)

Hochschule RheinMain
Fachbereich DCSM - Informatik
Marc Stöttinger

Safety
a)zielt auf Übereinstimmung der Ist- mit der Soll-Funktionalität der Komponenten(Gefahrenabwendung,Ausfallssicherheit Schutz von Leib & Leben).
b)Security: alle Vorkehrungen zum Schutz von elektronisch gespeicherten Informationen sowie IT-Systemen (SW & HW)
c) Privacy: regelt die Verwendung und Weitergabe personenenbezogener Daten (DSGVO)
d) Safety: Airbag, Sicherheitsgurt ; Security: ; Privacy: Infotainment

Security

SoSe 23

LV 4120, 7240

Übungsblatt 1

Ziel dieser Übung ist es, die Terminologie der Informationssicherheit und ihre Abgrenzungen zu verstehen. Darüber hinaus werden wir die potenzielle Bedrohungslage in der IT-Umgebung sowie die allgemeine Sorge um die Informationssicherheit erörtern. Insbesondere werden wir zwischen den Begriffen Angriff, Bedrohung, Schwachstelle, Gefährdung und der daraus resultierenden Bedrohungslage unterscheiden.

Aufgabe 1.1 (Der Begriff Sicherheit):

a) Erklären Sie den Begriff Funktionssicherheit.

b) Erklären sie den Begriff Sicherheit.

c) Erklären Sie den Begriff Datenschutz.

d) Beschreiben Sie anhand eines Autos Beispiele für Security-, Safety- und Privacy- Anforderungen.

2)

Aufgabe 1.2 (Weaknesses, Threats, Hazards and Vulnerabilities):

a) Weakness: "sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution". Bsp.: schwache Passwörter, offene Ports, Bugs, Mensch

a) Was ist ein Schwachstelle?

b) Threat: "ein Umstand oder ein Ereignis, durch den oder das ein Schaden entstehen kann" Bsp: Passwort-raten, Netzwerkscans

b) Was ist eine Bedrohung?

c) hazard: "eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt". Bsp: Angreifer rät Passwort

c) Was ist eine Gefährdung?

d) Eine Sicherheitslücke ist eine Schwachstelle. Ein Exploit nutzt diese Sicherheitlücke aus

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

e) eine Sicherheitslücke führt zu einer Gefährdung, wenn ein Angreifer diese ausnutzt um z.B. vollen Zugriff auf ein System zu erlangen

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

Aufgabe 1.3 (Fall Beispiel):

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 einen 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 bestätigt. 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 Angriffsart 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-Browsers bewerkstelligt?

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

Aufgabe 1.4 (Blutspende APP):

Im Rahmen eines Projekts soll eine Blutspende-App entwickelt werden. Mit Hilfe dieser App können sich Nutzer registrieren und ihre Blutgruppe angeben. Die Benutzerdaten sowie ein Individualisierungstoken werden in einer Datenbank auf einem Server gespeichert. Über ein Portal können Krankenhäuser und Ärzte bei Bedarf nach Blutspenden suchen. Dabei werden Anfragen basierend auf der Blutgruppe der registrierten Nutzer und ihrem Standort an die App gesendet und der Benutzer wird informiert. Im Falle einer Bereitschaft kann der Benutzer zusagen oder, falls keine Zeit vorhanden ist, absagen. Bei einer Zusage erhält der Benutzer die Wegkoordinaten zum Spendeort auf sein Mobiltelefon und der Krankenhaus- oder Arztanfrage wird mitgeteilt, dass ein Spender gefunden wurde.

a) Welche Aspekte von Sicherheit müssen hier beachtet werden (Safety, Security, Privacy)? Begründen Sie ihre Aussage mit einem Beispiel.

b) Was für Bedrohungen oder Gefährdungen können Sie aus der Beschreibung des Systems ableiten?

3)

a) Phising

b) Passwörter müssen nicht stark sein, Benutzer speichern meistens Passwörter

c) Hyperlink überprüfen, Impressum/Originalseite finden und vergleichen

4)
a)
Safety: Wenn die Daten falsch übertragen/gespeichert werden, werden Menschen in Gefahr gebracht
Security: Blutdaten können geklaut und verkauft werden
Privacy: Die Daten dürfen nicht weitergegeben werden

b)
Menschen können in Gefahr gebracht werden, wenn ihr Blutdaten manipuliert werden.
Es ist bekannt wann und wo eine Person Blut spenden will/wird.