Hochschule RheinMain
Fachbereich DCSM - Informatik
Marc Stöttinger

Security
SoSe 23
LV 4120, 7240

Übungsblatt 2

In dieser Übung beschäftigen Sie sich mit Schutzzielen und den dazugehörigen Bedrohungen. Das Ziel ist es, wichtige abstrakte Schutzziele für ein IT-System oder eine Komponente formulieren zu können, basierend auf den potentiellen Bedrohungen. Hierzu ist es besonders wichtig zu verstehen, auf welche Sicherheitseigenschaften eine Bedrohung abstrakt einwirkt, wer der Angreifer oder die Angreiferin sein kann und welche Motivation er oder sie hat.

Aufgabe 2.1 (Sicherheitssziele):

Machen Sie sich besser mit den sechs vorgestellten Sicherheitszielen (Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit, Autorisierung, Verbindlichkeit) vertraut, indem Sie:

Vertraulichkeit: Passwort raten Lsg: 2FA

a) für jedes der Sicherheitsziele eine beispielhafte Bedrohung angeben.

Integrität: Festplattenfehler. Lsg: Raid-Konfiguration

Authentifizität: unverschlüsselte Kommunikation (Man-in-the-Middle) Lsg: verschlüsselte Kommunikation mit Authentifizierung

Verfügbarkeit: Stromausfall. Lsg: Notstromgenerator

Autorisierung: Alle Mitarbeiten haben Admin-Rechte. Lsg: Administrator schränkt Rechte ein

Verbindlichkeit/Nicht-Abstreitbarkeit: kein Login notwendig. Lsg: Benutzer muss sich anmelden um auf die Daten zuzugreifen

b) für jedes der Sicherheitsziele einen beispielhaften Sicherheitsmechanismus angeben.

c) Überlappungen zwischen den Sicherheitszielen beschreiben.

Aufgabe 2.2 (Sicherheitssziele im Bezug auf Malware und Angriffstechniken):

Welche der sechs Sicherheitsziele werden jeweils durch die folgenden Angriffstechniken und Malwarearten bedroht? Begründen Sie Ihre Antwort:

a) Ransomware

b) Trojaner/Viren/Würmer

c) Spyware

d) Cryptominer

e) Denial of Service

a) Vertraulichkeit: Informationen werden "geleakt" wenn der Erpresste nicht den Forderungen des Erpressers nachkommt
Integrität: Ransomware verschlüsselt die Daten
Verfügbarkeit: Ransomware kann das "System" sperren (Offline nehmen)

b) Vertraulichkeit: Trojaner speichern die Daten
Integrität: Viren können die Daten verschlüsseln oder löschen
Authentizität:
Verfügbarkeit: Viren können das System sperren (Offline nehmen)
Autorisierung: Knacken der Passwörter

c) Vertraulichkeit

d) Verfügbarkeit: Überlastung des Systems

e) Verfügbarkeit

Aufgabe 2.3 (Schutzziele, Bedrohung und Monetarisierung):

Der Blood2Donate-Service (B2DS) ermöglicht es, mit Hilfe der dazugehörigen App, registrierte Blutspender innerhalb eines bestimmten Radius zu ermitteln und bei Blutspende-Anfragen von Krankenhäusern zu vermitteln. Die Vermittlung eines Blutspenders zu einer Anfrage erfolgt wie folgt:

a) Dr. Alice löst Anfrage *0 negativ innerhalb von 5km* Radius aus

b) Suche nach Spender:innen in der Datenbank innerhalb der Radius

c) B2DS-Server sendet Anfrage auf Spende innerhalb eines gesonderten Radius aus

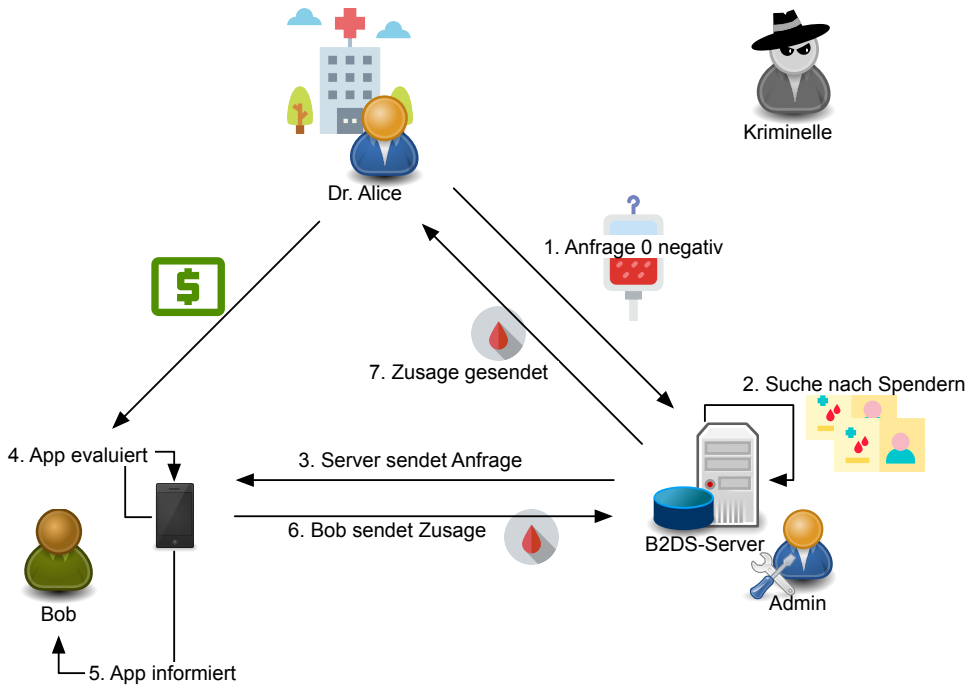
d) App evaluiert, ob Bob passende Blutgruppe hat

e) App informiert Bob

f) Bob sendet Zusage zur Spende zurück zum B2DS-Sever

g) B2DS-Server sendet Zusage an Dr. Alice

h) Bob wird für Spende finanziell entlohnt



Sie werden bei D2B im Bereich IT-Sicherheit eingestellt. Denken Sie sich drei beispielhafte Angriffe aus und geben Sie dabei für jeden Angriff die folgenden Informationen.

a) Wer ist der Angreifer?

b) Welche Methode benutzt der Angreifer (grobe Beschreibung)?

c) Wie kann der Angreifer den Angriff monetarisieren?

d) Welches Sicherheitsziel wird bei dem Angriff verletzt?