Assignment 2: Graf Daniel, Dimitrie Diez

# Exercise 1-2

## a)

**Spezifisches Problem**

Ein potenzieller Angreifer sieht aktuell welches Authentifizierungsverfahren eine Person für welches Konto verwendet. Darüber hinaus ist sofort bekannt, ob ein Authentifizierungsvorgang erfolgreich war oder nicht. Dies stellt eine Schwachstelle hinsichtlich der Sicherheit dar, da die Schwachstellen der jeweiligen Authentifizierungsmethode gezielt ausgenutzt werden können und ein Angreifer sofort erfährt, ob er erfolgreich war oder nicht.

**Persona**

Allgemein: Junge Menschen die technisch versiert sind.

Hans Meierhuber ist 25 Jahre alt und Informatik Student. Er fragt sich wie er die Sicherheit seiner hochsensiblen Daten gewährleisten kann. Er besitzt ein modernes Smartphone und achtet immer auf eine aktuelle Version seines Betriebssystems. Technische Neuerungen findet er interessant. Folglich ist er in entsprechenden Foren aktiv. Er besitzt ein Social Media Konto.

**Szenario**

Login – Hans stört es, dass er bei jedem fehlgeschlagenen Login Versuch sofort erfährt ob PW oder Email falsch war. Er findet dies unsicher.

**Focus Group:**

* Hans Meierhuber möchte sich in sein Social Media Konto einloggen. Er bekommt alle aktuell möglichen Authentifizierungsverfahren aufgelistet. Nur wenn er ein für dieses Konto aktiviertes Verfahren auswählt und sich korrekt authentifiziert gelangt er in sein Konto. Falls er ein nicht aktiviertes Verfahren wählt oder die Authentifizierung scheitert, gelangt er in ein generiertes Fake Profil, welches nur vom Inhaber des echten Profils als solches identifiziert werden kann. Das Fake Profil besitzt einen eingeschränkten Funktionsumfang. Wird dort beispielsweise eine Nachricht versendet, wird diese zwar als versendet markiert, jedoch nicht wirklich abgeschickt. Ohne Einblick in das Konto des Empfängers dieser Nachricht ist es somit nicht möglich dies zu ermitteln.
* Nur 3 fehlgeschlagene Logins zulassen. Dann Sicherheitsauthentifizierung (Personalausweis (Online-Funktion), Handynummer)
* 2-Wege Authentifizierung (Mail + PW eingeben 🡪 IMMER Anzeige dass Pushmitteilung an Handy geschickt wird, Nur wenn PW + Mail korrekt: Pushmitteilung wirklich versendet 🡪 Pushmitteilung muss noch bestätigt werden)

**Description:**

Peter möchte sich in sein Konto bei der neuen Social Media Plattform „Secure Social Network“ (SSN) einloggen. Auf der Startseite muss er sich zunächst mit seiner Mail-Adresse und seinem Passwort authentifizieren. Anschließend wird er aufgefordert sein hinterlegtes Authentifizierungsverfahren aus einer Liste möglicher Verfahren auszuwählen und sich mit diesem zu authentifizieren. Unabhängig davon, ob E-Mail und Passwort oder das gewählte zusätzliche Authentifizierungsverfahren korrekt waren, wird ihm ein erfolgreicher Login. Nur wenn alle Schritte der Authentifizierung korrekt waren, gelangt er in sein Konto von SSN. Andernfalls gelangt er in ein täuschen echt aussehendes, zufällig generiertes Fake Konto von SSN. Der Funktionsumfang des Fake Kontos unterscheidet sich nicht von dem eines echten Kontos. Nur der Inhaber des echten Kontos ist in der Lage das Fake Konto als solches zu entlarven. Durch die Nutzung des Fake Kontos soll kein Schaden für die echten Nutzer entstehen. Gepostete Beiträge und versendete Nachrichten werden lediglich angezeigt, jedoch nicht wirklich versendet.

