Parallel World

Daniel Graf
Hochschule Mnchen
Mnchen
graf12@hm.edu

Ludwig Wagner
Hochschule Mnchen
Mnchen
wagner43@hm.edu

Dimitrie Diez
Hochschule Mnchen
Mnchen
diez@hm.edu

ABSTRACT

EINLITUNG

Einleitung mit einer Statistik über Angriffe und Sicherheitslücken aktueller Social Media Plattformen, Identifikation des Problems bei aktuellen Authentifizierungsverfahren (Der Angreifer weiss, dass Login fehlgeschlagen ist)

WEITERFHRENDE LITERATUR

BESCHREIBUNG DES KONZEPTS

Kernpunkt des Konzept ist die Erschaffung eines parallelen Fake-Netzwerkes. Dadurch soll verhindert werden, dass ein Angreifer in das Netzwerk gelangt oder Informationen über die Mitglieder des Netzwerkes gewinnen kann. Im folgenden wird der Aufbau des Netzwerkes anhand eines Login-Vorgangs beschrieben.
Auf der Startseite des Netzwerkes werden die Nutzer zunächst aufgefordert E-Mail Adresse und Passwort einzugeben, bevor sie zum zweiten Schritt der Authentifizierung gelangen. Hierfür muss jeder Nutzer bei der Registrierung eines, oder mehrere Authentifizierungsverfahren hinterlegen. Zur Auswahl stehen einen Authentifizierung mittels eines Codes, welcher per SMS zugesandt wird, mittels Push-Benachrichtigung am Mobiltelefon oder mittels biometrischer Daten. Unabhängig davon, ob E-Mail Adresse, Passwort, die Wahl des Verfahrens oder die Durchführung des Verfahrens korrekt waren, gelangt der Nutzer in das Netzwerk. Doch nur im Falle eines vollständig korrekten Vorgangs befindet sich der Nutzer in seinem Account im ëchten"Netzwerk. Andernfalls gelangt der Nutzer in ein täuschend echt aussehendes Fake-Profil, welches nur vom Inhaber als solches enttarnt werden kann. Der Angreifer erfährt dadurch weder ob seine eingegebenen Angaben korrekt waren bzw. welche nicht korrekt waren, noch kann er sich sicher sein, ob er im echten Netzwerk ist. Sämtliche, für ihn sichtbaren Informationen sind folglich nicht verifizierbar und daher nahezu wertlos.
Die größte Herausforderung bei der Umsetzung des Konzeptes stellt die Generierung des Fake-Netzwerkes dar. Hierfür wurden 4 unterschiedliche Umsetzungsvarianten definiert, welche im Folgenden beschrieben werden.
In der ersten Variante, muss jeder Nutzer bei der Registrierung neben seinem echten Profil auch ein Fake Profil anlegen. Welche Informationen er hierfür verwendet, ist ihm überlassen.

In der zweiten Variante erstellt der Nutzer lediglich sein echtes Profil. Er kann jedoch für jede Information, beispielsweise dem Namen, seinem Alter oder dem Profilbild durch setzen eines Hakens entscheiden, ob diese Information für die Erstellung des Fake-Profils verwendet werden darf, oder nicht. Restliche Daten werden durch das System zufällig generiert. BILD
In der dritten Variante werden alle Fake-Profile automatisch generiert. Die Nutzer können den Prozess hierbei nicht beeinflussen. BILD
In der vierten Variante werden die Fake-Profile, analog zu Variante 3 automatisch generiert. Hierbei wird der Nutzer jedoch aufgefordert Bilder für die Fake-Profil Generierung zur Verfügung zu stellen. Dadurch soll erreicht werden, dass die Fake-Profile für einen Angreifer authentischer Wirken. BILD

METHODIK

Fokusgruppe

Aufbau der Umfrage, des Experimentes...

Einzelbefragungen

Aufbau der Umfrage, des Experimentes...

Ergebnisse

auch das Mindmap reinnehmen... Oder CLusterbildung... usw.

Diskussion der Herausforderungen bei der Umsetzung des Konzepts

Ergebnisse von Fokusgruppe + Einzelbefragungen, Diskussion der wichtigsten Aspekte

Handlungsempfehlungen

Lösungsansätze der vorher beschriebenen Probleme vorstellen. + Diskussion der Umsetzbarkeit

Speichern des Logins

Mechanismen, die es erlauben Logins temporär zu speichern sind State of The Art. Diese Mechanismen müssen auch bei diesem Konzept angewendet werden um eine akzeptable Usability zu gewährleisten.

Integration in ein bestehendes Sozial Network statt Entwicklung eines neuen
Da Nutzer sich nicht wegen dem Sicherheitskonzept in einem Netzwerk registrieren, sondern wegen Kontakten soll das Konzept in ein bestehendes Netzwerk integriert werden und kein neues Netzwerk entwickelt werden.

Klare Erluterung des Sicherheitskonzeptes
Durch attraktiv gestaltete Grafiken, Illustrationen, Videos oder Tutorials muss der Benutzer in kurzer Zeit über die Vorteile des Konzepts informiert werden.

Automatische und manuelle Fakeprofil Erstellung
Die Fakeprofil Erstellung muss automatisiert erfolgen. Den Nutzern muss die Möglichkeit gegeben werden Daten für die Generierung des Fake Profils zur Verfügung zu stellen. Den Nutzern muss bewusst gemacht werden, dass die Fake Profile durch die Angaben persönlicher (echter) Daten authentischer wirken.

Umgang mit Passwortverlust
Das Zurücksetzen des Passworts muss möglich sein.

Auswahl unterschiedlicher Verfahren fr die 2-Wege Authentifizierung
Dem Nutzer muss eine große Anzahl an hinterlegbaren Authentifizierungsmechanismen zur Auswahl gestellt werden

Kommunikation im Netzwerk
Die Kommunikation mit Fake Profilen muss möglich sein. Das suchen von Profilen muss möglich sein. Aus Fake Profilen müssen alle Aktionen möglich sein, die auch mit echten Profilen getätigt werden können.

ZUSAMMENFASSUNG UND FAZIT

Was wurde gemacht, Handslungsempf zusammenfassen.. Die Wichtigsten erläutern

AUSBLICK