Secure Social Network - Parallel World

Daniel Graf
Hochschule München
München
graf12@hm.edu

Ludwig Wagner
Hochschule München
München
wagner43@hm.edu

Dimitrie Diez
Hochschule München
München
diez@hm.edu

ABSTRACT

In der heutigen Zeit existieren zahlreiche unterschiedliche Authentifizierungsverfahren, die den Menschen vertraut sind. Der Mensch nutzt heute verschiedene Plattformen und Devices um Informationen aufzubewahren oder mit anderen Personen zu teilen. Der Zugang zu diesen Daten muss durch Authentifizierungsverfahren bestmöglich geschützt werden. Die am häufigsten verwendete Methode ist E-Mail Adresse und Passwort.[11]

Bei zahlreichen Onlineplattformen, wie beispielsweise Yahoo, SchülerVZ oder Sony wurden Millionen Kundendatensätze gestohlen und im Darknet veröffentlicht.[3]

In diesen Fällen fehlen Angreifern lediglich die Passwörter um in die Accounts zu gelangen. Diese versuchen Angreifer häufig durch Brute-Force Angriffe zu ermitteln.[6]

Der Erfolg dieser Methode basiert darauf, dass der Angreifer bei fehlerhaften Login Informationen informiert wird. Um dies zu verhindern wurde ein Konzept für einen Authentifizierungsvorgang entwickelt, bei dem der Angreifer genau diese Informationen nicht erhält. Das Konzept wurde für Soziale Netzwerke ausgelegt, ist jedoch vielseitig, beispielsweise auch für E-Mail Accounts, verwendbar. Bei einem fehlgeschlagenen Authentifizierungsvorgang wird ein erfolgreicher Login durch die Anzeige eines möglichst realen Fake-Kontos vorgetäuscht.

Um das Konzept zu bewerten und zu verfeinern, wurde eine Gruppenbefragung durchgeführt und mit Hilfe der gewonnenen Erkenntnisse ein Schema für Einzelbefragungen erarbeitet. Aus den anschließenden Einzelbefragungen ging hervor, welche Punkte bei der Umsetzung zu beachten sind, um eine gute Akzeptanz der Benutzer zu erreichen. Es hat sich ergeben, dass es wichtig ist, den Fokus auf Benutzerfreundlichkeit zu legen, um diese Akzeptanz zu erreichen.

Darauf basierend wurden für die Umsetzung des Konzepts verschiedene Handlungsempfehlungen erarbeitet und limitierende Faktoren aufgezeigt. Anschließend erfolgt eine Bewertung des Konzepts hinsichtlich Sicherheit, Umsetzbarkeit und Benutzbarkeit.

EINLEITUNG

In der Vergangenheit wurden häufig schwerwiegende Sicherheitslücken auf verschiedenen Online Plattformen für soziale Medien genutzt, um private Daten der Benutzer abzugreifen und die Accounts zur massiven Verbreitung von Werbung zu nutzen. Durch die steigende Aktivität der Hackerszene kam es in den letzten Jahren fortlaufend zu einem Anstieg der Cyberkriminalität. [4]

Trotz dieser Tatsachen machen sich nur wenige Benutzer Gedanken über den Schutz ihres Accounts. [9] Viele Benutzer sind gar nicht erst bereit, zusätzlichen Aufwand zu betreiben, um einen besseren Schutz der Benutzerkonten zu erreichen. Selbst wenn erweiterte Schutzmethoden wie z.B. Two-Factor-Authenfication zur Verfügung stehen, werden diese meist nur von wenigen Nutzern aktiv genutzt. [5] Der Nutzungskomfort eines einfachen Logins steht im Vordergrund. Dies zeigt, dass es vor allem in der Verantwortung der Betreiber von Plattformen liegt, neue Authentifizierungsverfahren zu entwickeln, die ohne störenden Mehraufwand einen besseren Schutz gewährleisten.

Der größte Angriffspunkt eines regulären Logins besteht darin, dass der Angreifer darüber informiert wird, wenn der Login fehlgeschlagen ist. So lässt sich der Login mit verschiedenen Passwörtern wiederholen, bis das richtige Passwort erraten wurde. Durch den von den Nutzern geschätzten Komfort, werden meist einfache Passwörter gewählt, die durch einen Brute-Force Angriff schnell erraten werden können. [9]

Um nun die Sicherheit von sozialen Netzwerken zu erhöhen, ohne den Nutzer mit einem Mehraufwand zu belasten, muss genau an dieser Stelle ein neues Konzept erarbeitet werden.

SACHVERWANDTE ARBEITEN

Das Thema wurde bereits in mehreren Arbeiten unterschiedlicher Autoren untersucht und behandelt. Viele Arbeiten zeigen dabei, dass die Sicherheit durch einen Login mit Benutzername und Passwort nicht ausreichend ist. [2] [12]

Infolge dessen wurde von ebenso vielen Autoren auf vielseitige Art und Weise untersucht, wie sich die Sicherheit verbessern lässt. Dabei wird der Fokus in den meisten Arbeiten auf alternative oder erweiterte Mechanismen

zur Authentifizierung der Benutzer gelegt. Die Benutzerfreundlichkeit gerät dabei oft in den Hintergrund. [8] [1] [7]

Diese Arbeit setzt an einer anderen Stelle an und nimmt es sich zum Ziel, einen idealen Mittelweg zwischen minimalem Mehraufwand und maximaler Sicherheit zu erreichen. Die gewohnte Benutzerfreundlichkeit wird durch die Nutzung der gewohnten Login Mechanismen sichergestellt, während die Sicherheit durch Verwirrung möglicher Angreifer erzielt wird.

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. Die Sicherheit wird somit durch Verwirrung erzeugt. 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 beispielsweise ein Code, welcher per SMS zugesandt wird, eine Push-Benachrichtigung am Mobiltelefon oder die Verwendung biometrischer Daten (z.B Fingerabdruck).
Unabhängig davon, ob E-Mail Adresse, Passwort, die Wahl des zusätzlichen Verfahrens oder die Durchführung des gewählten Verfahrens korrekt waren, gelangt der Nutzer in das Netzwerk. Doch nur im Falle eines vollständig korrekten Authentifizierungsvorgangs befindet sich der Nutzer in seinem Account im „echten“Netzwerk. Andernfalls gelangt der Nutzer in ein täuschend echt aussehendes Fake-Profil, welches nur vom Inhaber als solches enttarnt werden kann. Der Login Vorgang ist in Abbildung 1 aufgeführt. Der Angreifer erfährt dadurch weder ob seine

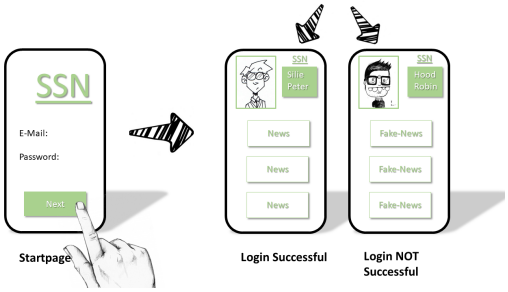

Figure 1. Login Vorgang

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. Ob er hierbei korrekte oder falsche Angaben macht kann jeder Nutzer selbst entscheiden. Abbildung 2 zeigt ein Beispiel hierfür. Ziel dieser Variante ist es, mög-

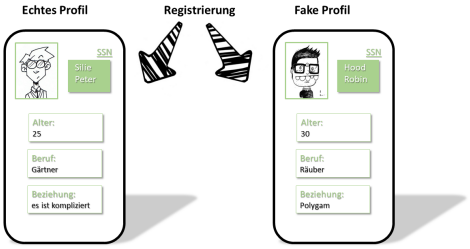

Figure 2. User legt das Fake-Profil selbst an

lichst authentische Fake-Profile zu erstellen. Je authentischer diese auf einen Angreifer wirken, desto sicherer sind die ëchten”Daten der Nutzer.
In der zweiten Variante erstellt der Nutzer lediglich sein echtes Profil. Er kann jedoch für jede Information, beispielsweise bei seinem Namen, seinem Alter oder seinem 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. Abbildung 3 veranschaulicht diese Variante. Dadurch sollen durch die Zusatzangaben

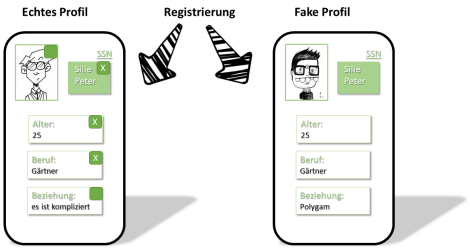

Figure 3. Vom User ausgewählte Informationen werden für die Fake-Profile verwendet.

einerseits authentische Fake-Profile erzeugt werden können und andererseits der zeitliche Aufwand für die Nutzer reduziert werden.
In Variante 3 verläuft der gesamte Vorgang automatisiert. Der User hat keinen Einfluss auf die Erstellung der Fake-Profile. Sie werden vom System im Hintergrund generiert. Der Ablauf ist in Abbildung 4 dargestellt.
Variante 4 stellt eine Kombination aus den bisherigen drei Varianten dar. Die Fake-Profile werden, analog zu Variante 3 automatisch generiert. Es besteht jedoch für jeden Nutzer die Möglichkeit Daten, wie beispielsweise Bilder für die Fake-Profil Generierung zur Verfügung zu stellen. Somit ist einerseits kein Nutzer gezwungen Daten bereit zu stellen, andererseits können authentischere

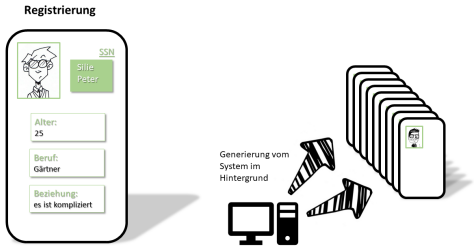

Figure 4. Fake-Profile werden vom System generiert.

Fake-Profile als z.B bei Variante 3 generiert werden. Eine Veranschaulichung dieser Umsetzungsvariante ist am Beispiel von Profilbildern in Abbildung 5 aufgeführt.

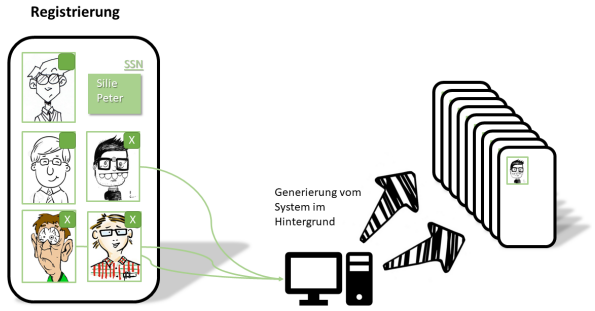

Figure 5. Fake-Profile werden vom System generiert. Der User kann freiwillig Daten zur Verfügung stellen.

METHODIK

Für eine Diskussion, welche der Varianten bei Nutzern bevorzugt werden könnte und bei welchen Teilaspekten des Konzepts es möglicherweise Probleme bei der Umsetzung geben könnte, wurde eine Fokusgruppe organisiert. Basierend auf den Ergebnissen der Fokusgruppe wurden interessante Aspekte im Zuge einer Umfrage qualitativ vertieft. Sowohl für die Fokugruppe, als auch für die Umfrage wurden ausschließlich Personen in Betracht gezogen, welche mindestens ein soziales Netzwerk aktiv nutzen. Dadurch soll eine erhöhte Vergleichbarkeit zwischen dem Sicherheitskonzept herkömmlicher Netzwerke und dem im vorherigen Kapitel beschriebenen Konzept erzielt werden. In diesem Kapitel werden zunächst der Aufbau der Fokusgruppe und der Einzelbefragungen erläutert. Anschließend werden die Ergebnisse von beiden zusammengefasst. Basierend darauf erfolgt eine Diskussion potenzieller Herausforderungen bei der Umsetzung des Konzepts. Abschließend werden konkrete Handlungsempfehlungen für die Umsetzung beschrieben.

Fokusgruppe

Die Fokusgruppe bestand aus dem Projekt Team und 8 Studenten der Hochschule München. Zu Beginn der Fokusgruppe wurden den Teilnehmern allgemeine Fragen zu sozialen Netzwerken gestellt und über potenzielle Schwachstellen bzgl. Sicherheit in vorhandenen Netzwerken diskutiert. Im zweiten Schritt erfolgte die Erläuterung der Konzeptidee und eine anschließende Diskussion bzgl. Machbarkeit, Usability und Sicherheit. Anschließend wurden den Teilnehmern stufenweise alle 4 Umsetzungsvarianten erläutert. Nach jeder Variante erfolgte erneut eine (kurze) Diskussion bezüglich der Machbarkeit, Usability und Sicherheit der jeweiligen Variante. Abschließend erfolgte eine freie Diskussion über die nicht berücksichtigten Aspekte und es wurden weitere Umsetzungsideen erfragt.

Einzelbefragungen

Insbesondere Aspekte, bei denen es mehrere, unterschiedliche Meinungen zwischen den Teilnehmern der Fokusgruppe gegeben hat, wurden im Zuge von Einzelbefragungen vertieft. Hierfür wurden insgesamt 9 Befragungen durchgeführt. Der gesamte Fragebogen ist im Anhang in Abbildung 8 angefügt.

Ergebnisse

In Abbildung 6 ist ein Ausschnitt aus den Ergebnissen der Fokusgruppe und der anschließenden Einzelbefragungen zu sehen. Die gesamten Ergebnisse sind in einem Mind-Map geclustert im Anhang aufgeführt. Die wichtigsten Aspekte sind im folgenden genauer beschrieben.

1. Für die Usability des Netzwerkes ist es essenziell zu definieren, wann eine Authentifizierung des Nutzers erforderlich ist. Beispielsweise bei wiederholtem Login vom gleichen Gerät sagen die Teilnehmer von Fokusgruppe und Umfrage einstimmig, darf keine erneute Authentifizierung gefordert werden.

2. Viele Teilnehmer sehen nicht das Sicherheitskonzept als ausschlaggebend für die Entscheidung, ob sie sich in einem Netzwerk registrieren würden. Andere Aspekte, wie Bekanntheit des Netzwerkes und Anzahl der registrierten Personen, insbesondere der jeweiligen Freunde, wird bei der Wahl eines Netzwerkes als bedeutend wichtiger angesehen.

3. Der tiefere Sinn dieses Sicherheitskonzeptes ist insbesondere für Personen ohne technische Kenntnisse meist nicht zu verstehen. Folglich wird nur der Mehraufwand bei der Registrierung oder beim Login in das Netzwerk betrachtet. Die Mehrheit der Personen ohne technischen Hintergrund empfanden folglich den Mehraufwand als unnötig. Für die Mehrheit der Personen mit technischem Hintergrund war der Sinn und Zweck des Konzeptes offensichtlich. Diese wären auch mehrheitlich bereit einen gewissen Mehraufwand für eine erhöhte Sicherheit in Kauf zu nehmen. Andererseits beurteilte die Mehrheit der Teilnehmer, unabhängig vom technischen Hintergrund, die Sicherheit bestehender sozialer Netzwerke als nicht ausreichend.

4. Viele Teilnehmer gaben an, dass sie nicht bereit wären Daten für die Erstellung von Fake-Profilen zur Verfügung zu stellen. Darüber hinaus wären auch nur wenige Teilnehmer bereit Zeit für die Erstellung und

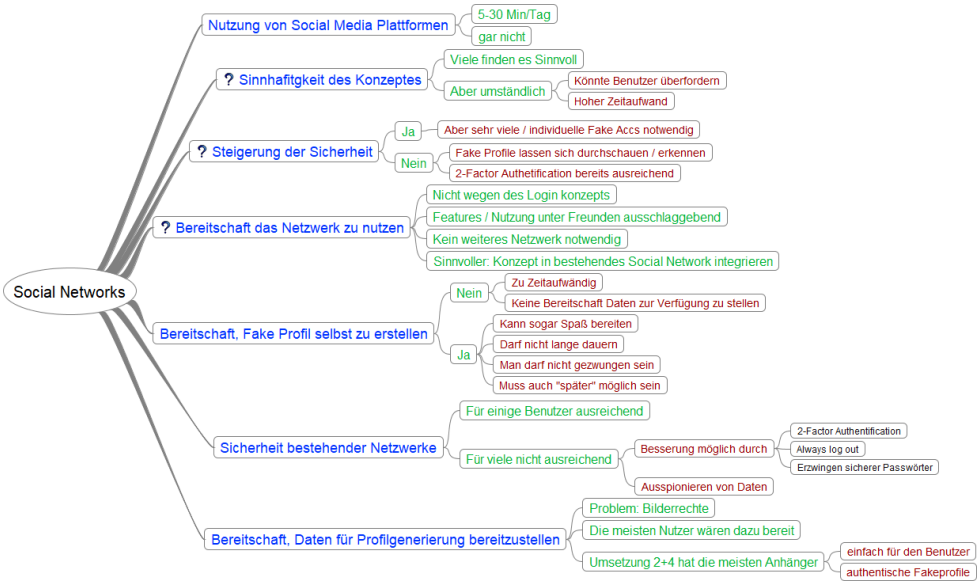

Figure 6. Ausschnitt aus den Ergebnissen von Fokusgruppe und Einzelbefragung

Verwaltung von Fake-Profilen zu investieren. Ca. 20% der Teilnehmer wären weder bereit Daten bereit zu stellen, noch Zeit für die Erstellung der Fake-Profile zu investieren.

5. Die Mehrheit der Teilnehmer von Fokusgruppe und Umfrage sehen das Zurücksetzen des Logins in das Netzwerk bei Verlust von Login Daten kritisch. Ermöglicht man die Zurücksetzung über eine E-Mail, wird der sicherere Login in das Netzwerk durch eine „einfache“Authentifizierung mittels E-Mail und Passwort ausgehebelt.

6. Generell sahen die Teilnehmer eine Zwei-Wege Authentifizierung über ein Gerät, in der Regel das Mobiltelefon, als unzureichend. Die Sicherheitsvorkehrungen würde in diesem Fall aufgehoben, sobald ein Angreifer Zugang zum Gerät bekommt.

7. Insbesondere der Umgang mit den Fake-Profilen führte zu vielen Fragen und Diskussionen. Diese werden im folgenden Kapitel näher erläutert.

Diskussion der Herausforderungen bei der Umsetzung des Konzepts

Neben den erläuterten Ergebnissen müssen für die Umsetzung des Konzepts auch einige Anmerkungen einzelner Teilnehmer diskutiert werden. In die Diskussion wurden ergänzend auch eigene Lösungsideen und potenziell kritische Punkte eingearbeitet.

1. Eine große Herausforderung bei der Umsetzung ist die Generierung der Fake-Profile. Einerseits wirken diese authentischer, wenn Mitglieder des Netzwerkes Daten hierfür bereit stellen. Andererseits ist nicht jedes Mitglied bereit Daten bereitzustellen sodass eine Generierung der Fake-Profile ermöglicht werden muss. Darüber hinaus ist es für eine wirkliche Verwirrung des Angreifers durch die sog. ”Parallel World”nicht ausreichend, wenn es pro echtes Profil lediglich ein Fake-Profil gibt (statische Generierung bei Registrierung des Teilnehmers). Versucht ein Angreifer beispielsweise das Passwort für ein Konto zu erraten, muss er pro falsches Passwort in einem anderen Fake-Profil landen. Andernfalls kann ein Fake-Profil zu schnell als solches identifiziert werden. Das Sicherheitskonzept funktioniert nur, wenn ein Angreifer keine Möglichkeit hat zwischen einem echten und einem Fake-Profil zu unterscheiden. Es müssen folglich für jedes Profil alle falsch eingegebenen Passwörter (und ggf. weitere Authentifizierungsverfahren wie z.B falsche Codes) gespeichert und mit einem jeweils erstelltem Fake-Profil verknüpft werden (dynamische Generierung bei Bedarf).

2. Die Lösung der im vorherigen Punkt beschriebenen Herausforderung führt zu einem weiteren Problem. Gerade durch die Vielzahl möglicher Fake-Profile pro echtes Profil, muss eine große Menge Daten gespeichert werden. Dies führt zu einem enormen Bedarf an Speicherkapazität und Rechenleistung, was wiederum einen Anstieg der Kosten für den Betrieb eines solchen Netzwerkes bedeutet. In diesem Zusammenhang wäre ein möglicher Angriffsvektor, dass ein Angreifer versucht das System zu überlasten.

3. Es muss ins Detail definiert werden, welche Funktionalitäten den echten und den Fake-Profile zur Verfügung stehen. Eine Kommunikation zwischen Fake-Profilen, sowie zwischen Fake- und echten Profilen muss aus Gründen der Tarnung möglich sein. Dies stellt jedoch eine Gefahr dar, da mittels des Fake-Profils z.B Nachrichten mit Links zu schadhaften Seiten versendet werden können.
Andererseits muss sicher gestellt sein, dass jeder Nutzer aus seinem echten Profil auch die echten Profile

seiner Kontakte finden kann. Werden aus einem Fake-Profil Nachrichten versendet, müssen diese ebenso wie erstellte oder angezeigte Statusnachrichten oder Bilder im entsprechenden Fake-Profil gespeichert werden. Gelangt man zu einem späteren Zeitpunkt erneut in das Fake-Profil, kann dieses ansonsten enttarnt werden. Es ist jedoch essenziell, dass der Zugriff auf persönliche Daten eines (echten) Profils aus einem Fake-Profil unterbunden wird.

4. Es ist zu definieren, ob Fake-Profile mittels Suchmaschinen gefunden werden könnte. Beispielsweise kann nahezu jedes Profil im Netzwerk Facebook seit dem Jahr 2007 mittels google gefunden werden [10]. Findet man jedoch lediglich echte Profile, können Fake-Profile auf diese Weise enttarnt werden. Eine mögliche und umsetzbare Lösung hierfür wäre, wenn jedes Fake-Profil alle öffentliche Informationen eines echten Profils verwendet. Sucht man nun nach dem Profil, ist es ausreichend wenn die öffentlichen Daten des echten Profils angezeigt werden. Da lediglich die öffentlichen Daten sichtbar sind, kann folglich nicht zwischen einem Fake- und einem echten Profil unterschieden werden.

5. Eine identifizierte Schwachstelle des Netzwerkes sind Personen, die das Mitglied (gut) kennen. Je besser jemand ein Mitglied des Netzwerkes kennt, desto einfacher ist es für diese Person ein potenzielles Fake-Profil dieses Mitglieds zu enttarnen. Grund hierfür ist, dass die Person möglicherweise Freunde, Bekannte oder Familienmitglieder des Mitgliedes kennt. Befindet sich die Person nun in einem potenziellen Fake-Profil in welchem sich keinerlei Nachrichten oder Bilder von besagten Personen befinden, kann dieses als Fake-Profil enttarnt werden. Eine direkte Lösung für diese Problematik konnte nicht identifiziert werden.

Handlungsempfehlungen

Aus den Ergebnissen der Fokusgruppe, der Einzelbefragungen sowie der diskutierten Aspekte werden nun Handlungsempfehlungen für die Umsetzung des Konzepts herausgearbeitet.

Speichern des Logins

Viele Teilnehmer sind nicht bereit viel Zeit in den Authentifizierungsprozess zu investieren. Mechanismen, die es erlauben Logins temporär zu speichern sind Stand der Technik. Diese Mechanismen müssen auch bei diesem Konzept angewendet werden um eine akzeptable Usability zu gewährleisten.

Integration in ein bestehendes Soziales Netzwerk

Da Nutzer sich nicht allein wegen dem Sicherheitskonzept in einem Netzwerk registrieren, sondern wegen den bereits registrierten Kontakten, ist es sinnvoll das Konzept in ein bereits bestehendes Netzwerk zu integrieren und kein neues Netzwerk zu entwickeln.

Klare Erläuterung des Sicherheitskonzeptes

Durch attraktiv gestaltete Grafiken, Illustrationen, Videos und Anleitungen muss der Benutzer in kurzer Zeit über die Vorteile des Konzepts informiert werden. Auch Personen ohne technische Kenntnisse müssen sowohl den Sinn des Konzeptes verstehen, als auch die Bedienung des Netzwerks beherrschen.

Automatische und manuelle Fake-Profil Erstellung

Die Fake-Profil 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. Der Mehraufwand für den Nutzer muss jedoch minimiert werden.

Umgang mit Verlust von Login-Informationen

Es muss sichergestellt werden, dass auch ein Nutzer, welcher die Login-Informationen verliert, wieder Zugang zu seinem Profil erlangen kann. Zum Beispiel muss das Zurücksetzen des Passworts möglich sein.

Verfahren für die Zwei-Wege-Authentifizierung

Dem Nutzer muss eine große Anzahl an hinterlegbaren Authentifizierungsmechanismen zur Auswahl gestellt werden. Zum einen steigert es die Sicherheit, da es für den Angreifer schwerer zu erraten ist, welche Methode die richtige ist. Zum anderen erhöht dies die Usability für den Nutzer, da ihm mehr Auswahlmöglichkeiten zur Verfügung stehen.

Authentische Fake-Profile

Die Erstellung von möglichst authentischen Fake-Profilen ist der Kernpunkt des Konzeptes. Sowohl die Kommunikation mit Fake-Profilen, als auch das Suchen von Profilen im Netzwerk muss möglich sein. Fake-Profilen müssen die gleichen Funktionalitäten zur Verfügung stehen, die auch echten Profilen zur Verfügung stehen.

ZUSAMMENFASSUNG UND FAZIT

Diese Arbeit beschäftigt sich mit der Umsetzung des Konzeptes aus der Sicht des Nutzers. Zusammenfassend lässt sich sagen, dass zwei wichtige Aspekte für die erfolgreiche Umsetzung dieses Konzeptes zu beachten sind. Zum einen ist eine möglichst einfache Einrichtung und Benutzung des Netzwerks durch den Nutzer essentiell. Dabei sollte der Nutzer möglichst keinen Einfluss den Sicherheitsmechanismus selbst haben. Ihm soll jedoch die Möglichkeit gegeben werden, durch eine freiwillige Bereitstellung von Daten zum Sicherheitskonzept beizutragen. Dadurch soll die Usability sichergestellt und gleichzeitig eine mögliche Fehleinrichtung durch den Nutzer verhindert werden. Die gewohnten Funktionen wie das Verschicken von Nachrichten oder das Teilen von Bildern dürfen durch das neue Konzept nicht eingeschränkt werden.

Dem gegenüber steht die Generierung von Fake-Profilen. Der Erfolg dieses Konzeptes hängt maßgeblich von der Generierung von möglichst authentischen Profilen ab. Die echte Welt und die Parallelwelt sind keine eigenständigen Konstrukte, sondern müssen mit einander kommunizieren. So können sich zum Beispiel die echten Profile und

die dazugehörigen Fake-Profile die öffentlichen Daten teilen. Dabei müssen klare Schnittstellen zwischen echter und Parallelwelt geschaffen werden. Letztendlich lässt sich sagen, dass dieses Konzept in bereits bestehende Netzwerke integriert werden muss. Es hat sich gezeigt, dass Nutzer nicht bereit wären sich nur wegen diesem Sicherheitskonzept in einem Netzwerk zu registrieren.

AUSBLICK

Die Arbeit hat bei der Betrachtung des Konzeptes den Fokus auf den Nutzer gelegt. Es müssen jedoch noch weitere Aspekte für die Umsetzung des Konzepts betrachtet werden. Insbesondere das Angreifermodell muss genauer analysiert werden. Dabei gilt es zu betrachten, ob das Konzept robust gegen bereits bekannte Angriffsszenarien ist. Darüber hinaus ist es notwendig zu untersuchen, ob dieses Konzept neue Angriffsszenarien eröffnet. So könnte ein neues Angriffszenario beispielsweise darin bestehen, durch die mutwillige Erzeugung von zahllosen Fake-Profilen das Netzwerk zu überlasten.

Viele Fragen stellen sich jedoch erst während der technischen Umsetzung des Konzeptes. Hierfür ist es notwendig einen Prototypen zu erstellen. Die ausgearbeiteten Angriffsmodelle sowie die Usability müssen dann an diesem Prototypen getestet und im Zuge weiterer Studien analysiert und verifiziert werden.

Ein solcher Prototyp kann Probleme bei der Umsetzung aufzeigen und limitierende Faktoren definieren. Darüber hinaus kann dadurch bewertet werden, welche Teilkonzepte am erfolgversprechendsten und welche nicht machbar sind.

REFERENCES

1. Ruhul Amin, S Rajkumar, and Rahul Kumar. 2017. Security on "Secure Remote Login Scheme with Password and Smart Card Update Facilities". In Mathematics and Computing: Third International Conference, ICMC 2017, Haldia, India, January 17-21, 2017, Proceedings, Vol. 655. Springer, 26.
2. Michael Bachmann. 2014. Passwords are Dead Alternative Authentication Methods. IEEE, The Hague, Netherlands.
3. Tom Berchem. 2016. 200 Millionen Yahoo Nutzer-Daten im Darknet. (2016). https://blog.botfrei.de/2016/08/200-millionen-yahoo-nutzer-daten-im-darknet/.
4. BKA. 2017. Bundeslagebilder Cybercrime. (2017). https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.
5. Russell Brandom. 2017. Two-factor authentication is a mess. (2017). https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess.
6. Esheridan. 2006. Blocking Brute Force Attacks. (2006). https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks.
7. Stanislaw Jarecki, Hugo Krawczyk, Maliheh Shirvanian, and Nitesh Saxena. 2018. Two-Factor Authentication with End-to-End Password Security. In International Conference on Practice and Theory of Public Key Cryptography (PKC).
8. Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. 2015. Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound.. In USENIX Security Symposium. 483–498.
9. Annika Kremer. 2017. Passwort-Sicherheit: Viel Raum für Verbesserungen. (2017). http://www.netzpiloten.de/passwort-sicherheit-verbesserungen/.
10. Stefan Schultz. 2007. Facebook wird googlebar. (2007). http://www.spiegel.de/netzwelt/web/strategiewechsel-facebook-wird-googlebar-a-504169.html.
11. Deb Shinder. 2001. Understanding and selecting authentication methods. (2001). https://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/.
12. Viktor Taneski, Marjan Hericko, and Bostjan Brumen. 2014. Password security—No change in 35 years?. In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on. IEEE, 1360–1365.

ANHANG

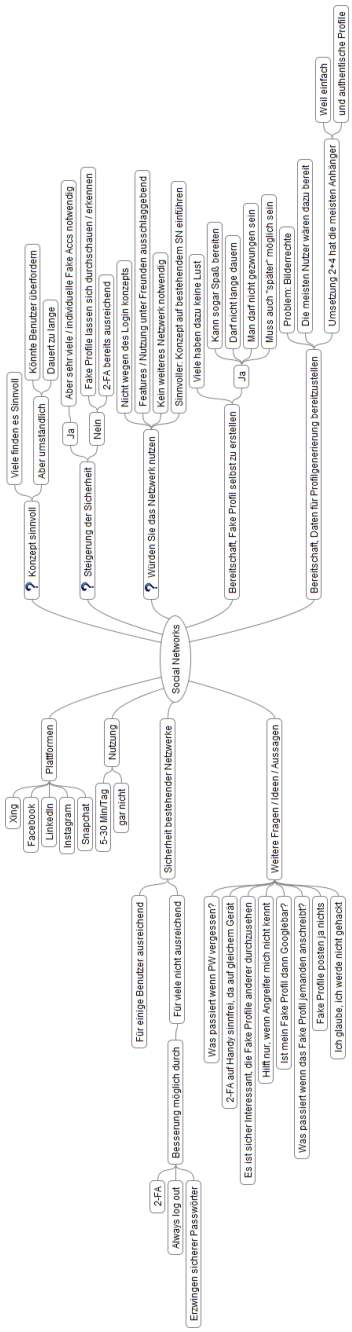

Figure 7. Ergebnisse der Fokusgruppe und der Einzelbefragung

Fragen für Umfrage:

1) Welche Social Media Plattformen nutzen Sie?
2) Falls Sie eine Social Media Plattform nutzen: Wie viel Zeit verbringen Sie dort durchschnittlich?
3) Falls Sie eine Social Media Plattform nutzen: Finden Sie die Sicherheit dort ausreichend?
4) Was könnte man an der Sicherheit der Plattform noch verbessern?

An dieser Stelle wird unser Konzept erklärt

5) Finden Sie das Konzept intuitiv?
6) Glauben Sie dieses Konzept steigert die Sicherheit Ihres Kontos?
7) Würden Sie sich in solch einem Netzwerk registrieren?
8) Wären Sie grundsätzlich bereit neben der normalen Registrierung auch ein Fake Profil anzulegen?
9) Wie viel Zeit wären Sie bereit in die Registrierung in das Netzwerk und in die Erstellung des Fake Kontos zu investieren?

Figure 8. Aufbau des Fragebogens für die Einzelbefragungen