

Datenschutz in Sozialen Netzwerken: Freund oder Feind?

Dominik Birk
dominik@code-foundation.de
Felix Gröbert
felix@groebert.org
Christoph Wegener
christoph.wegener@rub.de

Abstract: Profile im Internet haben in der heutigen Zeit einen wichtigen Stellenwert eingenommen, um eine Identität online zu repräsentieren und erfreuen sich nicht zuletzt deswegen immer größerer Beliebtheit - die allgemeine Beteiligung an sozialen Netzwerken hat in den letzten Jahren drastisch zugenommen. Dies führt unter anderem dazu, dass auch soziale Netzwerke und deren Profile zur Zielscheibe von Internetkriminellen geworden sind. Dieser Beitrag diskutiert die allgemeine Problematik, persönliche Daten in sozialen Netzwerken zu veröffentlichen und versucht Funktionen zu definieren, die von Angreifern genutzt werden könnten, um raffinierten Identitätsdiebstahl zu betreiben. Es werden Hinweise auf Gegenmaßnahmen seitens der Anwender und Betreiber entsprechender Plattformen gegeben und eine Funktion zur Messung der Kritikalität einer Identität im Internet diskutiert. Zudem stellen wir eine Methode vor, wie Behörden und Datenschutzzentren Nutzer im Internet auf das mögliche Missbrauchspotential aufmerksam machen könnten und so Nutzer zu mehr Datensparsamkeit motivieren könnten.

1 Einführung

Die Jahre 2003 und 2004 waren der Beginn moderner sozialer Netzwerke und deren breiten, weltweiten Akzeptanz durch die Internetgemeinschaft. Generell ist dabei zunächst einmal festzustellen, dass ein soziales Netzwerk im Internet auch als eine Struktur aus Knoten und Kanten angesehen werden kann, in der die Knoten Individuen repräsentieren und die Kanten die Relationen zwischen diesen Individuen abbilden. Darauf aufbauend ist die Soziale-Netzwerk-Analyse (SNA) eine Methode zur Verhaltensanalyse innerhalb sozialer Netzwerke. Sie beschäftigt sich mit Beziehungen zwischen Entitäten eines sozialen Netzwerks und wird weitläufig im Bereich der Sozial-, Verhaltens- und Wirtschaftsforschung genutzt.

Allerdings können SNA-Methoden auch von Angreifern genutzt werden, um Informationen über Nutzer sozialer Netzwerke zu beziehen. Unvollständige Datensätze könnten mit Hilfe mathematischer Funktionen ergänzt werden und so den raffinierten Identitätsdiebstahl¹ ermöglichen.

¹Spear Phishing, vgl. <http://www.microsoft.com/protect/yourself/phishing/spear.mspx>

Laut einer Studie [1] wird die Bekämpfung von Identitätsdiebstahl eines der Hauptanliegen in der Zukunft sein: Im Jahr 2007 führten Phishing-Angriffe allein in den USA zu einem Verlust von 3 Milliarden US\$.

In diesem Beitrag werden wir den aktuellen Stand der Diskussion darstellen und anschließend die mathematischen Grundlagen sozialer Netzwerke behandeln. Dabei werden wir die verschiedenen Phasen eines ausgeklügelten Angriffs auf Identitäten sozialer Netzwerke aufzeigen. Des Weiteren werden wir vorstellen, wie die Kritikalität der vom Nutzer in sozialen Netzwerken veröffentlichten Eigenschaften bezüglich der gezeigten Angriffe gemessen werden kann.

2 Verwandte Arbeiten

Jakobsson et al. [2] untersuchten bereits 2005 das Konzept vom sogenannten *Social Phishing* und diskutierten Möglichkeiten, wie Phisher die Profile sozialer Netzwerke ausnutzen könnten, um ihre Opfer auf Phishing-Webseiten zu locken. Das Ergebnis der Studie zeigte klar auf, dass die Erfolgsrate eines Identitätsdiebstahls dramatisch erhöht werden kann, wenn persönliche Informationen der Opfer in den eigentlichen Phishing-Angriffen enthalten sind. Das automatische Beziehen einer großen Anzahl von persönlichen Daten wird auch als *Crawling* bezeichnet. Crawling, sowie eine anschließende Visualisierung als Graphen wurden zudem bereits 2005 von Heer et al. in der Software *Vizster* [3] implementiert.

SNA-Methodiken wurden auch in diversen Arbeiten [4] im Zusammenhang mit der Identifizierung und Überwachung krimineller und terroristischer Gruppen besprochen. Die daraus resultierenden Ergebnisse zeigten, wie SNA und Verhaltensanalyse sozialer Netzwerke wichtige Instrumente heutiger kriminalistischer Untersuchungen geworden sind. In der Arbeit von Aleman-Meza et al. [5] wurde zudem gezeigt, dass eine reale Identität mit Hilfe zweier Identitäten in zwei verschiedenen sozialen Netzwerken auffindig gemacht werden kann. Des Weiteren präsentierte Matsuo et al. [6] ein System namens *POLYPHONET*, um Relationen zwischen Personen, Gruppen und Schlüsselwörter aus sozialen Netzwerken zu extrahieren.

Dass Datenschutz nicht als Feature von den Betreibern vermarktet wird, zeigt eine aktuelle Studie [13], welche 45 soziale Netzwerke untersucht hat. Die Studie zieht den Schluss, dass zwar Datenschutzbestimmungen bei vielen Netzwerken ausgearbeitet sind, die Anbieter sozialer Netzwerke die Nutzer jedoch weiterhin dazu animieren personenbezogene Informationen freizugeben. Eine weitere aktuelle Studie [14] beschreibt die Verbindung von flickr- und twitter-Profilen ähnlich der hier beschriebenen Methoden mit einer Fehlerquote von 12%.

3 Mathematische Betrachtung Sozialer Netzwerke

Im mathematischen Kontext bestehen soziale Netzwerke aus Knoten V und Kanten E , die so angeordnet sind, dass sie eine soziale Struktur durch die Form eines Graphen G repräsentieren. Die Menge A der persönlichen Attribute a formen dann den individuellen Charakter einer Identität \hat{i} . Diese Attribute werden in einer eindimensionalen Datenreihe gespeichert, die wie folgt aussehen kann:

$\{\text{Name, Vorname, Adresse, Email, Hobbies, Geburtsdatum ...}\}$.

UUID
Vorname
Nachname
Geburtstag
E-Mail Adresse
Hobbys
Politische Orientierung
Relationen

Abbildung 1: Datenstruktur eines Identitätsprofils

\hat{i}_n	43	56	98	42
w_n	0.98	0.56	0.21	1

Abbildung 2: Beispiel einer Relationsmenge eines Identitätsprofils

Definition 1. Eine Identität \hat{i} besteht aus einem Tripel $(i, A, R) \in \hat{I}$ wobei A die Menge von Attributen $a \in A$ beschreibt, die \hat{i} definieren. R ist die Menge der Relationen $r \in R$, die eine Identität mit anderen Identitäten besitzt. Die Relationen r_n werden dabei in einer zweidimensionalen Matrix $K := (a_{x,y})_{2 \times y}$ gespeichert. i bezeichnet die zugehörige Identifikationsnummer einer Identität \hat{i} .

Die Summe R definiert die Relationen r zwischen einer gewählten Identität und allen anderen n Identitäten, ein Beispiel ist in Tabelle 2 zu finden. Die Datenstruktur einer Identität eines sozialen Netzwerks zeigen wir in Abbildung 1. Bei der Identifikationsnummer i handelt es sich um einen *Universally Unique Identifier* (UUID). Diese dient dazu, mögliche Kollisionen zwischen zwei Identifikationsnummern zu vermeiden.

Die erste Reihe der Matrix beinhaltet die Identifikationsnummer, zu der eine Relation gepflegt wird, die zweite Reihe speichert den Relationskoeffizienten w_n , welcher wie folgt definiert ist:

Definition 2. Der Relationskoeffizient w_n zwischen \hat{i} und \hat{i}_n ist definiert als $w_n := K_{2n}$ wobei $0 \leq w_n \leq 1$ und $\hat{i}, \hat{i}_n \in \hat{I}$.

Der Relationskoeffizient w_n kann nun beispielsweise automatisch mit Hilfe von Algorithmen berechnet werden. Ein Relationskoeffizient von 0 bedeutet dabei immer, dass keine Verbindung einer Identität \hat{i} zu der spezifischen Identität \hat{i}_n festgestellt werden konnte. Im Gegensatz dazu bedeutet ein Wert von 1 für w_n , dass die beiden Identitäten eine ausgeprägte Beziehung besitzen.

Aus der Sicht eines Angreifers ist der Relationskoeffizient w_n eigentlich nur eine optionale Information, kann aber die Chance für den Erfolg eines Angriffs entscheidend erhöhen. In der Praxis ist dieser Wert allerdings nicht einfach zu berechnen.

4 Fortgeschrittener Identitätsdiebstahl

Wir diskutieren in den folgenden Abschnitten nun vier verschiedene Phasen, die ein Angreifer nutzen könnte, um einen Angriff zu perfektionieren.

4.1 Datenaggregation

Bei den meisten sozialen Netzwerken ist die Profilstruktur statisch. Dies bietet für einen Angreifer den entscheidenden Vorteil, dass er den (automatisierten) Crawler lediglich auf die jeweilige Struktur des sozialen Netzwerks anpassen muss. Somit kann in relativ kurzer Zeit eine enorme Menge an Daten aggregiert werden. Dies ist für einen Angreifer aber nicht die einzige Möglichkeit der Datenbeschaffung, denn mittlerweile ist auch der Kauf von entsprechenden Datensätzen nicht mehr unüblich.

Soziale Netzwerke leben davon, persönliche Daten zu verarbeiten. Ein Nutzer, der sich an einem sozialen Netzwerk anmeldet, hat in den meisten Fällen ein persönliches und explizites Interesse daran, seine persönlichen Daten zu veröffentlichen. In Abbildung 3 ist das Verhältnis zwischen einem geschlossenen und offenen Nutzer dargestellt. Die Herausforderung liegt nun darin, eine Balance zwischen diesen beiden Nutzeigenschaften zu finden. Dabei sollte allerdings der kritische Grenzwert -in der Abbildung 3 mit einer gestrichelten Linie markiert- nicht überschritten werden, denn die Gefahr eines Datenmissbrauchs steigt danach weiter an, obwohl der Nutzer kaum noch einen Mehrwert durch die Veröffentlichung seiner Daten erhält.

4.2 Datenkorrelation

Während der in Kapitel 4.1 beschriebenen Phase hat der Angreifer in großen Mengen Daten aus verschiedenen sozialen Netzwerken bezogen. Ausgestattet mit diesen Informationen ist es ihm nun möglich, einen Graphen G_n für jedes seiner n durchgesuchten sozialen Netzwerke zu erstellen. Der Angreifer nimmt dabei im Folgenden an, dass ein Nutzer nicht nur in einem sozialen Netzwerk aktiv ist, sondern sich mehrerer Netzwerke und eventuell auch Identitäten bedient: Ein Netzwerk zum Beispiel zur Pflege von Freundschaften, eins zur Speicherung und zum Austausch von Bildern und ein anderes zur Pflege von Geschäftsbeziehungen. Bei diesen drei virtuellen Identitäten handelt es sich aber letztendlich um eine reale Identität, auch wenn dies für den Angreifer nicht auf den ersten Blick erkennbar sein muss.

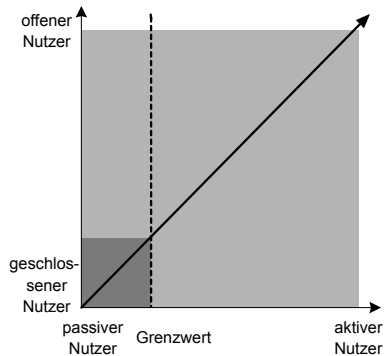


Abbildung 3: Verhältnis zwischen geschlossenem und offenem Nutzer

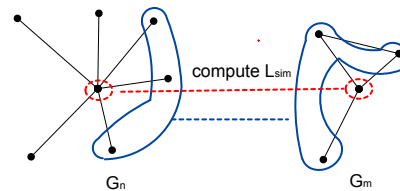


Abbildung 4: Vergleich von Identitäten und deren Nachbarschaft

Die verschiedenen Graphen G_n , die die verschiedenen sozialen Netzwerke repräsentieren, sind zu diesem Zeitpunkt noch nicht miteinander verbunden, es bestehen demnach noch keinerlei Relationen von Identitäten aus beispielsweise Graph G_1 zu Identitäten aus Graph G_2 . Mittels zweier Schritte kann ein Angreifer nun aber mehrere virtuelle Identitäten einer realen Identität zuzuordnen.

Schritt 1: Profil-Korrelation

Zunächst vergleicht der Angreifer sukzessive die Hauptattribute der persönlichen Attribute a einer Identität aus einem Graphen G_n mit allen Identitäten aus den anderen Graphen (rote Markierung in Abbildung 4). Als Hauptattribut kommen dabei möglichst eindeutige persönliche Attribute zum Einsatz, beispielsweise Geburtsdatum, Vorname, Name und E-Mail-Adresse. Dabei ist eventuell noch zu bedenken, dass Identitäten mit selteneren Attributen (etwa sehr ungewöhnlichen Vornamen und Namen) im Regelfall einfacher zugeordnet und identifiziert werden können, da sich die Identitäten in verschiedenen sozialen Netzwerken dann einfacher korrelieren lassen.

Für zwei bereits abgegliche Identitäten kann dann ein Wert L_{sim} berechnet werden, der die Wahrscheinlichkeit beschreibt, dass es sich bei beiden virtuellen Identitäten um ein und dieselbe reale Identität handelt.

Zur weiteren Verifikation können zudem die Hauptattribute der Identitäten in der direkten Nachbarschaft der beiden in Frage stehenden Identitäten wechselseitig miteinander verglichen werden (blaue Markierung in Abbildung 4), die Ergebnisse können direkt in den Wert L_{sim} einfließen. Sobald L_{sim} einen gewissen Grenzwert überschreitet, geht der Angreifer zu Schritt 2 über.

Schritt 2: Graphenbasiertes Data-Mining

Die Suche nach einem Sub-Graph-Isomorphismus stellt die Basis für das Abgleichen und Aufzählen identischer Teile in zwei spezifischen Graphen, in denen die

verdächtigen Identitäten lokalisiert sind, zur Verfügung. Allerdings ist das Sub-Graph-Isomorphie-Problem in der Gruppe der \mathcal{NP} -harten Probleme anzusiedeln. Fokussiert ein Angreifer jedoch in unserem Szenario lediglich auf topologische Strukturen, die aus einem Hauptknoten (Identität) und der direkten Nachbarschaft dieses Knotens besteht, wird der Suchraum entscheidend reduziert. Als topologische Strukturen bezeichnen wir hier individuelle soziale Strukturen in sozialen Netzwerken, beispielsweise die direkte(n) Nachbarschaft(en) zwischen Identitäten.

Diese Phase ist für den Angreifer aber lediglich optional. Der Aufwand lohnt sich meist dennoch, denn je mehr Informationen über eine Identität gesammelt werden können, desto größer ist die Chance, dass es sich bei dieser Identität um ein für den eigentlichen Angriff geeignetes Opfer handelt. In Abbildung 5 ist der so gewonnene Mehrwert für den Angreifer zu erkennen.

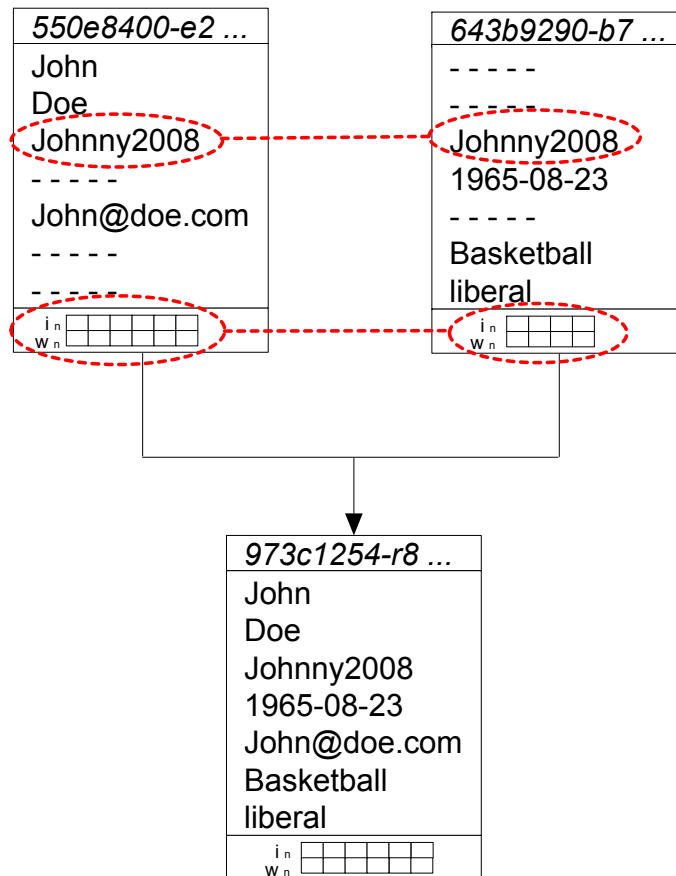


Abbildung 5: Zwei verflochtene Identitäten aus verschiedenen sozialen Netzwerken

4.3 Datenanalyse und Opferwahl

Die Basis des Angriffs wurde während den letzten beiden Phasen gelegt. Es werden nun einige Voraussetzungen definiert, die einem Angreifer bei der Suche nach einem geeigneten Opfer helfen könnten.

- **Maximaler Informationsgrad**

Der Informationsgrad über eine Identität muss möglichst maximal sein, um die Erfolgchancen eines Angriffs zu erhöhen. Je mehr Informationen ein Angreifer über ein potentielles Opfer besitzt, desto raffinierter kann der jeweilige Angriff ausgeführt werden und desto wahrscheinlicher hat der Angreifer auch Erfolg mit seinem Vorhaben.

- **Existenz eines Brokers**

Ein Broker [7] innerhalb eines Graphen G hält zwei nicht verbundene Knoten oder Untergraphen zusammen und stellt eine sehr wichtige Rolle in einem sozialen Netzwerk dar. Im Kontext dieser Arbeit ist ein Broker ein zentraler Punkt eines Graphen und wir nehmen an, dass die Anzahl der Knoten in der direkten Nachbarschaft des Brokers größer ist als die Anzahl der Knoten anderer Identitäten.

- **Auffinden einer Clique**

Eine Clique ist nun eine Untermenge von Knoten, die einen vollständigen Untergraphen definieren. Allerdings ist die Fragestellung, ob es eine Clique einer gewissen Größe in einem Graphen gibt, auch ein \mathcal{NP} -hartes Problem. Es gibt aber diverse Brute-Force Algorithmen, die unter gewissen Umständen dieses Problem in polynomineller Zeit lösen.

- **Cluster-Koeffizient**

Eine Identität \hat{i} besitzt die Nachbar-Knoten $N_{\hat{i}} = \{\hat{i} : e_{\hat{i}j} \in E\}$.

Der lokale Cluster-Koeffizient einer Identität \hat{i} mit $|N_{\hat{i}}|$ direkten Nachbarn definiert das Verhältnis der Anzahl der innerhalb der Nachbarschaft bestehenden Relationen zur Anzahl aller möglichen Relationen.

$$C_{\hat{i}} = \frac{2|\{e_{j_k}\}|}{|N_{\hat{i}}|(|N_{\hat{i}}|-1)} : e_{jk} \in E, v_j, v_k \in N_{\hat{i}} \quad (1)$$

Ein maximaler lokaler Cluster-Koeffizient impliziert eine ausgeprägte Nachbarschaft.

4.4 Angriffsphase

Vertrauen ist die Basis jeglicher Kommunikation. Laut einer Studie aus dem September 2007 ² vertrauen über 36% der Internetnutzer Informationen, die sie von ihren Freunden in sozialen Netzwerken erhalten.

²Rob Dickerson, CEO von Faves.com

Während eines Identitätsdiebstahls wird nun genau dieses Vertrauen von einer böartigen dritten Partei missbraucht. Der Angreifer gibt sich dabei als eine Identität aus und kontaktiert in deren Namen die zweite Identität. Um ein Opfer oder eine Gruppe von Opfern auf eine böartige Webseite zu locken und dort zur Eingabe von privaten Information zu verleiten, benutzt der Angreifer beispielsweise normale Textnachrichten, die per E-Mail, als private Nachricht über das soziale Netzwerk, SMS oder auch Instant-Messaging-Services übertragen werden können. Das genaue Verfahren hängt dabei maßgeblich davon ab, welche Informationen der Angreifer über das Opfer besitzt. In der Textnachricht werden aber meist immer sämtliche gesammelte Informationen aus der vorherigen Phasen verarbeitet.

Im folgenden Angriffsszenario nehmen wir an, dass der Angreifer die folgenden Informationen besitzt: Es existiert eine Identität u eines sozialen Netzwerks, die die Rolle eines Brokers innehält, aber trotzdem nur einen geringen Cluster-Koeffizienten C besitzt. Des Weiteren besitzt die Identität u Relationen zu den Identitäten v, x, y, z im selben sozialen Netzwerk.

Der Angreifer startet nun einen Phishing-Angriff auf die Identitäten v, x, y, z indem er sich als Identität u ausgibt. Die entsprechende Nachricht an die Opfer v, x, y, z könnte wie folgt lauten:

*Hallo \$Identität-[v-x-y-z],
ich bin durch Zufall auf folgenden Weblink gestoßen \$böartige.Webseite und dachte,
dass Dich diese Information interessieren könnte, da Du Dich ja für \$Identitätsattribut-[v-x-y-z]-1 und \$Identitätsattribut-[v-x-y-z]-2 interessierst.
Ach ja, und weißt Du was \$Identitätsrelation-[v-x-y-z]-1 derzeit so treibt? Hängt er immer noch mit \$Identitätsrelation-[v-x-y-z]-2 rum?
Hoffe, wir sehen uns bald wieder,
\$Identität-[u]*

4.5 Problemstellungen

Trotz der hier vorgestellten Techniken bleiben aber immer noch etliche Schwierigkeiten für einen Angreifer. Zunächst sind einige Eigenschaften von sozialen Netzwerken, wie bereits von Holder et al. [8] diskutiert, nicht direkt offensichtlich. Beispielsweise könnten Relationen als stark angesehen werden, obwohl sie in Wirklichkeit sehr schwach sind. Des Weiteren könnte eine Identität A eine Relation zu einer zweiten Identität B als stark ansehen, Identität B diese Relation aber als eher schwach deklarieren. In anderen Fällen könnten die persönlichen Attribute und Relationen einer potentiellen Opfergruppe von Identitäten dem Angreifer nicht vollständig vorliegen [9].

Soziale Netzwerke sind zudem dynamische Netzwerke. Familiäre Strukturen in sozialen Netzwerken sind zwar relativ statisch, im allgemeinen werden Netzwerke aber durch Knoten und Kanten geprägt, die entstehen und wieder verschwinden. Die Korrektheit der Datensätze sozialer Netzwerke kann daher durch einmaliges Crawlen nicht gewährleistet werden.

4.6 Gegenmaßnahmen

Nutzer sozialer Netzwerke sind gegen die hier beschriebenen Angriffe nicht komplett wehrlos. Um Gegenmaßnahmen zu entwickeln, soll aber zunächst der Kreislauf eines Angriffs näher betrachtet werden.

In der Angriffsphase sind zwei grundlegende Schwächen der Opfer zu identifizieren: Die Unfähigkeit, die Vertrauenswürdigkeit einer (unbekannten) Nachricht einzuschätzen, und die Reaktion auf eine nicht vertrauenswürdige Nachricht. In diesem Zusammenhang gab es bereits in der Vergangenheit zahlreiche Vorschläge für Gegenmaßnahmen. Diese reichen von der Etablierung eines Sicherheitsbewusstseins beim Nutzer bis hin zu technischen Gegenmaßnahmen wie S/MIME und PGP.

Bezüglich der Datenkorrelation können zudem die folgenden Gegenmaßnahmen die Erfolgchancen eines Angriffs reduzieren bzw. die Auswirkung eines Angriffs mindern:

Die Nutzung von Pseudonymen in Kombination mit der Eingrenzung von persönlichen Attributen vermindert die Chance, dass der Angreifer eine Korrelation zwischen den Profilen herstellen kann. Der Datenaggregation kann zum einen technisch mit Anti-Crawler Techniken begegnet werden, zum anderen müssen die Nutzer über die möglichen Auswirkungen der maßlosen, zuordnungsfähigen Veröffentlichung personenbezogener Daten besser informiert werden. Eine somit motivierte Eingrenzung von persönlichen Attributen, welche auch in der Korrelationsphase schützt, macht es dem Angreifer unmöglich, personenbezogene Attribute in der Phishingnachricht weiter zu verwenden.

Die Herausforderung der Umsetzung solcher Gegenmaßnahmen liegt aber nicht nur auf Seiten des Nutzers. Auch Anbieter großer sozialer Netzwerke müssen auf Sicherheitsrisiken noch stärker als bisher hinweisen. Da die Betreiber solcher Netzwerke aber von Datensätzen mit persönlichen Daten profitieren, haben sie zunächst wenig Interesse daran, dem Nutzer die Veröffentlichung zu erschweren bzw. zu verbieten. Hinzu kommt, dass natürlich auch der Erfolg des sozialen Netzwerks in Frage gestellt würde, wenn alle Nutzer extrem datensparsam wären: Niemand hat großes Interesse daran, mit unbekanntem und pseudonymisierten Nutzern Geschäfte zu machen oder näheren Kontakt zu pflegen.

5 Kritikalitätsvisualisierung

Das Hauptproblem sozialer Netzwerke liegt in der Tatsache, dass die Nutzer sich der eigentlichen Gefahr nicht bewusst sind, sondern in der Veröffentlichung ihrer persönlicher Informationen lediglich Vorteile sehen. Wir diskutieren daher eine Funktion zur Berechnung der Gefährdung einer Identität in einem sozialen Netzwerk, um den Nutzer und Anbietern ein Messinstrument in die Hand zu geben, um detaillierte Aufklärung bezüglich Datensparsamkeit oder Datenschutzmaßnahmen zu betreiben. Als Proof-of-Concept haben wir dieses Messinstrument zur besseren Visualisierung der Kritikalität mittels einer Webanwendung umgesetzt.

5.1 Einschränkung

Zunächst muss einschränkend erwähnt werden, dass die Gefahr, der sich eine Identität im Internet aussetzt sobald sie personenbezogene Daten publiziert, nicht genau in Zahlen gemessen werden kann. Dies liegt vor allem daran, dass das menschliche Verhalten auf eine Angriffsnachricht nie exakt vorausgesagt werden kann. Selbst wenn ein Nutzer eine offene Identität besitzt, heisst das nicht, dass ein Angriff auch wirklich Erfolg haben muss.

Des Weiteren muss beachtet werden dass die Kritikalität nicht wie im klassischen Sinn der Risikobetrachtung als *Kritikalität = Auswirkung des Angriff · Wahrscheinlichkeit des Angriff* definiert ist. Wir betrachten hier die Kritikalität bzw. Wahrscheinlichkeit des einzelnen Nutzer durch den Angreifer als Opfer für die Angriffsphase ausgewählt zu werden.

5.2 Berechnung der Kritikalität

Dennoch versucht unser Ansatz, eine ungefähre Aussage über die Kritikalität einer Identität zu geben. Ein genauer Wert ist jedoch auch nicht notwendig denn, wie in Abbildung 3 zu sehen, kann man grundlegend zwischen drei verschiedenen Stadien einer Identität unterscheiden. Die ausgearbeitete Funktion soll lediglich dabei helfen, eine Identität in eine dieser drei Stadien einzuordnen.

- **Offene Identität**

Es wurden sehr viele personenbezogene Daten der Identität im Internet publiziert und sind für jeden einsehbar. Daraus resultiert, dass die Identität einem größeren Risiko des Identitätsdiebstahls bzw. -missbrauchs ausgesetzt ist.

- **Neutrale Identität**

Es sind nur wenige persönliche Informationen einer Identität im Internet, so dass sich das Risiko, ein Opfer eines Identitätsdiebstahls zu werden, im Rahmen hält.

- **Geschlossene Identität**

Es sind keine persönlichen Daten einer Identität im Internet einsehbar bzw. nicht für Dritte einsehbar. Dies verringert das Risiko eines Identitätsdiebstahls enorm.

Es ist offensichtlich, dass die Kritikalität je nach Art des veröffentlichten Attributs variieren muss. Das bedeutet beispielsweise, dass ein veröffentlichter Nachname nicht so die Kritikalität beeinflusst, wie ein veröffentlichtes Geburtsdatum dies tun würde. Daher müssen persönliche Attribute einer Gewichtung unterzogen werden, bei der bestimmt wird, wie gefährlich letztendlich eine Veröffentlichung des spezifischen Attributes sein kann. Eine beispielhafte Gewichtung persönlicher Attribute wird in Tabelle 2 aufgelistet. Je höher der Wert, desto kritischer ist die Veröffentlichung des zugehörigen Attributs.

In Tabelle 2 wurden drei verschiedene Werte eingepflegt, welche mit weiteren, notwendigen Notationen in Tabelle 1 beschrieben sind.

Variabel	Beschreibung
r	Anzahl persönlicher Attribute
δ_i	boolescher Wert (1,0) der definiert, ob das persönliche Attribut i dem Angreifer bekannt ist
g_i	Gewichtskoeffizient, der die Relevanz des Attributes i in Hinsicht auf die Privatsphäre der Identität beschreibt
s	Anzahl der Relationen, die eine Identität besitzt
w_n	Relationskoeffizient, der die Stärke der Relation zwischen zwei Identitäten beschreibt

Tabelle 1: Grundlegende Notationen in Gleichung 2

Persönliche Attribute a_i	δ_i	g_i
Name	1	0.35
Vorname	0	0.44
Adresse	0	0.76
Pseudonym	1	0.12
Geburtsdatum	1	0.81
Hobby	0	0.45
Politische Richtung	1	0.73
Sexuelle Vorlieben	0	0.52
Geschlecht	1	0.67

Tabelle 2: Gewichtung persönlicher Attribute mit beispielhaften g_i

5.3 Die Kritikalitätsfunktion

Ziel der Kritikalitätsfunktion ist es, bei Eingabe persönlicher Informationen eine ungefähre Abschätzung der Gefährdung der Identität zu berechnen. Dies bedeutet, dass die Anzahl der publizierten persönlichen Attribute mit ihren Gewichtungen (siehe Tabelle 2) und Relationen als Eingabewerte genommen werden und die Funktion als Ausgabe einen Wert zwischen 0 und 1 ausgibt. Dieser Ausgabewert kann dann wie folgt gewertet werden: Je höher der Wert, desto gefährdeter ist die Identität.

Die vollständige Funktion zur Berechnung der Kritikalität κ lässt sich wie folgt beschreiben.

$$\kappa = \underbrace{\left(\sum_{i=1}^r \frac{\delta_i \cdot g_i}{r} \right)}_{\text{Attribute}} \cdot \underbrace{\left(\sum_{n=1}^s \frac{w_n}{s} \right)}_{\text{Relationen}} \quad (2)$$

Prinzipiell besteht die Funktion aus zwei Teilen, die multiplikativ miteinander verknüpft sind, um letztendlich einen Ausgabewert zwischen 0 und 1 zu erreichen. Die linke Klammer enthält das Verhältnis der einzelnen Attribute (ausgedrückt durch den booleschen Wert δ_i) mit ihrer spezifischen Gewichtung g_i zur Gesamtzahl aller Attribute r . Der Wert δ_i drückt hierbei aus, ob ein Angreifer das Attribut besitzt oder nicht. Letztere Tatsache geht dann als Wert 0 in die Funktion mit ein. Wir nehmen weiterhin an dass das Attribut wahrheitsgemäß

durch den Anwender ausgefüllt wurde.

Die rechte Klammer summiert alle Relationskoeffizienten w_n relativ zur Gesamtanzahl der Relationen auf. Hier handelt es sich hier um das arithmetische Mittel von Relationskoeffizient w_n und der Gesamtanzahl der Relationen.

Es existieren zwar Sonderfälle, wie zum Beispiel dass eine Identität keine Relationen angeben hat, und somit die Kritikalität 0 wäre, jedoch betrachten wir diese Sonderfälle zur besseren Anschaulichkeit in der Beschreibung hier nicht. Eine Erweiterung der Funktion für Anbieter sozialer Netzwerk könnte eine rekursive Berechnung der Kritikalität darstellen. Hier könnten Anbieter, da sie im Besitz der nötigen Informationen sind, die einzelnen Relationen einer Identität mit der Kritikalität der jeweiligen Relation gewichten. Dies ist von Vorteil, da es immer Schnittmengen zwischen den Attributen von Identitäten gibt und somit eine passive Identität einer höheren Kritikalität ausgesetzt ist, wenn sie extrem aktive Relationen hat.

Zum besseren Verständnis schlagen wir vor, die Funktion in einem Webinterface anzubieten, mit dem der Nutzer ein Formular ausfüllen und die Kritikalität κ berechnen lassen kann.

5.4 Webanwendung für Kritikalitätsvisualisierung

Die Motivation für eine Kritikalitätsvisualisierung per Webanwendung ist klar erkennbar: Der Nutzer eines sozialen Netzwerkes kann wenig mit mathematischen Formeln anfangen und benötigt für das Verständnis eine anschaulichere Visualisierung. Es macht daher Sinn, dem Nutzer eine klar strukturierte Webseite anzubieten, auf der er ein Formular ausfüllen muss, das ihm anschließend die Kritikalität κ berechnet.

Der von uns vorgeschlagene Prozess für die Berechnung der Kritikalität κ per Webanwendung wird in zwei aufeinanderfolgende Phasen eingeteilt. In der ersten Phase übermittelt der Nutzer die Anzahl und den Status seiner persönlichen Attribute (siehe linke Klammer in Formel 2). Dies könnte beispielsweise durch ein einfaches Formular wie in Abbildung 6 realisiert werden. Der Nutzer muss in diesem Beispiel für das soziale Netzwerk zu jedem dort behandelten Attribut angeben, ob dies wahrheitsgemäß publik gemacht wurde oder nicht.

Nachdem das erste Formular erfolgreich ausgefüllt wurde, wird der Nutzer im zweiten Schritt zur Eingabe der Informationen über seine Relationen aufgefordert. Beispielhaft ist dies in Abbildung 7 veranschaulicht. Das Feld für die Gesamtanzahl der Freunde repräsentiert in der Funktion den Wert s . Da man den Nutzer aber nicht dazu auffordern kann, jede einzelne Relation in Bezug auf die Stärke der Beziehung zu gewichten, führen wir drei Stufen der Relationsstärke ein: stark, mittelmässig und schwach. Diesen Stufen geben wir statische Relationskoeffizienten w_n , um somit das Relationsgefüge ungefähr bewerten zu können. Ein erweitertes Formular für Nutzer, die vor der Gewichtung jeder einzelner Relation nicht zurückschrecken, wird in zukünftigen Implementierungen beachtet werden.

Attribut	Öffentlich	Nicht Öffentlich
Nickname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Vorname	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Nachname	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Adresse	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Telefonnummer	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Hochschule	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Studiengang	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Geschlecht	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Geburtstag	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ICQ-Nummer	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Beziehungsstatus	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Politische Richtung	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Hobbies	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Art der Arbeit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Arbeitgeber	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Persönliches Foto	<input type="checkbox"/>	<input checked="" type="checkbox"/>
		zum nächsten Schritt

Abbildung 6: Beispielhafter erster Schritt der Kritikalitätsberechnung

Der Datenschutz dieser Webanwendung muss natürlich auch beachtet und klar herausgestellt werden. Die Webanwendung kann zwar zur besser Erforschung und Bewertung der Kritikalitätsfunktion, angegebene Daten speichern, jedoch sollten keine weiteren Nutzerbezogenen Daten wie zum Beispiel die IP Adresse gesichert werden.

Um mehr Nutzer für die Berechnung der Kritikalität zu motivieren, könnte komplementär zur Webanwendung eine Browsererweiterung³ angeboten werden, welche die benötigten Informationen zur Berechnung beim Login auf das soziale Netzwerk automatisch bezieht und die Kritikalität auf Wunsch separat anzeigt oder in die Webseite integriert.

6 Fazit

Für persönliche Daten gibt es vielerlei Missbrauchsmöglichkeiten. Dabei lässt sich zunächst zwischen der gewollten und der ungewollten unerwünschten Veröffentlichung durch priva-

³z.B. via Greasemonkey

Anzahl der Freundschaften:		13
davon	starke	6
	mittelmässige	4
	schwache	3
		Kritikalität berechnen

Abbildung 7: Beispielhafter zweiter Schritt der Kritikalitätsberechnung

te und/oder gar staatliche Stellen zu den verschiedensten Zwecken unterscheiden. Darüber hinaus lassen sich spätestens mit Hilfe der Korrelation von Profildaten auch rasterfahndungsähnliche Methoden umsetzen. Und nicht zuletzt birgt die Veröffentlichung von Daten auch ein großes ökonomisches Potenzial, das beim Nutzer in Form von (unerwünschter) Werbung wieder ankommt. Eine Proof-of-Concept-Implementierung eines aufgefalten, automatisierten Angriffs auf die Identitäten in einem sozialen Netzwerk ist zudem Gegenstand von weiteren laufenden Arbeiten.

Eine sichere Separierung der Identitäten bleibt bisher eine noch ungelöste Aufgabe für die einzelnen Nutzer, für die Technik und für die Gesetzgebung. Dabei ist es dringend notwendig, den Nutzer bei der Justierung und Einhaltung des von ihm gewünschten Datenschutzniveaus zu unterstützen. Konzepte, die versuchen, dieses Niveau anhand der Anzahl und Qualität der veröffentlichten Daten zu ermitteln, können ein erster Schritt zu einem besseren Verständnis sein und damit insgesamt zu einem höheren Datenschutzniveau beitragen.

Literatur

- [1] Gartner Inc., Technischer Report, Dezember 2007
- [2] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson und Filippo Menczer. Social phishing. *Commun. ACM*, 50(10):94, 100, 2007.
- [3] Jeffrey Heer and Danah Boyd. Vizster: Visualizing online social networks. *IEEE Symposium on Information Visualization*, 2005
- [4] Larsen Henrik Legind Memon Nasrullah. Detecting terrorist activity patterns using investigative data mining tool. *International Journal of Knowledge and System Sciences*, 2006
- [5] Boanerges Aleman-Meza, Meenakshi Nagara jan, Cartic Ramakrishnan, Li Ding, Pranam Kolari, Amit P. Sheth, I. Budak Arpinar, Anupam Joshi und Tim Finin. Semantic analytics on social networks: experiences in addressing the problem of conflict of interest detection. *15th international conference on World Wide Web*, 2006
- [6] Yutaka Matsuo, Junichiro Mori, Masahiro Hamasaki, Keisuke Ishida, Takuichi Nishimura, Hideaki Takeda, Koiti Hasida, and Mitsuru Ishizuka. Polyphonet: an advanced social network extraction system from the web. *15th international conference on World Wide Web*, 2006

- [7] V.E. Krebs. Uncloaking terrorist networks. First Monday, 7, 2002.
- [8] L. B. Holder M. Mukherjee. Graph-based data mining on social networks. Workshop on Link Analysis and Group Detection, 2004.
- [9] V.E. Krebs. Uncloaking terrorist networks. First Monday, 2002
- [10] Clark, John ; Holton, Derek A.: A First Look at Graph Theory. World Scientific Publishing Co. Pte. Ltd., 1991
- [11] Harrer, Andreas; Malzahn, Nils ; Zeini, Sam ; Hoppe, H. U.: Combining Social Network Analysis with Semantic Relations to Support the Evolution of a Scientific Community. In: Chinn, Clark (Hrsg.) ; Erkens, Gijbert (Hrsg.) ; Puntambekar, Sadhana (Hrsg.): Mice, Minds, and Society - The Computer Supported Collaborative Learning (CSCL) Conference 2007, International Society of the Learning Sciences, 2007, S. 267, 276
- [12] Jansen, Dorothea: Einführung in die Netzwerkanalyse - Grundlagen, Methoden, Forschungsbeispiele. 3. Wiesbaden : VS Verlag für Sozialwissenschaften, 2006
- [13] Joseph Bonneau, Sören Preibusch: The Privacy Jungle: On the Market for Data Protection in Social Networks
- [14] Arvind Narayanan, Vitaly Shmatikov: De-anonymizing Social Networks