

# Sicherheitsrisiko: Social Networks

Daniel Leese, Philipp Waldhauer

## Index Terms

IT-Security, Social Networks, Web 2.0



- 
- *Daniel Leese, Phillip Waldhauer, Studenten der Hochschule Furtwangen, Studiengang Computer Networking, 4. Semester  
E-mail: leese@hs-furtwangen.de, waldhau@hs-furtwangen.de*

## INHALTSVERZEICHNIS

<b>1</b>	<b>Was sind Social Networks?</b>	<b>4</b>
1.1	Entwicklung . . . . .	4
1.2	Möglichkeiten . . . . .	5
<b>2</b>	<b>Sicherheitsrisiken</b>	<b>5</b>
2.1	Datacrawling . . . . .	5
2.2	Identitätsdiebstahl . . . . .	7
2.3	Datenmissbrauch . . . . .	7
2.3.1	Facebook . . . . .	7
2.3.2	studiVZ . . . . .	8
2.4	Sensible Informationen . . . . .	8
2.4.1	Nach Frankreich fahr ich nur auf Ketten . . .	9
2.4.2	Mordfall in Toronto . . . . .	9
2.5	Spear-Phishing . . . . .	9
2.5.1	Ablauf . . . . .	10
2.6	Fallbeispiel: Angriff auf Unternehmensdaten . . . . .	11
2.6.1	Suchen von Mitarbeiternamen . . . . .	11
2.6.2	Recherche in Businessnetzen . . . . .	12
2.6.3	“Gefälschte” Profilseite erstellen . . . . .	12
2.6.4	Recherche im Netz des angegriffenen . . . . .	12
2.6.5	Das Lügennetzwerk . . . . .	13
<b>3</b>	<b>Fazit</b>	<b>14</b>
	<b>Quellen</b>	<b>15</b>

**ABBILDUNGSVERZEICHNIS**

1	Zeitliche Entwicklung populärer Social Networks . . . . .	4
2	Nutzen von Korrelationen verschiedener Profile . . . . .	6
3	Ein Beispiel für besonders kryptische Captchas . . . . .	6
4	Differenzierung zwischen Phishing und Spear-Phishing . . . . .	10
5	Zugriff auf die Profilseite des Marketing-Mitarbeiters . . . . .	12
6	Das entstandene Beziehungsgeflecht . . . . .	13

## 1 WAS SIND SOCIAL NETWORKS?

Als Social Network bezeichnet man Dienste für Online-Communities. Diese sind meist webbasiert und bieten Funktionen wie das Anlegen eines persönlichen Profils, Pflegen einer Kontaktliste und dem Empfang und Versenden von privaten Nachrichten. Die Ausrichtung dieser Plattformen kann unterschiedlich sein. Es existieren soziale Netzwerke für Studenten (studivz), berufsbezogene (XING), interessenbezogene (animexx) und regionsbezogene Netzwerke (lokalisten).

### 1.1 Entwicklung

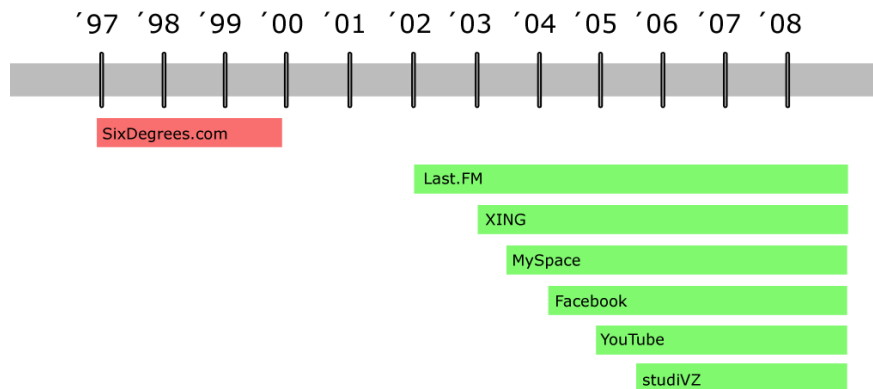


Abbildung 1. Zeitliche Entwicklung populärer Social Networks

Mit SixDegrees.com startete im Jahr 1997 die erste Online-Plattform, die man nach unserer Definition als Social Network bezeichnen konnte. Sie bot alle vorgestellten Funktionen, war allerdings nicht sehr erfolgreich und ging bereits 2000, nach drei Jahren Aktivität vom Netz. Der Betreiber der Seite gab später in einem Interview zu, dass die Idee seiner Zeit voraus war.

Im Jahr 2002 begann dann der große Boom der noch bis heute anhält. Portale wie Last.FM, XING, MySpace und Facebook starteten und fanden in kürzester Zeit erheblichen Zuspruch in Form von registrierten Benutzern, aber auch in Form von Kopien. Das bekannteste Beispiel dafür ist wohl das deutsche Studentenportal studivz, das seinem amerikanischen Vorbild facebook sehr ähnlich ist.

Bis heute hält sich der Social-Network-Boom, auch im Zusammenhang mit der Entwicklung des "Web 2.0". Mittlerweile gibt es soziale Netzwerke für jeden denkbaren Bereich des menschlichen Lebens.

## 1.2 Möglichkeiten

Durch das Anlegen eines persönlichen Profils erhält man die Möglichkeit der Darstellung der eigenen Person. Oft ist es möglich sehr viele Daten über sich anzugeben, Bildergalerien anzulegen oder gar Tagebücher zu schreiben, durch die man den Besuchern seiner Seite viele Informationen zur Verfügung stellen kann.

Eine weitere gebotene Möglichkeit ist das Finden, beziehungsweise wiederfinden von Freunden. Durch umfangreiche Suchmöglichkeiten kann man Menschen aus der Umgebung, alten Schulen oder gleichen Interessen finden und in Kontaktlisten speichern. Um Kontakt aufzunehmen kann man dann private Nachrichten austauschen oder an Diskussionen in Foren teilnehmen.

Je nach Ausrichtung des Netzwerkes ist es auch möglich seine Zukunftschancen zu steigern, zum Beispiel im Hinblick auf den Beruf.

Eine, für das Opfer eher negative Möglichkeit, ist natürlich auch das Stalken, d.h. das Ausspionieren und Verfolgen anderer Benutzer. Je nachdem wie leichtsinnig das Opfer mit seinen Daten umgeht ist es unter Umständen möglich sehr viel über sein Leben zu erfahren.

## 2 SICHERHEITSRISIKEN

### 2.1 Datacrawling

Datacrawling bezeichnet die maschinelle Sammlung und Speicherung von Daten. Diese Tätigkeit gibt es natürlich schon seitdem es das Internet gibt und wird für die verschiedensten Zwecke eingesetzt. Das Sicherheitsrisiko, das durch die sozialen Netzwerke entsteht, basiert auf der Tatsache, dass die umfangreichen Daten, die von den Benutzern angegeben werden, meist in einer strukturierten Form dargeboten werden, die leicht analysierbar ist. So war es im Web 1.0 kompliziert schnell an Daten von vielen Benutzern zu gelangen. Zuerst mussten die Datensätze ausfindig gemacht werden (zum Beispiel in Form von privaten Webseiten), danach mussten dann viele verschieden aufgebaute Webseiten analysiert werden. Mit den Profildaten in den Netzwerken hat man nun Zugriff auf tausende identisch aufgebaute Webseiten. Somit muss man nur ein einziges mal einen Parser schreiben, welcher die Seite analysiert und die Benutzerdaten extrahiert.

Dazu kommt dass die Plattformen oft keine wirklichen Schutzmaßnahmen gegen Crawler bieten. Oft ist es nicht einmal nötig die Benutzernamen zu kennen, da man auf die Datensätze über eine laufende Nummer zugreifen kann (meist Datensatz-Id in der Datenbank).

Als Erweiterung zum einfachen Datacrawling kann man nun noch Korrelationen zwischen Profilen gleicher Benutzer in verschiedenen Netzwerken analysieren[Birk et al., 2008].

Hierbei kombiniert der Crawler die Daten des Benutzers  $X$  aus dem Netzwerk  $A$  mit den Daten des gleichen Benutzers (Erkennung z.B. an gleichem

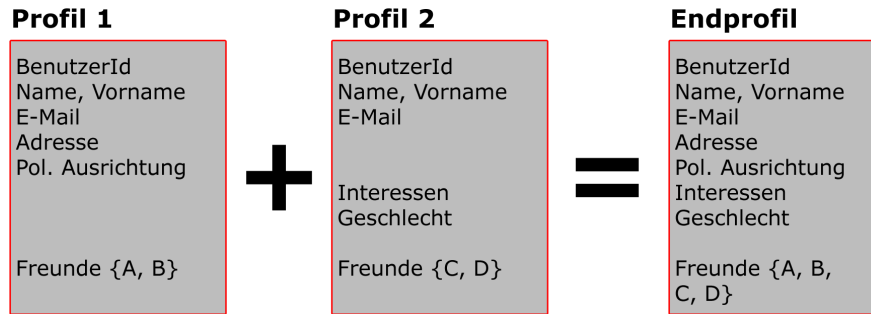


Abbildung 2. Nutzen von Korrelationen verschiedener Profile

Benutzernamen, Namen oder E-Mail-Adresse) aus dem Netzwerk *B* und erstellt somit einen sehr umfangreichen Datensatz.

Als Resultat hat man in relativ kurzer Zeit eine große Menge an umfangreichen Datensätzen gewonnen. Diese Datensätze können untereinander verknüpft sein, was durch die Freundesbeziehungen in den Netzwerken möglich ist. Diese Datensätze können nun an Datenhändler verkauft werden, oder genutzt werden um Vertrauen zu generieren (Social Engineering).

Als Beispiel kann man hier die Aktion zweier Studenten des MIT aufführen, die im Jahr 2005 als Teil eines Forschungsprojekts 70000 facebook-Profile erfasst und analysiert haben. Diese Daten wurden dann analysiert und in Form von Diagrammen aus verschiedenen Blickwinkeln dargestellt. Einige Zeit später gab es eine ähnliche Aktion auch auf die deutsche Plattform studivz.



Abbildung 3. Ein Beispiel für besonders kryptische Captchas

Zum Schutz gegen das automatisierte Sammeln von Daten kann man Captchas einsetzen. Captcha ist ein Akronym für "Completely Automated Public Turing test to tell Computers and Humans Apart", also ein Mechanismus um festzustellen ob sich ein Mensch hinter der Anfrage verbirgt oder ein automatisches Skript.

## 2.2 Identitätsdiebstahl

Ein weiteres Problem ist, dass die wenigsten Plattformen eine Authentizitätsüberprüfung der grundlegenden Benutzerdaten wie Name und Anschrift durchführen. Damit ist es für jeden Benutzer möglich Profile unter falschem Namen anzulegen und sie mit falschen Daten und Fotos auszuschnücken. Dadurch ist es möglich sensible Informationen über beliebige Personen zu publizieren, die unter Umständen nie für die Öffentlichkeit bestimmt gewesen wären, oder falsche Tatsachen darstellen.

In England gab es einen Fall von Identitätsdiebstahl via Facebook. Ein ehemaliger Schulkamerad legte ein Fake-Profil an und veröffentlichte falsche Daten über die sexuelle und politische Ausrichtung des Unternehmers Grant Raphael. Am Ende musste der Schuldige Schadensersatz in Höhe von 26000 Euro zahlen.

Die Maßnahmen gegen Identitätsdiebstahl sind aufwendig. Einerseits könnte der Betreiber die Echtheit jedes Benutzers überprüfen, zum Beispiel über PostIdent. Andererseits können die Benutzer sich schützen indem sie regelmäßig nach Fake-Profilen suchen oder sich "einfach" in jedem sozialen Netzwerk ein Profil anlegen.

## 2.3 Datenmissbrauch

Leider kann ein Mitglied eines sozialen Netzwerks, trotz vehementer Datenschutzbekundungen deren Betreiber, in keinster Weise davon ausgehen, dass seine Daten vertraulich behandelt werden. Dass viele Betreiber den Versuchungen der legalen und illegalen Weitergabe von Benutzerdaten nicht widerstehen können wird nachvollziehbar, wenn man Statistiken und Daten zur Nutzung sozialer Netze betrachtet.

So wurde z.B. in einer Studie ermittelt, dass 13% aller deutschen Arbeitnehmer von ihrem Arbeitsplatz aus soziale Netze nutzen und über die Hälfte dieser Nutzer auch sensible Daten, wie z.B. geschäftliche Termine oder Adressen darüber versenden[ecin.de, 2008]. Daher erscheint es auch begründet, dass der Wert eines solchen Benutzeraccounts, auf dem Datenschwarzmarkt, mit ca. 15 Euro betitelt wird.

Auch betreiben die meisten sozialen Netze personalisierte Werbeprogramme, die aus Datenschutzgesichtspunkten zumindest als fragwürdig zu bewerten sind. Ein gutes Beispiel hierfür ist Facebooks "Beacon", ein System zum Anzeigen personalisierter Werbung[Perez, 2007] in den Profildaten der Mitglieder. Abgesehen von der Personalisierung, die sich leider immer größerer Akzeptanz erfreut, geriet "Beacon" auch aus anderen Gründen in die Kritik:

### 2.3.1 Facebook

Zum Einen handelt es sich um ein sog. "Opt-out-System", d.h. die Defaulteinstellungen sind so gesetzt, dass von vornherein persönliche Daten weitergegeben werden. Möchte der Benutzer dies nicht muss er es, in tief verborgenen

Menüs, manuell abwählen. Hierbei setzt Facebook natürlich darauf, dass sich viele Benutzer nicht so sehr mit dem System auseinandersetzen um diese Optionen zu entdecken [Jones et al., 2005].

Doch selbst wenn alle Einstellungen auf maximale Privatsphäre gesetzt wurden, sind oftmals Daten, die als "Nicht öffentlich" markiert waren, für Werbekunden zugänglich gemacht worden, wie einige Datenskandale zeigten.

### 2.3.2 *studiVZ*

Bei Unternehmen aus den Vereinigten Staaten gehören solche Meldungen schon lange zur Tagesordnung, jedoch ist es um die deutschen sozialen Netze in keinster Weise besser bestellt. So gerät auch der Facebook-Klon *studiVZ* oft in die Kritik der Datenschützer, wie z.B. im Dezember 2007 als er die AGBs um Paragraphen erweiterte, die *studiVZ* die Möglichkeit personalisierte Werbung zu schalten einräumte [Barnitzke, 2008].

Den Usern wurden dabei folgende Optionen angeboten: Akzeptanz der Änderungen oder Löschung des Accounts nach einer bestimmten Frist. Diese Frist, und auch mehrfach gesetzte Nachfristen, verstrichen jedoch ohne das die Accounts gelöscht wurden. Mittlerweile wurden die AGBs erneut abgeändert und erlauben die Nutzung auch ohne aktivierte "personalisierte Werbung". Es ist anzunehmen das *studiVZ* diese Änderungen nicht aus einer plötzlich gesteigerten Sorge um die Persönlichkeitsrechte der Nutzer durchführte, sondern weil ansonsten zu viele Accounts verloren gegangen wären.

Doch nicht nur junge Unternehmen, wie die o.g. Startups, öffnen dem Datenmissbrauch vorsätzlich oder fahrlässig Tür und Tor. Auch "alte Hasen", wie die Deutsche Telekom, hatten in der jüngsten Vergangenheit etliche Datenskandale, über die selbst in den Massenmedien ausgiebig berichtet wurde [n24.de, 2008].

Vor diesen Hintergründen sollte für mündige und am modernen Leben irgendwie interessierte Bürger, jederzeit die Devise gelten, nur so wenige Daten wie irgendwie möglich gegenüber Datendiensten anzubieten. Dass sich mittels Addition der eventuell abgegebenen, optionalen Daten aus mehreren Quellen, letztendlich komplette Benutzerbiographien erstellen lassen, wurde schon im Kapitel "Datacrawling" gezeigt. Somit ist der Weg zum "Gläsernen Benutzer" schon vorgezeichnet. Leider ist jedoch all zu oft, wie auch das nächste Kapitel zeigen wird, eine extrem freizügige Preisgabe persönlicher Daten der Fall.

## 2.4 **Sensible Informationen**

Die Nutzung sozialer Netze kann sich auch oft, auch ganz ohne Preisgabe vertraulicher Informationen durch den Betreiber des Netzes als fatales "Ei-

gentor“ herausstellen. Viele Nutzer geben in erschreckendem Maß völlig freiwillig intimste Informationen in ihren Profilen an. Dies reicht von der Freizeitgestaltung, durch Mitgliedschaft in Gruppen wie “Komasaufen ist der Sinn meines Lebens“, über die politische Einstellung, bis hin zu fragwürdigen sexuellen Vorlieben.

Es ist mittlerweile bei Bewerbungen, vor Allem in der IT-Branche, Standard, die Namen der potentiellen neuen Mitarbeiter “mal zu googeln“. Ob sich nun die Mitgliedschaft in einer der unzähligen Saufgruppen positiv auf eine Bewerbung auswirkt ist nach Meinung der Autoren eher zu bezweifeln.

Prominente Beispiele zu dieser Problematik gibt es viele; zur Veranschaulichung der Tragweite hier einige Beispiele:

#### *2.4.1 Nach Frankreich fahr ich nur auf Ketten*

Bei diesem Ende 2008 bekannt gewordene Skandal ging es um die Mitgliedschaft eines CDU-Politikers in eben dieser Gruppe, die auf die erfolgreiche Eroberung großer Teile Frankreichs durch Deutschland im 2. Weltkrieg anspielt. Die Mitgliedschaft in so einer, klar dem (Neo)-Nazi-Umfeld zuordenbare Gruppe, bedeutete für den 21-jährigen Kreischef der Jungen Union Nord, völlig zurecht, das politische Aus[bild.de, 2008].

#### *2.4.2 Mordfall in Toronto*

Nach dem Mord der jugendlichen Stefanie Rengel wollten ihr ihre Freunde einen besonderen Freundschaftsdienst erweisen. Sie gründeten eine Facebook-Gruppe[facebook.com, 2009] zu diesem Fall, die neben einem Nachruf auch die Namen der beschuldigten Mordverdächtigen enthielt. Diese, von den Jugendlichen vermutlich als besonders mitfühlend und gerecht empfundene Aktion, sorgte jedoch nur für zusätzliches Leiden bei den Hinterbliebenen und verstieß darüber hinaus noch gegen mehrere Gesetze[citynews.ca, 2009].

So wollte Stefanies Familie die Tragödie zu diesem Zeitpunkt noch nicht bekanntgeben und hatte dies auch der Polizei und den Medien untersagt. Auch wurde gegen den “Youth Criminal Justice Act“ verstoßen, der es verbietet, die Namen minderjähriger Verbrecher zu veröffentlichen, zumal diese noch nicht als Mörder überführt waren, was Rufmord und Selbstjustiz erster Güte darstellt[digitaljournal.com, 2009].

## **2.5 Spear-Phishing**

Hinter diesem englischen Begriff verbirgt sich eine Angriffsmethode aus dem Bereich des “Social Engineering“, d.h. eine Hackingtechnik die weniger technische Schwachstellen, sondern gezielte Manipulation, Gesprächstaktiken und Streuen von Fehlinformationen, nutzt.

Dieses Verfahren baut auf dem herkömmlichen Phishing auf, ist jedoch wesentlich raffinierter. Während beim “normalen“ Phishing eine große Anzahl

unpersonalisierter Nachrichten, oftmals per E-Mail, an beliebige Empfänger gesendet wird, geht Spear-Phishing gezielter vor. Dadurch ist die Erfolgsquote wesentlich höher, jedoch ist auch der Aufwand größer, da der Spear-Phishing Vorgang nur teilweise automatisiert werden kann [Birk et al., 2008].

### 2.5.1 Ablauf

Zuerst werden automatisiert Benutzerprofile eines sozialen Netzwerks nach bestimmten Kriterien gescannt. Solche Kriterien könnten z.B. Mitglied in bestimmten Vereinen, eine Abteilung in einem Unternehmen oder Punkte des beruflichen Werdegangs sein. Die dadurch aus der großen Menge "herausgefischten" interessanten Opfer werden dann gezielt angegriffen.

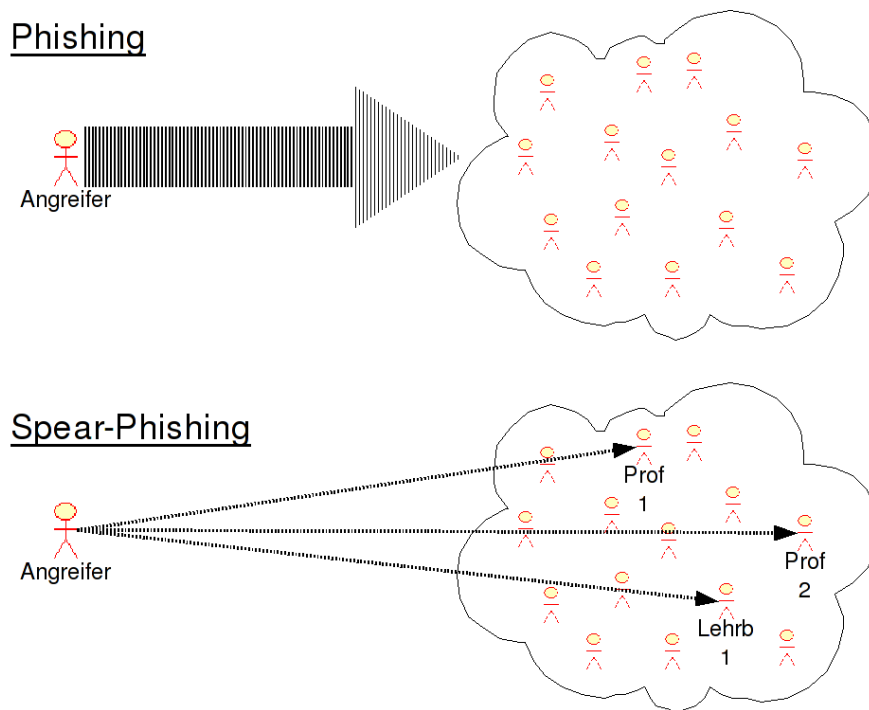


Abbildung 4. Differenzierung zwischen Phishing und Spear-Phishing

Der nächste Schritt im Angriff ist die Kontaktaufnahme zu den Opfern unter Vorspiegelung einer falschen Identität. Ziel ist das Aufbauen eines Vertrauensverhältnisses, wobei dem "Social Engineer" die in den Netzwerken preisgegebenen Informationen zu Gute kommen.

Wurde das Vertrauensverhältnis über einen längeren Zeitraum aufgebaut stehen dem Angreifer, im Gegensatz zu klassischem Phishing, viele Optionen mit großer Erfolgsaussicht offen, so z.B.:

- Einschleusen von Schadware

- Gerne wird das Opfer für den E-Mail-Anhang von seinem vermeintlichen Freund sogar die Sicherheitsfeatures seines Computers deaktivieren.
- Auch das Einschleusen manipulierter Hardware, aus geschäftlichen Gründen oder als Geschenk, z.B. Computerperipherie mit integrierter Abhörfunktion ist denkbar.
- Erhalten vertraulicher Informationen.
  - Der Angreifer kann mit genügend Detailwissen vorspiegeln er hätte die eintsprechende Sicherheitsstufe.
  - In das Unternehmen, auch in sicherheitskritische Bereiche, einladen lassen.
- Generell alle Optionen eines konspirativen Vorgehens deutlich erleichtert.

Wie nun die einzelnen Schritte der Manipulation aussehen könnten wird das folgende Kapitel an einem Praxisbeispiel erläutern:

## **2.6 Fallbeispiel: Angriff auf Unternehmensdaten**

Ziel dieses Beispiels ist es aufzuzeigen, wie ein Angreifer des Typs "Social Engineer" (vgl. Kevin Mitnick) sich, unter Anwendung von Spear-Phishing auf soziale Netze, das Vertrauen des Projektleiters eines mittelständischen Unternehmens erschleichen könnte.

### *2.6.1 Suchen von Mitarbeiternamen*

Der Angreifer bedient sich verschiedener Methoden um an Namen der Mitarbeiter der Zielfirma zu kommen. Am simpelsten und oft auch sehr erfolgreich, ist eine Suche auf der Firmenhomepage. Zumindest bis zur Abteilungsleiterenebene lassen sich die Namen bei den meisten Firmen, z.B. in Organigrammen finden. Auch die Suche in Personensuchmaschinen wie yasni.de kann schnell Erfolge bringen.

Eine weitere, zunächst abstrus klingende Methode, ist das "Garbage can diving"<sup>1</sup>. Bei dieser Methode werden die Mülleimer des Unternehmens nach interessanten Dokumenten wie Rechnungen, Abteilungspräsentationen, Mitarbeiter oder Inventarlisten durchwühlt. Viele der dabei gefundenen, zunächst uninteressant erscheinenden Dokumente, können im weiteren Verlauf des Angriffs genutzt werden um durch Kenntnis von Firmeninterna Vertrauen aufzubauen.

In diesem Beispiel gehen die Autoren davon aus dass der Angreifer ca. 10 relevante Mitarbeiternamen gefunden hat.

1. Mitnick, Kevin et al., Die Kunst der Täuschung, Mitp-Verlag, 2006

### 2.6.2 Recherche in Businessnetzen

Die im vorherigen Schritt gefundenen Namen werden nun in XING, linkedin oder anderen Businessnetzen weiter recherchiert. Hierbei werden zu vier Mitarbeitern und einem ehemaligen Mitarbeiter verwertbare Daten ermittelt. Darüber hinaus findet der Angreifer auch Informationen zu Produkten der angegriffenen Firma.

Der Angreifer intensiviert nun die Suche nach diesen fünf relevanten Personen. Dadurch gelingt es ihm die Position von zwei Mitarbeitern im Unternehmen zu ermitteln.

Die Menge der "nutzbaren Opfer" hat sich bereits auf folgende Personen deutlich verringert:

- *Mitarbeiter 1* aus dem Marketing
- *Mitarbeiter 3* aus der Qualitätssicherung
- Der *ehemalige Mitarbeiter*

Der Angreifer beschließt den eigentlichen Angriff mit diesen "Opfern" durchzuführen und geht in die aktive Phase des Angriffs über.

### 2.6.3 "Gefälschte" Profilseite erstellen

Der Angreifer meldet sich, natürlich mit gefälschten Daten, in dem sozialen Netzwerk an, in dem die Mitarbeiter des Zielunternehmens aktiv sind. Er gibt sich selbst ebenfalls als Abteilungsleiter eines mittelgroßen Unternehmens aus und täuscht Interesse an einem Produkt der Zielfirma vor. Dafür kontaktiert er den *MA 1* aus dem Marketing.

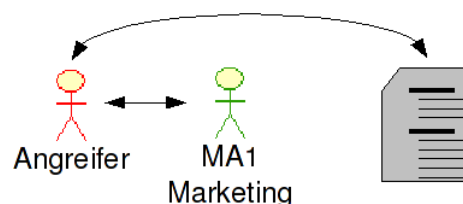


Abbildung 5. Zugriff auf die Profilseite des Marketing-Mitarbeiters

Der Marketing-Mitarbeiter akzeptiert den Kontakt, somit hat der Angreifer Zugriff auf sein komplettes soziales Netz.

### 2.6.4 Recherche im Netz des angegriffenen

Nun durchforscht der Angreifer das soziale Netz des *MA 1*, d.h. dessen Kontakte, Gruppen, Werdegang, ...

Hierbei stößt er auf die Namen von zwei ehemaligen Mitarbeitern, die noch keine Profilseite in diesem sozialen Netzwerk haben. Der Angreifer beschließt, zusätzlich zu seiner bereits (gefälschten) Identität, eine weitere Identität aufzubauen. Um diese Identität auch plausibel imitieren zu können

benötigt der Angreifer jedoch viele Informationen über die Person, die er nachahmen will.

Daher startet er eine weitere Internetrecherche nach den beiden gefundenen ehemaligen Mitarbeitern. Zu Einem, der anscheinend sehr aktiv im Internet ist, finden sich viele persönliche Informationen und Fotos, zum Zweiten eher weniger. Daher erstellt er einen weiteren gefälschten Account im Namen des "ergiebigeren" ehemaligen MA.

Nun verfügt der Angreifer bereits über zwei gefälschte Identitäten; die des interessierten Kunden und, die des ersten ehemaligen Mitarbeiters.

Unter der gerade gefälschten Identität nimmt der Angreifer Kontakt mit dem ganz zu Anfang gefundenen ehemaligen Mitarbeiters 1 auf und tauscht sich ein wenig mit diesem aus. Als Gesprächsansatz verwendet er z.B. "Hallo, du hast ja auch mal bei <Zielfirma> gearbeitet". Er wird sofort akzeptiert und hat Zugriff auf ein weiteres Netzwerk. Es fällt dem Angreifer mit den bisher ermittelten Informationen auch leicht das Vertrauen des ehemaligen MA 1 zu gewinnen und an erste Firmeninterna zu gelangen, z.B. durch "Lästern" über vermeintliche gemeinsame Ex-Kollegen oder Kunden.

### 2.6.5 Das Lügennetzwerk

Parallel dazu pflegt der Angreifer auch die Kontakte zu dem Marketingmitarbeiter. Hierbei dienen ihm der "Gefakte" ehemalige MA 2 und der ehemalige MA 1, zu dem er mittlerweile ein Vertrauensverhältnis aufgebaut hat, als Referenzen und "Leumund". Dadurch wirkt der Angreifer vertrauenswürdig, er kann ja sogar seine Aussagen durch den ehemaligen MA 2, selbst bestätigen.

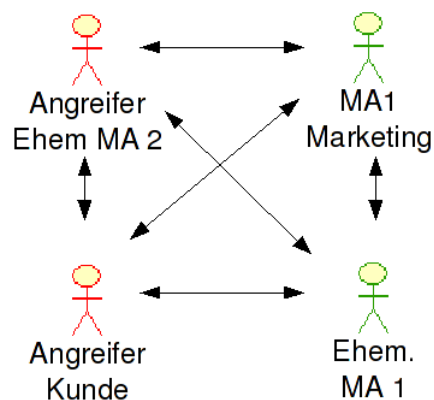


Abbildung 6. Das entstandene Beziehungsgeflecht

Der Angreifer ist nun in einer hervorragenden Ausgangslage für weitere Manipulationen oder Infiltrationen auf die Firma. So kann er z.B. "trojani-

sierte“ Anfragen oder Anforderungskataloge schicken, die Mitarbeiter telefonisch aushorchen oder als vertrauenswürdiger Kunde (er ist ja mittlerweile bei ehemaligen Mitarbeitern persönlich bekannt und Freund des Marketings) das Unternehmen besuchen und höchstwahrscheinlich auch Sicherheitsbereiche betreten.

### 3 FAZIT

An dieser Stelle muss festgehalten werden, dass die meisten der angesprochenen Probleme und Angriffsvektoren leicht zu entschärfen sind, wenn es gelänge das Sicherheitsbewusstsein allgemein zu steigern. Hier sind besonders die aktuellen und zukünftigen IT-Schaffenden und Informatiker gefragt andere Menschen aufzuklären und gegen Leichtgläubigkeit und blindes Vertrauen vorzugehen.

Auch sollten, vor Allem die Nutzer sozialer Netze, sogenannte “Internetfreunde” relativieren und nüchtern betrachten wie gut sie Jemanden, dem sie noch nie gegenüberstanden, wirklich kennen.

Gegen die in dieser Arbeit angesprochenen Gefahren *können* technische Schutzmaßnahmen wie z.B. Firewalls oder Schadsoftwarescanner helfen, jedoch müssen sie auch konsequent eingesetzt und gar erzwungen werden. Jedoch hilft auch die beste technische Schutzmaßnahme nichts wenn die daran sitzende Person nicht genügend sensibilisiert ist.

Abschließend möchten die Autoren noch erwähnen, dass einmal in Netzwerke “entlassene” Informationen für immer “verloren” sind und sich oft niemals vollständig wieder entfernen lassen. Daher muss Jeder selbst genau prüfen was die potenziell böswillige Welt wirklich über Einen wissen muss.

## QUELLEN

- [Birk et al., 2008] "Social Hacking", Dominik Birk, Felix Göbert, Christoph Wegener, iX 9/2008
- [Barnitzke, 2008] "Spionage 2.0: Social Networks abschalten?", Arin Barnitzke, EMC ON Sommer/Herbst 2008
- [Willhalm, 2008] "Script: Informationssicherheit in der Praxis", Matthias Willhalm, Hochschule Furtwangen WS08/09
- [Mitnick, 2006] "Die Kunst der Täuschung", Kevin Mitnick, William Simon, Mitp-Verlag, 2006
- [Jones et al., 2005] "Facebook: Threats to Privacy", Jones, Harvey, Soltren, Jose Hiram, Massachusetts Institute of Technology, 14.12.2005
- [ecin.de, 2008] "Sicherheitsrisiken durch Web 2.0 am Arbeitsplatz", <http://www.ecin.de/news/2008/07/17/12138/>, 14.11.2008
- [Zschunke, 2008] "'Stasi' im Internet", Peter Zschunke, <http://www.heute.de/ZDFheute/inhalt/22/0,3672,7150486,00.html>, 15.11.2008
- [Perez, 2007] "Facebook's Beacon More Intrusive Than Previously Thought", Juan Carlos Perez, PC World, 30.11.2007
- [n24.de, 2008] "Hintergrund: Telekom-Bespitzelung kein Einzelfall", [http://www.n24.de/news/newsitem\\_943400.html](http://www.n24.de/news/newsitem_943400.html), 31.05.2008
- [bild.de, 2008] "Skandal um CDU-Jungpolitiker", Olaf Schiel, <http://www.bild.de/BILD/hamburg/aktuell/2008/03/20/skandal-um-cdu-jungpolitiker/er-hetzt-gegen-auslaender.html>, 20.03.2008
- [facebook.com, 2009] "Memory of Stefanie Rengel", <http://de-de.facebook.com/group.php?gid=24342540224>, 20.01.2009
- [citynews.ca, 2009] "Funeral Held For Slain Teen Stefanie Rengel", [http://www.citynews.ca/news/news\\_18304.aspx](http://www.citynews.ca/news/news_18304.aspx), 20.01.2009
- [digitaljournal.com, 2009] "Angry Facebook Users Illegally Leaked the Names of Accused Underage Murderers", [http://www.digitaljournal.com/article/248379/Angry\\_Facebook\\_Users\\_Illegally\\_Leaked\\_the\\_Names\\_of\\_Accused\\_Underage\\_Murderers](http://www.digitaljournal.com/article/248379/Angry_Facebook_Users_Illegally_Leaked_the_Names_of_Accused_Underage_Murderers), 20.01.2009

## DANKSAGUNGEN

Die Autoren danken hiermit den folgenden Personen:

- Kevin Mitnick für die Inspiration durch sein Werk "Die Kunst der Täuschung"
- Prof. Dr. Reich für die IEEE Vorlage