Soziale Netzwerke: Wer, wo, wann, mit wem und warum?

Frank Innerhofer-Oberperfler

Zusammenfassung

Soziale Netzwerke gewinnen weiterhin an Bedeutung, nicht nur für die Kommunikation von Privatpersonen, sondern auch in zunehmendem Maße im geschäftlichen Umfeld von Unternehmen. Neue Soziale Netzwerke entstehen laufend und erreichen teils in kürzester Zeit Nutzerzahlen in Millionenhöhe. Kaum ein Netzwerk finanziert sich jedoch direkt über Zahlungen der Nutzer, sondern meist indirekt durch den Verkauf zielgerichteter Werbung. Somit sind die Daten der Nutzer das eigentliche Kapital dieser Netzwerke. Im Beitrag werden Strategien und technische Ansätze der Sozialen Netzwerke zu einer möglichst umfassenden Datensammlung über Nutzer aufgezeigt. Insbesondere wird anhand von Beispielen auf Risiken eingegangen, die sich aus neueren Entwicklungen und durch die zunehmende Verknüpfung Sozialer Netzwerke ergeben.

Nutzen und Risiken sozialer Netzwerke

Unter einem Sozialen Netzwerk versteht man eine „*im Zuge des Web 2.0 entstandene, virtuelle Gemeinschaft, über die soziale Beziehungen via Internet gepflegt werden können*“ (Gabler Verlag 2012, Stichwort „Soziales Netzwerk“). Soziale Netzwerke bieten als Kommunikationsplattform einzigartige Möglichkeiten für Personen und Unternehmen. Als Person kann man bestehende Kontakte pflegen, alte Kontakte wiederherstellen, sich mitteilen, austauschen und über aktuelle Trends informieren. Für viele jüngere Anwender haben Soziale Netzwerke bereits Kommunikationskanäle wie E-Mail abgelöst.

Zunehmend erkennen auch Unternehmen die Potenziale und Möglichkeiten, die sich durch diese Plattformen ergeben. Man denke nur an die Erreichbarkeit unzähliger potenzieller Endverbraucher, zukünftiger Mitarbeiter und die Pflege bereits bestehender Kontakte. Gerade für kleinere und mittlere Unternehmen bieten Soziale Netzwerke bei richtiger Nutzung ein vergleichsweise günstiges, aber doch sehr mächtiges Instrument der Vermarktung.

Die vielfältigen Chancen Sozialer Netzwerke lassen es kaum zu, diesen Kommunikationskanal sowohl als Unternehmen als auch als Privatperson ungenutzt zu lassen. Es ist jedoch essenziell, laufend aktuelle Trends und Entwicklungen im Auge zu behalten, um sich der ebenso vielfältigen Bedrohungen und Risiken bewusst zu sein. Im vorliegenden Beitrag wird auf den unersättlichen Datenhunger der Sozialen Netzwerke eingegangen und aufgezeigt, mit welchen Methoden die Anbieter von Sozialen Netzwerken versuchen, immer mehr Daten über die Nutzer zu erlangen.

Daten: Das Kapital der Sozialen Netzwerke

Die Daten und Kontakte der Nutzer und eine möglichst umfassende Aufzeichnung von deren Verhalten sind das Kapital der Sozialen Netzwerke. Der primäre Pfeiler der Geschäftsmodelle Sozialer Netzwerke ist bis dato immer noch der Verkauf möglichst zielgerichteter Werbung. Es geht also darum, möglichst genau zu verstehen, wer was wann mit wem und warum macht, um diese Information gewinnbringend an Werbetreibende zu verkaufen. Zudem fahren die Sozialen Netzwerke eine Reihe von Strategien, um auch außerhalb ihrer originären Plattform an Daten über Nutzer und deren Verhalten zu gelangen. Dies betrifft auch Nutzer, die in den Netzwerken bis dato nie ein Konto angelegt haben. Nachfolgend werden einige der Tricks, Praktiken und Strategien beschrieben, mit deren Hilfe die Sozialen Netzwerke mehr oder weniger seriös nach Daten fischen. Untermauert werden diese Ansätze durch Beispiele.

Digitale Dorfplätze

Soziale Netzwerke zeichnen naturgemäß bereits eine Unmenge an Daten über ihre Nutzer auf, die sich durch die Anwendungsfälle und die technische Umsetzung der Plattform selbst bereits ergeben. Dies beginnt mit Nutzungsdaten, wie beispielsweise um welche Uhrzeit sich jemand in ein Soziales Netzwerk einloggt und wie lange er sich dort aktiv aufhält. Es wird protokolliert, von welchen Endgeräten aus man auf die Netzwerke zugreift. IP-Adressen (Internet-Protokoll-Adresse) und damit der jeweilige Internet-Service-Provider inkl. Standort werden ebenfalls mitprotokolliert.

Der Grundpfeiler Sozialer Netzwerke ist die soziale Vernetzung. Damit spiegelt sich in den Datenbeständen zwingenderweise ein wesentlicher Teil der sozialen Beziehungen der Anwender wider. Über die Qualität und den Umfang der sozialen Beziehungen hinaus lassen sich auch Rückschlüsse auf die Interessen der Anwender ziehen. Welche anderen Personen oder Profile werden häufiger angesurft? Interessiere ich mich für bestimmte Themen eher als für andere? Welche Links, Aussagen, Fotos oder Videos werden von mir eher empfohlen als andere? Mit wem unterhalte ich mich regelmäßig, in welchen Abständen, wie umfangreich?

All diese Daten entstehen allein dadurch, dass man ein bestimmtes Netzwerk nutzt. Man bezahlt sozusagen die Nutzung der Plattform mit der Bereitstellung dieser persönlichen Daten. Allein die Daten, die im jeweiligen Netzwerk selbst anfallen, erlauben schon die Erstellung eines umfassenden Profils der Anwender. Genau diese Profile ermöglichen den Verkauf zielgerichteter Werbung. Je zielgerichteter die Werbung, umso eher kauft ein Anwender. Eine Werbung, die eher zu einem Kauf führt, kann teurer verkauft werden. Damit erklärt sich der unersättliche Datenhunger der Sozialen Netzwerke.

Auswerfen immer größerer Netze

Wie können die Sozialen Netzwerke nun an noch mehr Daten der Anwender kommen? Eine Möglichkeit ist, innerhalb der Sozialen Netzwerke mehr Daten zu generieren. Dies geschieht, indem die Anwender dazu animiert werden, mehr Zeit auf Sozialen Netzwerken zu verbringen

und noch mehr Aktivitäten dorthin zu verlagern. Die andere Möglichkeit ist, nicht nur im eigenen Teich zu fischen, sondern größere Netze auszuwerfen und auch in fremden Gewässern zu fischen. Für die Sozialen Netzwerke bietet sich ein solches schier unerschöpfliches Datenreservoir in Form des Surfverhaltens im klassischen World Wide Web.

Zu wissen, wer auf welche Webseiten surft und sich dort wie lange aufhält, erlaubt, das bereits bestehende Bild der Anwender um viele zusätzliche Facetten zu erweitern. Interessiert sich jemand vor allem für Politik und Wirtschaft oder eher für Kunst und Kultur? Werden aktuell sehr häufig Informationen über Reiseziele und Flugpreise eingeholt? Es ist keine Frage, dass diese Informationen gerade im Hinblick auf zielgerichtete Werbung sehr wertvoll sind.

Die Herausforderung der Sozialen Netzwerke aus technischer Sicht besteht darin, dieses Surfverhalten aufzuzeichnen. Diese Webseiten liegen auf Servern anderer Provider und sind nicht unter der Kontrolle der Sozialen Netzwerke. Prinzipiell ist für die Sozialen Netzwerke also nur nachvollziehbar, wohin jemand surft, wenn der Anwender einen Link zu einer Webseite direkt aus dem Sozialen Netzwerk heraus aufruft. Um zu protokollieren, wohin sich Anwender dann bewegen, müsste das jeweilige Soziale Netzwerk eine Art Sensor auf diesen Webseiten platzieren.

Technisch umgesetzt werden kann so eine Art Sensor, indem auf Webseiten ein Codeschnipsel eingebaut wird, der beim Besuch nicht nur Daten vom Webserver der jeweiligen Webseite liefert, sondern auch Daten vom Webserver des Sozialen Netzwerks bezieht. Kombiniert mit einem Cookie[1], das auf dem Rechner des Anwenders abgelegt ist, kann damit vom Sozialen Netzwerk protokolliert werden, dass ein Besuch stattfindet und auch von wem (vgl. Schneider 2011). Realisiert wurde dieser Sensor in Form der sogenannten Like-Buttons im Fall von Facebook oder Tweet-Buttons im Fall von Twitter. Diese Social-Media-Buttons sind mittlerweile massenhaft im Web verbreitet und in den letzten Monaten auch stark in Diskussion gekommen aus Sicht des Datenschutzes.

Den Sozialen Netzwerken wird dadurch die Möglichkeit geboten, Surf-Verhalten von Nutzern aufzuzeichnen, wie es bis dato eigentlich nur klassischen Werbenetzwerken und Suchmaschinenbetreibern wie Google möglich war. Der Konflikt zwischen dem deutschen Heise Verlag und Facebook (vgl. Schmidt 2011), der sich im September 2011 zugespitzt hat, zeigt, wie elementar diese Datenquellen für die Sozialen Netzwerke sind.

Warum werden so viele Like-Buttons dann freiwillig von Webseiten-Betreibern platziert? Man schafft damit die Möglichkeit, dass Besucher einer Webseite diese sogleich empfehlen können und damit sämtliche ihrer Kontakte im Sozialen Netzwerk weiterleiten. Dies generiert zusätzliche Besucher, was wiederum für die Webseiten-Betreiber elementar ist.

---

[1] Unter einem Cookie versteht man in „einer Datei auf einem lokalen Rechner abgelegte Daten einer Website, die den Anwender, der an diesem Rechner das World Wide Web nutzt, eindeutig identifizieren und Informationen über sein Surf-Verhalten speichern können“ (Gabler Verlag 2011, Stichwort „Cookie“).

Social Engineering und zu viel Vertrauen

Eine weitere Angel, die von fast allen Sozialen Netzwerken ausgeworfen wird, um an Daten zu kommen, ist die Möglichkeit, sein gesamtes Adressbuch hochzuladen um mögliche Freunde zu finden. Dieses „Feature" wird durch Methoden beworben, die fast schon an Social Engineering[2] erinnern: „Diese und jene Freunde haben das bereits genutzt, um Freunde zu finden!" Kombiniert mit einem zu hohen Maß an Vertrauen, das dem Sozialen Netzwerk entgegengebracht wird, gibt es unschöne Beispiele von leichtfertigem Umgang mit Adressdaten beispielsweise durch Ärzte, Rechtsanwälte und andere Berufsgruppen.

Über das eigene Adressbuch hinaus liefert der Nutzer damit den Netzwerken auch Daten über Personen, die bisher noch nie ein Konto auf solchen Netzwerken angelegt haben. Diese Personen können sodann von den Sozialen Netzwerken aktiv angeschrieben und als neue Anwender beworben werden. Man wirbt dann praktischerweise damit, dass diese oder jene Freunde ja ebenfalls schon Mitglieder des Netzwerks sind.

Es sollte sich also niemand wundern, warum dieses oder jenes soziale Netzwerk jemanden direkt anschreiben kann und woher diese Adressen stammen. Ebenso wenig sollte man sich der Illusion hingeben, man könne irgendwelche aktiv genutzten E-Mail-Adressen vor diesen Netzwerken verheimlichen. Hat man jemals mit irgendjemandem oder gar mehreren Personen über eine solche E-Mail-Adresse kommuniziert, so kann man sich ziemlich sicher sein, dass zumindest einer dieser Kontakte sein Adressbuch einem Sozialen Netzwerk zur Verfügung gestellt hat und damit natürlich auch diese E-Mail-Adresse.

Dass Soziale Netzwerke hierbei teils wenig zimperlich vorgehen, zeigt der Skandal, der sich rund um das Soziale Netzwerk Path Anfang 2012 abgespielt hat (vgl. N.N. (2012): „Netzwerk Path greift Nutzer-Adressbuch ab"). Ohne die explizite Zustimmung der Anwender einzuholen wurde bei Installation der entsprechenden App auf einem iPhone direkt das gesamte Adressbuch des Anwenders „raubkopiert". Nachdem das von einem Nutzer des Sozialen Netzwerks erkannt wurde und nach einem Sturm der Entrüstung, wurden diese Daten nicht mehr im Klartext übertragen. Man begnügt sich mittlerweile mit einem Hashwert, der zur Identifikation bereits bestehender Kontakte verwendet wird. Für das Soziale Netzwerk Path dürfte sich dieser Raubzug trotz der negativen Presse gelohnt haben.

Zunehmende Verknüpfung Sozialer Netzwerke

Bedingt durch die Vielzahl diverser Sozialer Netzwerke, in denen User und auch Unternehmen aktiv sind, entsteht der Bedarf, diese möglichst einfach und über einen einzigen Zugang zu nutzen. Dieser Trend spiegelt sich in einer fortschreitenden Integration zwischen Sozialen

[2] Unter Social Engineering versteht man „zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhalten hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen" (Wikipedia 2012).

Netzwerken wider. So ist es möglich, Statusmeldungen auf Facebook direkt an Twitter weiterzuleiten bzw. umgekehrt. Für Anwender ergeben sich daraus einige potenzielle Fallstricke.

So ist es durch diese Verknüpfung der Sozialen Netzwerke zunehmend schwieriger, berufliche und private Aktivitäten auf Sozialen Netzwerken zu trennen. Für die Anwender ist durch eine Verknüpfung der Sozialen Netzwerke häufig nicht mehr klar und transparent nachvollziehbar, welche Wege eine Statusmeldung dann letztendlich einnimmt und über welche Netzwerke diese zusätzlich verteilt wird. Nicht immer soll eine private Statusmeldung, die über Twitter verbreitet wird, ihren Weg direkt in ein berufliches Netzwerk wie beispielsweise LinkedIn finden.

Ein weiterer oft nicht erkannter Aspekt ist der weitgehende Zugriff und Datenabgleich, der zwischen den verknüpften Netzwerken stattfindet. Automatisch werden bei einer solchen Verknüpfung sämtliche Kontakte abgeglichen und auch die bisherige Kommunikationshistorie steht weiteren Netzwerken zur Verfügung. So wird häufig überrascht festgestellt, dass ein bestimmtes Soziales Netzwerk wie beispielsweise Windows Live plötzlich sämtliche Geburtsdaten der eigenen Kontakte aus Facebook kennt.

Findet eine solche Verknüpfung von Sozialen Netzwerken auf einem PC oder über eine Weboberfläche statt, so werden zumeist mindestens einmal explizit diese Zugriffsrechte dem Anwender zur Zustimmung und Bestätigung vorgelegt. Findet die Verknüpfung hingegen auf mobilen Endgeräten statt, so ist dieser Prozess weitgehend intransparent und eine Zustimmung wird teilweise gar nicht direkt eingeholt. Der Datenabgleich findet dennoch statt.

Mobil in Sozialen Netzwerken – Ortung inbegriffen

Für die Sozialen Netzwerke ergeben sich durch den Zugriff über mobile Endgeräte weit mehr mögliche Datenspuren über die Anwender als etwa durch den Zugriff über einen Stand-PC. Sämtliche Soziale Netzwerke verlangen bei Installation einer entsprechenden App auf einem mobilen Endgerät Zugriff auf Ortungsinformationen. Dies mag für einzelne Anwendungsfälle durchaus sinnvoll und notwendig sein, für den Großteil der Anwendungsszenarien ist die geografische Ortsangabe jedoch nicht zwingend erforderlich.

Für die Sozialen Netzwerke sind geografische Ortsangaben ein wichtiges zusätzliches Datum, um ortsbezogene Werbung zu verteilen. Das Wissen, ob ein Anwender sehr viel reist bzw. sehr mobil ist und wohin dessen Wege führen, lässt weitere wichtige Rückschlüsse auf die Person und auch auf das mögliche Einkommen zu. Über die Zeit ergeben sich auch sehr umfangreiche Bewegungsprofile. Vor allem trifft dies auf mobile Endgeräte zu, in die Soziale Netzwerke bereits eng in das Betriebssystem integriert wurden, wie beispielsweise Windows Phone 7.5 Mango.

Integration in bestehende Plattformen

Die Integration der Sozialen Netzwerke beschränkt sich nicht nur auf mobile Endgeräte bzw. deren Betriebssysteme. In den letzten Monaten hat sich dieser Trend auf eine Reihe von zusätz-

lichen Plattformen und Anwendungen ausgedehnt. Der Hintergrund dürfte klar sein. Es handelt sich auch hierbei um ein Fischen in fremden Gewässern. Schafft es ein Soziales Netzwerk, seine Anwender zu motivieren, weitere Anwendungen zu verknüpfen, so wird auch das entsprechende Anwendungsverhalten inklusive Kontaktdaten und Kommunikationsverlauf für das Soziale Netzwerk verfügbar gemacht.

Ein Beispiel für eine solche Integration in bestehende Plattformen ist die Integration von Facebook in den Skype Client. Aus dem Skype Client heraus können Chatsessions und auch Videokonferenzen direkt mit Facebook-Kontakten geführt werden. Abgesehen davon, dass sich durch eine solche Integration zusätzliche potenzielle Sicherheitslücken auftun, ist immer auch der damit preisgegebene Datenschatz zu beurteilen. Darüber hinaus entwickeln sich die Sozialen Netzwerke durch diese Ausbreitung mehr und mehr zu zentralen Plattformen, über die sämtliche Nutzeraktivitäten ablaufen.

Ein weiteres Beispiel ist die Integration von Sozialen Netzwerken wie LinkedIn, XING und Facebook in Microsoft Outlook über den Outlook Social Connector. Laut den entsprechenden Datenschutzbestimmungen werden zwar keine E-Mail-Adressen im Klartext an das jeweilige Soziale Netzwerk übertragen, sondern nur Hashwerte der lokalen E-Mail-Adressen mit den Hashwerten der im Netzwerk bereits bekannten Teilnehmer verglichen. Somit kommt es zumindest in der Theorie nicht zu einem automatischen Abgleich des Adressbuchs.

Was jedoch praktisch damit wiederum preisgegeben wird, ist ein extrem umfassendes Kommunikationsprofil des Anwenders. Wird eine E-Mail in Outlook geöffnet, so werden in diesem Moment sämtliche E-Mail-Adressen in den TO- und CC-Feldern als Hashwerte an das Soziale Netzwerk übertragen. Ist einer dieser Adressaten bereits Mitglied des Sozialen Netzwerks – nicht mal zwingend ein Kontakt des Anwenders –, so werden das aktuelle Foto und die letzten Statusmeldungen an Outlook zurückübermittelt. Für das Soziale Netzwerk ist damit nachvollziehbar, wann der Nutzer welche E-Mails von welchen Kontaktpersonen geöffnet hat.

Erste Analysen deuten darauf hin, dass hier wiederum nicht nur die aktuell geöffnete E-Mail übertragen wird, sondern im Hintergrund sämtliche TO- und CC-Kontaktadressen des gesamten E-Mail-Bestands auf bestehende Mitglieder des Sozialen Netzwerks hin überprüft werden.

Soziale Netzwerke als Torwächter

Ein Trend, der sich ebenfalls erst in den letzten Monaten erkennbar abgezeichnet hat, ist eine weitere sehr effektive Strategie der Sozialen Netzwerke, um an noch mehr Information und Daten der Anwender zu gelangen. Soziale Netzwerke bieten Webseiten die Möglichkeit an, deren Anwender direkt über einen Login-Button zu authentifizieren. Diese sogenannten Facebook- und Twitter-Logins erlauben es, sich in eine Webseite einzuloggen, ohne extra einen neuen Benutzernamen und ein neues Passwort zu erstellen. Zweifelsohne bequem für die Anwender, der Preis für diese Bequemlichkeit ist jedoch wiederum die Preisgabe weiteren Nutzungsverhaltens.

Besonders perfide stellt sich dieser Ansatz dar, wenn bei bestimmten Webseiten oder Plattformen nur mehr ein Login über beispielsweise Facebook oder Twitter möglich ist. Damit wird ein solches Konto zwingend vorausgesetzt, andernfalls kann eine Anwendung gar nicht mehr genützt werden. Prominentes Beispiel einer solchen Symbiose ist die Musikstreamingplattform Spotify, die in Österreich Mitte November 2011 in den Markt getreten ist. Eine Anmeldung für Spotify ist ausschließlich über Facebook möglich. Ohne Facebook kein Spotify. Auch hier wird wiederum umfassendes Datenmaterial generiert. Wer hört wann welche Musik?

Diese Informationen werden auch in der Standardeinstellung laufend automatisch als Statusmeldung den entsprechenden Kontakten und Freunden mitgeteilt. Damit kommen die Sozialen Netzwerke ihrem Ziel, möglichst umfassend das Verhalten der Nutzer aufzuzeichnen und auch mitzuteilen, einen bedeutenden Schritt näher.

Ausblick

An der Nutzung Sozialer Netzwerke und der Entwicklung einer entsprechenden Strategie werden kaum ein Individuum und auch ein Unternehmen vorbeikommen. Aus der rasanten Weiterentwicklung der Sozialen Netzwerke und der zunehmenden Integration in bestehende Plattformen ergeben sich laufend neue Chancen, aber auch Risiken. Vor allem in Hinblick auf den Umgang mit den Daten der Anwender hat sich in den letzten Jahren zunehmend eine begrüßenswerte kritische Diskussion entwickelt (vgl. Adamek 2011; Janson 2011), die seitens der Sozialen Netzwerke auch bereits zu ersten Verbesserungen geführt hat. Hervorzuheben ist in diesem Zusammenhang einerseits die Auseinandersetzung Wiener Studenten mit der irischen Niederlassung von Facebook (vgl. Europe vs. Facebook 2012). Andererseits ist gerade durch Datenschutzbehörden in Deutschland, hier im Besonderen aus Schleswig-Holstein, starker Druck in Richtung stärkeren Datenschutzes bei Sozialen Netzwerken aufgebaut worden (vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein 2012).

Literatur

Adamek, Sascha (2011): *Die Facebook-Falle. Wie das soziale Netzwerk unser Leben verkauft*. München: Heyne Verlag.

N.N. (08.02.2012): *Netzwerk Path greift Nutzer-Adressbuch ab*. Hamburg: ZEIT ONLINE. Abgerufen unter: http://www.zeit.de/digital/datenschutz/2012-02/internet-netzwerk-path-datenschutz [Stand vom 31.03.2012]

Janson, Simone (2011): *Nackt im Netz*. München: Redline Verlag.

Schmidt, Jürgen (2011): *2 Klicks für mehr Datenschutz*. Abgerufen unter: http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html [Stand vom 31.03.2012].

Schneider, Christian (2011): *Tracking Performed by Social Networks*. Abgerufen unter: http://www.webappsecblog.com/TrackingBySocialNetworks.html [Stand vom 31.03.2012].

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2012): *Datenschutz in sozialen Netzwerken*. Abgerufen unter: https://www.datenschutzzentrum.de/internet/20111208-DK-B-Soziale-Netzwerke.html [Stand vom 12.06.2012].

Weblinks

Europe vs. Facebook. Abgerufen unter: http://europe-v-facebook.org/DE/de.html [Stand vom 31.03.2012]

Gabler Verlag (Hrsg.): *Gabler Wirtschaftslexikon, Stichwort: Soziales Netzwerk*. Abgerufen unter: http://wirtschaftslexikon.gabler.de/Definition/soziales-netzwerk.html [Stand vom 12.06.2012].

Gabler Verlag (Hrsg.): *Gabler Wirtschaftslexikon, Stichwort: Cookie*. Abgerufen unter: http://wirtschaftslexikon.gabler.de/Archiv/81877/cookie-v7.html [Stand vom 12.06.2012].

Wikipedia (2012): *Social Engineering (Sicherheit)*. Abgerufen unter: http://de.wikipedia.org/wiki/Social_Engineering_(Sicherheit) [Stand vom 12.06.2012].