Soziale Netzwerke im Internet

Status: Kommentare zur Berichterstattung „Monitor“, am 20.05.10

Stand: **20/05/2010**

Autoren: Norbert Pohlmann, Marco Smiatek, Malte Woelky

Kontakt: Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit

Fachhochschule Gelsenkirchen
Fachbereich Informatik
Neidenburgerstr. 43
45877 Gelsenkirchen

Fon: 0209 / 9596 515 oder 0173 30 21 838

E-Mail: norbert.pohlmann@internet-sicherheit.de

Web: www.internet-sicherheit.de

1. Einleitung

Soziale Netzwerke wie Facebook, StudieVZ, XING, LinkedIn, usw. sind Mitmach-Webs. Das Mitmach-Web oder Web 2.0 ist unter anderem dadurch definiert, dass es keinen erkennbaren Unterschied mehr zwischen Nutzer und Autor von Informationen gibt. Ein Anbieter, wie z.B. Facebook, stellt lediglich die Infrastruktur mit ihren Diensten im Internet zur Verfügung und die Nutzer bearbeiten die Inhalte selbst. Der Betrieb einer Infrastruktur eines Sozialen Netzwerkes kostet bei großen Systemen mehrere Millionen Euro pro Jahr.

Die grundsätzliche Idee von Sozialen Netzwerken im Internet ist, dass die Nutzer persönliche Daten, wie Werdegang, Hobbys, Freunde, Vorlieben oder Bilder/Videos von Reisen und Partys, selber in das Soziale Netzwerk eingeben, mit dem Ziel, dass sich die Nutzer in verschiedener Art und Weise kennen lernen, miteinander vernetzen und interagieren.

Um beim Mitmach-Web richtig und angemessen agieren zu können, müssen die Nutzer aber die Ziele des Angebotes und die Regeln kennen.

Ein großes Problem sind die unterschiedlichen Ziele von Betreibern und Nutzern!

Der **Betreiber** eines Mitmach-Web, z.B. Facebook, hat das Ziel, **Werbung zu verkaufen,** um die Kosten für die IT-Infrastruktur zu decken und entsprechende Gewinne zu erwirtschaften. Die Werbeangebote werden zunehmend sehr individualisiert auf einzelne Personen zugeschnitten. Dafür benötigt der Betreiber so viele Informationen wie möglich über seine Nutzer, um möglichst präzise Profile über die Nutzer erstellen, die er dann verkaufen kann.

Der **Nutzer** auf der anderen Seite möchte sich z.B. in einem Sozialen Netzwerk **verwirklichen können**, aber unter Aufrechterhaltung der Sicherheit seiner Daten und des individuellen Levels der Privatsphäre.

Diese sehr unterschiedlichen Ziele des Betreibers und des Nutzers müssen klar und deutlich, auf jeden Fall sehr viel besser als bisher dargestellt werden. Außerdem müssen faire Mechanismen vorhanden sein, die beiden Seiten ermöglichen Ihr Ziel zufriedenstellend zu erreichen. Das ist insbesondere bei Sozialen Netzwerken eine große Herausforderung.

2. Rechte an Daten in Sozialen Netzwerken

Hier wird am Beispiel von Facebook erläutert, wie es mit den Rechten an Daten im Sozialen Netzwerk aussieht.

Rechtliche Voraussetzungen für das Hochladen von Daten

Nutzer dürfen nur Daten (Texte, Bilder, Musik, Videos, …) hochladen, wenn sie die Rechte daran besitzen, beziehungsweise die Inhalte selbst erstellt haben. Fotos, Videos, usw., auf denen Dritte, wie Freunde, Kollegen oder Nachbarn, gezeigt werden, dürfen nur mit vorheriger Zustimmung der entsprechenden Personen verwendet werden. Auch personenbezogene Daten von andern Nutzern (E-Mail und weitere Adressen, Geburtsdatum, usw.) dürfen nur mit der entsprechenden Zustimmung hochgeladen und weitergegeben werden.

Wem gehören rechtlich die Daten nach dem Hochladen

Der Nutzer behält selbstverständlich seine Rechte an den hochgeladenen Daten. Aber bei Facebook stimmt der Nutzer zu, dass Facebook diese Daten auch verwenden kann (… einfache, übertragbare, unterlizenzierbare, unentgeltliche, weltweite Lizenz für die Nutzung aller IP-Inhalte. – siehe Nutzungsbedingungen von Facebook).

3. Schutz der Daten in Sozialen Netzwerken

Wenn der Benutzer seine Daten in das Soziale Netzwerk eingestellt hat, ist er darauf angewiesen, dass der Betreiber, wie Facebook, für die Sicherheit der Daten und den Schutz der Privatsphäre sorgt.

Sicherheit der Daten während der Übertragung im Internet

Die Sicherheit der Daten wärend der Übertragung im/ins Internet wird in der Regel durch die Nutzung der SSL/TLS-Verschlüsselung zwischen dem Browser und den Webseiten des Sozialen Netzwerkes realisiert (siehe http://www.internet-sicherheit.de/institut/buch-sicher-im-internet/workshops-und-themen/verschluesselung-und-identitaeten/ssltls-verschluesselung/). Facebook unterstützt diese Technologie nach eigenen Angaben für das Passwort und für Kreditkarteninformationen (siehe Datenschutzrichtlinien von Facebook: http://www.facebook.com/terms.php?ref=pf#!/policy.php).

Forderung an die Betreiber:

Eine bessere, sichere und vertrauenswürdigere Lösung wäre sicherlich, dass alle Daten nur mit SSL/TLS-Verschlüsselung zwischen dem Browser des Nutzers und den Webseiten des Sozialen Netzwerkes ausgetauscht würden!

Sicherheit der Daten in der IT-Infrastruktur des Betreibers

Der Betreiber des Sozialen Netzwerkes speichert die Daten der Nutzer in seiner IT-Infrastruktur in der Regel in einer Datenbank. Der Betreiber sorgt dann über ein Regelwerk dafür, dass immer nur bestimmt Nutzer und Werbende auf Teile der Daten zugreifen dürfen. In Sozialen Netzwerken haben die Nutzer die Möglichkeit, über z.B. Privatsphäre-Einstellungen mit zu bestimmen, welche Daten andere sehen dürfen.

Die Einstellungsmöglichkeiten sind zum Teil sehr komplex und stellen einen hohen Aufwand für den Nutzer dar. Dieser ist aber notwendig, um den eigenen Bedürfnissen entsprechend die richtigen Privatsphäre-Einstellungen wählen zu können. Bei diesem Punkt werden die unterschiedlichen Ziele zwischen Betreiber und Nutzer deutlich! Der Betreiber möchte mit allen Daten uneingeschränkt arbeiten können, um möglichst viel Werbegeld einnehmen zu können. Der Nutzer möchte seine Daten und seine Privatsphäre optimal schützen, was dem Ziel des Betreibers im Prinzip entgegenwirkt!

Forderung an die Betreiber:

Die Betreiber sollten es den Benutzern sehr viel einfacher machen, die Konsequenzen der unterschiedlichen Einstellungen und deren Bedeutung für den Nutzer zu verstehen. Nur dann ist ein Nutzer in der Lage, seine für ihn persönlich richtige Einstellung vorzunehmen.

4. Auslesen von Adressdateien und E-Mail-Konten

Ein wichtiger Aspekt bei Sozialen Netzen ist der Wunsch der Nutzer sich mit anderen zu verbinden und eine Gruppe zu bilden. Der Nutzer hat hier die Möglichkeit bei Sozialen Netzwerken, wie auch bei Facebook, seine Freunde zu suchen und einen Verbindungswunsch zu äußern. Der Angefragte hat dann die Möglichkeit, diesem Wunsch zu entsprechen oder abzulehnen.

Die Betreiber von Sozialen Netzwerken bieten den Nutzern unterschiedliche Hilfestellungen an, dass Finden von Freunden (Kollegen, Geschäftspartner, Nachbarn, usw.) zu erleichtern.

Für den Nutzer besteht die Möglichkeit die Adressdatei aus seinem Mail-Client (Outlook, Live-Mail, Thunderbird, ...) oder direkt aus seinem E-Mail-Account dem Betreiber des Sozialen Netzwerkes zu Verfügung zu stellen. Dieser führt dann mit Hilfe von Softwareprogrammen eine automatische Suche bzw. einen Abgleich durch.

Was bedeuten diese Angebote für den Nutzer?

Um diesen Vorgang besser verstehen zu können, soll mit einer Analogie gearbeitet werden. In der Analogie ist ein Fitness-Studio mein Soziales Netzwerk: hier trainiere ich und habe soziale Kontakt zu anderen Menschen.

Weitergabe der Adressdatei des E-Mail-Clients des Nutzers

Eine Möglichkeit ist, dass der Nutzer eine Kopie der Adressdatei seines E-Mail-Programms, wie z.B. Outlook, an Facebook übergibt, damit Facebook einen Abgleich durchführen kann.

In der Analogie gebe ich einem Mitarbeiter des Fitness-Studios eine Kopie meines persönlichen Adressbuches und der schaut in der Mitgliederliste des Fitness-Studios nach, ob einer meiner Kontakte schon im Fitness-Studio ist und er lädt alle weiteren Kontakte aus meinem Adressbuch ein, im Fitness-Studio mitzumachen.

Probleme bei dieser Vorgehensweise:

- Im Outlook-Adressbuch stehen sehr viel mehr Informationen, als notwendig sind, um diese Aufgabe vorzunehmen. Im Adressbuch stehen neben dem Namen und der E-Mail-Adresse auch noch das Geburtsdatum, die Adresse, die Telefonnummer und Notizen, die ich über die Person gemacht habe (z.B. spielt im selben Tennisclub).
- Facebook lädt die anderen mit dem Hinweis ein, dass ich schon in Facebook bin. Diese Vorgenweise soll aus der Sicht von Facebook die Wahrscheinlichkeit erhöhen, dass derjenige sich entscheidet auch mitzumachen. Die Frage ist nur, ob ich das wirklich möchte.
- Was der Betreiber mit diesen Informationen sonst noch macht, ist nicht festgelegt!

Empfehlung

- Es sollte sorgfältig überlegt werden, ob dieser Dienst wirklich eine Hilfe ist?
- Wenn dieser Dienst genutzt wird, sollten auf jeden Fall alle nicht notwendigen Informationen vorher gelöscht werden!

Weitergabe der Zugangsdaten zu meinem E-Mail-Account.

Eine weitere Möglichkeit ist, dass ich Facebook die Anmeldeinformationen zu anderen Diensten, wie Skype, einem Instant Messenger oder einem E-Mail-Postfach zur Verfügung stelle und Facebook mit diesen Zugangsdaten unter meinem Namen diesen Dienst nutzt, um die Informationen auszulesen.

In der Analogie gebe ich jetzt einem Mitarbeiter des Fitness-Studios eine Kopie meines Schlüssels und bitte ihn, in meine Wohnung zu gehen, mein persönliches Adressbuch zu suchen, alle meine Briefe zu sichten und zu schauen, ob einer meiner Kontakte schon im Fitness-Studio ist. Alle Kontakte, die noch nicht im Fitness Studio sind, lädt Facebook dann ein.

Probleme bei dieser Vorgehensweise:

- In diesem Fall gebe ich Facebook meine Zugangsdaten für einen anderen Dienst. Da ich nicht nachvollziehen kann, was Facebook tatsächlich dort macht, gehe ich ein sehr großes Risiko ein.
- Facebook verspricht zwar den Nutzern in ihren Datenschutzrichtlinien „Wenn du vertrauliche Daten (wie z. B. Kreditkartennummern und Passwörter) eingibst, werden diese Informationen mithilfe der SSL-Technologie (Secure Socket Layer) von uns verschlüsselt.“. Leider hält sich Facebook nicht daran. Die Mitarbeiter des Instituts für Internet-Sicherheit haben bei der Bewertung einiger der hier besprochenen „Freunde finden“ Mechanismen festgestellt, dass Facebook die Anmeldeinformationen der anderen Dienste unverschlüsselt überträgt (siehe: www.internet-sicherheit.de).
- Was der Betreiber wirklich ausliest und was er mit diesen Informationen sonst noch macht, ist nicht festgelegt!

Empfehlung

- Dieser Dienst sollte auf keinen Fall genutzt werden, da ich dafür meine Zugangsdaten preisgeben muss und diese auch noch unverschlüsselt im Internet übertragen werden und somit von Dritten gelesen werden können!
- Falls Sie das schon gemacht haben, ändern Sie Ihr Passwort!

5. Die Zukunft von Sozialen Netzwerken

Wie können wir gemeinsam bei Sozialen Netzwerken eine zufriedenstellende, vertrauenswürdige und nachhaltige Lösung erzielen? Wir haben im Prinzip drei Parteien, die helfen müssen, den Umgang mit Sozialen Netzwerken zu verbessern.

1.) Der Staat

Der **Staat muss die passenden Gesetze umsetzen**, die unsere Daten und unsere Privatsphäre angemessen schützen. Dazu gehört, dass eindeutig klar sein muss, was erlaubt ist und was nicht. Hier werden wir sicherlich noch einiges lernen müssen, aber ein wichtiger Punkt ist, dass vorhandende Gesetze auch umgesetzt werden müssen! Zurzeit werden kaum Bußgelder an Betreiber von Sozialen Netzwerken vergeben, die sich nicht an die Gesetze halten.

Unsere Gesellschaft verändert sich mehr und mehr zur vernetzten Informations- und Wissensgesellschaft. Das ist von der Staatengemeinschaft gewollt und wird auf vielen Ebenen von dieser gefördert. Der Staat ist damit auch dafür verantwortlich, seine Bürger auf das gesellschaftliche Leben vorzubereiten und dazu gehört heute auch die positive Nutzung des Internets. Wir müssen uns als Gesellschaft überlegen, was wir in den Kindergärten, Schulen, Volkshochschulen, Universitäten sowie in Firmen unterstützend vermitteln wollen, damit wir als mündige Bürger unsere gesetzlich verankerte Selbstbestimmung auch eigenverantwortlich wahrnehmen können.

2.) Die Betreiber von Sozialen Netzwerken

Die Betreiber, die Soziale Netzwerke anbieten, müssen die IT-Infrastruktur so umsetzen, dass Sie unsere Daten sichern und unsere Privatsphäre angemessen schützen. Sätze wie „Ihre Privatsphäre ist uns wichtig“ reichen nicht aus! Die IT-Infrastruktur muss diese Ansprüche konsequent umsetzen. Das ist sicherlich aufwendiger, als sich das die Betreiber gedacht haben. Aber anders kann es langfristig nicht funktionieren! Hier ist noch einiges von der Betreibern zu tun! Wenn die Betreiber es nicht schaffen, ein Vertrauen zu den Nutzern aufzubauen, werden sie langfristig nicht erfolgreich sein!

Die Aufrechterhaltung der Sicherheit und der Privatsphäre ist ein kontinuierlicher Wettlauf mit den Angreifern, die immer neue Angriffsmodelle entwickeln. Identitäts-Diebstahl über Phishing-Mails oder Malware sind nur zwei Beispiele, die zurzeit immer bedeutsamer für Soziale Netzwerke werden.

3.) Der Nutzer

Der Nutzer eines Sozialen Netzwerkes muss eine Internet-Kompetenz aufbauen, die ihn befähigt, sich angemessen im Internet zu bewegen. Das ist sicherlich aufwendig und anstrengend für den Nutzer, es ist aber die einzige Möglichkeit, die Vorteile des Internets zu nutzen und die Risiken zu minimieren.

Was müssen wir als Internet-Nutzer tun?

Um unsere Daten und unsere Privatsphäre zu schützen, müssen wir unseren Computer vor Viren und Trojanern mit einem Anti-Malware-Programm und einer Personal Firewall ausstatten, bevor wir uns mit dem Internet verbinden. Automatische Updates zuzulassen, sehr gute Passworte zu verwenden und für jeden Internet-Dienst ein anderes zu wählen, sind weitere wichtige Voraussetzungen.

Wir müssen unseren gesunden Menschenverstand nutzen!

Wir sollten die Möglichkeiten des Schutzes der Privatsphäre in sozialen Netzwerken kennen und aktiv nutzen. Wenn ich zu einer Feier eingeladen werde, dann ist mir schnell klar, was ich anziehen muss. Zur Schulabschlussfeier meiner Kinder ziehe ich mich festlich an. Zur Geburtstagsfeier meines Nachbarn kann ich in T-Shirt und Jeans gehen. Ähnlich wie beim Dresscode muss ich eine Einschätzung in sozialen Netzen durchführen können. In ein Soziales Netzwerk für Business-Kontakte wie Xing werde ich ein seriöses Bild einstellen. Im sozialen Netzwerk meiner Stadt werde ich mich privat darstellen. Auch die Informationen, die ich anderen zur Verfügung stelle, muss ich in Abhängigkeit von den anderen Teilnehmern im Sozialen Netzwerk sorgfältig abwägen.

Ich muss sofort nach dem Beitritt zu einem Sozialen Netzwerk festlegen, wer auf mein Profil zugreifen darf. Zum Schutz der personenbezogenen Daten sollte ich die AGBs des Sozialen Netzwerk-Betreibers prüfen. Dabei ist zu beachten, ob Informationen an Dritte weitergegeben werden und besonders in welchem Ausmaß. Eine aktuelle Untersuchung der Stiftung Warentest hat ergeben, dass bei vielen sozialen Netzwerken großer Handlungsbedarf besteht, weil der Datenschutz als mangelhaft eingestuft wird.

Wir brauchen eine Internet-Kompetenz, in der wir lernen, sicher mit dem Internet umzugehen. Erst dann können wir das Potential, das das Internet bietet, voll ausschöpfen. Wir müssen für einen richtigen, bewussten Umgang geschult werden, das heißt, wir müssen die Regeln und richtigen Verhaltensweisen verinnerlichen, um die Risiken und Gefahren erkennen und abschätzen zu können.

Weitere Informationen zur Internet-Kompetenz siehe www.sicher-im-internet.de