Blaue Reihe

7

ULD

Soziale Netzwerke: Wo hört der Spaß auf?

Fragen und Antworten zu Facebook und Co.

Inhaltsverzeichnis

Impressum:
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98, 24103 Kiel, www.datenschutzzentrum.de
Ersteller: Henry Krasemann | Titelbild: Gerd Altmann / pixelio.de
Stand: Juni 2012

Was sind Soziale Netzwerke?

Soziale Netzwerke sind virtuelle Treffpunkte im Internet, die sich besonders bei jungen Menschen großer Beliebtheit erfreuen. Sie zeichnen sich u. a. durch folgende Merkmale aus:

- Nutzerinnen und Nutzer registrieren sich bei einem Internetdienst und geben dabei persönliche Informationen über sich zur Erstellung eines (oftmals öffentlichen) Profils an.
- Das eigene Profil kann mit Profilen anderer verbunden werden (z. B. als „Freundschaft").
- Mitglieder können miteinander kommunizieren und sich über gemeinsame Interessen austauschen.

Wie finanzieren sich soziale Netzwerke?

Kommerzielle soziale Netzwerke finanzieren sich in der Regel überwiegend durch Werbung und andere Formen der kommerziellen Verwertung der Daten ihrer Nutzerinnen und Nutzer. Hierbei werden oftmals sowohl die eingegebenen Daten verwendet, aber auch das Verhalten der Nutzerinnen und Nutzer im Netzwerk selbst ausgewertet (z. B. welche Inhalte angeklickt werden). Beides erlaubt Rückschlüsse auf die Nutzerinnen und Nutzer und ihre Interessen. Dies erlaubt wiederum zielgerichtete (Werbe-) Ansprache. Viele soziale Netzwerke behalten sich auch vor, Daten (was auch Informationen über die Interessen der Nutzer beinhaltet) direkt an Dritte zu verkaufen. Im günstigsten Fall sind davon „nur" (vermeintlich) anonymisierte Daten betroffen. Allerdings sind auch Fälle bekannt, bei denen das gesamte Netzwerk mit allen Daten verkauft wurde. Die meisten Netzwerke lassen sich dieses Recht in den Nutzungsbedingungen einräumen.

Soziale Netzwerke werden teilweise auch durch Geldgeber aus der Wirtschaft und anderen Organisationen (z. B. Geheimdiensten) mitfinanziert. Die damit verbundenen genauen Zwecke sind nicht

immer transparent.

Einige Netzwerke finanzieren sich zumindest zum Teil über (optionale) Mitgliederbeiträge (z. B. Xing, Flickr, Xbox Live). Eine wachsende Einnahmequelle ist zudem der Verkauf von Zusatzfunktionen an die Nutzer, wie etwa zum Erwerb besonderer Fähigkeiten und virtueller Gegenstände in Onlinespielen, die in ein soziales Netzwerk integriert sein können.

Was sind typische soziale Netzwerke?

Beispiele für soziale Netzwerke sind: Diaspora, Facebook, Flickr, Friendica, Google+, LinkedIn, Pinterest, Playstation Network, Stayfriends, StudiVZ (inkl. SchülerVZ, MeinVZ), Xbox Live, Xing, Youtube und viele mehr.

Unterscheidet sich die Architektur dieser Netzwerke?

Die grundlegende Architektur ist bei den meisten sozialen Netzwerken sehr ähnlich. In der Regel gibt es einen zentralen Anbieter wie Facebook oder Xing, der die Plattform für das soziale Netzwerk zur Verfügung stellt. Das bedeutet, dass dieser Betreiber auch Zugriff auf sämtliche Daten der Nutzer hat und somit besonders in der Pflicht ist, sich gegen fremden, aber auch eigenen Missbrauch abzusichern. Der Nutzer muss hier ein hohes Maß an Vertrauen in den Betreiber aufbringen.

Netzwerke wie Diaspora oder auch Friendica hingegen erlauben eine dezentrale Teilnahme. Dabei verbinden sich mehrere Betreiber, ohne dass ein zentraler Betreiber existiert, der sämtliche Nutzungsvorgänge und die Inhalte beobachten und für sich verwenden kann. Wenn der Nutzer möchte, dann kann er dabei sogar seinen eigenen Server betreiben und in das Netzwerk einklinken. Er hat damit die Kontrolle, wo seine Daten liegen und wer hierauf

Zugriff hat. Allerdings schützt dieses nicht davor, dass Personen, denen man Zugriff auf die eigenen Daten gewährt, diese kopieren und dann missbrauchen.

Welche Daten werden von sozialen Netzwerken verarbeitet?

Offensichtlich ist natürlich die Verarbeitung der Daten, die der Nutzer selber über sich preisgibt (z. B. Name, Email-Adresse, Interessen). Hinzu kommen Informationen über Verbindungen mit anderen Nutzern. Nicht jedem ist jedoch bewusst, dass auch das eigene Verhalten innerhalb des Netzwerkes erfasst wird. Das bedeutet, dass z. B. in der Regel gespeichert wird, von wann bis wann man in dem Netz aktiv ist, welche anderen Profile sich jemand wie lange angesehen hat, welche anderen Inhalte konsumiert wurden und auf welche Links geklickt wurde. Dies geht so weit, dass durch Zusatzdienste wie Gefällt-Mir-Knöpfen (Facebook) oder +1-Knopf (Google+) sogar erfasst werden kann, welche sonstigen Inhalte im Internet – also außerhalb des eigentlichen sozialen Netzwerks - von wem besucht werden.

Wieso sind die sog. Social-Plugins wie der Gefällt-Mir- oder +1-Knopf so problematisch?

Werden die Social-Plugins von Webseitenanbietern (außerhalb der sozialen Netzwerke) eingebunden, wie es die Betreiber der Netzwerke empfehlen, dann werden Informationen über den Seitenbesucher an den Betreiber des sozialen Netzwerkes weitergeleitet.

In der Praxis bedeutet dies, dass beim Aufruf einer solchen Webseite mit z. B. „Gefällt-Mir"-Knopf nicht nur eine Verbindung zum Server dieser Webseite hergestellt wird. Stattdessen wird parallel zum eigentlichen Seitenabruf eine Verbindung zum sozial Netzwerk hergestellt, um beispielsweise den Facebook-Knopf von dort nachzuladen. Wenn ein Nutzer bei dem betreffenden sozialen

Netzwerk eingeloggt ist oder auf dem Rechner bereits einmal dort eingeloggt war, kann das Netzwerk den Besuch auf der eigentlich aufgerufenen Webseite registrieren. Auf diese Weise erfassen soziale Netzwerke weite Bereiche des World Wide Web außerhalb ihrer eigenen Grenzen – und nicht immer sind die Nutzer sich hierüber im Klaren. Kurz gesagt bedeutet dies, dass Facebook und Co. in weiten Teilen sehen, speichern und auswerten können, welche Seiten ein Nutzer im Internet sonst so besucht.

Ich bin bei keinem sozialen Netzwerk registriert. Werden dennoch Daten über mich über die Social-Plugins gesammelt?

Selbst, wenn man nicht bei einem sozialen Netzwerk registriert ist, werden Informationen über den Besucher einer Webseite an Facebook und Co. übertragen, wenn der Betreiber der Webseite die Social-Plugins wie die originalen Gefällt-Mir-Knöpfe eingebunden hat. Dies betrifft zum einen die IP-Adresse des Nutzers, aber auch ggf. eine eindeutige Nummer, die in einem sog. Cookie gespeichert werden kann. Einen solchen Cookie bekommt man z. B. bei Facebook schon, wenn man nur die Seite www.facebook.com aufgerufen hat, ohne sich anzumelden. Zwar können ohne persönliche Registrierung die Betreiber der sozialen Netzwerke nur mit der IP-Adresse und dem Cookie nicht ohne Weiteres den Namen und die Adresse des Nutzers herausbekommen. Wenn man sich jedoch im weiteren Verlauf der Internetnutzung doch noch bei einem Dienst anmeldet, der mit dem sozialen Netzwerk zusammenhängt (z. B. Youtube oder Googlemail bei Google+), dann könnte der Betreiber des sozialen Netzwerkes in dem Moment ggf. rückwirkend die schon gesammelten Informationen zusammenführen und für sich nutzen.

Sammeln denn die Betreiber der sozialen Netzwerke tatsächlich all diese Daten über mich, selbst wenn ich gar nicht diese Netzwerke nutze?

Was genau die Betreiber der sozialen Netzwerke mit den Daten machen, die sie von Nichtnutzern über Social-Plugins sammeln, ist nicht immer öffentlich bekannt. Sicher ist, dass diese Daten bei den Betreibern anfallen und zumindest zeitweise auch verarbeitet werden. Begründet wird dieses u. a. mit Sicherheitsvorkehrungen z. B. zur Verhinderung von Mehrfachanmeldungen und Hacking-Angriffen. Eine unabhängige Auditierung, dass diese Daten wirklich nur hierfür verwendet werden, gibt es nach unserem Wissen bisher nicht. Dabei muss man beachten, dass viele der Anbieter die Server in den USA betreiben. Die USA weisen jedoch nicht das gleiche Schutzniveau im Datenschutzbereich auf wie die EU. Die Möglichkeiten des Zugriffs durch und der Zusammenarbeit mit Sicherheitsbehörden sind in den USA deutlich weitergehend, als in Europa. Somit ist unserer Ansicht nach auch das Missbrauchsrisiko höher.

Hinzu kommt, dass selbst Sicherheitsgründe die Datenverarbeitung von Daten der Nichtnutzer nicht rechtfertigen können, wenn diese (wie im Fall der Social-Plugins) in der Regel beim Besuch einer normalen Webseite gar nicht wissen, dass dabei auch personenbeziehbare Daten an ein soziales Netzwerke weitergeleitet werden.

Wie kann ich mich selber gegen die Social-Plugins schützen?

Ist man bei einem sozialen Netzwerk registriert, dann sollte man sich vor dem Weitersurfen auf externen Seiten zunächst bei dem Dienst abmelden. Dies löscht aber z. B. im Fall von Facebook nicht sämtliche Cookies, die die einfache Wiedererkennung ermöglichen. Der sog. „datr-Cookie“ bleibt erhalten. Daher sollte man zur Sicherheit auch diesen Cookie manuell löschen. Die gängigen

Browser bieten hierzu eigene Funktionen, die auch eine Automatisierung der Cookie-Löschung ermöglichen. Daneben bieten einige Browser eigene Funktionen oder auch Plugins, die den Aufruf der externen Social-Plugins unterbinden.

Ich bin Webseitenbetreiber und möchte Social-Plugins auf meiner Webseite nutzen. Darf ich das?

Die direkte Nutzung der Social-Plugins ist in der Regel rechtlich nicht möglich, da hierzu die Einwilligung der Besucher der Webseite erforderlich wäre. Notwendig ist, dass die Einwilligung des Besuchers in den Aufruf des Social-Plugins (und damit die Übermittlung von Daten an den Betreiber des sozialen Netzwerkes) vor den Aufruf des Plugins eingebunden wird. Bei der Gestaltung dieser Einwilligung steht man meist jedoch vor dem Problem, dass man gar nicht genau weiß, was der Betreiber des sozialen Netzwerkes mit den übermittelten Daten macht. Dies wäre jedoch für eine informierte Einwilligung im Sinne der Datenschutzgesetze erforderlich.

Welches sind die größten Datenschutzprobleme bei sozialen Netzwerken?

Grundsätzlich muss man beachten, dass gerade die großen sozialen Netzwerke eine solche Fülle an Informationen über einen großen Teil der (Welt-) Bevölkerung, deren Interessen, Vorlieben und Freundschaften haben, dass sich hieraus eine besondere Verantwortung für den Schutz der Daten ergibt. Dies betrifft nicht nur die Betreiber der Netzwerke, sondern auch (staatliche) Stellen hinsichtlich der Kontrolle der Dienste. Auch der Gesetzgeber ist aufgefordert, für diese gesamtgesellschaftlich wichtige Aufgabe die richtigen Rahmenbedingungen zu setzen, die eine freie Nutzung und Kommunikation aller sicherstellen.

Die folgende nicht abschließende Aufstellung führt einige Problembereiche auf, die wir bei sozialen Netzwerken erkannt haben. Sie dient als Orientierung und bezieht sich in ihrer Fülle nicht auf ein einzelnes Netzwerk allein.

- Intransparenz hinsichtlich des Umfangs der gesammelten Daten, Speicherfristen und Löschung,
- unklare Beschreibung des Zwecks der Datenverwendung bzw. Offenlassen einer sehr weitgehenden Verwendung in den Nutzungsbedingungen,
- intransparente Speicherung des Nutzerverhaltens innerhalb des Netzwerkes,
- Erstellung von (Nutzungs-) Profilen der Nutzer,
- Weitergabe von Daten an Dritte etwa über Apps, zu Werbezwecken oder bei Verkauf des Dienstes bzw. Insolvenz,
- unklare bis gar keine Möglichkeit zur endgültigen Löschung von Daten und des Accounts,
- mangelnder Jugendschutz (z. B. durch einheitliche Voreinstellungen und Regelungen für alle Altersgruppen und mangelnde Abschottung gegen Missbrauch)
- Wahl von Voreinstellungen, die die Freigabe von Daten bewirken, ohne dass man hierin ausdrücklich eingewilligt hat,
- Verpflichtung zur Nutzung des echten Namens bzw. mangelnde Möglichkeit zur Nutzung von Pseudonymen,
- Beanspruchung von Rechten an Fotos, Videos etc. durch den Betreiber des sozialen Netzwerkes,
- mangelhafte Auskunftsmöglichkeit bzgl. der über einen gespeicherten Daten,
- schwer erreichbarer Support zur Meldung von Datenschutzverstößen / Missbrauch (ggf. außerhalb Deutschlands),
- mangelnde interne und externe Kontrolle,
- Speicherung von Daten außerhalb der EU in Ländern, die kein

vergleichbares Datenschutzniveau haben und deren Sicherheit nicht garantiert werden kann,

- mangelhafte Absicherung der Daten,
- Vorbehalt der jederzeitigen Änderung von Bedingungen / Datenschutzvorgaben,
- Analyse und Zusammenführung von Fotos bzw. den darauf abgebildeten Gesichtern (Gesichtserkennung),
- durch mangelnde Authentisierung der Nutzer können leicht unberechtigte Profile über dritte Personen eingestellt werden,
- insbesondere in Berufsnetzwerken kann schon der Umstand, dass man mit einer Person eine Verbindung in dem sozialen Netzwerk eingegangen ist, einen Verstoß gegen Geheimnisvorgaben des Arbeitgebers darstellen.

Was kann ich für den eigenen Datenschutz tun, wenn ich soziale Netzwerke nutzen möchte?

1. Wählen Sie nur Netzwerke aus, denen Sie vertrauen können und achten Sie dabei unter anderem auf die Nutzungsbedingungen, den Standort des Betreibers und die Berichterstattung in den Medien bzw. durch Verbraucherschutzorganisationen und Datenschutzorganisationen.
2. Lesen Sie die Datenschutzbestimmungen.
3. Besuchen Sie sofort nach der Registrierung den Bereich „Privateinstellungen" bzw. „Datenschutzeinstellungen" des sozialen Netzwerkes und stellen Sie alles nach Ihren Wünschen ein.
4. Geben Sie dem sozialen Netzwerk in der Regel nicht ihr Passwort des Email-Postfaches. Das soziale Netzwerk könnte damit nicht nur ihre Emails analysieren, sondern auch Daten von ihren Kommunikationspartnern als unbeteiligte Dritte abgreifen.
5. Beachten Sie bei allen Informationen, Fotos und Beiträgen, die Sie in ein soziales Netzwerk einstellen, dass Sie die Einstellungen so wählen, dass nur die Personen davon erfahren, von de-

nen Sie dieses wollen. Bedenken Sie immer, dass nie völlig ausgeschlossen werden kann, dass durch eigene oder fremde Fehlkonfigurationen Informationen auch unbeabsichtigt an Dritte gehen können. Der Netzwerkbetreiber hat immer, anders als beim Telefonieren, Zugriff auf Inhalte und kann diese auch über längere Zeiträume analysieren.

6. Posten Sie keine Informationen über andere Personen insbesondere negativer Art, es sei denn, Sie wissen oder können davon ausgehen, dass diese damit einverstanden sind.
7. Kontrollieren Sie regelmäßig ihre Datenschutzeinstellungen. Betreiber von sozialen Netzwerken neigen dazu bei Überarbeitung des Dienstes neu hinzukommende Einstellungsmöglichkeiten so zu wählen, dass wieder Informationen ohne ausdrückliche Freigabe durch den Nutzer veröffentlicht werden.
8. Kontrollieren Sie regelmäßig alte Pinnwand-Einträge darauf hin, ob Sie deren Veröffentlichung immer noch wollen.
9. Geben Sie nicht ihr Passwort für das soziale Netzwerk weiter. Wenn Sie es doch gemacht haben, dann ändern Sie es umgehend.

Was muss ich besonderes beachten, wenn ich soziale Netzwerke über Handy / Smartphone nutze?

Grundsätzlich gelten die gleichen Vorsichtsmaßnahmen wie bei der Nutzung des Netzwerkes über den Computer. Hinzu kommt jedoch, dass in der Regel zusätzlich die Information über ihren Standort an den Netzwerkbetreiber weitergegeben wird. Diese Information wird oftmals mit dem Beitrag veröffentlicht. Daher sollten die Voreinstellungen der App bzw. des Handys vorher diesbezüglich überprüft werden. Besondere Gefahren drohen bei der Nutzung von Apps von Drittanbietern. Diese benötigen in der Regel die Zugangsdaten des sozialen Netzwerkes. Wenn diese Funktionalität durch ein anderes Unternehmen als den Betreiber des

sozialen Netzwerkes bereit gestellt wird, dann prüfen Sie bitte, ob Sie diesem Unternehmen trauen können. Greifen Sie im Zweifel auf die Apps zurück, die die Betreiber des Netzwerkes selber zur Verfügung stellen.

Ich möchte Fotos oder Videos in das soziale Netzwerk einstellen. Was muss ich beachten?

Bedenken Sie, dass die abgebildeten Personen ein Recht am eigenen Bild haben. Das bedeutet, dass Sie in der Regel die ausdrückliche Einwilligung dieser Personen benötigen, dass Sie die Fotos veröffentlichen dürfen. Eng umrissene Ausnahmen hiervon gibt es nur, wenn die Personen Beiwerk zu einer Landschaft bzw. einem Gebäude oder Teil einer größeren Versammlung sind. Die Personen dürfen in diesen Fällen nicht individuell herausstechen. Eine Freigabe für „Gruppen" etwa in Größen von 7 oder 12 Personen gibt es nicht. Auch die Veröffentlichung eines Klassenfotos bedarf z. B. der Einwilligung der Abgebildeten. Die sozialen Netzwerke erlauben es in der Regel, den Personenkreis einzuschränken, der Zugriff auf die Fotos hat. Dies sollte man nutzen. Beachten Sie jedoch, dass einige Netzwerke sich Rechte an den eingestellten Fotos und Videos vorbehalten. In diesen Fällen müsste sich die Einwilligung der abgebildeten Personen auch hierauf beziehen.

Jemand hat ohne meinen Willen ein Profil über mich angelegt oder beleidigende Inhalte über mich in das soziale Netzwerk eingestellt. Was kann ich tun?

Alle sozialen Netzwerke bieten eine Melden-Funktion, mit der unberechtigte Profile (sog. Fake-Profile), aber auch unangemessene Inhalte gemeldet werden können. Wenn Sie selber nicht Kunde des sozialen Netzwerks sind, müssen Sie ggf. zunächst über die Hilfe oder die Kontakt-Seite des Betreibers nach dieser Funktion suchen. Sollte auf Ihre Meldung nicht in angemessener Zeit rea-

giert werden, dann wenden Sie sich an Ihre Datenschutzaufsichtsbehörde oder den Verbraucherschutz. In entsprechend gelagerten Fällen können Sie auch eine Anzeige bei der Polizei erstatten.

Ich will mich bei dem sozialen Netzwerk abmelden. Wie mache ich das?

Beachten Sie, dass viele Netzwerke im Rahmen der Abmeldung nur den Zugang zu dem Profil sperren. Die Daten bleiben jedoch für den Fall, dass man es sich anders überlegt, weiterhin gespeichert. Sie haben allerdings ein Recht darauf, dass Ihre Daten nach der Kündigung vollständig gelöscht werden. Bei Facebook muss zur Umsetzung dieses Rechts zum Beispiel über die Hilfe-Funktion nach „Löschen" gesucht werden. Dort finden Sie dann einen Text, der einen Link auf einen entsprechenden Antrag auf Löschung enthält. Hierüber können Sie die Löschung anstoßen, die dann nach einigen Tagen / Wochen ausgeführt worden sein sollte.

Wo kann ich mich weiter über das Thema informieren?

- https://www.datenschutzzentrum.de/facebook/
- http://www.verbraucher-sicher-online.de/thema/soziale-netzwerke/
- http://www.klicksafe.de/
- http://www.surfer-haben-rechte.de/

Kontakt

Wenn Sie Fragen, Anregungen oder Beschwerden zum Datenschutz haben, wenden Sie sich bitte an uns. Wir beraten Sie und helfen Ihnen gern.

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98
24103 Kiel
Telefon: 0049 (0) 431 988-1200
Telefax: 0049 (0) 431 988-1223
E-Mail: mail@datenschutzzentrum.de
www.datenschutzzentrum.de

Broschüren zu den Themen:

- Verbraucher-Scoring
- Verbraucherdatenschutz
- Videoüberwachung und Webkameras
- Internet: Alltag online
- Illegaler Datenhandel
- Soziale Netzwerke

können Sie unentgeltlich bei uns bestellen oder von unserer Homepage unter www.datenschutzzentrum.de/blauereihe herunterladen.