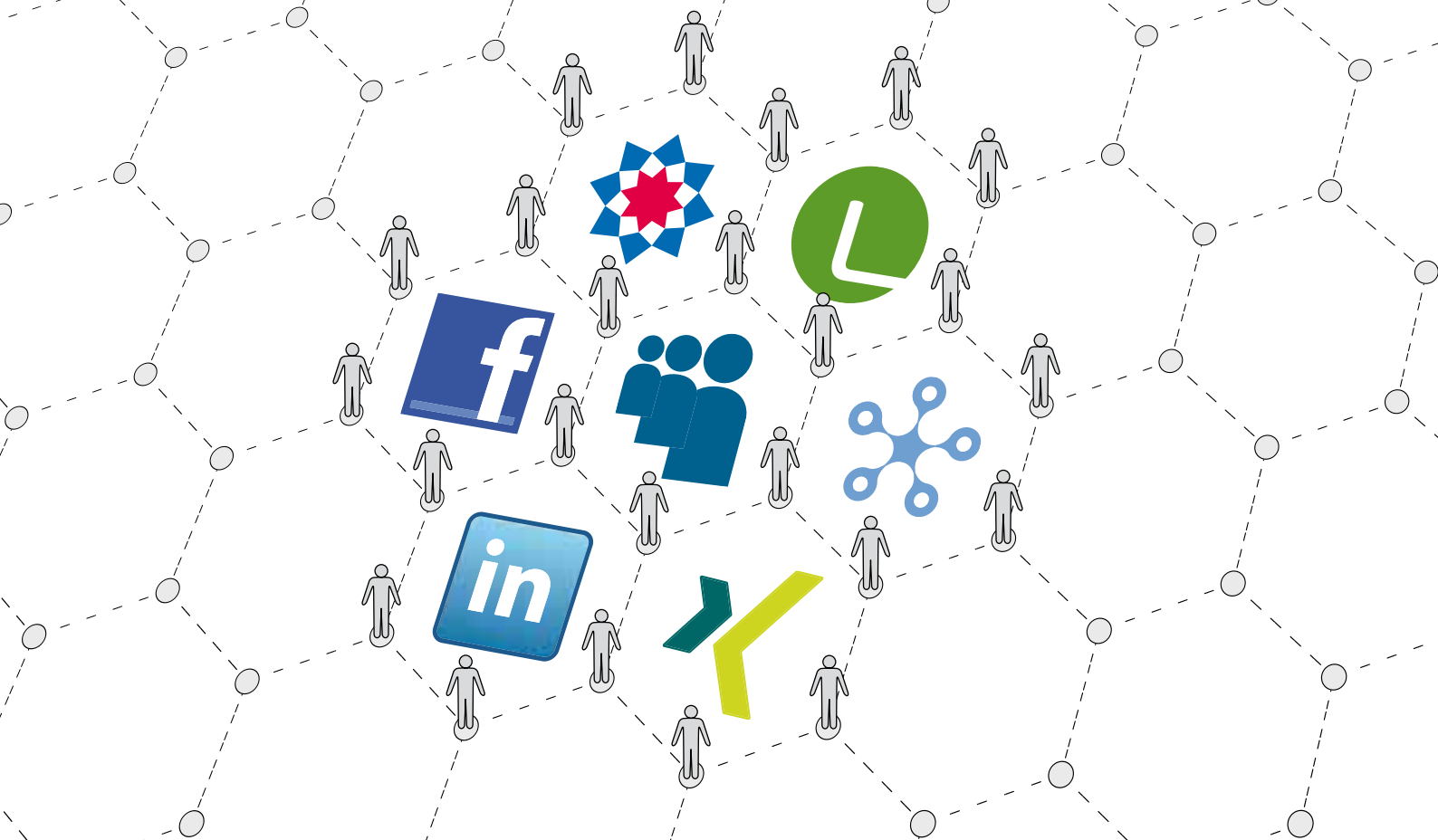
Fraunhofer Institut Sichere Informations-Technologie

Privatsphärenschutz in Soziale-Netzwerke-Plattformen



Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
D-64295 Darmstadt

Tel.: +49 (0)6151-869-0
Fax: +49 (0)6151-869-224
http://www.sit.fraunhofer.de

Veröffentlicht am 23. September 2008
Stand: Ende August 2008

Die Studie im Überblick

Diese Studie untersucht Mechanismen zum Privatsphärenschutz von sieben »Soziale-Netzwerke-Plattformen« (myspace, facebook, studiVZ, wer-kennt-wen, lokalisten, XING und LinkedIn). »Soziale-Netzwerke-Plattformen« sind internetbasierte Anwendungen, in die Nutzer ihre Beziehungen zu anderen Personen abbilden, um diese Daten für wesentliche Dienstfunktionen weiterzuverwenden.

Die verarbeiteten Daten sind fast ausschließlich personenbezogener Natur. Entsprechend hoch ist das Gefährdungspotential für die Nutzer, wenn Sicherheitsschwachstellen existieren und Schutzmechanismen fehlen.

Mit einem Test aus der Perspektive eines regulären Internetnutzers (Black-Box-Test), wurden die Sicherheitsmaßnahmen und Schutzmechanismen der geprüften Plattformen erfasst und bewertet. Ein solcher Test bietet zwar methodisch bedingt **keine umfassende Sicherheitsanalyse**. Auch lassen sich aus den Testergebnissen **keine Aussagen ableiten, inwiefern die Dienstbetreiber rechtlichen Anforderungen aus dem Datenschutz nachkommen**. Der Test ist jedoch ausreichend um Nutzern wertvolle Hinweise zur sicheren Verwendung der Internetdienste zu liefern und Dienstanbietern erste Verbesserungsmöglichkeiten aufzuzeigen.

Prüf- und Bewertungsgrundlage ist ein für diese Studie erarbeiteter Kriterienkatalog, der spezifische Gefährdungen von Soziale-Netzwerke-Plattformen berücksichtigt und an ausgewählte Konzepte aus dem Datenschutz angelehnt ist. Die Tester wendeten die erstellten Kriterien einheitlich auf alle getesteten Plattformen an.

Von den getesteten Plattformen konnte keine vollständig überzeugen. Vielfach ist sogar von der Nutzung bestimmter Dienstfunktionen abzuraten.

Unter den Privatplattformen erhielt facebook die meisten guten Bewertungsergebnisse, wenngleich selbst diese Plattform erhebliche Schwächen offenbarte. Die Dienste myspace, studiVZ und wer-kennt-wen erreichten mit ihren Bewertungen ein Mittelfeld. Den positiven Bewertungen standen hier verschiedene Mängel wie Lücken in der Zugriffskontrolle, Eigenheiten bei der Nutzerführung oder fehlende Verschlüsselung gegenüber.

Die Plattform lokalisten markiert das untere Ende der Bewertungsskala, insbesondere weil viele notwendige Zugriffskontrollfunktionen schlichtweg fehlten.

Bei den Geschäftsplattformen konnte LinkedIn gegenüber XING besser abschneiden. Zum einen erlaubt LinkedIn im begrenzten Rahmen die Nutzung eines Pseudonyms. Zum anderen war die Aufgabe der Mitgliedschaft einfacher und das anschließende Löschen privater Daten umfangreicher als beim Konkurrenten XING.

Inhaltsverzeichnis

1 Einleitung

Die Entwicklung neuer Internetanwendungen ist in den letzten Jahren zunehmend von einem Trend geprägt, der gemeinhin mit dem Modewort Web 2.0 bezeichnet wird. Eine der Grundideen des Web 2.0 ist, dass Dienstanbieter Plattformen zur Verfügung stellen, deren inhaltliche Ausgestaltung ihre Nutzer maßgeblich selbst übernehmen.

Die Nutzer haben den Vorteil, sich nicht mit den technisch-organisatorischen Voraussetzungen einer solchen Plattform auseinandersetzen zu müssen. Der Dienstbetreiber wiederum hofft, durch anwendergenerierte Inhalte ein schnelles Wachstum seiner Nutzerzahlen zu erreichen. Das ist notwendig, um die Attraktivität der Plattform dauerhaft zu erhalten.

Die Anzahl der Nutzer spielt auch ökonomisch eine wichtige Rolle. Dienstanbieter erwirtschaften einen Großteil ihrer Einnahmen durch Marketingmaßnahmen von Dritten, die in der Plattform platziert werden. Je mehr Nutzer angemeldet sind, desto größer ist die Reichweite der im Netzwerk präsentierten Werbung. Die Einbeziehung personenbezogener Daten eröffnet zudem weitere Vorteile aus Sicht der Werbetreibenden: Sie erlaubt zielgruppenspezifischeres und damit effizienteres Marketing.

Ein besonderer Teilbereich von Web 2.0-Anwendungen ist Soziale Software. Gemeint sind damit internetbasierte Software-Anwendungen, die Menschen bei ihren sozialen Interaktionen, Kollaborationen und Kommunikationsvorgängen unterstützen. Nach Schmidt [35] wird diese Unterstützung durch drei wesentliche Funktionen gewährleistet:

- **Informationsmanagement**, die Verwaltung und Recherche von Informationen
- **Identitätsmanagement**, die Präsentation der eigenen Person als eine Art Online-Identität
- **Beziehungsmanagement**, die Pflege und Neuknüpfung von Beziehungen zu anderen Personen

Eine spezielle Ausprägung Sozialer Software sind Soziale-Netzwerke-Plattformen, welche in dieser Studie untersucht werden. Eine Soziale-Netzwerke-Plattform zeichnet sich durch folgende Merkmale aus:

- Nutzer erzeugen ein eigenes, weitgehend selbstgestaltetes Profil in der Plattform, welches ihre Online-Identität widerspiegelt. (Identitätsmanagement-Aspekt)

- Nutzer verknüpfen sich mit anderen Nutzern, zu denen sie in einer besonderen Beziehung stehen. Diese besondere Beziehung ergibt sich aus einer zuvor durchgeführten sozialen Interaktion zwischen den verknüpften Nutzern. Die Verknüpfung erfolgt mithilfe einer speziellen Plattformfunktion und wird im Datenbestand der Software gespeichert.
- Die an der Plattform angemeldeten Nutzer (Knoten) und die Verknüpfungen der Nutzer untereinander (Kanten) bilden einen Graphen. Dieser wird als soziale Vernetzung oder soziales Netzwerk bezeichnet.
- Dieser Graph, das soziale Netzwerk, ist die Basis für die Bereitstellung weiterer Plattformfunktionen zur Kommunikation und zum Datenaustausch der Nutzer untereinander. (Beziehungs- und Informationsmanagement-Aspekt)

Die beschriebenen Merkmale sind nicht hinreichend, um Soziale-Netzwerke-Plattformen von anderer Sozialer Software wie Foren, Chat-Programmen oder Wikis abzugrenzen. Ein entscheidender letzter Punkt ist, dass für die Nutzer wesentliche Funktionen der Anwendungen auf der Vernetzung beruhen. Die Plattformen bieten somit ihren Nutzern keinen wesentlichen Mehrwert, wenn sie keine Vernetzungen ausbilden und keine Funktionen existieren, die sich des Netzwerkgraphen bedienen.

Soziale-Netzwerke-Plattformen erweitern prinzipiell die Palette an Interaktionsmöglichkeiten zwischen Menschen im Internet. Die verwendete Technik birgt aber auch neue Risiken für die Privatsphäre ihrer einzelnen Anwender. Die Ursachen für diese Risiken sind Bedrohungen, die eng mit den nutzbringenden Möglichkeiten der Software verbunden sind:

- **Eingabe vieler und sensibler privater Daten**, um diese mit anderen Nutzern zu teilen,
- **Zentrale Datenspeicherung** bei *einem* Internet-Dienstleister um einfachen Zugang und hohe Dienstverfügbarkeit zu gewährleisten,
- Geringe oder **keine Bedingungen für die Aufnahme neuer Nutzer** in die Plattform, um ein schnelles Wachstum hinsichtlich Nutzerzahlen und Vernetzung zu erreichen,
- Starke Verknüpfung von Daten entlang der in den Plattformen abgebildeten Beziehungen zwischen den Nutzern. Diese **Verknüpfungen ermöglichen das Extrahieren neuer Informationen** über den Informationsgehalt einzelner Datenobjekte hinaus,
- **Leichtes Auffinden von Nutzern** und ihrer Daten in der Plattform

Um Bedrohungen entgegenzuwirken sind Gegenmaßnahmen in Form von Schutzmechanismen notwendig. Sie verhindern z. B. unerwünschtes Offenlegen, Beschädigen oder Verändern von Daten durch Angreifer. Weiterhin sollen sie erwünschte Plattformfunktionen soweit einschränken, dass bei der Plattformnutzung die Privatsphäre der Mitglieder gewahrt bleibt. Es gilt Verfahren

bereitzustellen, die es jedem Nutzer individuell ermöglichen, einen für ihn akzeptablen Ausgleich zwischen gewollter Datenpreisgabe und dem Schutz seiner Privatsphäre nach seinen Bedürfnissen zu etablieren.

In dieser Studie wird geprüft, ob und wie ausgewählte Soziale-Netzwerke-Plattformen Mechanismen zum Privatsphärenschutz zur Verfügung stellen.

Dazu wurden im Zeitraum **März 2008 bis August 2008** die folgenden Internetdienste einem Black-Box-Test unterzogen:

- **Privatplattformen**, für den Einsatz im privaten Bereich
  - myspace
  - facebook
  - studiVZ
  - wer-kennt-wen
  - lokalisten
- **Geschäftsplattformen**, zur Pflege von geschäftlichen Kontakten
  - XING
  - LinkedIn

Black-Box-Test bedeutet dabei, dass die Tester in der Rolle normaler Internetnutzer agierten. Diese Testmethode erlaubt zwar keine vollständige Sicherheitsanalyse. Sie ermöglicht es aber, wichtige Mängel aufzudecken, welche die Privatsphäre der Plattformennutzer bereits erheblich beeinträchtigen.

Die Untersuchung basiert auf einem zu diesem Zweck entwickelten Kriterien- und Anforderungskatalog. Dieser folgt pragmatischen Gesichtspunkten und orientiert sich an bekannten Konzepten zum Privatsphärenschutz. Die Kriterien und Anforderungen sind in dieser Studie nachvollziehbar dokumentiert. Die Tester wendeten sie einheitlich auf alle Plattformen an.

Prüfergebnisse sind für jedes Kriterium einzeln auf eine abschließende Bewertung abgebildet. Grundlage ist ein dreistufiges Bewertungsschema. Es ist derart konzipiert, dass eine Plattform mit Schutzmaßnahmen nach dem Stand der Technik durchweg positive Bewertungen erhält.

Ziel der Studie ist es, ein erstes Rahmenwerk für die Beurteilung des Privatsphärenschutzes von Soziale-Netzwerke-Plattformen aufzustellen. Es kann als Grundlage für über diese Studie hinausgehende Evaluierungen dienen und ist um Elemente wie z.B. Penetrations- und White-Box-Tests oder auch juristische Prüfungen erweiterbar.

Die Untersuchungsergebnisse sollen für Internetanwender eine Entscheidungsgrundlage zur Auswahl geeigneter Dienste liefern. Für Dienstbetreiber soll die Studie Kriterien für die Dienstgestaltung aufzeigen. Weiterhin helfen die Testresultate Schwachstellen und Mängel im eigenen Dienstangebot zu identifizieren. Damit macht die Studie Verbesserungspotentiale sichtbar, die es ermöglichen eine Soziale-Netzwerke-Plattform privatsphäre-respektierend weiterzuentwickeln.

2 Vorbetrachtungen

In diesem Kapitel werden Grundlagen erarbeitet, die für die weitere Analyse notwendig sind. Dabei werden Schritt-für-Schritt folgende Fragen erörtert:

- Wie ist der Begriff »Privatsphäre« im Kontext von Soziale-Netzwerke-Plattformen einzuordnen?
- Wie sieht ein abstraktes Modell einer Soziale-Netzwerke-Plattform aus, welches zur Entwicklung von einheitlichen Kriterien und Anforderungen hinzugezogen werden kann?
- Wie werden personenbezogene Daten in den Plattformen eingegeben, gespeichert, verarbeitet und weiterübermittelt?
- Welche Prozesse durchlaufen die Nutzer beim Verwenden der Plattformen?

2.1 Offener Informationsaustausch versus Privatsphäre

Die Verbreitung privater, personenbezogener Informationen ist zentraler Zweck einer Soziale-Netzwerke-Plattform. Die Anwender treten Internetgemeinschaften bei, um sich dieser Funktionalität in verschiedenen Anwendungsszenarien zu bedienen (vergleiche [34] und [30]):

Typischerweise gehört dazu die Pflege von aktuellen sozialen Kontakten oder die Etablierung von neuen Verbindungen. Dies geschieht teilweise auch über geographisch größere Distanzen und ohne direkte Interaktion der Beteiligten im realen Leben. Genutzt werden dafür Kommunikationsmittel (in verschiedenen Konstellationen der Kommunikationspartner zueinander), wie Chats, Blogs, Diskussionsforen, Kommentarfunktionen, Frage-und-Antwort-Werkzeuge usw.

Daneben erfolgt die schlichte, empfängerunspezifische Veröffentlichung von Informationen. Hierbei spielt das sogenannte Profil und damit verknüpfte Datenablageorte eine wichtige Rolle (zur weiteren Erörterung siehe 2.2).

Trotz dieser offenen Praxis des Informationsaustauschs wird unterstellt, dass die Nutzer Sozialer-Netzwerke-Plattformen gewisse Vorstellungen und Bedürfnisse bezüglich Privatsphäre haben. Konkreter betrachtet wird erwartet, dass sich offenbarte Informationen nur in einer bestimmten, erhofften Art und Weise an erwünschte Empfängerkreise verbreiten. Als klassisches Beispiel möchte man bestimmte Fotos zwar mit seinen Freunden teilen, aber nicht mit einem potentiellen Arbeitgeber.

Diese Perspektive kann auch in die Zukunft verlängert werden. So möchte man z. B. nach einer gewissen Zeit zuvor verbreitete Fotos oder andere Daten vollständig wieder entfernen. Dieser Wunsch ist damit begründet, dass die Aktualität von Informationen über der Zeit abnimmt. Veraltete Informationen können ebenfalls negative Auswirkungen für den Betroffenen haben, wenn sie zu ungewollten oder falschen Rückschlüssen führen. Ähnliche Probleme verursachen falsche oder unerwünschte Daten die Dritte eingeben oder die durch unberechtigte Manipulation enstehen.

Dass diese gesamte Problemstellung eine erhebliche Komplexität besitzt, zeigt sich in den sehr ambivalenten Vorstellungen von Privatsphäre, je nach betrachtetem Einzelfall [32]:

Es kann vorkommen, dass eine Person bestimmte Informationen an einen kleinen Kreis nahestehender Menschen übermitteln möchte, aber keinesfalls an unbekannte Außenstehende. Ein Beispiel dafür ist z. B. eine Fotosammlung aus dem letzten Urlaub, die an Familienmitglieder und enge Freunde geschickt wird.

Gleichzeitig gibt es aber auch Situation in denen ausdrücklich Unbekannte angesprochen werden sollen, aber die Informationen keinesfalls für die Augen von nahestehenden Personen bestimmt sind. Ein typisches Beispiel sind Personen mit schweren Erkrankungen, die Hilfe bei Betroffenen in einem Internetforum suchen.

Der offene Informationsaustausch und die Privatsphärenbedürfnisse der Nutzer sind konkurrierende Ziele. Der Dienstbetreiber kann durch die Gestaltung seiner Plattform gezielt den Schwerpunkt zwischen beiden Polen verschieben. Sowohl theoretisch als auch empirisch ist jedoch nicht geklärt, welche Fixierung den größeren Erfolg hinsichtlich Nutzerzahlen, Zugriffszahlen und Nutzungsdauer bringt.

In Anbetracht dieser Aspekte, lag der Fokus für die Untersuchung auf den Privatsphärenbedürfnissen der Nutzer und wie diesen Rechnung getragen wird. Es wurde primär untersucht, ob, wie, in welchem Umfang und mit welchen Mitteln Nutzer den Informationsfluss in der Plattform steuern können.

Diese Festlegung benachteiligt Dienstanbieter, die eher auf »offene Konzepte« setzen und bewusst den Schutzmechanismen für die Privatsphäre weniger Aufmerksamkeit beimessen. In dieser Studie wird aber der Ansatz vertreten, dass Techniken, welche die Privatsphäre fördern, dem Nutzer insgesamt mehr Anwendungsmöglichkeiten eröffnen und damit einen höheren persönlichen Mehrwert generieren. Beispielsweise können Nutzer mehr authentische Informationen über Soziale-Netzwerke-Plattformen mit ihrem Umfeld teilen, wenn sie eine Gewissheit haben, dass Daten vor unbefugtem Zugriff wirksam geschützt sind. Das kann dem Erfolg des gesamten Dienstes zuträglich sein.

Man muss an dieser Stelle nicht verleugnen, dass diese Sichtweise umstritten ist. Auf der anderen Seite steht das häufig zitierte »nichts zu verbergen«-Argument,

welches eine ganze Sammlung anderer Ansichten zu diesem Thema vertritt (siehe dazu unter anderem [37] oder [28]). Diese spielen hier aber bewusst keine Rolle.

Datenschutzrechtliche Aspekte werden in dieser Studie nur begrenzt untersucht. Der Fokus der Untersuchung liegt auf der Technologie und nicht auf der Klärung juristischer Fragen (siehe auch 4.3).

2.2 Speicherung und Verarbeitung personenbezogener Daten

Diese Studie bewertet, wie Informationsflüsse in Soziale-Netzwerke-Plattformen organisiert sind und insbesondere wie der Anwender sie steuern kann, um einen adäquaten Schutz seiner Privatsphäre zu erlangen.

Wenn man dieses übergeordnete Ziel von der Ebene der Technik- und Prozesssicht betrachtet, dann stehen im Fokus der Untersuchung die personenbezogenen Daten des Anwenders. Diese personenbezogenen Daten liefern kontextbezogenen Informationen, die mithilfe der Plattform verbreitet werden. Ein Beispiel ist das Foto einer bestimmten Person auf einer Veranstaltung, z. B. einem Vereinsfest. Dabei handelt es sich technisch gesehen zunächst um ein simples Datenobjekt. Die Informationen, die dieses Foto jedoch offenbart, sind vielfältig und abhängig vom Betrachterkontext. Als Datenobjekt kann es z. B. die Information liefern, dass sich die abgebildete Person zu einem definierten Zeitpunkt an einem bestimmten Ort aufhielt und nicht an einem anderen. Es kann aber auch als Information bezüglich des Bekanntenkreises der Person interpretiert werden, wenn man andere Menschen auf dem Foto in die Betrachtung einbezieht.

Während also Daten von ihren menschlichen »Konsumenten« verschiedenartig als Informationen interpretiert werden, setzen Soziale-Netzwerke-Plattformen nur eine durch Technik und Prozessabläufe determinierte Datenverarbeitung um. Daten durchlaufen dabei in den Plattformen verschiedene Verarbeitungsschritte und sind mit verschiedenen Funktionen verknüpft.

Im Folgenden wird deshalb zunächst beschrieben, *welche* personenbezogenen Daten *wo* in den Plattformen gespeichert und verarbeitet werden. Desweiteren wird dargestellt, *welchen Verarbeitungsprozess* sie grob durchlaufen und *welche Plattformkomponenten* in diese Verarbeitung eingebunden sind.

Somit ist es Ziel dieses Abschnitts, über die vorgefundene Datenverarbeitung in Soziale-Netzwerke-Plattformen eine Vorstellung über den Informationsfluss zu erhalten, der mithilfe dieser Software etabliert wird. Diese Analyse ist notwendig, um aus den abstrakten Anforderungen an eine privatsphärenrespektierende Informationsverarbeitung, technische Anforderungen an die zu untersuchenden Plattformen herzuleiten.

(Anmerkung: Aus Gründen der Vereinfachung werden personenbezogenen Daten im Folgenden nur noch kurz als »Daten«, »private Daten« oder »Daten des Anwenders« bezeichnet, um die Lesbarkeit des Textes zu erhöhen.)

2.2.1 Privatsphärenrelevanz von Daten

Zunächst wird untersucht, welche Arten von privaten Daten in Soziale-Netzwerke-Plattformen gespeichert und verarbeitet werden.

Dabei spielt insbesondere eine Rolle, wie relevant einzelne Daten für die Privatsphäre einer Person sind. So liefert z. B. eine Altersangabe in einem Profil recht wenig Informationen über das Privatleben eines Menschen, auch wenn es sich dabei zweifelsohne zunächst um ein personenbezogenes Datum handelt. Andere Daten sind in dieser Hinsicht auskunftsfreudiger, z. B. wenn sie die Religionszugehörigkeit erfassen.

In einer genaueren Definition wird der Begriff der »privatsphärenrelevanten Daten« in dieser Studie wie folgt verstanden:

»Privatsphärenrelevante Daten« sind Daten, die detailiert Einblick in die Privat- und Intimsphäre eines Menschen liefern oder mit deren Kenntnis ein gezieltes Einwirken auf den Betroffenen möglich wird. Der Begriff des »Einwirkens« umfasst dabei:

- Eine verbesserte Vorhersage von Aktionen des Betroffen.
- Die Möglichkeit, mithilfe der Kenntnis von Lebensumständen des Betroffenen, diesen gezielt zu manipulieren. Ein solcher Eingriff soll derart wirken, dass der Betroffene zukünftige Aktionen im Sinne der manipulierenden Person ausführt.
- Das bewusste oder unbewusste Einwirken einer Person in einer vom Betroffenen nicht gewünschten Art und Weise infolge einer ihm nicht intendierten Interpretation seiner personenbezogenen Daten.

Eine detaillierte Erörterung des Begriffs findet sich unter anderem in Abschnitt 2.2.5 »Privatsphärenrelevante Eigenschaften von Identitätsattributen« in [33]. In der Rechtsprechung wird zuweilen auch von »Persönlichkeitsrelevanz von Informationen« gesprochen, wie beispielweise in [26].

Die gegebene Definition ist verschiedenartig auslegbar. Man kann aber durch Rückgriff auf das Datenschutzrecht zumindest eine Mindestmenge an Daten definieren, die in jedem Fall privatsphärenrelevant sind. Diese werden juristisch als »besondere Kategorien personenbezogener Daten« bezeichnet. Ihrer besonderen Sensibilität wird durch spezielle gesetzliche Bestimmungen Rechnung getragen.

In den einschlägigen Rechtsnormen ist vom Gesetzgeber festgelegt, welche Daten »besondere Kategorien personenbezogener Daten« sind (siehe [4] und [14]). Gemeint sind Daten, welche Informationen liefern über:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder politische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit oder Sexualleben

Jedes Datum, welches offensichtlich geeignet ist, über einen der oben genannten Faktoren Aussagen zu liefern, ist privatsphärenrelevant. Hinzu kommen andere Daten, die plausibel als privatsphärenrelevant einzuordnen sind, z. B. wenn sie umfangreich Einblick in den Tagesablauf des Betroffenen gewähren. Zusätzlich ist zu berücksichtigen, dass Daten die für sich genommen belangslos erscheinen, in ihrer Verknüpfung mit anderen Daten völlig neue, sensible Informationen offenbaren können.

Privatsphärenrelevant ist also beispielsweise die proklamierte Zugehörigkeit zu einer bestimmten Gruppe innerhalb einer Soziale-Netzwerke-Plattform (z. B. Mitglied einer Gruppe »Student und Christ«). Hingegen ist eine Altersangabe allein wenig privatsphärenrelevant. Sie kann aber in Kombination mit anderen Daten durchaus unerwünschte Informationen liefern.

Soziale-Netzwerke-Plattformen speichern und verarbeiten sowohl privatsphärenrelevante als auch nicht-privatsphärenrelevante Daten. Prinzipiell sind beide schützenswert. Allerdings wird privatsphärenrelevanten Daten eine besondere Bedeutung in dieser Studie beigemessen, da sie einem besonderem, individuellem Schutzbedürfnis gegenüber stehen. Die Befriedigung dieses Schutzbedürfnisses wiegt schwerer, als bei anderen personenbezogenen Daten.

Im Umkehrschluss sind Mängel an Schutzmechanismen für privatsphärenrelevante Daten wesentlich gravierender, als bei anderen personenbezogenen Daten.

2.2.2 Unterscheidung von Daten anhand der Quelle und Ablageort

In 2.2.1 wurde das Kriterium der »Privatsphärenrelevanz« zur Unterscheidung von Arten privater Daten erläutert. Weitere in dieser Studie genutzte Unterscheidungskriterien sind die **Quelle der Daten** und ihr **Ablageort innerhalb der Plattform**. Beide werden im Folgenden beschrieben:

Die Quelle für personenbezogene Daten ist der Betroffene selbst oder ein anderer Plattformnutzer der Daten zum Betroffenen eingibt. Der letztere Fall hat eine besondere Relevanz. Man spricht dann von **fremdgenerierten Daten**. Beispiele dafür sind das Markieren auf einem Foto abgebildeter Personen (Fotoverknüpfungen) durch andere Plattformmitglieder oder auch Gästebucheinträge in fremde Gästebücher.

Hinsichtlich fremdgenerierter Daten wird deren Ablageort hier nicht weiter differenziert, da der Privatsphärenschutz für diese Datenart *umfassend* ausgelegt

sein muss. Diese Forderung ist damit begründet, dass der Betroffene selbst nicht Quelle der Daten beziehungsweise Initiator der Dateneingabe ist. Ohne Schutzmechanismen würde er unerwünschten Informationsverbreitungen deshalb hilflos gegenüberstehen.

Demgegenüber wird bei **selbstgenerierten Daten**, also Daten die der Betroffene selbst in die Plattform eingibt, der Ablageort unterschieden:

Einen überwiegenden Teil der eigenen personenbezogenen Daten speichert der Nutzer im sogenannten »Profil« (**Profildaten**). Es bildet die Identität des Nutzers in der Plattform ab. Dabei wirkt es gleichzeitig als zentraler Zugriffspunkt auf Nutzerdaten, ähnlich einer Karteikarte in einem Register.

Daneben legen Plattformnutzer auch eigene private **Daten außerhalb des Profils** ab, z. B. als Beitrag in einem Forum oder als Kommentar in einem fremden Gästebuch.

Je nach Speicherort hat der Nutzer andere Erwartungen hinsichtlich des Privatsphärenschutzes. Daten die der Anwender außerhalb des eigenen Profils verbreitet, werden in einem öffentlichem Raum in der Plattform preisgegeben. Da er diesen Raum mit anderen Nutzern gemeinsam gestaltet, kann man hier nur begrenzt Schutzmechanismen erwarten.

Ein dritter Speicherort für personenbezogene Daten sind die **Bestandsdaten beim Plattformbetreiber**. Sie sind hinsichtlich des Vertragsverhältnisses zwischen Dienstanbieter und Dienstnutzer notwendig. Der Nutzer gibt diese Daten zum Eröffnen des Nutzerkontos ein. Sie können teilweise in die Profildaten einfließen, wie z. B. der Vorname und Name, müssen es aber nicht.

Abbildung 2.1 gibt zu den getroffenen Unterscheidungen nach Quelle und Speicherort einen Überblick. Dabei werden auch verschiedene Aktionen über diesen Daten dargestellt.

2.2.3 Phasen der Datenverarbeitung und -nutzung

Die Datenverarbeitung innerhalb der Plattform durchläuft für jeden einzelnen Nutzer verschiedene Phasen. Diese werden grob wie folgt eingeteilt:

1. **Anmelden** bzw. Registrieren an der Plattform und Erzeugen des Profils. Dabei gibt der Nutzer auch die Bestandsdaten für den Plattformbetreiber ein.
2. **Eingabe** von Daten zum Auffüllen des Profils. Ein Teil davon kann bereits bei der Anmeldung verpflichtend erfolgt sein.
3. **Nutzung** der Plattform durch Interaktion mit anderen Personen. Dabei werden zwangsläufig bewusst oder unbewusst Daten an (bestimmte) andere Anwender übermittelt. Der Nutzer generiert durch die Interaktion mit der Plattform Daten außerhalb des Profils. Die anderen Anwender der Plattform erzeugen wiederum fremdgenerierte Daten, die eindeutig mit dem Nutzer verknüpft sind.

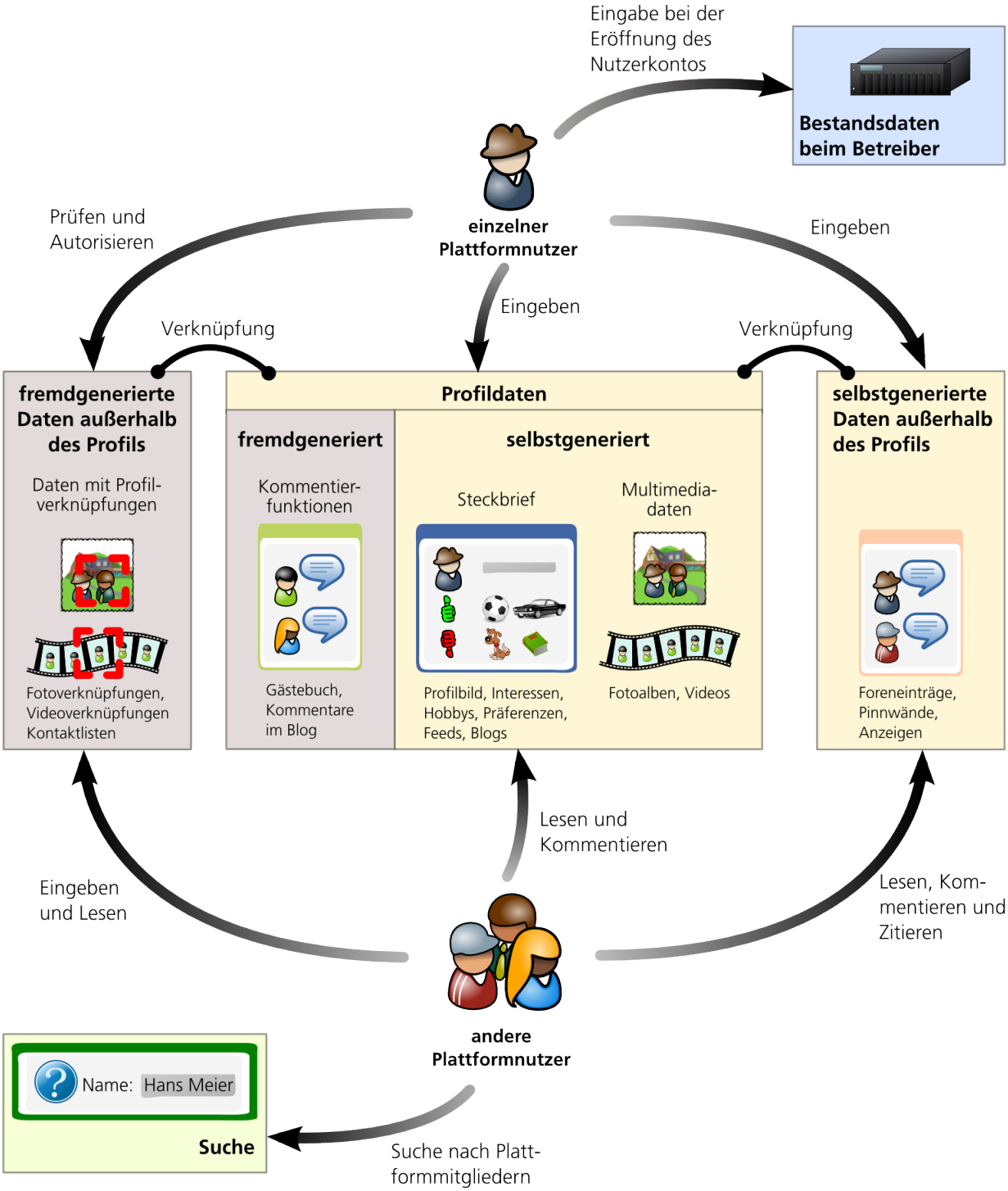


Abbildung 2.1: Verschiedene Datenarten und mit ihnen verbundene Nutzeraktionen

4. **Abmelden** von der Plattform und permanente Aufgabe der Mitgliedschaft.

Bei der späteren Aufstellung der Testkriterien wird gezeigt, dass einige nur in bestimmten Phasen relevant sind (siehe Kapitel 3).

2.2.4 Komponenten von Soziale-Netzwerke-Plattformen

Abschließend erfolgt noch eine kurze Erläuterung, welche Komponenten Soziale-Netzwerke-Plattformen zur Verfügung stellen, um private Daten zu speichern und zu verarbeiten. Einige wurden in vorhergehenden Abschnitten schon erwähnt (z. B. in Abbildung 2.1).

Gruppen

Gruppen erfüllen verschiedene Funktionen in Soziale-Netzwerke-Plattformen: Gruppenzugehörigkeit wird dazu verwendet, sich von anderen Nutzern zu differenzen, die dieser Gruppe nicht angehören. Ebenso werden bestimmte Präferenzen und gemeinsame, verbindende Eigenschaften der Mitglieder durch die Gruppenmitgliedschaft zum Ausdruck gebracht.

Nutzer können Gruppen jeweils gesondert beitreten, beziehungsweise die Mitgliedschaft später auch wieder beenden. Die Gruppen in denen ein Nutzer Mitglied ist, werden bei einigen Plattformen in seinem Profil aufgelistet (siehe Abbildung 2.2).

Gruppen können ausgezeichnete Mitglieder besitzen, die zusätzliche Rechte wahrnehmen. Zu diesen Rechten gehört z. B. die spezielle Erlaubnis, Gruppenmitglieder aufnehmen und ausschließen zu können. Möglich ist auch die Moderation von angeschlossenen Foren. Bei einigen Plattformen besitzen Gruppen ein eigenes »Profil«, in dem der Gruppenzweck, bestimmte gruppenspezifische Information und eine Mitgliederliste gespeichert sind (siehe Abbildung 2.3).

Fotoalben

Fotoalben dienen zur Ablage von Fotos innerhalb der Plattform. Jeder Nutzer kann ein Album erstellen und mithilfe seines Webbrowsers Bilder in dieses Album hochladen. Die Alben eines Nutzers sind in dessen Profil verlinkt. Ein anderes Plattformmitglied, welches das Profil besucht, kann die Alben öffnen und die darin enthaltenen Bilder betrachten und herunterladen (siehe Abbildung 2.4).

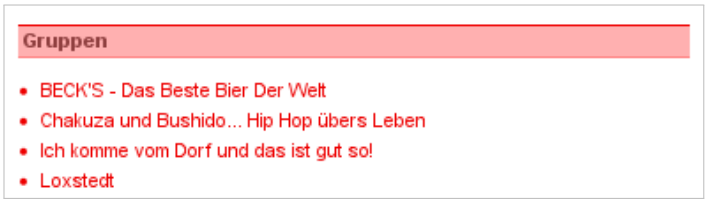


Abbildung 2.2: Gruppenauflistung aus einem studiVZ-Profil (Quelle: studivz.de)

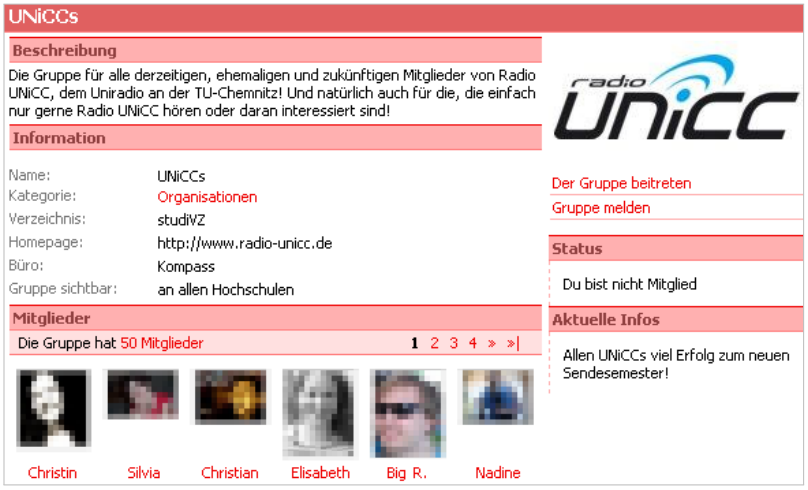


Abbildung 2.3: Profil einer Gruppe in studiVZ (Quelle: studivz.de)

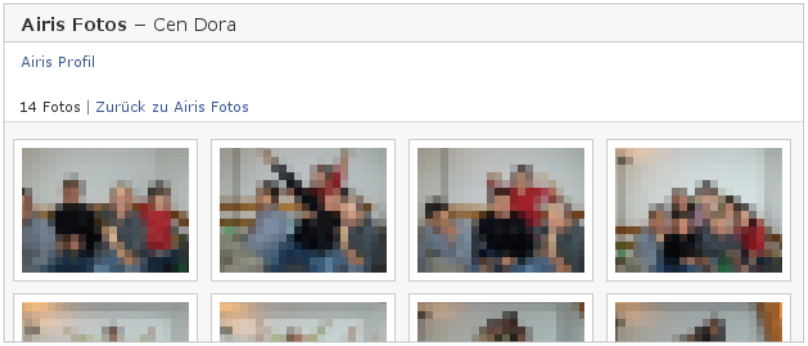


Abbildung 2.4: Fotoalbum bei facebook (Quelle: facebook.com)

Weiterhin bieten viele Plattformen an, Personen in Fotos zu markieren. Dabei wird mit dem Mauszeiger um ein Gesicht, welches man erkannt zu haben meint, ein Rahmen gezogen. Dieser Rahmen wird dann mit einem Profil verknüpft (siehe Abbildung 2.5).

Diese Verknüpfung wirkt bidirektional. Das bedeutet, dass in dem Profil der verknüpften Person ein Liste von Fotos gespeichert wird, auf denen diese Person zu sehen ist. Andersherum gelangt man beim Anklicken des Rahmens sofort zum Profil des abgebildeten Nutzers.

Abbildung 2.5: Fotoverknüpfung (grauer Rahmen) bei facebook (Quelle: facebook.com)

Suchfunktion

Die Suche ist eine wichtige Funktion in Soziale-Netzwerke-Plattformen. Sie dient dem gezielten Auffinden von Nutzerprofilen, um so der großen Datenmenge Herr zu werden.

Die Suche besitzt häufig einen vereinfachten und einen erweiterten Modus:

Im vereinfachten Modus wird nur der Name als Suchkriterium angegeben. Diese Funktion dient dem gezielten Suchen nach Einzelpersonen. Im erweiterten Modus sind weitere Kriterien erlaubt, so z. B. die Angabe einer Hochschule oder eines Hobbys. Ziel solcher erweiterten Suchanfragen ist es beispielsweise Personen mit ähnlichen Interessen zu finden.

Wurde die Plattformsuche abgeschlossen, so wird das Suchergebnis in Form einer Liste aller passenden Profile ausgegeben. Der Nutzer kann diese Liste dann »abarbeiten«, indem er die einzelnen Profile betrachtet und die für ihn interessanten Personen für weitere Aktionen vorsieht.

Gästebücher

Gästebücher sind direkt in den Nutzerprofilen eingeblendet. Sie bieten anderen Plattformmitgliedern die Möglichkeit, Kommentare zum Profil oder dem Profilinhaber zu hinterlassen. Solche Kommentare werden dann, nach der Reihenfolge ihres Veröffentlichungszeitpunktes geordnet, im Gästebuch aufgelistet.

Die Kommentare sind in der Regel mit den Nutzerprofilen ihrer Autoren verknüpft.

Blogs

Blogs sind digitale Tagebücher in denen der Plattformnutzer zu bestimmten Zeitpunkten aktuelle Gedanken und Erlebnisse festhält. Im Gegensatz zu News-Feeds beschränken sich die Einträge häufig nicht auf kurze Mitteilungen, sondern können umfangreiche Texte darstellen.

Das Blog eines Plattformnutzers ist über dessen Profil direkt erreichbar oder sogar auf der Profilseite eingeblendet.

News-Feeds

In News-Feeds legt der Nutzer aktuelle, kurze Meldungen ab, die in der Regel Ereignisse aus seinem Privatleben wiedergeben. Einige Plattformen protokollieren in News-Feeds auch Veränderungen im Profil oder Vorkommnisse bei den Kontakten des Nutzers (siehe Abbildung 2.6).

Videos

Einige Plattformen erlauben auch das Speichern von Videodateien. Die Funktion ähnelt der Ablage von Fotos. Es sind sogar Verknüpfungen mit den Profilen abgebildeter Personen möglich, analog zur Fotoverknüpfung.

Abbildung 2.6: Beispiel für einen News-Feed (Quelle: facebook.com)

Abbildung 2.7: Beispiel für ein Forum (Quelle: öffentliches Forum bei xing.com)

Foren

Foren werden von den Plattformmitgliedern genutzt, um Meinungen, Standpunkte oder Wissen zu bestimmten Themen auszutauschen. Der Austausch wird in sogenannten »Threads« (Gesprächsfäden) organisiert, die zu einem Thema generierte Nachrichten sammeln. Die Nachrichten sind dabei chronologisch nach dem Zeitpunkt ihrer Veröffentlichung sortiert.

Erstellt ein Nutzer eine neue Nachricht, so ist es üblich, Teile der vorhergehenden, älteren Nachrichten anderer Nutzer zu zitieren und sich darauf zu beziehen. So wird das diskutierte Thema systematisch weiterentwickelt (siehe auch Abbildung 2.7).

In der Regel können alle Nutzer, die Zugang zu einem Forum besitzen, alle dort veröffentlichten Nachrichten einsehen. Foren existieren separat neben den Nutzerprofilen, können aber Gruppen untergeordnet sein. So kann z. B. eine Gruppe »Hundeliebhaber« ein geschlossenes Forum besitzen, in dem Tierkrankheiten diskutiert werden. Nur die Gruppenmitglieder haben dann die Erlaubnis im Forum zu lesen oder zu schreiben.

Es ist weiterhin üblich, einzelne Forennachrichten mit dem Nutzerprofil des Autors zu verknüpfen. Diese Verknüpfung ist eine Variante, wie der direkte Personenbezug der Daten hergestellt wird. Eine andere ist z. B. das Unterschreiben der Nachricht mit dem vollständigen, realen Namen des Autors.

Abbildung 2.8: Kontaktliste bei facebook (Quelle: facebook.com)

Kontaktlisten

Die Kontaktliste oder auch Freundesliste ist im Profil eines jeden Nutzers verankert und aggregiert seine eigenen Kontakte zu anderen Plattformnutzern (siehe Abbildung 2.8). Diese Aggregation stellt de facto sein persönliches soziales Netzwerk innerhalb der Plattform dar.

Verknüpfungen über Kontaktlisten müssen, je nach Plattform, nicht zwingend bidrektional ausgebildet sein: Erscheint Person A in der Kontaktliste von Person B, so muss das nicht zwangsläufig umgekehrt der Fall sein.

Die privaten Daten der Kontakte lassen, wenn auch begrenzt, Rückschlüsse auf nicht sichtbare Eigenschaften des Profilinhabers zu. Das ist z. B. dann der Fall, wenn eine Person über viele Kontakte zu Mitgliedern einer bestimmten politischen Partei verfügt. Es ist dann plausibel anzunehmen, dass diese Person ebenfalls dieser Partei nahesteht. Genauso gut besteht aber auch die Gefahr, über diesen Weg als Betrachter falsche Informationen zu generieren. Diese können zur Vorurteilsbildung oder Stigmatisierung führen. Die Kontaktliste ist deshalb besonders anfällig für die Offenbarung sensibler Informationen durch Verknüpfung mit den Daten anderer Nutzer.

Weitere Komponenten

Folgende weitere Komponenten sind in einzelnen Plattformen implementiert:

- **Statusanzeige**, welche anzeigt, ob eine Person momentan an einer Plattform eingeloggt ist.
- **Kleinanzeigen**, mit denen ein Nutzer Anfragen oder Angebote in die Plattform einstellen kann. Eine speziellere Form von Kleinanzeigen ist ein Stellenmarkt.
- **Kalender**, der geplante Aktivitäten und Termine eines Nutzers anzeigt.

3 Testkriterien und Anforderungen an Plattformen

Zur Durchführung der Evaluation werden Testkriterien festgelegt, welche sich aus der Verknüpfung zweier in Kapitel 2 erörterter Aspekte ergeben:

- Zum einen hegen Nutzer der Plattformen den Wunsch, dass eingegebene private Informationen nur zu bestimmten Zwecken verarbeitet werden (vergleiche 2.1). Weiterhin sind Informationen nur an einen bestimmten Empfängerkreis weiterzuleiten. Auf diesen Empfängerkreis sollte der Nutzer Einfluss haben. Dieser Wunsch nach Privatsphärenschutz kann als übergeordnetes Ziel angesehen werden, an dem sich Kriterien und Anforderungen orientieren.
- Dem gegenüber steht die konzeptionelle und technische Ausgestaltung der Plattformen mit ihren verschiedenen Komponenten, Funktionen und Prozessen (vergleiche 2.2). Auf dieser technischen Ebene sollte der abstrakte Wunsch der Anwender nach Privatsphäre weitestgehend Berücksichtigung finden.

Mit den Kriterien werden Anforderungen verknüpft, welche ebenfalls in diesem Kapitel erläutert sind. Der Umfang, in dem eine hier formulierte Anforderung erfüllt wird, bestimmt die Einzelbewertung für das zugehörige Kriterium.

Die aufgeführten Kriterien berücksichtigen hauptsächlich den Schutz der Vertraulichkeit von Daten. Kriterien, die die Integrität oder auch die Verfügbarkeit betreffen, sind in dieser Studie aufgrund der eingeschränkten Testmethodik nicht anwendbar (Black-Box-Test, legale Einschränkungen, vergleiche auch 4.3). Sie werden deshalb nicht aufgestellt, wenngleich sie aus Sicht des Betroffenen ebenfalls relevant sein können und einer Untersuchung bedürfen.

Im Bereich des Datenschutzes sind bereits verschiedene Anforderungen an Datenverarbeitungsanlagen und die damit verknüpften Prozesse einschlägig (siehe z. B. [3] oder [39] mit [38]). Beispiele dafür sind:

- Frühzeitige Pseudonymisierung oder Anonymisierung
- Vorhandensein einer Zugriffskontrolle
- Sichern von Datenübertragungen
- Löschen nach Wegfall des Verwendungszwecks
- Datensparsamkeit
- Protokollierung der Ein- und Ausgabe von Daten

Jedoch liegt im »klassischen« Datenschutz der Fokus primär auf Beziehungen des Staates zum Bürger oder von Unternehmen zu Einzelpersonen (Verbraucher, Mitarbeiter etc.). Diese Kategorien treffen hier nur teilweise zu. Vielmehr geht es im hohen Maße um die Beziehungen zwischen Privatpersonen im Daten- bzw. Informationsaustausch.

Der Kriterienkatalog für diese Studie orientiert sich aus Gründen der Transparenz dennoch in ausgewählten Punkten an oben beschriebenen organisatorisch-technischen Anforderungen aus dem Datenschutz. Weiterhin erfolgt ein Zuschnitt auf die speziellen Eigenschaften und Besonderheiten von Soziale-Netzwerke-Plattformen. Die Kriterien sind somit unmittelbar, ohne eine weitere Zwischenstufe in der Betrachtung, einheitlich auf Privat- und auf Geschäftsplattformen anwendbar. Folglich sind die resultierenden Bewertungsergebnisse untereinander direkt vergleichbar.

Teile des Anforderungskatalogs dieser Studie ähneln denen in anderen Publikationen zum Thema. Als Beispiele seien hier das »Rom Memorandum« der International Working Group on Data Protection in Telecommunications (IWGDPT)[25] oder eine entsprechende Entschließung der Obersten Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich (Düsseldorfer Kreis) [31] erwähnt.

Die weiteren Abschnitte sind wie folgt strukturiert:

Zu Beginn steht eine kurze Zusammenfassung, die Prüfkriterien und Anforderungen benennt. Diese Zusammenfassung ist durch einen grauen Balken am Textrand hervorgehoben. Anschließend wird erläutert, wie das Kriterium genau zu verstehen ist und wie die Anforderungen hergeleitet beziehungsweise zu begründen sind.

3.1 Geforderte Daten bei der Anmeldung

Prüfkriterien

Für diese Studie wurde untersucht, welche Daten der Nutzer bei der Neuanmeldung an der Plattform angeben muss und ob der Betreiber den Zugang zum Dienst nach dem Stand der Technik oder aufgrund rechtlicher Auflagen tatsächlich nur nach deren Eingabe gewähren kann.

Anforderungen

Eine Soziale-Netzwerke-Plattform sollte für die Eröffnung der Mitgliedschaft so wenig wie möglich Pflichtangaben vom neuen Nutzer fordern. Es dürfen nur Daten abgefragt werden, welche für die technische Realisierung des Dienstes oder die Erfüllung rechtlicher Auflagen notwendig sind.

Bei der Anmeldung an einer Soziale-Netzwerke-Plattform werden bereits bestimmte Daten abgefragt, um die Registrierung überhaupt durchführen zu können. Sie sind primär als Bestandsdaten für das Vertragsverhältnis zwischen Plattformnutzer und Plattformbetreiber notwendig. Zum anderen werden sie häufig dazu genutzt, das Nutzerprofil mit initialem Inhalt zu füllen.

Um eine hier beschriebene Web-Anwendung überhaupt zugänglich zu machen, ist nach der derzeit gängigen, technischen Praxis zumindest eine Nutzerkennung und ein Passwort erforderlich. Eine Erfassung dieser Daten steht im beiderseitigem Interesse des Plattformbetreibers und -anwenders. Darüber hinausgehende, weitere Angaben sind eher kritisch zu sehen. Es bedarf einer Begründung um sie zu erheben. Dabei dürfen die Daten nur zwingend erforderlich sein, um den Dienst zu erbringen und auszugestalten.

Ein Beispiel ist die Erhebung des Geburtsdatums, welche mit Jugendschutz begründet wird. Es könnten alternativ datensparsamere Mechanismen vorgezogen werden, wie z. B. eine Abfrage »Sind Sie älter als 18?«. Das vollständige Geburtsdatum ist also nicht zwingend erforderlich.

Weiterhin kann beispielsweise der Schutz vor Plattformmissbrauch die Erhebung bestimmter Daten notwendig machen. Dazu zählt z. B. der vollständige Name und eine E-Mail-Adresse. Allerdings ist auch die Eignung dieser Daten bezüglich des Erhebungszweckes zu prüfen. So erscheint es fraglich, ob bei geplanter missbräuchlicher Nutzung der Anwender zuvor korrekte Angaben macht.

3.2 Pseudonyme Nutzung

Prüfkriterien

Getestet wurde, ob und in welcher Form eine Soziale-Netzwerke-Plattform eine Nutzung mittels Pseudonym zulässt.

Anforderungen

Die getesteten Plattformen müssen eine Möglichkeit zur pseudonymen Plattformnutzung vorsehen. Weiterhin dürfen sie keine Funktionen anbieten, mit denen eine Depseudonymisierung erfolgen kann.

Pseudonymisierung stellt eine besondere Vorgehensweise dar, mit der Nutzer den Zugriff auf private Daten regulieren. Die Idee ist, den Identifikator zu ersetzen, unter dem eine reale Person erreicht wird. Anstatt eines mehr oder weniger eindeutigen Identifkationsmerkmals, wie z. B. Name und Vorname eines Nutzers, wird ein Pseudonym verwendet. Ein Pseudonym ist ein Kennzeichen, von dem nicht oder nur mit erheblichem Aufwand auf den »echten« Identifikator geschlossen werden kann. Für Soziale-Netzwerke-Plattformen eignen sich dafür fiktive Namen (Spitznamen etc.) besonders gut.

Die Annahme ist, dass durch Pseudonymisieren der Personenbezug von Daten teilweise aufgehoben wird. Private Daten können dann zwar einer »virtuellen Identität« zugeordnet werden, aber nur schwer einer realen Person. Damit wird die Privatsphäre geschützt. Allerdings besteht immer die Gefahr einer Depseudonymisierung, also der ungewollten Offenlegung der realen Identität.

Trotzdem handelt es sich bei der Pseudonymisierung um einen Mechanismus, der bei vielen Web 2.0-Diensten angeboten wird. Er sollte deshalb auch von Soziale-Netzwerke-Plattform unterstützt werden, zumindest wenn sie für den privaten Anwendungsbereich konzipiert sind.

Pseudonyme Nutzung impliziert an dieser Stelle nicht, dass der Plattformbetreiber in seinen Bestandsdaten nicht den Klartextnamen des Anwenders speichern darf (vergleiche 3.1). Dieser darf dann aber nicht innerhalb der Plattform kommuniziert werden, sondern ist immer durch das Pseudonym zu ersetzen.

3.3 Einsatz von Verschlüsselung

Prüfkriterien

Im Rahmen dieser Prüfung wurde untersucht, ob eine Verschlüsselung des Kommunikationskanals zwischen dem Webbrowser des Nutzers und der Web-Anwendung des Dienstbetreibers vorhanden ist. Weiterhin wurde getestet auf welche der übermittelten Daten sich die Verschlüsselung genau erstreckt.

Anforderungen

Eine Soziale-Netzwerke-Plattform muss während einer Nutzersitzung Datenübertragungen zwischen dem Webbrowser des Nutzers und der Webanwendung beim Betreiber vollständig verschlüsseln.

Private Daten sind nicht nur in der Plattform selbst gefährdet, sondern auch auf dem Übertragungsweg zwischen Plattformbetreiber und Dienstnutzer. Deshalb sind die verwendeten Kommunikationskanäle zu verschlüsseln. Andernfalls kann ein Angreifer private Daten ausspionieren oder auch Passwörter und Sitzungsgeheimnisse mithören.

Der Grad der Verschlüsselung wird in drei Kategorien unterschieden werden:

- **Vollverschlüsselung** über die gesamte Nutzersitzung hinweg (inklusive Login-Daten).
- **Teilverschlüsselung** zum ausschließlichen Schutz des Nutzergeheimnisses (Passwort) beim Login und beim Laden ausgewählter Plattformseiten (z. B. Konfigurationsdialoge)
- **kein Einsatz von Verschlüsselung**

Besonders ungünstig ist die letzte Variante, da sie einem Angreifer beliebigen Vollzugriff auf die Datenübertragungen ermöglicht. Aber auch die Teilverschlüsselung etabliert nur ein geringes Sicherheitsniveau. In dieser Variante wird beim Übertragen von Nutzername und Passwort zum Plattform-Server und einigen anderen Aktionen kurzzeitig ein verschlüsselter Kanal aktiviert. Der Plattform-Server antwortet nach erfolgreicher Authentifizierung des Nutzers mit dem Setzen eines dedizierten Cookies im Webbrowser des Nutzers. Anschließend wird der verschlüsselte Kanal wieder abgebaut. Die weiteren Übertragungen erfolgen nun unverschlüsselt.

Das Cookie ist der Nachweis für das erfolgte Login und ist somit vergleichbar »wertvoll« wie ein Passwort. Es wird bei jeder Datenübertragung zwischen dem Webbrowser des Nutzers und dem Plattform-Server unverschlüsselt übermittelt. Dieser Mechanismus endet frühestens beim Logout. Ein Angreifer kann es bis zu diesem Zeitpunkt leicht abhören und sich selbst in die Sitzung einschalten oder die Sitzung übernehmen (sogenanntes »Session Hijacking«). Gegen derartiges Abhören auf Netzwerkebene ist als Sicherheitsmaßnahme die Vollverschlüsselung notwendig.

Szenarien in denen eine solche Attacke durchgeführt werden kann, sind begrenzt. Allerdings erfreut sich gerade die Nutzung von Soziale-Netzerk-Plattformen in öffentlichen Netzwerken, also z. B. öffentlichen WLAN-Netzen in Bahnhöfen oder Internetcafes zunehmender Beliebtheit. Angreifer finden somit leicht lohnende Angriffsziele.

Besonders kritisch ist, dass das Einbrechen in einen Nutzerzugang nicht nur den betroffenen Anwender selbst kompromittiert, sondern auch die Plattformmitglieder, die diesem Anwender spezielle Zugriffsrechte auf eigene Daten eingeräumt haben (vergleiche 3.4). Mit anderen Worten: Wenn ein Freund eines Anwenders ein unsicheres Drahtlosnetzwerk betreibt, dann sind die in der Plattform gespeicherten Daten dieses Anwenders über den Nutzerzugang des Freundes genauso bedroht, als wenn er selbst unsicher im Internet »surfen« würde.

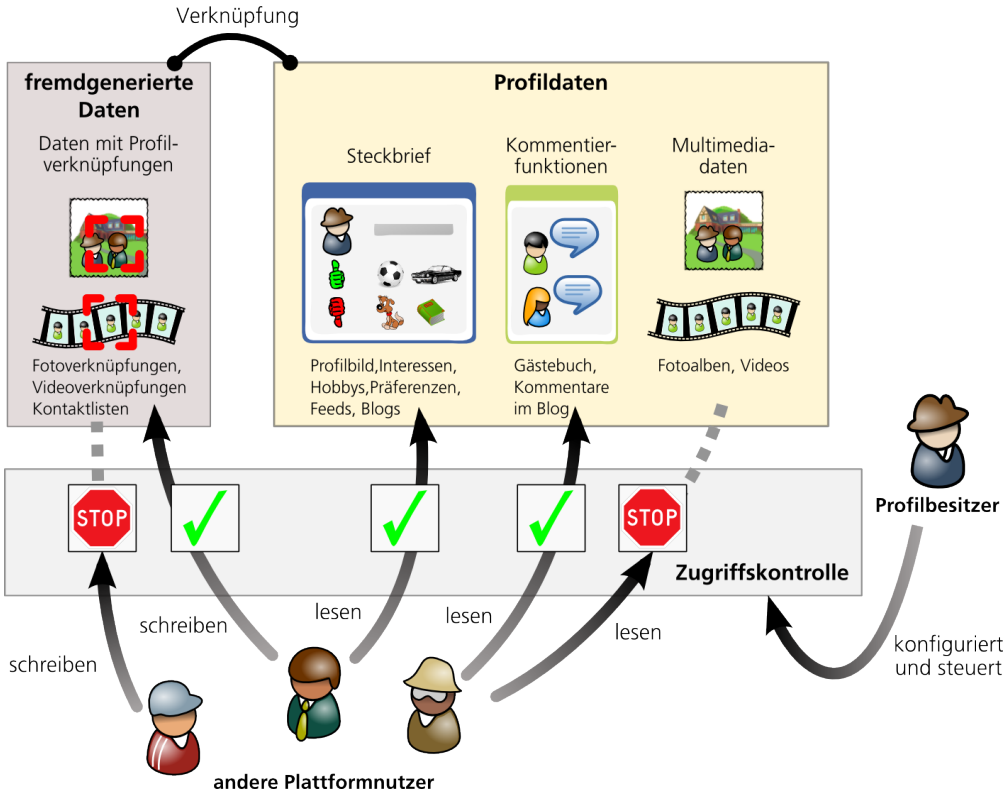


Abbildung 3.1: Wirkungsweise von Zugriffs-kontrollen in Soziale-Netzwerke-Plattformen

3.4 Funktionsumfang der Zugriffskontrollen

Prüfkriterien

Untersucht wurde, wie die Zugriffskontrollen zum Schutz privater Daten gestaltet sind. Hauptkriterien sind dabei die Gruppen der Zugreifenden, die schützbaren Datenobjekte und die Handhabung fremdgenerierter Daten.

Anforderungen

Die Plattform muss Funktionen vorsehen, mit deren Hilfe der Nutzer den Zugriff auf seine privaten Daten steuern kann. Es muss also gewährleistet sein, dass der Nutzer selbst Regeln festlegen kann, nach denen andere Plattformmitglieder oder beliebige Internetnutzer seine privaten Daten lesen und schreiben dürfen. Der aktivierbare Schutz muss dabei zwingend privatsphärenrelevante Daten erfassen.

Der Zugriff auf private Daten wird auf der Basis von Regeln gestattet oder verweigert, die vom Profilbesitzer bzw. Betroffenen zuvor eingegeben wurden. Dieses Prinzip ist in Abbildung 3.1 erläutert.

Tabelle 3.1: Beispiel für eine Zugriffskontrollmatrix

	Gruppen		
	Internet	Plattform-mitglieder	Kontakte 1. Grades
lesender Zugriff			
Name	✔	✔	✔
Hobbys	✖	✖	✔
Kontaktliste	✖	✖	✔
Fotos	✖	✔	✔
schreibender Zugriff			
Gästebuch	✖	✖	✔

Lesender Zugriff

Anwender können den lesenden Zugriff auf bestimmte Daten innerhalb einer Plattform einschränken. So möchte man z. B., dass die eigenen Hobbys von jedermann lesbar sind, das Geburtsdatum aber nur von Freunden.

Bei Soziale-Netzwerke-Plattformen werden üblicherweise Gruppen-basierte Zugriffskontrollen verwendet. Anwender werden in einer bestimmten Art und Weise einer Gruppe bezüglich eines anderen Anwenders zugeordnet. Solche Gruppen sind z. B. »Freund« eines Anwenders oder »Freund eines Freundes« eines Anwenders. Der Anwender kann die Zusammensetzung dieser Gruppen für sich teilweise selbst bestimmen, im Fall des »Freund eines Freundes« wird diese Zusammenstellung aber auch von Anderen, eben den »Freunden 1. Grades« beeinflusst.

Hinzu kommt, dass die Gruppen selbst einer Hierarchie unterliegen. Ein Plattformanwender ist als »Freund« gleichzeitig in der Gruppe »Alle Anwender der Plattform«. Diese Hierarchie bewirkt eine Rechtevererbung hin zu den spezialisierteren (kleineren) Gruppen.

Orthogonal zu den Gruppen stehen Objekte auf die potentiell zugegriffen werden kann, also z. B. ein Fotoalbum oder eben das eigene Geburtsdatum. Somit ergibt sich eine Zugriffskontrollmatrix, wie in Tabelle 3.1 gezeigt.

Im Idealfall erlaubt eine Soziale-Netzwerke-Plattform ihren Nutzern, an jedem Punkt der Matrix den Zugriff zu beschränken oder freizugeben.

Darüberhinaus sollte zumindest die Möglichkeit bestehen, einzelne Nutzer komplett auszuschließen (sogenanntes »Blacklisting«). Allerdings kann ein ausgeschlossener Nutzer das Blacklisting in bestimmten Szenarien leicht umgehen. Dazu wird einfach ein weiteres Nutzerkonto angemeldet und mit der neuen

Identität auf die Daten zugegriffen. Blacklisting ist deshalb nur in besonderen Fällen hilfreich, so z. B. wenn parallel eine Einschränkung auf eine spezielle-re Gruppe erfolgt, der ein Nutzer mit einer gefälschten Plattformidentität nur schwer beitreten kann.

Auch ein explizites, verdecktes Freigeben des Lesezugriffs für einzelne Personen sollte möglich sein (sogenanntes »Whitelisting«). Der Begriff »verdeckt« bezieht sich darauf, dass die Freigabe für andere Nutzer, egal welcher Gruppe sie auch immer angehören, nicht sichtbar ist. Kann eine Freigabe für eine Einzelperson so z. B. nur über die Aufnahme in eine »Freundesliste« erfolgen, dann ist immer zu bedenken, dass der Inhalt dieser Liste selbst in der Plattform verbreitet wird. Dieser Umstand ist nicht in jedem Fall erwünscht.

Schreibender Zugriff

Wie bereits in 2.2 beschrieben, werden in Soziale-Netzwerke-Plattformen auch Daten mit Personenbezug[1] hinterlegt, die nicht der Betroffene selbst, sondern andere Plattformmitgliedern eingegeben. Beispiele dafür sind Gästebucheinträge, Kontaktverknüpfungen in fremden Profilen oder Verknüpfungen auf Fotos.

Die Plattform muss dem Anwender Funktionen an die Hand geben, mit denen er auch diese Daten kontrollieren kann. Im Idealfall muss jedes einzelne, fremderzeugte Datum vom Anwender vor Veröffentlichung individuell autorisiert werden (vorgelagerte Autorisierung). Als Mindestmaßnahme ist ein »Vetorecht« vorzusehen, welches dem Anwender erlaubt zumindest im Nachhinein die mit seiner Person verknüpften Daten zu löschen (im Folgenden als nachgelagertes Vetorecht bezeichnet).

Existiert ausschließlich ein nachgelagertes Vetorecht, so muss der Anwender zumindest die Gruppe derer beschränken können, die Daten mit Personenbezug auf ihn selbst erstellen dürfen. Im Grunde handelt es sich dann um eine Zugriffskontrolle, die schreibenden Zugriffe Gruppen-basiert einschränkt. Ein Beispiel wäre, dass z. B. nur Personen in der Kontaktliste eines Anwenders einen Eintrag in dessen Gästebuch hinterlassen dürfen.

Geprüfte Funktionen

Zur genaueren Bewertung der Zugriffskontrolle wurde untersucht:

- Welche Gruppen unterscheidet die Zugriffskontrolle?
- Auf welche Datenobjekte kann der Zugriff gegenüber diesen Gruppen eingeschränkt werden?
- Existieren Gruppen deren Zusammensetzung der Anwender unmittelbar und vollständig selbst beeinflussen kann?

[1] Gemeint sind hier nur Daten, die technisch direkt mit dem betroffenen Anwender verknüpft sind, so z. B. per Hyperlink auf sein Profil oder durch Abbildung im Profilkontext des Betroffenen.

- Ist das Ausschließen einzelner Nutzer vom Zugriff auf private Daten möglich? (sogenanntes »Blacklisting«)
- Ist das verdeckte Gewähren des Datenzugriffs gegenüber einzelnen Nutzern möglich? (sogenanntes »Whitelisting«)
- Welche Daten mit direktem Personenbezug (z. B. Verknüpfung mittels Hyperlink) können von anderen Plattformmitgliedern erzeugt werden? (fremdgenerierte Daten)
- Hat der Anwender per vorgelagerter Autorisierung oder nachgelagertem Veto Einfluss auf die Veröffentlichung fremdgenerierter Daten? Kann gruppenspezifisch Schreibzugriff gewährt werden? Wird beim nachgelagerten Veto der Nutzer über neu geschriebene Daten von der Plattform informiert?

Umgehen von Zugriffskontrollen

Unter Umständen kann ein Angreifer Zugriffskontrollen aushebeln, indem er Schwachstellen in der Software ausnutzt. Dieses Problem wird in dieser Studie aufgrund legaler Einschränkungen nur begrenzt untersucht (siehe auch 4.3). Zwei der folgenden Kriterien zielen aber darauf ab, derartige technische und konzeptionelle Mängel ansatzweise offenzulegen:

- Schwachstellen beim Schutz von Multimediadaten (siehe 3.6)
- Auslesen privater Daten durch geschicktes Ausnutzen der Suchfunktion (siehe 3.7)

3.5 Standardkonfiguration

Prüfkriterien

Im Test wurden die Einstellungen der Zugriffskontrolle unmittelbar nach der Anmeldung geprüft.

Anforderungen

Die Standardkonfiguration der Zugriffskontrollen muss gewährleisten, dass die privaten Daten nach der Anmeldung bereits geschützt sind. Damit ist gemeint, dass nur solche Personengruppen standardmäßig auf die Daten zugreifen können, deren Zusammensetzung der Nutzer *vollständig* selbst bestimmen kann. Der Schutz muss sich in jedem Fall auf privatsphärenrelevante Daten erstrecken.

Nach der Anmeldung an der Plattform befinden sich die Einstellungen der Zugriffskontrolle in einem »Auslieferungszustand«. Diese sind bereits sehr restriktiv oder eher offen konfiguriert. In Hinblick darauf, dass viele Nutzer der Plattform technisch weniger versiert sind, ist die restriktive Variante vorzuziehen. Die

bestehenden Einschränkungen kann der Nutzer dann bewusst selbst schrittweise aufheben. Dies kann geschehen indem er in die bereits freigegebenen Personengruppen weitere Nutzer aufnimmt (z. B. durch Hinzufügen eines neuen »Freundes«) oder ganze Personengruppen neu hinzuzieht (z. B. Freigabe für »alle Plattformmitglieder«).

3.6 Externer Zugriff auf Multimediadaten

Prüfkriterien

Untersucht wurde, ob Multimediadaten wie Fotos und Videos durch Ausnutzung der Ressourcenverknüpfungen (Hyperlinks) zugänglich sind. Entscheidend war dabei, ob der Zugriff an den Zugriffskontrollen vorbei möglich war.

Anforderungen

Eine Soziale-Netzwerke-Plattformen muss gewährleisten, dass der Zugriff auf Multimediadaten wie Bilder oder Videos nur innerhalb der Plattform und gemäß den vom Nutzer gesetzten Zugriffskontrollen erlaubt ist. (Ausnahme: Nutzer gibt Daten für den beliebigen Internetzugriff frei.)

Private Daten werden in Soziale-Netzwerke-Plattformen auch in Form von Multimediadateien abgelegt. Diese sind besonders sensibel:

Bilder und Videos offenbaren umfangreiche Informationen über die Lebensumstände eines Nutzers. Dabei geht der potentielle Informationsgehalt zum Teil über den textbasierter Daten hinaus. Häufig sind diese »Schnappschüsse« zudem ohne Kenntnis des Entstehungskontexts nur schwer zu interpretieren. Es entstehen schnell Fehlschlüsse beim Betrachter, welche nicht im Interesse des Betroffenen liegen.

Problematisch ist aus technischer Sicht die Ablage solcher Mediendateien. Bilder und Videos werden häufig auf einem separaten Server gespeichert und an entsprechender Stelle per Link eingefügt, z. B. in ein Fotoalbum oder im Profil.

Zu prüfen ist, ob der Plattformbetreiber sicherstellt, dass Bilder und andere Mediendateien ausschließlich den Personen zugänglich sind, die dafür die nötigen Rechte besitzen und sich an der Plattform eingeloggt haben, also z. B. die Freunde eines Nutzers, bei entsprechend konfigurierter Zugriffskontrolle. Links auf Daten bzw. Medien dürfen nicht außerhalb der Plattform gültig sein, wenn der Nutzer dies nicht ausdrücklich wünscht.

Warum dieser Aspekt so wichtig ist, zeigt ein Blick auf zukünftige Technologien. So existiert bereits jetzt eine Suchmaschine namens »Polar Rose«[11] im Betastadium, welche mithilfe eines Browser-Plugins die URL von Bildern einsammelt

und an eine zentrale Datenbank übermittelt. Nach dem Erkennen von Gesichtern in den übermittelten Bildern, können Nutzer diesen Namen zuordnen. Auf dieser Datenbasis arbeitet dann der eigentliche Suchmaschinendienst. Es existiert damit eine externe Speicherung von Multimediadaten ohne ein weiteres Einwirken der Plattform-Zugriffskontrollen.

Desweiteren kann ein anderer Nutzer, möglicherweise aus bösartigen Gründen, gewollt eine Verknüpfung auf eine Mediendatei außerhalb der Plattform vorhalten. So kann z. B. ein Blog einen Hyperlink auf ein kompromittierendes Foto aus den Fotoalben eines Plattformnutzers speichern. Das mag vielleicht aus pragmatischen Gesichtspunkten heraus uninteressant sein, da dieser »Angreifer« genausogut eine simple Kopie der Bilddatei platzieren könnte. Allerdings ist es z. B. juristisch wenig problematisch, nicht das Bild zu kopieren, sondern den Link auf das »öffentliche« Bild zu setzen (Urheberrecht, Kunsturheberrecht).

Für die Tests wurde u.a. eine Betaversion von Polar Rose verwendet, um zu prüfen, ob die Software in der Lage war, Bilder aus den getesten Plattformen in den Suchindex des Dienstes zu übertragen. Wenn ja, dann deutet dies bereits auf eine Schwäche der Zugriffskontrolle hin.

3.7 Suchfunktion

Prüfkriterien

Bei den Tests wurde geprüft, welche Suchkriterien für die Plattformsuche erlaubt sind. Weiterhin wurde untersucht, ob die Zugriffskontrollen auch auf die Suche wirken oder durch diese ausgehebelt werden.

Anforderungen

Als Anforderung muss die Suchfunktion einer Soziale-Netzwerke-Plattform die vom Nutzer gesetzten Zugriffskontrollen berücksichtigen. Privatsphärenrelevante Daten, die nicht geschützt werden können, sind als Suchkriterium aus der Plattformsuche auszuschließen.

Bei fehlerhafter Gestaltung kann die Suchfunktion leicht Schwachstellen erzeugen, die es einem Angreifer erlauben private Daten unberechtigt auszulesen.

Grundsätzlich soll die Suche den Mitgliedern das gegenseitige Auffinden in der Plattform ermöglichen. Üblicherweise erfolgt daraufhin die, wie auch immer geartete Kontaktaufnahme zwischen den Suchenden und den Gefundenen.

Ohne Suche wäre der Nutzen der Plattformen stark eingegrenzt. Auf der anderen Seite stellt sie auch eine sensible Funktion dar: Ist sie zu umfassend und schrankenlos umgesetzt, kann sie leicht den Charakter einer »Rasterfahndung« annehmen. Das bedeutet, dass unspezifisch Nutzer in der Plattform gesucht

werden, die bestimmte Attribute (»das Raster«) aufweisen. Derartige Verfahren besitzen negative Auswirkungen auf die Privatsphäre.

Deswegen müssen Suchfunktionen die vom Nutzer gesetzten Regeln für Lesezugriffe berücksichtigen, da jede Suchanfrage selbst diverse Leseoperationen über seinen privaten Daten auslöst. Konfiguriert ein Anwender sein Profil also z. B. so, dass nur verlinkte Freunde den Berufsstatus »Student« einsehen können, dann muss die Suchfunktion dieses Profil aus der Ergebnismenge für eine Suchanfrage nach »Student« in »Darmstadt« entfernen, falls die Anfrage nicht von einem »Freund« generiert wurde. Eine Ergänzung um zusätzliche Regeln speziell für die Lesezugriffe der Suchfunktion ist ebenfalls denkbar. Allerdings dürfen sie nutzer- oder gruppenspezifische Beschränkungen nicht abschwächen oder gar aufheben.

Ohne Berücksichtigen der nutzerspezifischen Leseregeln schützt die Zugriffskontrolle zum einen nicht vor Rasterfahndungseffekten (»Suche alle Personen aus Frankfurt mit linkspolitischer Ausrichtung«), auf der anderen Seite wird die Zugriffskontrolle an für sich teilweise unwirksam:

Ist dem Angreifer der Name des Opfers bekannt, so kann er mithilfe der Suchfunktion verdeckte Daten aufdecken. Dazu iteriert er das passende Suchkriterium über die Elemente der diskreten Wertemenge des verdeckten Datums. Dieser Angriff funktioniert umso schneller, je weniger Elemente diese Wertemenge enthält.

Ein Beispiel ist ein Nutzer der seinen »Berufsstatus« als »nicht sichtbar« konfiguriert. Die Plattform lässt für den Berufsstatus nur den Wert »Schüler«, »Student« oder »Alumni« zu. Der Angreifer kennt den Namen des angegriffenen Nutzers und möchte seinen Berufsstatus herausfinden, wenngleich er das Datum nicht sehen darf. Der Angreifer gibt den Namen des Opfers in die Suche ein und wählt als zusätzliches Suchkriterium den Berufsstatus »Schüler«. Erscheint nach Abschluss der Suche das Opfer in der Ergebnismenge, dann kann der Angreifer darauf schließen, dass »Schüler« der verdeckte Berufsstatus ist. Erscheint das Opfer nicht, dann muss der Angreifer zusätzlich noch die Werte »Student« und »Alumni« ausprobieren.

3.8 Zugriffsprotokollierung

Prüfkriterien

Untersucht wurde, ob eine Protokollfunktion existiert und wie umfangreich die aufgezeichneten Daten sind. Desweiteren wurde geprüft, wie sie von Seiten des Profilinhabers und des Profilbesuchers konfiguriert werden kann. Im nächsten Schritt wurde auch beurteilt, wie die Interessenabwägung zwischen Protokollierer und Protokollierten vorgenommen wurde.

Anforderungen

Das Protokollieren von Zugriffen auf das Nutzerprofil muss die Privatsphärenschutz-Interessen von Profilinhaber und Profilaufrufer in einen fairen Ausgleich stellen. Das Protokoll darf keine privatsphärenrelevanten Daten des Profilbesuchers speichern. Es sollte überhaupt nur so viel Daten sammeln, wie zur Erstellung einfacher Nutzungsstatistiken erforderlich sind.

Zugriffe auf das Profil, und damit auch auf die privaten Daten, können für den Profilinhaber protokolliert werden. Solche Funktionen werden auch als »Besucherliste« oder ähnlich bezeichnet.

Das Dilemma derartiger Aufzeichnungen besteht darin, dass sie selbst personenbezogene Daten der zugreifenden Person beinhalten. Dazu zählt allein schon die Aussage »Person XY hat das Profil besucht«. Im verschärften Fall könnte z. B. auch der genaue Zeitpunkt des Zugriffs erfasst werden. Damit lassen sich Rückschlüsse auf Plattform-Nutzungsverhalten und Tagesabläufe ziehen. Es ist anzunehmen, dass eine solche Datensammlung in den meisten Fällen den Interessen der erfassten Person widersprechen. Auf der anderen Seite steht das Interesse des Profilinhabers einen Überblick über die Aufrufe seiner personenbezogenen Daten zu erhalten. Die Interessen des Profilinhabers und des Profilbesuchers sind fair auszugleichen.

Um zu definieren, welche Praxis »fair« und welche »unfair« ist, muss zunächst ein Zweck festgelegt werden, den das Zugriffsprotokoll grundsätzlich erfüllen soll. Die reine Neugierde des Profilinhabers bezüglich seiner Profilbesucher ist kein Zweck der einen tiefen Eingriff in die Privatsphäre der Protokollierten rechtfertigt. Gleichwohl kann der Nutzer anhand des Protokolls generelle Rückschlüsse auf die Nutzung seiner privaten Daten ziehen. Dieses Wissen ist hilfreich um z. B. Zugriffskontrollen den eigenen Vorstellungen anzupassen. Dafür ist es aber nicht notwendig, die einzelnen Profilbesucher detailiert zu erfassen.

Im Zweifelsfall wiegen aber die Interessen der protokollierten Nutzer höher, da sie sich gegen die Protokollierung schwerlich wehren können. Hingegen kann der Profilinhaber zum Schutz seiner Daten zumindest Zugriffskontrollen aktivieren.

Um das Problem zu verdeutlichen, zeigt folgendes Beispiel, wie ein »fairer Ausgleich« bei gleichzeitiger Wahrung des Zweckes aussehen kann:

Ein Protokoll kann so eingeschränkt werden, dass es dem Profilinhaber nur Aussagen über Gruppen von Zugreifenden (z. B. welcher Firma oder Hochschule sie angehören) und statistische Daten (Gesamtzahl der Besucher etc.) liefert. Einzelne Personen sind dann nicht direkt identifizierbar, was dem Privatsphärenschutz der Profilbesucher hinreichend Rechnung trägt.

3.9 Abmelden bei der Plattform und Löschen der Daten

Prüfkriterien

Es wurde untersucht, wie Nutzer ihre Plattformmitgliedschaft wieder aufgegeben können und welche Daten von dem anschließend ausgelösten Löschprozess in welcher Form erfasst werden.

Anforderungen

Der Nutzer muss seine Mitgliedschaft bei der Plattform in einem einfachen Prozess leicht aufgeben können. Personenbezogene Daten müssen dann, soweit technisch prinzipiell möglich, vollständig aus der Plattform gelöscht werden.

Ein wichtiges Prinzip im Datenschutz ist das Löschen privater Daten nach dem Wegfall des Speicherungsgrundes. Meldet sich eine Person bei einer Soziale-Netzwerke-Plattform ab, dann tritt genau dieser Fall ein:

Eine weitere Speicherung und Verarbeitung der zuvor eingegebenen Daten ist nicht mehr notwendig; möglicherweise sogar unzulässig durch den Wegfall des Verarbeitungszweckes. Deshalb muss die Plattform einen Löschprozess in Gang setzen, der diese Daten entfernt. Ist das technisch nicht möglich, so sind die Daten zumindest zu sperren.

Was das Abmelden und Löschen betrifft, sind zwei wichtige Punkte zu beachten:

Zum einen ist entscheidend, wie leicht das Abmelden möglich ist. Kann der Anwender das Profil mit einem einzigen Mausklick löschen oder ist ein umständliches Prozedere (z. B. E-Mail an den Anbieter) notwendig? Oder ist ein Löschen überhaupt nicht möglich, sondern nur das temporäre Deaktivieren des Zugangs? Desweiteren spielt eine Rolle, wie einfach die Abmeldefunktion auffindbar ist.

Untersucht wurde auch, auf welche Daten sich die Löschung erstreckt. Als Mindestanforderung sind die Profildaten aus der Plattform zu entfernen. Das Gleiche gilt für fremdgenerierte Daten (vergleiche 2.2).

Vom Anwender erzeugte Daten außerhalb des Profils, also z. B. ein Diskussionsbeitrag in einem Forum, sind auch zu löschen, sofern sie als Datenobjekt unmittelbar mit dem Nutzer verknüpft sind. Allerdings wird nicht erwartet, dass andere Foreneinträge, die den Beitrag zitieren oder aufgreifen, bearbeitet werden. Der technische Aufwand wäre dafür unverhältnismäßig hoch, da die Inhalte mit denen anderer Anwender vermengt sind. Zudem sind sie in der Regel nicht mit dem zu löschenden Nutzerzugang in der Datenbasis verknüpft.

Anstatt Daten außerhalb des Profils zu löschen, ist mit Einschränkungen auch eine Anonymisierung möglich (z. B. Ausblenden des Autorennamens). Dieses Verfahren wirkt aber nur auf die ehemalige Verknüpfung des Datenobjekts (z. B. eines Gästebuchkommentars oder Forenbeitrags) mit dem gelöschten Profil. Das Datum selbst kann aber Informationen enthalten, welche den Personenbezug trotzdem wieder herstellen (z. B. wenn der Name des Autors im Text des Forenbeitrags zusätzlich vermerkt ist). Das Verfahren kann deshalb nur als Notlösung dienen. Besser ist das vollständige Löschen.

3.10 Nutzerführung

Prüfkriterien

Die einzelnen Plattformen wurden dahingehend untersucht, wie und in welcher Form die Nutzer Zugang zu privatsphärenrelevanten Konfigurationsmöglichkeiten erhalten. Zusätzlich wurde das Vorhandensein und die Vollständigkeit der zugehörigen Dokumentation geprüft.

Anforderungen

Von den Plattformen ist zu fordern, dass ihre Nutzer leicht Zugang zu privatsphärenrelevanten Optionen erhalten und diese logisch und struktuiert aufgebaut sind. Offensichtliche Fragen müssen durch die Hilfe und andere Dokumentationen geklärt werden.

Neben dem Vorhalten von technischen Maßnahmen zum Privatsphärenschutz ist auch entscheidend, ob sie überhaupt vom Nutzer bedient werden können. Aus diesem Grund wurde auch eine Prüfung der Bedienerfreundlichkeit und Nutzerführung der relevanten Funktionen durchgeführt. Dabei wurde untersucht:

- Wie leicht sind Privatsphäre-Einstellungen zu erreichen? An wievielen Stellen in der Web-Anwendung befinden sich Einstellmöglichkeiten?
- Sind die Konfigurationsmöglichkeiten für den Nutzer systematisch und logisch aufgebaut?
- Ist eine angemessene Dokumentation vorhanden, um zumindest die plattformspezische Terminologie für den Anwender zu »übersetzen« und die

einzelnen Funktionen zu erklären? Wie selbsterklärend sind Funktionen gestaltet?

- Gibt es Fallstricke bei der Konfiguration beziehungsweise irreführende oder überflüssige Einstellmöglichkeiten? Existieren Inkonsistenzen?
- Werden bereits bei der Anmeldung oder an anderer geeigneter Stelle seitens der Web-Anwendung Hinweise und Hilfestellungen zur Konfiguration angeboten? (z. B. beim Anlegen eines Fotoalbums oder dem ersten Erzeugen einer Bildverknüpfung)

Die generelle Benutzbarkeit der Plattform wurde nicht untersucht.

4 Testablauf

Während der Plattformtests beachteten die Tester bestimmte Vorgaben. So durften sie nur in genau definierten Rollen mit den Plattformen interagieren. Auch der Umfang der einzelnen Prüfungen orientierte sich an einem festgelegtem Nutzer- und Angreifermodell. Es erfolgte weiterhin eine Limitierung auf rechtlich zulässige Untersuchungen, ohne die geprüften Plattformen in irgendeiner Art zu kompromittieren.

Die Richtlinien nach denen die Tester vorgingen, sind in diesem Kapitel dokumentiert.

4.1 Rolle des Testers

Während der Prüfung schlüpfte der Tester in die Rolle eines normalen Plattformnutzers. Dazu erstellte er auf den Plattformen ein persönliches Profil, um die angebotenen Dienste zu nutzen.

Als Testwerkzeug diente ein Internetbrowser. Abgesehen von dem in 3.6 beschriebenen Browser-Plugin, war keine zusätzliche Software erforderlich.

Der Tester begab sich in zwei verschiedene Rollen:

- **Anwender**; in dieser Rolle war der Tester ein Nutzer, der die Plattform regulär verwendet, um ein soziales Netzwerk aufzubauen, Persönliches zu veröffentlichen und beispielsweise Bilder mit Freunden zu teilen. Diese Rolle diente dazu, die Handhabbarkeit der Web-Anwendung, sowie ihre Funktionen und deren Konfigurationsmöglichkeiten beurteilen zu können.
- **Angreifer**; in dieser Rolle versuchte der Tester, Informationen über ein Mitglied der Plattform zu sammeln. Das Opfer war dabei ein selbsterstellter Nutzer in der zuvor beschriebenen »Anwender«-Rolle. Ziel war es, die Wirksamkeit bestimmter, zuvor konfigurierter Funktionen zu testen. Auch wenn hier von einer »Angreifer«-Rolle gesprochen wird, so ist darauf hinzuweisen, dass kein Angriff auf die Plattform selbst, im Sinne von klassischem »Hacking«, durchgeführt wurde (siehe auch 4.3). Auch in der »Angreifer«-Rolle agierte der Tester als normaler Nutzer ohne besondere technische Tricks.

Während der Tests erfolgte häufig ein schneller Wechsel zwischen beiden Rollen um Aktionen in der »Anwender«-Rolle unmittelbar an ihren Auswirkungen in der »Angreifer«-Rolle zu messen und umgekehrt.

4.2 Nutzer- und Angreifermodell

Zur Durchführung der Tests müssen Annahmen über das Verhalten der Nutzer und über die Fähigkeiten von Angreifern gemacht werden. Diese Annahmen sind notwendig, um die Prüfung auf realitätsnahe Szenarien einzuschränken.

Prinzipiell kann ein Angreifer, der über unbegrenzt Ressourcen verfügt, nahezu jeden Sicherheitsmechanismus umgehen. Andererseits wird ein Nutzer der professionelle Erfahrung im Bereich der IT-Sicherheit hat, bei der Konfiguration einer Zugriffskontrolle weniger Fehler machen, als ein technischer Laie. Für die hier durchgeführten Betrachtungen gilt es beide Extrema zu vermeiden.

Über den Plattformanwender wird deshalb angenommen, dass er über grundlegende Kenntnisse und Erfahrungen im Umgang mit dem Internet verfügt. Eine strukturierte, durch eine berufliche Ausbildung vorhandene Wissensbasis wird nicht vorausgesetzt. Folgende andere Fähigkeiten sind vorhanden:

- Der Anwender verwendet einen aktuellen Internetbrowser und ist in der Lage, diesen korrekt zu bedienen.
- Dem Anwender ist bewusst, dass Nutzergeheimnisse, wie z. B. ein Passwort, geheim zu halten oder sicher aufzubewahren sind.
- Der Anwender hat, auch in einer offenen Soziale-Netzwerke-Plattform, ein Grundbedürfnis an Privatsphäre (vergleiche 2.1).

Es wird über den Anwender jedoch nicht angenommen, dass er aktiv nachvollziehen kann, wie sich Daten im Internet verbreiten, wie Zugriffskontrollen wirken (oder in Spezialfällen eben nicht) oder welche Methoden Angreifer verwenden können, wie z. B. sogenanntes »Google-Hacking«[1] oder Verkettung von Daten[2].

Dem Angreifer werden wiederum folgende Fähigkeiten unterstellt:

- Der Angreifer ist in der Lage sich anonym an einer Soziale-Netzwerke-Plattform anzumelden und die von dieser Plattform angebotenen Funktionen zu bedienen.
- Der Angreifer kann alle anderen, öffentlich verfügbaren Informationsquellen, wie beispielsweise Suchmaschinen, im Internet nutzen. Er verfügt auch über das Wissen, welche Informationsquellen zu welchem Zweck geeignet sind.
- Der Angreifer verfügt über einschlägige Kenntnisse zu Internet- und Netzwerktechniken.

[1] Geschicktes Ausnutzen der Suchmaschine Google, um vertrauliche Daten aufzufinden.

[2] Verknüpfen von personenbezogenen Daten, um Informationen über den Informationsgehalt der Einzeldaten hinaus zu erhalten.

Auf der anderen Seite ist der Angreifer nicht in der Lage, aktiv Sicherheitsmechanismen, wie z. B. eine Nutzerauthentifizierung zu umgehen (vergleiche 4.3). Er verfügt auch nicht über detailiertes Schwachstellenwissen bezüglich Webanwendungen. Auch wird der Angreifer kein sogenanntes »Social Engineering«[3] durchführen, noch direkten Kontakt zu einem Opfer oder zu einer mit dem Opfer in Beziehung stehenden Person suchen.

4.3 Nicht durchgeführte Tests

Nicht im Fokus der Evaluierung standen typische Lücken von Web-Anwendungen, wie Anfälligkeit für Cross-Site-Scripting (XSS), Cross-Site-Request-Forgery (CSRF) oder SQL-Injections. Derartige Untersuchungen erfordern einen Penetrationstest, der nur mit Zustimmung des Betreibers durchzuführen ist.

Die Prüfung kann deshalb auch keinerlei Aussagen über die internen Datenverarbeitungs- und Organisationsprozesse beim Plattformbetreiber liefern. Unberücksichtigt bleiben somit Aspekte wie:

- Datensicherung,
- Zugriffskontrollen zum Schutz von Nutzerdaten vor Innentätern,
- Physische Zugangskontrolle zu Datenverarbeitungsanlagen,
- Härtung von Webservern, Dateiservern und anderen Rechnern gegen Angriffe,
- Verfügbarkeit von Datenverarbeitungsanlagen,
- Angriffe gegen die Integrität von privaten Daten
- Regelungen zur direkten Weitergabe von Daten an Dritte, zum Zwecke der Werbung, Markt- und Meinungsforschung oder anderen Drittverwertungen,
- usw.

Desweiteren wurden die jeweiligen Datenschutzrichtlinien und Geschäftsbedingungen nicht bewertet. Hierfür ist eine juristische Prüfung notwendig, die im Rahmen dieser Studie nicht geleistet wird.

Ebenso wurden keine Bestandteile getestet, die Daten an andere Anbieter von Webdiensten übertragen, wie z. B. spezielle eingebettete Anwendungen. Das betrifft auch die Gegenrichtung, also den Empfang von Daten von Drittanbietern.

[3] Manipulieren einer Person mit Hilfe von Wissen über ihr persönliches Umfeld.

5 Testauswertung

In diesem Kapitel wird das Schema beschrieben, nach dem die Prüfergebnisse für die einzelnen Kriterien bewertet werden.

Der Funktionsumfang der Zugriffskontrollen wurde von den Testern mithilfe einer Funktionsmatrix erfasst. Sie ist ein wichtiges Hilfsmittel beim Bewerten. Abschnitt 5.1 erläutert, wie eine solche Funktionsmatrix aufgebaut ist und wie sie von den Testern interpretiert wird.

Auf die Konfigurationsmöglichkeiten der Zugriffskontrollen wird besonderer Wert gelegt. Sie sind für den Nutzer eine wichtiges Werkzeug zur Anpassung des Privatsphärenschutzes an die eigenen Bedürfnisse. Entsprechend ist für jede der getesteten Plattform eine Funktionsmatrix in Kapitel 7 aufgeführt. Damit sind die vergebenen Bewertungen nachvollziehbar.

5.1 Funktionsmatrix für die Zugriffskontrolle

Bevor eine Zugriffkontrolle bewertet wird, werden zunächst ihre Fähigkeiten abgebildet. Dazu wird als Hilfsmittel für jede einzelne Plattform eine Übersichtstabelle, eine sogenannte Funktionsmatrix, erstellt. Sie zeigt, für welche private Daten der Betroffene den Kreis der Zugriffsberechtigten einschränken kann.

In den Tabellenspalten sind dazu Nutzergruppen abgebildet, die die Plattform zur Zugriffskontrolle unterscheidet. Wie diese Einteilung genau erfolgt, ist von Plattform zu Plattform unterschiedlich. Einige differenzieren verschiedene Gruppen nach Kontaktnähe zum Betroffenen (»Kontakte 1. Grades«, »Kontakte 2. Grades«, etc.). Diese sind folglich für jeden Nutzer individuell, je nachdem welche Kontakte er in die Plattform eingegeben hat.

Eine andere Möglichkeit ist die Definition von globalen Nutzergruppen in der Plattform. Diese sind in ihrer Zusammensetzung nicht individuell vom Betroffenen beeinflussbar. Sie werden durch Beitritt der Mitglieder gebildet. Beispiele dafür sind regionale Netzwerke (z. B. »alle Nutzer in Deutschland«) oder nach anderen Semantiken aufgebaute Personenkreise (»Studenten der TU Darmstadt«, »Katzenliebhaber«, etc.).

Die Gruppenanordnung im Tabellenkopf gibt eine Hierarchie wieder. Eine Gruppen ist immer auch Teil der links vor ihr stehenden Gruppen. Zugriffsrechte werden umgekehrt von links nach rechts vererbt. Ebenso nimmt die Anzahl der Gruppenmitglieder von links nach rechts immer ab, da links generalisiertere und rechts spezialisierte Gruppen stehen.

Die Zeilen der Matrix bezeichnen die Datenobjekte, die personenbezogen einem Nutzer zugeordnet werden. Unterschieden wird der lesende und der schreibende Zugriff. Ein Datum kann aus diesem Grund zweimal in der Tabelle erscheinen, wenn es von anderen Nutzern sowohl geschrieben, als auch gelesen werden kann, wie z. B. bei einem Gästebuch.

Für die Felder der Matrix wird eine Schlosssymbolik verwendet. Sie bildet zum einen die Standardeinstellung der Zugriffskontrolle ab. Weiterhin zeigen die einzelnen Schlosssymbole an, ob der Nutzer diese Einstellung verändern kann:

- Anhand des Verschlusszustands ist erkennbar, ob in der Standardkonfiguration die Mitglieder einer Gruppe auf das Datenobjekt zugreifen können (Schloss offen) oder nicht (Schloss zu).

  Werden Schreibzugriffe nur über ein nachgelagertes Veto oder eine vorgelagerte Autorisierung gesteuert (vergleiche 3.4), so wird einem nachgelagerten Veto ein offenes Schloss zugeordnet, da zum Zeitpunkt des Schreibvorgangs kein Schutzmechanismus wirkt. Mit einer vorgelagerten Autorisierung ist folglich ein verschlossenes Symbol assoziiert.
- Die Füllung des Schlosssymbols beschreibt, ob der Nutzer die Standardkonfiguration ändern kann (Schloss leer mit Schlüsselsymbol links) oder nicht (Schloss gefüllt ohne Schlüsselsymbol links).

Entsprechend finden sich die in Tabelle 5.1 abgebildeten Symbole wieder.

Tabelle 5.1: Erläuterung der Funktionsmatrix-Symbole

Symbol	Beschreibung
	Die Zugriffskontrolle **verbietet** in der Standardkonfiguration den Zugriff auf das Datum für die Gruppe. Die Einstellung ist vom Nutzer **änderbar**.
	Die Zugriffskontrolle **erlaubt** in der Standardkonfiguration den Zugriff auf das Datum für die Gruppe. Die Einstellung ist vom Nutzer **änderbar**.
	Die Zugriffskontrolle **erlaubt** in der Standardkonfiguration den Zugriff auf das Datum für die Gruppe. Die Einstellung ist vom Nutzer **nicht änderbar**. Die Gruppe kann also in jeder möglichen Konfiguration der Zugriffskontrolle auf das Datum zugreifen.
	Die Zugriffskontrolle **verbietet** in der Standardkonfiguration den Zugriff auf das Datum für die Gruppe. Die Einstellung ist vom Nutzer **nicht änderbar**. Die Gruppe kann also in keiner möglichen Konfiguration der Zugriffskontrolle auf das Datum zugreifen.

Tabelle 5.2 zeigt ein Beispiel für eine Funktionsmatrix:

Tabelle 5.2: Beispiel für eine Funktionsmatrix zur Zugriffskontrolle einer Plattform

	Gruppen		
	Internet	Plattform-mitglieder	Kontakte 1. Grades
lesender Zugriff			
Name			
eMail			
Kontaktliste			
Gästebuch			
Gruppen			
Alter			
schreibender Zugriff			
Gästebuch			
Fotoverknüpfung			

Die Beispieltabelle 5.2 sagt folgendes aus:

- Auf den Namen kann jede Person beliebig zugreifen. Der Profilinhaber kann das nicht verhindern.
- Auf die E-Mail-Adresse können Plattformmitglieder und Kontakte ersten Grades beliebig zugreifen. Der Profilinhaber kann das nicht verhindern. Andere Internetnutzer können in keinem Fall die E-Mail-Adresse lesen.
- Auf die Kontaktliste können potentiell beliebige Internetnutzer und Plattformmitglieder zugreifen. Der Profilinhaber kann dies aber deaktivieren, wenn er es wünscht. Kontakte ersten Grades können hingegen die Kontaktliste immer lesen. Standardmäßig können Plattformmitglieder und Kontakte ersten Grades die Kontaktliste lesen, Internetnutzer aber nicht.
- Gästebucheinträge können von Internet- und Plattformnutzern, oder von Kontakten ersten Grades geschrieben werden. Der Profilinhaber kann das Gästebuch aber soweit einschränken, dass niemand Gästebucheinträge verfassen kann. Standardmäßig können nur Kontakte ersten Grades Gästebucheinträge erzeugen.
- usw.

Die Funktionsmatrix lässt durch Betrachten der Symbolverteilung bereits einfache Interpretationen zu:

- Eine große Anzahl von Gruppen (Spalten in der Matrix) deutet darauf hin, dass Nutzer sehr differenziert Personenkreise wählen können, die Zugriff zu den Daten erhalten.
- Je mehr leere (grüne) Schlösser mit Schlüsselsymbol in der Matrix vorhanden sind, desto mehr Schutzmöglichkeiten kann der Anwender für seine Daten aktivieren.
- In den einzelnen Zeilen sollten sich möglichst wenig offene Schlösser befinden. Wenn doch, dann sollten sie sich soweit als möglich rechts befinden. Im linken und mittleren Teil der Zeilen stehen optimalerweise nur geschlossene Schlösser. In diesem Fall ist die Zugriffskontrolle nach der Neuanmeldung an der Plattform bereits sehr restriktiv eingestellt.
- Befinden sich sehr viele offene, ausgefüllte (rote) Schlösser in der Matrix, dann bietet die Plattform ihren Nutzern nur wenige Funktionen zur Zugriffskontrolle.

5.2 Bewertung der Prüfergebnisse

Zur Gegenüberstellung der einzelnen Plattform wurden die untersuchten Aspekte jeweils einzeln bewertet. Dabei wurde auf ein dreistufiges Bewertungsschema zurückgegriffen, welches in Tabelle 5.3 dargestellt ist.

Tabelle 5.3: Vergebene Bewertungen für die einzelnen untersuchten Anforderungen und Kriterien

Symbol	Bewertung	Beschreibung
⊕	Positiv	Die Prüfung hat gezeigt, dass die Plattform ein Kriterium überwiegend positiv erfüllt.
○	Neutral	Die Plattform erfüllt ein Kriterium weder überwiegend positiv noch negativ.
⊖	Negativ	Die Mängel überwogen bei der Prüfung eines Kriteriums.
—	Nicht geprüft	Das Kriterium wurde bei der Plattform nicht geprüft.

Im Folgenden wird erläutert, wie genau ein Prüfresultat für ein einzelnes Kriterium auf eine Bewertung abgebildet wurde.

Die Einordnung erfolgte nach pragmatischen Gesichtspunkten. Ein Dienstbetreiber kann nach dem Stand der Technik die höchste Bewertungsstufe mit realistischem, vertretbarem Aufwand erreichen.

5.2.1 Geforderte Daten bei der Anmeldung

Tabelle 5.4: Bewertung der bei der Anmeldung erforderlichen Daten

Bewertung	Begründung der Einordnung
⊕	Zur Registrierung ist nur die Eingabe eines Nutzernamens und die Wahl eines Passwortes erforderlich. Als Nutzername ist eine E-Mail-Adresse, ein Pseudonym oder der Klartextname des Anwenders zulässig.
○	Zusätzlich zum Nutzernamen und Passwort ist nur die Angabe des Geburtstages notwendig. Bei den Plattformen für Studenten ist auch die besuchte Hochschule erlaubt, wenn diese Angabe für die Zugriffskontrolle notwendig ist.
⊖	Zur Registrierung sind mehr Daten, als die zuvor genannten erforderlich.

Gemeint sind hier ausschließlich Daten, die bei der Anmeldung an der Plattform erforderlich sind, also die Bestandsdaten des Plattformbetreibers. Für dieses Kriterium ist es unerheblich, ob diese Daten außer für den Anwender und den Plattformbetreiber auch für Dritte, wie z. B. andere Plattformmitglieder, sichtbar sind.

5.2.2 Pseudonyme Nutzung

Tabelle 5.5: Bewertung der pseudonymen Nutzung

Bewertung	Begründung der Einordnung
⊕	Die Plattformnutzung ist pseudonym-basiert. An keiner Stelle ist für andere Plattformmitglieder ein Zugriff auf einen Identifikator wie Klartextname oder E-Mail-Adresse des Nutzers möglich.
○	Die Plattform bietet für einige Bereiche eine pseudonyme Nutzung an. Die Pseudonymisierung ist allerdings nicht umfassend. Es ist, wenn auch unter begrenzten Umständen, eine Depseudonymisierung möglich, beispielsweise durch indirekten Zugriff auf Klartextname oder E-Mail-Adresse.
⊖	Die Plattform unterstützt keine Pseudonyme.
–	Bei geschäftlich genutzten Plattformen wird nach diesem Kriterium nicht geprüft. Eine pseudonyme Nutzung ist hier wenig interessant, da sie in der Geschäftswelt unüblich ist.

Dieses Kriterium bezieht sich nur auf die Darstellung des Anwenders innerhalb der Plattform, z. B. durch das Profil. Die nur für den Anwender und den Plattformbetreiber sichtbaren Bestandsdaten können durchaus einen Klartextnamen

enthalten. Dies würde zu keiner Abwertung im Sinne dieses Kriteriums führen (vergleiche 5.2.1).

5.2.3 Einsatz von Verschlüsselung

Tabelle 5.6: Bewertung des Einsatzes von Verschlüsselung

Bewertung	Begründung der Einordnung
⊕	Während einer laufenden Nutzersitzung erfolgen *alle* Übertragungen zwischen dem Internetbrowser des Anwenders und den Servern der Web-Anwendung verschlüsselt. Dies schließt die Übertragung der Login-Daten ein (z. B. Nutzername und Passwort).
○	Um das Login durchzuführen werden der Nutzername und das Passwort verschlüsselt übertragen. Während der laufenden Nutzersitzung erfolgen andere Datenübertragungen unverschlüsselt.
⊖	Die Plattform bietet keine Verschlüsselungsfunktionen.

5.2.4 Funktionsumfang der Zugriffskontrollen

Wichtig für die Beurteilung der Zugriffskontrolle ist deren Fähigkeit privatsphärenrelevante Daten auf Wunsch des Nutzers zu schützen (vergleiche 2.2). Welche Bereiche dabei in den jeweiligen Plattformen hinsichtlich der ungewollten Offenbarung der Daten gefährdet sind, muss individuell beurteilt werden.

In jedem Fall muss die Zugriffskontrolle sensible Bereiche erfassen, sofern sie die eigenen Profildaten und fremdgenerierte Daten (vergleiche 2.2) betreffen.

Tabelle 5.7: Bewertung der Bereitstellung von Zugriffskontrollen

Bewertung	Begründung der Einordnung
⊕	Die Plattform erlaubt es in mehrstufigen Verfahren über verschiedene Nutzergruppen den Zugang auf privatsphärenrelevante Daten und auch andere Daten (z. B. das Alter, Wohnort, etc.) im Profil einzuschränken. Darüberhinaus gelten die Anforderungen an die neutrale Bewertungsstufe.
○	Der Nutzer kann zumindest *einen* Personenkreis *vollständig selbst* definieren, auf den er den Zugang zu privatsphärenrelevanten Profildaten einschränken kann. Global existierende Gruppen, deren Zusammensetzung der Nutzer nicht vollständig beeinflussen kann, wie z. B. »alle Plattformmitglieder« oder »beliebige Internetnutzer«, können die Daten ab dem Zeitpunkt der Zugriffseinschränkung nicht mehr lesen. Für fremdgenerierte Daten ist zumindest eine nachgelagerte Autorisierung vorgesehen (»Vetorecht«).
⊖	Die Plattform erlaubt es nicht, den Zugang auf privatsphärenrelevante Daten hinreichend einzuschränken.

Wie die Zugriffskontrolle genau erfolgt, ist dabei weniger wichtig, solange die gewählte Lösung dem Stand der Technik entspricht. So wird auch das technisch Machbare berücksichtigt. Stehen Daten außerhalb des Profils, z. B. ein Nutzerkommentar in dem Gästebuch einer anderen Person oder eine Bildverknüpfung in einem fremden Fotoalbum, dann ist Zugriffskontrolle nur begrenzt umsetzbar. Dies ist schon allein dadurch bedingt, dass die Interessen zweier Anwender, z. B. die eines Gästebuchinhabers und eines Kommentarautors, berührt sind.

Die Tatsache, dass ein bestimmtes Datum in einem Profil nicht angegeben werden muss (z. B. Freilassen des Feldes »Hobbys«), wird hier nicht als »Zugriffskontrolle« gewertet. Die Begründung ist, dass es eben der ureigenste Zweck einer Soziale-Netzwerke-Plattform ist, private Daten an andere Mitglieder zu übermitteln. Der Anwender wird damit unter Zugzwang gestellt, dass entweder niemand oder aber ein für ihn nicht kontrollierbarer Empfängerkreis auf eine bestimmte Information zugreifen kann. Es ist schwer zu begründen, warum dem Anwender eine solche Entscheidung aufgebürdet werden soll.

5.2.5 Standardkonfiguration

Tabelle 5.8: Bewertung der Standardkonfiguration nach der Anmeldung

Bewertung	Begründung der Einordnung
⊕	Die Zugriffskontrollen sind nach der Anmeldung bereits restriktiv konfiguriert.
○	Die Zugriffskontrollen sind nach der Anmeldung bereits so konfiguriert, dass zumindest privatsphärenrelevante Daten nur eingeschränkt, also nicht von allen anderen Plattformmitgliedern, lesbar sind.
⊖	Nach der Anmeldung sind die Zugriffskontrollen so konfiguriert, dass privatsphärenrelevante Daten nicht geschützt sind. Verfügt eine Plattform über mangelhafte Zugriffskontrollen, dann wird zwingend auch die Standardkonfiguration negativ bewertet.

5.2.6 Externer Zugriff auf Multimediadaten

Mit »externem Zugriff« sind zunächst zwei Formen des »Externseins« gemeint, die für die Bewertung nicht weiter unterschieden werden:

- »Extern« meint zum einen jeden Zugriffsversuch auf Daten der Plattform, der nicht aus einer mit einem gültigen Nutzerzugang erzeugten Plattformsitzung heraus erfolgt.
- »Extern« meint zum anderen Zugriffsversuche im Rahmen einer gültigen Sitzung, bei der der zuvor authentifizierte Anwender allerdings logisch vom Zugang auf Daten ausgeschlossen ist (durch entsprechend vom Betroffenen konfigurierte Zugriffskontrollen).

Im Rahmen dieser Prüfung wurde allerdings nur die Gültigkeit von Ressourcenverknüpfungen (Hyperlinks) geprüft. Aufwendigere Angriffe können auf Grund legaler Einschränkungen im Rahmen dieser Studie nicht durchgeführt werden (siehe auch 4.3). Ein realer Angreifer kann jedoch weitere, hier nicht untersuchte Angriffsmethoden entwickeln und anwenden.

Tabelle 5.9: Bewertung des externen Zugriffs auf Multimediadaten

Bewertung	Begründung der Einordnung
⊕	Ressourcenverknüpfungen zu Mediendateien sind nur innerhalb der Plattform zugreifbar. Der Zugriff wird entsprechend der gesetzten Zugriffskontrolle gewährt oder verweigert.
○	Ressourcenverknüpfungen zu Mediendateien sind nur während einer gültigen Plattformsitzung zugreifbar.
⊖	Ressourcenverknüpfungen zu Mediendateien sind auch außerhalb einer gültigen Plattformsitzung zugreifbar. Werden Bilder in der Plattform mit der Software »Polar Rose« (siehe auch 3.6) erfolgreich indiziert, so führt dies automatisch zur Abwertung als »negativ«.
–	Bei Geschäftsplattformen wird nach diesem Kriterium nicht bewertet, da auf diesen nur wenige oder gar keine Mediendateien abgelegt werden. Vorhandene Auffälligkeiten wurden separat dokumentiert und kommentiert.

5.2.7 Suchfunktion

Tabelle 5.10: Bewertung der Suchfunktion

Bewertung	Begründung der Einordnung
⊕	Für die Suchfunktion werden dem Nutzer separate Privatsphäre-Einstellungen angeboten. Diese erlauben eine zweckmäßige Anpassung der eigenen Auffindbarkeit innerhalb der Plattform.
○	Die Suchfunktion berücksichtigt die gesetzten Zugriffskontrollen des Nutzers. Es werden aber keine relevanten, zusätzlichen Privatsphärenfunktionen für die Suche angeboten, wie z. B. das Deaktivieren des eigenen Profils für die Suche. Alternativ wird eine Plattform für dieses Kriterium als »neutral« bewertet, wenn überhaupt keine Suche nach privatsphärenrelevanten Daten möglich ist.
⊖	Die Suchfunktion berücksichtigt nicht die gesetzten Zugriffskontrollen des Nutzers. Sind die Zugriffskontrollen ohnehin mangelhaft, dann fällt die Bewertung »negativ« aus, wenn die Plattform zusätzlich eine umfangreiche Suche nach privatsphärenrelevanten Daten erlaubt.

5.2.8 Zugriffsprotokollierung

Tabelle 5.11: Bewertung der Zugriffsprotokollierung

Bewertung	Begründung der Einordnung
⊕	Die Plattform protokolliert Zugriffe auf private Daten gegenüber dem Betroffenen. Protokolldaten werden aber insoweit eingeschränkt, dass die Interessen des Profilinhabers und des Zugreifenden fair gegeneinander abgewogen werden. Das kann z. B. geschehen, indem über einen sehr langen Zeitraum protokolliert wird, die Zugriffsreihenfolge nicht ersichtlich ist und mehrere Zugriffe einer Person zu einem einzigen zusammengefasst werden. Der Protokollierende erhält aus dem Protokoll keine Daten um unmittelbar Profile von Protokollierten aufrufen zu können. Zum Beispiel reicht das Anzeigen charakteristischer Angaben, wie z. B. die Hochschul- oder Firmenzugehörigkeit des Zugreifenden aus. Auf der anderen Seite kann der Protokollierte das Erfassen seines Zugriffs nicht verhindern.
○	Die Zugriffsprotokollierung ist unausgewogen. Allerdings wird durch die Unausgewogenheit weder die Privatsphäre des Profilinhabers noch die der Zugreifenden erheblich beeinträchtigt. In diese Bewertungskategorie passen Fälle, in denen keine Protokollfunktion vorhanden ist oder der Zugreifende sie abschalten kann.
⊖	Die Zugriffsprotokollierung ist unausgewogen und beeinträchtigt die Privatsphäre des Profilinhabers oder des Zugreifenden erheblich. Ein Beispiel ist ein Protokoll, welches den exakten Zeitpunkt des Zugriffs verzeichnet und damit die Erstellung von Tagesablauf- und Nutzungsprofilen zu den Protokollierten erlaubt.

5.2.9 Abmelden bei der Plattform und Löschen der Daten

Wie bereits in 3.9 erläutert, wurde das Abmelden von der Plattform mit zwei Kriterien bewertet:

Zum einen wird beurteilt, wie leicht ein Anwender überhaupt eine Abmeldung erreichen kann. Desweiteren wird der Umfang des anschließend durchgeführten Löschens bewertet. Es ergeben sich deshalb zwei Bewertungen.

Tabelle 5.12: Bewertung der Erreichbarkeit der Abmeldefunktion

Bewertung	Begründung der Einordnung
⊕	Das Abmelden ist mithilfe einer leicht zu erreichenden Funktion jederzeit möglich.
○	Für das Abmelden ist eine Funktion in der Plattform vorgesehen. Diese ist aber nur umständlich für den Anwender auffindbar.
⊖	Die Plattform besitzt keine direkt ausführbare Abmeldefunktion. Entweder ist überhaupt kein Prozess zum Abmelden vorgesehen oder der Anwender muss sich anderweitig, z. B. per E-Mail an den Plattformbetreiber wenden.

Tabelle 5.13: Bewertung des Löschumfangs

Bewertung	Begründung der Einordnung
⊕	Das Nutzerprofil und alle mit dem Nutzer verknüpften Daten außerhalb des Profils, ob fremdgeneriert oder nicht, werden gelöscht (soweit technisch möglich). Das schließt Bildverknüpfungen, Foren- und Gästebucheinträge usw. ein.
○	Das Nutzerprofil und alle fremdgenerierten Daten werden gelöscht. Daten außerhalb des Profils, wie z. B. Bildverknüpfungen, Foren- und Gästebucheinträge werden zwar nicht gelöscht, aber zumindest anonymisiert (soweit technisch möglich).
⊖	Das Nutzerprofil wird zwar gelöscht, aber Daten außerhalb des Profils, wie z. B. Bildverknüpfungen, Foren- und Gästebucheinträge, bleiben unverändert bestehen.

5.2.10 Nutzerführung

Bei der Bewertung der Nutzerführung und Bedienerfreundlichkeit lassen sich subjektive Eindrücke der Tester nicht völlig ausschließen. Folglich sind die Anforderungen an die einzelnen Bewertungsstufen nicht so klar zu definieren, wie bei den anderen Kriterien. Sie dienen nur als Richtschnur. Für die Bewertung spielte auch der Gesamteindruck eine wichtige Rolle.

Im Zweifelsfall wurde berücksichtigt, ob ein technisch unversierter Anwender Funktionen für den Privatsphärenschutz leicht auffinden, verstehen und bedienen kann (siehe auch 4.2).

Tabelle 5.14: Bewertung der Nutzerführung

Bewertung	Begründung der Einordnung
⊕	Die Privatsphäre-Einstellungen sind leicht über maximal zwei Links nach dem Einloggen zu erreichen, strukturiert aufgebaut und mit Erläuterungen versehen. Der Nutzer wird unmittelbar nach der Registrierung und an anderer geeigneter Stelle auf die Funktionen hingewiesen.
○	Die Nutzerführung weist einige, überschaubare Mängel auf. So sind z. B. Privatsphäre-Einstellungen zwar gut strukturiert aber nicht leicht zu erreichen.
⊖	Die Bedienoberfläche ist beispielsweise nicht geeignet, dem Nutzer leicht Zugang zu Privatsphäre-Einstellungen zu verschaffen. Zudem war der Aufbau der Konfigurationsmenüs unverständlich und wenig strukturiert.

5.3 Kritische Würdigung der Test- und Bewertungsmethodik

Für diese Studie wurde anhand der in Kapitel 3 beschriebenen Kriterien und Anforderungen geprüft, wie weit ein Anbieter seinen Dienst privatsphärenrespektierend gestaltet (vergleiche 2.1). Die Auswertung wurde mithilfe des in 5.2 beschriebenen Bewertungsschemas erstellt.

Aufgrund der Kriterienauswahl und des Bewertungsmaßstabs kann den Ergebnissen folgende Aussagekraft beigemessen werden:

- Je schlechter die Testergebnisse, desto vorsichtiger sollten privatsphärenbewusste Nutzer mit einer getesteten Plattform umgehen. Bei einem besonders schlechtem Niveau der Bewertung ist gegebenenfalls auch ganz von der Nutzung abzusehen.
- Stellt eine Plattform wirkungsvolle Mechanismen zur Verfügung, die Datenschutz und Datensicherheit fördern, und bietet sie zusätzlich Möglichkeiten für den Nutzer Informationsflüsse im Dienst weitreichend selbst zu steuern, dann erhielt sie gute Bewertungen für die verschiedenen Testkriterien. Als Einschränkung kann diese Studie allerdings nur Mechanismen bewerten, die im begrenzten Rahmen der Prüfung sichtbar waren. Diese Einschränkung betrifft auch das Auffinden von Mängeln, wie das Fehlen wichtiger Schutzmechanismen oder konzeptionelle und umsetzungsbedingte Fehler.

Gute Bewertungen stellen keinen »Freifahrschein« dar: Die Untersuchung wurde als Black-Box-Test aus Nutzerperspektive durchgeführt. Ein solcher Test lässt viele Fragen offen, z. B. bezüglich interner Abläufe beim Dienstbetreiber und nicht geprüfter Komponenten und Prozesse (siehe auch 4.3).

Um eine vollständige Bewertung des Privatsphärenschutzes zu erhalten, sind die systematisch bedingten Lücken mit weiteren Tests zu schließen. Diese bedürfen aber der Zustimmung und aktiven Mitarbeit der Dienstbetreiber.

6 Geprüfte Plattformen

Dieses Kapitel gibt einen Überblick zu den getesteten Plattformen. Zu Beginn jedes Unterabschnitts stehen statistische Daten (durch einen grauen Balken hervorgehoben).

Die Plattformen wurden anhand der folgenden Kriterien ausgewählt:

- Ausrichtung auf deutschlandweites oder internationales Publikum ohne Einschränkung auf spezielle Hobbys, Berufsgruppen oder Ähnlichem,
- mindestens eine Millionen Nutzer in Deutschland,
- bei Privatplattformen: gehört zu den 50 Internetangeboten mit dem meisten Datenverkehr in Deutschland [2]

6.1 Plattformen für Privatnutzer

6.1.1 myspace

Verfügbar seit	Juli 2003
Nutzerprofile gesamt	180 Millionen [15]
Eigentümer / Anteilseigner	News Corp
Internetadresse	`http://www.myspace.com`

Der Dienst myspace startete bereits Juli 2003 in den USA und ist damit der älteste im Test. Er war ursprünglich als Präsentationsplattform für weniger bekannte Künstler wie z. B. kleine Musikbands gedacht. In dieser Zielgruppe hat myspace immernoch einen besonderen Stellenwert.

Myspace fällt dadurch auf, dass Nutzer ihr eigenes Profil im Erscheinungsbild wesentlich freier gestalten können, als bei anderen Plattformen. So können z. B. eigene Hintergrundbilder und Schriftfarben gewählt werden. Zudem besteht die Möglichkeit externe Anwendungen, sogenannte »Widgets« einzubetten.

Abbildung 6.1: Eine Anwendung zur Anzeige der politischen Orientierung bei facebook (Quelle: facebook.com, washingtonpost.com)

6.1.2 facebook

Verfügbar seit	Gründung Februar 2004 [5]
Nutzerprofile in Deutschland	1 Millionen (Stand März 2008) [17]
Nutzerprofile gesamt	69 Millionen (Stand März 2008)
Eigentümer / Anteilseigner	Facebook, Inc.
Internetadresse	`http://www.facebook.com`

Die Plattform facebook stammt aus dem US-amerikanischen Raum und wurde zunächst an der Harvard University für die dort immatrikulierten Studenten bereitgestellt. Im Folgenden dehnte sich der Einzugsbereich der Plattform schnell auf weitere universitäre Einrichtungen und Schulen aus. Mittlerweile wird der Dienst auch für Personen außerhalb der USA angeboten. Entsprechend wurde die Plattform in verschiedene Sprachen übersetzt, unter anderem auch in Deutsch.

Die Tests erfolgten ausschließlich mit dem deutschen Dienstangebot von facebook. Es ist nicht auszuschließen, dass der Dienst für andere Regionen Besonderheiten implementiert, die bei dieser Prüfung keine Berücksichtigung fanden.

Wie myspace auch, bietet facebook auf Nutzerwunsch die Einbindung externer Anwendungen von Drittanbietern (siehe Abbildung 6.1). Diese sollen auf private Profildaten zugreifen können, wenn der Nutzer dies erlaubt. Die Daten werden dann zwecks Ausgestaltung der externen Anwendung zum Drittanbieter übertragen.

Nach myspace ist facebook weltweit die größte Soziale-Netzwerke-Plattform hinsichtlich der Nutzerzahlen.

6.1.3 studiVZ

Verfügbar seit	Gründung Oktober 2005 [19]
Nutzerprofile gesamt	5 Millionen (Stand März 2008, Hauptanteil in Deutschland) [13]
Eigentümer / Anteilseigner	Verlagsgruppe Georg von Holtzbrinck
Internetadresse	http://www.studivz.de

Die Plattform studiVZ wurde im Oktober 2005 in Deutschland (mit britischer Rechtsform) gegründet. Die Hauptzielgruppe waren zunächst deutschsprachige Studenten. Hier hat studiVZ mittlerweile eine hohe Marktdurchdringung erreicht. Die Plattform hat nicht nur einen vergleichbaren Ansatzpunkt wie facebook, sie besitzt auch eine frappierende Ähnlichkeit, sowohl im Aufbau als auch in der Seitengestaltung.

Während studiVZ stark auf die Zielgruppe Studenten fixiert ist, existiert mittlerweile vom selben Anbieter jeweils ein weiteres Derivat für Absolventen (meinVZ) und für Schüler (schülerVZ).

Für diesen Test wurde ausschließlich die Plattform studiVZ untersucht. Die Ergebnisse dieser Tests sind somit per se nicht auf die beiden anderen Plattformen übertragbar, auch wenn es offensichtliche Überscheidungen und Ähnlichkeiten gibt.

6.1.4 wer-kennt-wen

Verfügbar seit	Oktober 2006
Nutzerprofile gesamt	2 Millionen (Stand April 2008, Hauptanteil in Deutschland) [6]
Eigentümer / Anteilseigner	lemonline media ltd. RTL interactive GmbH (49% Beteiligung) [12]
Internetadresse	http://www.wer-kennt-wen.de

Der Internetdienst wer-kennt-wen ist die jüngste getestete Soziale-Netzwerke-Plattform. Nach eigenen Aussagen richtet sich das Angebot nicht an eine spezifische Zielgruppe, sondern soll für jedermann nutzbar sein [20].

6.1.5 lokalisten

Verfügbar seit	Gründung 2005 als private Plattform
Nutzerprofile gesamt	> 1,8 Millionen (Stand März 2008, Hauptanteil in Deutschland) [10]
Eigentümer / Anteilseigner	lokalisten media GmbH ProSiebenSat.1 Media AG (90% Beteiligung) [8]
Internetadresse	http://www.lokalisten.de

Bei den »lokalisten« handelt es sich um eine Internetgemeinschaft, die ursprünglich im süddeutschen Raum angesiedelt war. Die Plattformbetreiber behaupten, mittlerweile Nutzerkreise in diversen deutschen Großstädten etabliert zu haben [9]. Das Angebot richtet sich nicht an eine spezielle Zielgruppe.

6.2 Plattformen für Geschäftsnutzer

Beide Dienste, sowohl XING, als auch LinkedIn, bieten einen kostenlosen und weitere kostenpflichtige Zugänge an. Für diese Studie wurden ausschließlich die kostenlosen Angebote geprüft.

6.2.1 XING

Verfügbar seit	November 2003 (ehemals OpenBC)
Nutzerprofile in Deutschland	1,8 Millionen (Stand Dezember 2007)
Nutzerprofile gesamt	4,8 Millionen (Stand Dezember 2007) [22]
Eigentümer / Anteilseigner	börsennotierte Aktiengesellschaft, Streubesitz > 50% [21]
Internetadresse	http://www.xing.de

XING ist ein in Deutschland ansässiger Plattformbetreiber. Er ist seit 2003 verfügbar; anfangs zunächst unter der Bezeichnung OpenBC. Die Hauptzielgruppe sind Menschen, die geschäftliche Netzwerke mithilfe des Dienstes aufbauen und pflegen wollen. Neben klassischen Vernetzungsfunktionen steht der Austausch von Expertenwissen, wie auch die Etablierung von Verkaufs- und Akquisekanälen im Vordergrund [23].

Das Angebot der Plattform ist teilweise kostenpflichtig. Es wird zwar ein kostenloser Zugang angeboten, dieser hat aber eine eingeschränkte Funktionalität.

Um die Möglichkeiten der Plattform vollständig nutzen zu können, ist eine sogenannte »Premium-Mitgliedschaft« erforderlich. Sie kostet monatlich 5,95 € (Stand Juni 2008).

XING ist die einzige börsennotierte Aktiengesellschaft unter den getesteten Diensten (seit Dezember 2006).

6.2.2 LinkedIn

Verfügbar seit	Gründung Dezember 2002
Nutzerprofile gesamt	> 20 Millionen (Stand März 2008) [1]
Eigentümer / Anteilseigner	LinkedIn Corp.
Internetadresse	`http://www.linkedin.com`

LinkedIn ähnelt in seiner Art XING und sieht sich als direkter Konkurent dieser Plattform in Europa [16]. Dem Nutzer sollen ähnliche Mehrwerte wie durch die Nutzung von XING entstehen: Organisation von Kontakten geschäftlicher Natur, Zugriff auf Expertenwissen und die Pflege privater Kontakte z. B. zu ehemaligen Kommilitonen.

LinkedIn bietet ebenfalls einen erweiterten, kostenpflichtigen Zugang an. Dieser kostet in der günstigsten Variante US$ 19,95 pro Monat (Stand Juni 2008).

7 Prüfergebnisse

Die durchgeführten Tests lieferten eine Fülle an Ergebnissen, die in diesem Kapitel dokumentiert sind.

Zu Beginn sind in 7.1 die wichtigsten Erkenntnisse, mit einem Gesamtüberblick über die vergebenen Bewertungen, zusammengefasst. In den weiteren Abschnitten erfolgt eine genaue Begründung für die Entscheidung der Tester anhand einer detailierten Aufschlüsselung der Testergebnisse. Privat- und Geschäftsplattformen sind dabei voneinander getrennt abgehandelt.

7.1 Zusammenfassung

Im Folgenden wird für die einzelnen Kriterien ein kurzes Gesamtresümee gezogen, welches einen Überblick über die Leistungen der Plattformen liefert. Die Ergebnisse der Prüfung sind in Tabelle 7.2 zusammengefasst. Die Tabellen 7.3 und 7.4 zeigen für ausgewählte Prüfkriterien, welche Plattformen typische Mängel aufweisen.

Die detailierte Begründung für die jeweiligen Bewertungen, findet sich in Abschnitt 7.2 für die Privatplattformen und in Abschnitt 7.3 für die geschäftlich genutzten Plattformen.

7.1.1 Geforderte Daten bei der Anmeldung

Der Umfang der Anmeldedaten konnte bei keiner Plattform völlig überzeugen. Bei den privaten Plattformen hielt sich der »Datenhunger« jedoch insgesamt in Grenzen. Dennoch ist es im Grunde überflüssig, dass der Nutzer vollständige Geburtsdaten (facebook, studiVZ) oder die Postleitzahl des Wohnortes (myspace) angeben muss.

Bei den Geschäftsplattformen XING und LinkedIn sind Angaben zur beruflichen Situation verpflichtend (sogenannte »Business Daten« wie Firmenname, Position in der Firma, etc.). Dieser umfangreiche Datensatz ist nicht zwingend notwendig, um den Dienst technisch zu realisieren oder rechtliche Anforderungen abzudecken.

Abbildung 7.1: Nutzer mit Pseudonym bei studiVZ (Quelle: studivz.de)

7.1.2 Pseudonyme Nutzung

Eine Form des pseudonymen Auftretens wird nur von den Plattformen myspace, lokalisten und LinkedIn unterstützt. Allerdings ist sie bei myspace und lokalisten nicht vollständig. Ein Plattformnutzer kann trotz eines Pseudonyms gezielt in der Plattform gefunden werden. Der Grund ist, dass die Suche vollständige Namen als Suchkriterium erlaubt.

Dieses Problem hat LinkedIn nicht. Hier wirkt die Funktion auch auf die Suche.

Interessant ist, dass sich die Nutzer an dieser Stelle selbst Abhilfe schaffen, indem sie bei der Anmeldung absichtlich falsche Angaben machen (siehe Abbildung 7.1). Allerdings verstößt diese Praxis bei vielen Anbietern gegen die Allgemeinen Geschäftsbedingungen und kann zum Ausschluss aus dem Dienst führen. Das Beispiel zeigt jedoch deutlich, dass bei vielen Nutzern durchaus ein Wunsch nach einer Pseudonymisierungsfunktion besteht. Allein deshalb sollten Plattformbetreiber explizit eine pseudonyme Nutzung vorsehen.

7.1.3 Einsatz von Verschlüsselung

Das Thema »Verschlüsselung« ist bei fast allen Plattformen problematisch. Nur XING schützt die Nutzersitzung mit einer vollständigen Verschlüsselung.

Bei den Plattformen facebook, studiVZ und LinkedIn sind zumindest der Anmeldevorgang und die Konfigurationsseiten verschlüsselt. Nutzername und vor allem das Passwort sind damit geschützt. Ein Angreifer kann aber in einem geeigneten Szenario (z. B. Internetcafé mit Wireless LAN) die Nutzersitzung trotzdem leicht angreifen und übernehmen.

Nicht verschlüsselt wird bei myspace, wer-kennt-wen und lokalisten.

7.1.4 Funktionsumfang der Zugriffskontrollen

Bei den nutzerdefinierten Zugriffskontrollen bietet facebook die umfangreichsten Funktionen. Der Nutzer kann detailiert konfigurieren, welche Personen welche Daten lesen und schreiben dürfen. Für privatsphärenrelevante Daten, wie beispielsweise Hobbys, politische und religiöse Ausrichtungen ist in jedem Fall ein Schutz aktivierbar.

Diese Möglichkeiten bieten grundsätzlich auch myspace und studiVZ. Allerdings muss der Nutzer hier mehr Kompromisse eingehen. So können z. B. Personenkreise und Einschränkungen nicht so differenziert konfiguriert werden, wie bei facebook.

Die Plattform wer-kennt-wen bietet ähnliche Zugriffskontrollen wie facebook, besitzt aber keinen Schutz für die Kontaktliste und die Gruppenzugehörigkeiten. Beide stellen sensible Daten dar.

XING und LinkedIn haben beide keine Kontrollmöglichkeiten für die sogenannten »Geschäftsdaten«, die neben beruflichen Informationen (Fähigkeiten, beruflicher Werdegang) vielfach auch schützenswerte, private Daten enthalten (Hobbys, politische Ausrichtung etc.).

Bei der Verbreitung beruflicher Informationen, wie z. B. Tätigkeitsfelder, werden im Übrigen nicht nur die Interessen des Nutzers berührt. Der Arbeitgeber ist möglicherweise ebenfalls betroffen, wenn unerwünscht Firmeninternas offengelegt werden. Auch vor dem Hintergrund aktueller Probleme der Wirtschaftsspionage (siehe dazu z. B. [24] und [29]) ist es möglich, dass Arbeitgeber nicht möchten, dass ihre Angestellten im Internet zu offenherzig über ihre Arbeit Informationen verbreiten. Umso kritischer ist das Fehlen einer Zugriffskontrolle.

Schlusslicht sind die »lokalisten« mit einer mangelhaften Zugriffskontrolle, sowohl hinsichtlich der Menge an schützbaren Daten als auch bezüglich der Granularität und des Umfangs der Einstellmöglichkeiten.

Tabelle 7.1 zeigt ein Überblick über die von den Plattformen gebotenen Gruppenunterscheidungen und der Black- und Whitelisting-Funktionalität.

7.1.5 Standardkonfiguration

In dieser Kategorie haben alle Plattformen mangelhaft abgeschnitten. Die Zugriffskontrollen sind nach Eröffnen eines Nutzerzugangs häufig völlig offen und Daten damit ungeschützt.

Abgesehen von der Bewertung, hebt sich facebook dennoch von den anderen Plattformen ab: Ein Großteil der privatsphärenrelevanten Daten sind nach dem Anmelden nur für Kontakte ersten Grades sichtbar. Allerdings reichte es nicht für eine neutrale oder gar positive Bewertung, da die Kontaktliste standardmäßig für alle Personen sichtbar ist. Zudem werden die Zugriffsrechte automatisch erweitert, sobald der Nutzer einem Netzwerk beitritt (Regelfall unmittelbar nach dem Anmelden).

7.1.6 Externer Zugriff auf Multimediadaten

Bei allen privat genutzten Plattformen waren Mediendaten, wie Fotos und Videos, über die Kenntnis ihrer URL von außen zugänglich. Allerdings wirken

Tabelle 7.1: Überblick über die Funktionalität der Zugriffskontrollen

	Privat					Geschäftlich	
	myspace	facebook	studiVZ	wer-kennt-wen	lokalisten	XING	LinkedIn
Gruppen für Zugriffskontrolle							
Internet	●	●	○	○	○	●	●
Plattformmitglieder	●	●	●	●	●	●	●
Netzwerke	○	●	●	○	○	○	●
Kontakte von Kontakten	○	●	●	○	●	●	○
Kontakte ersten Grades	●	●	●	●	●	●	●
Blacklisting	○[1]	●	●	○[1]	○	○	○
Whitelisting	bei keiner Plattform möglich						

● Gruppe/Funktion vorhanden, ○ Gruppe/Funktion nicht vorhanden

[1] Für einige wenige Funktionen wie z. B. Nachrichtenempfang oder Gästebucheintrag möglich.

die URL-Verknüpfungen bei allen Plattformen kryptisch, wie z. B. `http://soz.netzwpl.attform.de/foto=A38hkHUGJAS578`. Man nimmt an, dass ein Angreifer derartige Links nur mit einer geringen Wahrscheinlichkeit vorhersagen kann.

Trotzdem existieren Wege, wie diese »geheimen« Hyperlinks leicht nach außen migrieren können. Als ein Beispiel wurde der Test mit der Software Polar Rose durchgeführt, der bei allen Plattformen erfolgreich verlief (zur genauen Erläuterung siehe 3.6). Ein Beispiel zeigt Abbildung 7.2 mit einem aus facebook heraus indiziertem Bild.

Abbildung 7.3 zeigt das Bild, wie es anschließend in der Suchmaschine erscheint. Zusätzlich war auch die »geheime« URL erfasst (nicht in Abbildung 7.3 erkennbar). Analog können auch andere Fotos bei allen anderen Privatplattformen mit beliebigen darauf abgebildeten Personen verarbeitet werden.

7.1.7 Suchfunktion

Die Prüfung der Suchfunktionen offenbarte zwei Problemfelder:

Zum einen war bei den Plattformen lokalisten und XING eine sehr umfangreiche Angabe von Suchkriterien möglich, denen auf der Nutzerseite keine Zugriffskontrollmechanismen gegenüber standen. Das führte bei diesen Plattformen zur Abwertung.

Abbildung 7.2: Indizierung eines Bildes mit Polar Rose in facebook (Quelle: www.facebook.com, Polar Rose, National Archives and Records Administration)

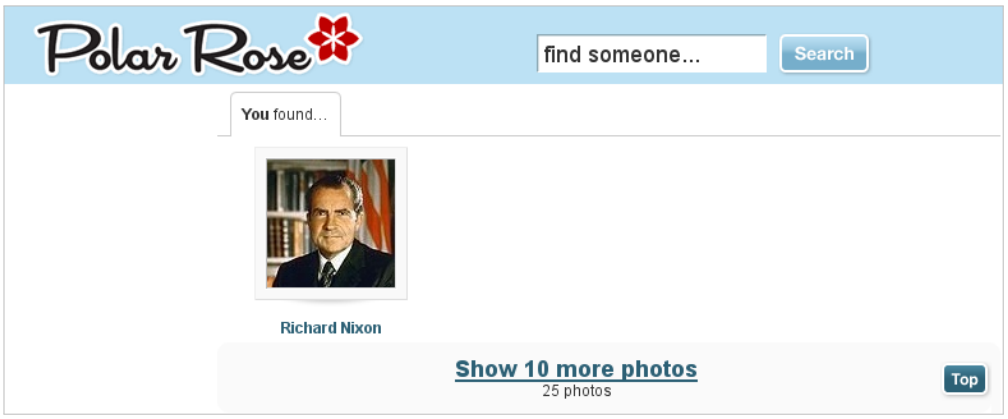


Abbildung 7.3: Erscheinen des in Abbildung 7.2 indizierten Bildes in der Suchmaschine Polar Rose (Quelle: www.polarrose.com, National Archives and Records Administration)

LinkedIn hat zwar prinzipiell dasselbe Problem, verbessert die Situation aber mit einer einfachen Pseudonymisierungsfunktion. Diese Pseudonymisierungsfunktion verhindert teilweise das Erscheinen in Suchergebnissen und verbirgt dort zumindest den Namen des Profilinhabers.

Im Gegensatz dazu war die Situation bei studiVZ und myspace umgekehrt. Hier waren Zugriffskontrollen (beispielsweise zum Schutz der Anzeige des »Beziehungsstatus« oder der »politischen Orientierung«) durchaus vorhanden. Nur leider setzt die jeweilige Suchfunktion vor diesen Zugriffskontrollen an, die damit teilweise wirkungslos wurden.

Die Plattform wer-kennt-wen erlaubt insgesamt wenig Suchkriterien und ist deshalb wenig problematisch.

Gut war in dieser Kategorie nur facebook, da hier sowohl Zugriffskontrollen auf Suchergebnisse wirkten, als auch separate Einstellmöglichkeiten für die Sichtbarkeit in der Suche vorhanden waren.

7.1.8 Zugriffsprotokollierung

Bei vielen der getesteten Plattformen war eine Besucherprotokollierung entweder nicht vorhanden oder das Erscheinen im Protokoll konnte von den Zugreifenden deaktiviert werden. Damit ist die Privatsphäre der Profilbesucher in dieser Hinsicht geschützt. Allerdings bekommt der Profilinhaber auch keinen Überblick über den Abruf seiner privaten Daten.

Bei lokalisten und XING ist ein Protokoll vorhanden. Der genaue Zeitpunkt des Zugriffs wird aber nicht vermerkt. Allerdings ist die Abfolge der Besuche erkennbar.

Hervorzuheben sind die Konfigurationsmöglichkeiten bei LinkedIn: Auf Wunsch kann der Nutzer einstellen, dass er mit Geschäftsfeld und Position, aber nicht mit seinem vollständigen Namen im Protokoll anderer Profilinhaber erscheint.

7.1.9 Profil abmelden

Das eigene Profil zu löschen war bei myspace, studiVZ, wer-kennt-wen und LinkedIn mit wenigen Mausklicks erledigt.

Bei XING geht dem Ganzen erst eine unnötige Suchaktion durch die Hilfe voraus. Wenn das Formular einmal gefunden wurde, ist aber auch hier das Abmelden schnell möglich.

Noch aufwendiger sind die Abmeldeprozeduren bei lokalisten (E-Mail an Kundendienst erforderlich) und facebook. Bei facebook ist ein reguläres Löschen gar nicht vorgesehen, sondern nur ein Deaktivieren ohne Entfernen der Daten. Wie lange das Profil deaktiviert ist wird vom Nutzer bestimmt. Will man seinen facebook-Zugang permanent kündigen, dann muss der Anwender, wie bei XING auch, die entsprechende Funktion in der Hilfe zu suchen. Das eigentliche Entfernen des Profils wird dann nicht sofort durchgeführt, sondern bedarf einer Bearbeitungszeit.

7.1.10 Löschumfang

Wichtig war bei diesem Kriterium, der Umgang mit den Daten innerhalb der Plattform, aber außerhalb des eigenen Profils. Das Profil selbst wird bei allen Plattformen entfernt. Darüberhinaus löschen myspace, facebook, lokalisten und LinkedIn auch viele anderen Daten, die eindeutig dem abgemeldeten Nutzer zugeordnet werden können, wie z. B. Gästebuch- und Foreneinträge, Fotoverknüpfungen und Blog-Kommentare.

Nicht so gründlich sind studiVZ und wer-kennt-wennt, bei denen die Daten nur durch Austausch des Autorennamens eingeschränkt anonymisiert werden.

Bei XING entfällt selbst dieser Austausch des Namens.

7.1.11 Nutzerführung

Die Nutzerführung wirkte bei den meisten Plattformen gut, auch wenn sich im Detail kleinere Mängel zeigten:

StudiVZ vermischt die eigenen Konfigurationsmöglichkeiten mit denen einer anderen Plattform, was dem Verständnis nicht förderlich ist. Bei XING und LinkedIn ist die Organisation der Privatsphäre-Optionen im Konfigurationsbereich teilweise nicht ganz schlüssig. Die Plattform facebook weist bei den Privatsphäre-Einstellungen Inkonsistenzen und undokumentierte Seiteneffekte auf.

Ein sehr ungewöhnliches Konzept liefert myspace. Hier sind viele Privatsphäre-Optionen weit über die gesamten Konfigurationsseiten verstreut.

Am übersichtlichsten erscheint wer-kennt-wen. Die Gestaltung des Konfigurationsdialoges ist an facebook angelehnt. Allerdings wurden die bei facebook bemängelten Schwächen nicht beobachtet.

Bei der Plattform lokalisten konnte dieses Kriterium, mangels geeigneter Konfigurationsmöglichkeiten, nur eingeschränkt beurteilt werden.

	Privat					Geschäftlich	
	myspace	facebook	studiVZ	wer-kennt-wen	lokalisten	XING	LinkedIn
Anmeldedaten	⊖	○	○	○	○	⊖[1]	⊖[1]
Pseudonyme Nutzung	○	⊖	⊖	⊖	○	–	–[2]
Einsatz von Verschlüsselung	⊖	○	○	⊖	⊖	⊕	○
Funktionsumfang der Zugriffskontrollen	○	⊕	○	⊖	⊖	⊖	⊖
Standardkonfiguration	⊖	⊖	⊖	⊖	⊖	⊖	⊖
Externer Zugriff auf Multimediadaten	⊖	⊖	⊖	⊖	⊖	–	–
Suchfunktion	⊖	⊕	⊖	○	⊖	⊖	○
Zugriffsprotokollierung	○	○	○	○	○	○	○
Profil abmelden	⊕	⊖	⊕	⊕	⊖	○	⊕
Löschumfang	⊕	⊕	○	○	⊕	⊖	⊕
Nutzerführung	⊖	○	○	⊕	○	○	○

⊖ Kriterium nicht erfüllt (Mängel überwiegen)
○ Kriterium teilweise erfüllt (weder Mängel noch positive Prüfergebnisse überwiegen)
⊕ Kriterium vollständig erfüllt (Prüfung mit positivem Ergebnis abgeschlossen)
– Kriterium nicht geprüft

[1] Geschäftsdaten, wie z. B. Firmenzugehörigkeit, Position etc. sind Pflicht
[2] War kein Kriterium bei Geschäftsplattformen, allerdings bietet LinkedIn eine simple Pseudonymisierungsfunktion mittels Abschneiden des Nachnamens

Tabelle 7.2: Zusammenfassung der Testergebnisse

	Privat					Geschäftlich	
	myspace	facebook	studiVZ	wer-kennt-wen	lokalisten	XING	LinkedIn
Anmeldung							
Angabe des vollständigen Geburtsdatums erforderlich	●	●	●	[1]	●	●	●
zu umfangreiche Pflichtdaten	●					●	●
Pseudonyme Nutzung							
keine pseudonyme Nutzung möglich		●	●	●		–	–
Suche nach vollständigem Nutzernamen möglich	●	●	●	●	●	–	–
Einsatz von Verschlüsselung							
unverschlüsselte Übertragung des Sitzungs-Cookies	●	●	●	●	●		●
unverschlüsselte Übertragung des Passworts	●			●	●		
Funktionsumfang der Zugriffskontrollen							
nicht alle privatsphärenrelevanten Daten schützbar				●	●	●	●
Standardkonfiguration							
nicht alle privatsphärenrelevanten Daten standardmäßig geschützt	●	●	●	●	●	●	●
Externer Zugriff auf Multimediadaten							
Fotos/Videos mit Kenntnis ihrer URL außerhalb der Plattform aufrufbar	●	●	●	●	●	–	–
Fotoverknüpfungen erlauben Zugriff auf Fotos aus geschützten Alben				●		–	–

● Mangel bei der Plattform festgestellt
– Kriterium nicht geprüft

[1] Geburtsjahr muss aber angegeben werden

Tabelle 7.3: Typische Mängel für ausgewählte Prüfkriterien (Fortsetzung in Tabelle 7.4)

	Privat					Geschäftlich	
	myspace	facebook	studiVZ	wer-kennt-wen	lokalisten	XING	LinkedIn
Suchfunktion							
keine separaten Privatsphäre-Optionen für Suchfunktion	●			●	●	●	●[1]
Suchfunktion umgeht Regeln der Zugriffskontrolle	●		●				
Suchfunktion erlaubt privatsphärenrelevante Daten als Kriterium	●	●	●		●	●	●
Profil abmelden							
Abmeldefunktion schwer auffindbar oder Abmelden insgesamt aufwändig		●			●	●	
Löschumfang beim Abmelden							
Daten außerhalb des Profils nur unvollständig gelöscht			●	●		●	
nach Abmeldung verbleibende Daten werden nicht anonymisiert						●	

[1] die Pseudonymisierungs-Funktion wirkt allerdings auf die Suche, deshalb kann die Suchbarkeit darüber eingeschränkt werden

Tabelle 7.4: Typische Mängel für ausgewählte Prüfkriterien (Fortsetzung von Tabelle 7.3)

7.2 Einzelbewertungen der Privatnutzer-Plattformen

7.2.1 myspace

Geforderte Daten bei der Anmeldung (⊖)

Zur Anmeldung an myspace ist der vollständige Name, eine E-Mail-Adresse, das Heimatland, die Postleitzahl, das Geburtsdatum und das Geschlecht anzugeben. Ein Zweck für den das Heimatland und die Postleitzahl angegeben werden müssen, ist nicht erkennbar. Die mit dem Kriterium verknüpften Anforderungen werden deshalb nicht erfüllt.

Pseudonyme Nutzung (○)

Die Plattform unterstützt die Angabe eines Pseudonyms als sogenannten »angezeigten Namen«. Die Suche erlaubt aber den vollständige Nutzernamen als Suchkriterium. Die Pseudonymisierung ist damit unvollständig.

Einsatz von Verschlüsselung (⊖)

Die Plattform verwendet keine Verschlüsselung.

Funktionsumfang der Zugriffskontrollen (○)

Für die Zugriffskontrollen bei myspace werden drei Nutzergruppen unterschieden:

- alle Nutzer im Internet,
- alle Mitglieder von myspace, und
- »Freunde«, die vom Anwender selbstständig als solche in einer Freundesliste eingetragen werden.

Die Zugriffskontrolle bietet keine Möglichkeit, die Anzeige des Pseudonyms, des Profilfotos, des Wohnorts und des Alters zu unterbinden.

Andere Daten im Profil wie z. B. Familienstand, sexuelle Orientierung, Religion, Einstellung bez. Alkoholkonsum u.a. können in ihrer Sichtbarkeit gegenüber den regulären Internetnutzern und Mitgliedern von myspace eingeschränkt werden. Der Nutzer kann somit diese privatsphärenrelevanten Daten schützen.

Gästebucheinträge (bei myspace als »Kommentare« bezeichnet) und Fotoverknüpfungen können generell nur von »Freunden« erzeugt werden. »Kommentare« und »Blog-Kommentare« können vor Veröffentlichung im Profil vom Anwender kontrolliert werden (vorgelagerte Autorisierung). Fotoverknüpfungen können nur im Nachgang wieder entfernt werden (nur nachgelagertes Veto).

Tabelle 7.5: Zugriffskontrolle myspace

	Gruppen		
	Internet	Plattform-mitglieder	Kontakte 1. Grades
lesender Zugriff			
Name [1]	🔒	🔒	🔒
Profilfoto	🔓	🔓	🔓
Weitere Daten [2]	🔑🔓	🔑🔓	🔓
E-Mail-Adresse [1]	🔒	🔒	🔒
Kontaktliste	🔑🔓	🔑🔓	🔓
Fotos [3]	🔒	🔑🔓	🔑🔓
Neuigkeiten [4]	🔒	🔒	🔑🔓
Status	🔑🔓	🔑🔓	🔑🔓
Gruppen [5]	🔑🔒	🔑🔒	🔑🔒
Wohnort	🔓	🔓	🔓
Alter	🔓	🔓	🔓
Kalender [3]	🔑🔒	🔑🔒	🔑🔓
Gästebuch	🔑🔓	🔑🔓	🔓
Blog [3]	🔑🔓	🔑🔓	🔑🔓
schreibender Zugriff			
Gästebucheintrag [6]	🔒	🔒	🔑🔓
Fotoverknüpfung [7]	🔒	🔒	🔓
Kommentare im Blog [8]	🔒	🔑🔓	🔑🔓

[1] Name und E-Mail-Adresse sind suchbar.
[2] z. B. Interessen, Ausbildung, Religion
[3] Einstellung wird separat für jedes Album/jeden Eintrag bei der Erzeugung vorgenommen.
[4] Neuigkeiten werden nicht im Profil angezeigt, sondern an alle Kontakte gesendet (sogenanntes »Profil-Updates«).
[5] Gruppen standardmäßig für niemanden sichtbar, Anzeige nachträglich aktivierbar
[6] vorgelagerte Autorisierung und nachgelagertes Veto (Standard) möglich
[7] nur nachträgliches Veto möglich
[8] Deaktivierung, vorgelagerte Autorisierung und nachgelagertes Veto (Standard) möglich

Standardkonfiguration (⊖)

In der Standardkonfiguration sind privatsphärenrelevante Daten wie z. B. Interessen, Religionszugehörigkeit und sexuelle Orientierung für Nichtplattformmitglieder lesbar.

Externer Zugriff auf Multimediadaten (⊖)

Die Plattform myspace erlaubt den Zugang zu Videos und Bildern mittels alleiniger Kenntnis ihrer URL. Eine Anmeldung zum Abruf der Daten ist nicht erforderlich.

Suchfunktion (⊖)

Die Suchfunktion erlaubt verschiedene Suchmodi, z. B. nach Name, nach Personen an einer bestimmten Schule oder mit bestimmten Interessen. Bei der Schulsuche, lässt sich das Suchergebnis dann mit neuen Kriterien, wie z. B. dem Beziehungsstatus, weiter verfeinern.

Während des Tests stellte sich heraus, dass myspace Suchergebnisse lieferte, bei denen der Profilinhalt nicht sichtbar war, aber Teile daraus als Suchkriterien verwendet wurden (z. B. »Musik Interessen«). Dieser Effekt ist nur damit zu erklären, dass die Suchfunktion die Regeln der Zugriffskontrolle nicht berücksichtigt. Das führte zu einer negativen Bewertung.

Zugriffsprotokollierung (○)

Die Plattform bietet keine Zugriffsprotokollierung.

Abmelden bei der Plattform (⊕) / Löschumfang (⊕)

Die Löschfunktion ist bei myspace leicht unter »Account-Einstellungen« und »Löschen eines Accounts« zu erreichen. Der Nutzer muss dann nur noch einen Bestätigungslink in einer E-Mail ausführen, um den Vorgang abzuschließen.

Gelöscht wird gründlich. Gruppennachrichten, Foreneinträge und Kommentare zu Blogs werden vollständig entfernt.

Nutzerführung (⊖)

Die Nutzerführung bei myspace wirkt sehr eigenwillig. Grundsätzlich finden sich die Funktionen auf der Startseite unter »Account-Einstellungen«, dort allerdings auf die Unterseiten »Datenschutz«, »Spam & Kommunikation«, »Widgets«, »Kalender« und »Verschiedenes« verteilt (siehe auch Abbildung 7.4). Aus Sicht eines Nutzer der Privatsphäre-Einstellungen sucht, wirkt das sehr hinderlich.

Auch innerhalb der jeweiligen Konfigurationsseiten ist keine klare Systematik erkennbar. Der Anwender muss die erläuternden Texte genau lesen, um zu verstehen, was er jetzt gerade einstellt. Nur die Hilfe in Form von »Häufig gestellten Fragen« ist gut strukturiert.

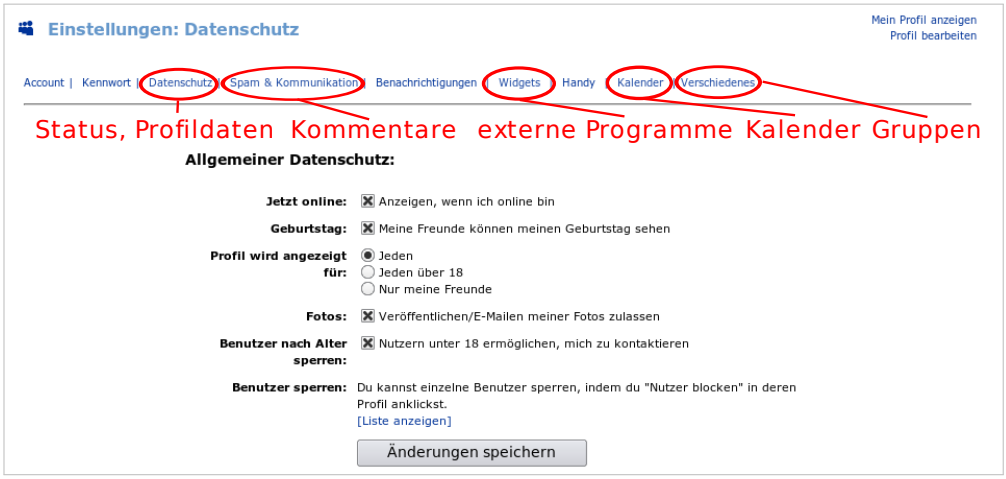


Abbildung 7.4: Einstiegspunkte zu Privatsphäre-Einstellungen für verschiedene Daten (rote Kommentare) bei myspace (Quelle: myspace.com)

Die Privatssphäre-Optionen waren somit schlecht zugänglich und wenig systematisch angeordnet. Die mit dem Kriterium verknüpften Anforderungen sind somit nicht erfüllt.

7.2.2 facebook

Geforderte Daten bei der Anmeldung (◯)

Bei der Anmeldung bei facebook sind der Name, Vorname, E-Mail-Adresse und das vollständige Geburtsdatum anzugeben.

Pseudonyme Nutzung (⊖)

Die Plattform unterstützt keine pseudonyme Nutzung.

Einsatz von Verschlüsselung (◯)

Die Plattform nutzt Verschlüsselung nur für die Anmeldung und die Veränderung der Nutzereinstellungen.

Funktionsumfang der Zugriffskontrollen (⊕)

Der Anwender kann die Zugriffskontrollen bei facebook differenziert und feingranular anpassen. Unterschieden werden dazu folgende Gruppen:

- Nutzer im Internet, die nicht Mitglieder von facebook sind,
- alle Mitglieder von facebook,
- Mitglieder eines Netzwerkes dem der Anwender zugehörig ist,
- Kontakte zweiten Grades (»Freundesfreunde«), und
- Kontakte ersten Grades (»Freunde«).

Entlang dieser Grupppen kann der Anwender den lesenden Zugriff auf Daten schrittweise zu den Kontakten ersten Grades hin limitieren. Ausgenommen von dieser Schutzvorrichtung sind einzig der Anwendername und die Namen der Netzwerke des Anwenders. Für diese Daten kann nur der Zugriff von Nichtmitgliedern aus dem Internet ausgeschaltet werden.

Teilweise können die Zugriffskontrollen noch feiner konfiguriert werden, als das in Tabelle 7.6 dargestellt wird. So ist es z. B. möglich für einige Daten den Zugriff auf die Mitglieder eines ganz bestimmten Netzwerkes zu limitieren (siehe Abbildung 7.5).

Die E-Mail-Adresse und andere Kontaktinformationen, wie z. B. Telefonnummer oder Anschrift, sind nur für Freunde ersten oder zweiten Grades oder für niemanden sichtbar. Gästebucheinträge und Fotoverknüpfungen können zudem grundsätzlich nur von »Freunden« erzeugt werden. Der Nutzer kann die Einträge und Verknüpfungen aber nur per nachgelagertem Veto beeinflussen, also nach ihrer Erstellung löschen. Eine Vorabkontrolle, oder ein präventives Abschalten der Funktionen ist nicht möglich. Es besteht einzig die Möglichkeit das Gästebuch (»Pinnwand«) vollständig zu deaktivieren. Dann kann aber niemand die vorhandenen Einträge lesen.

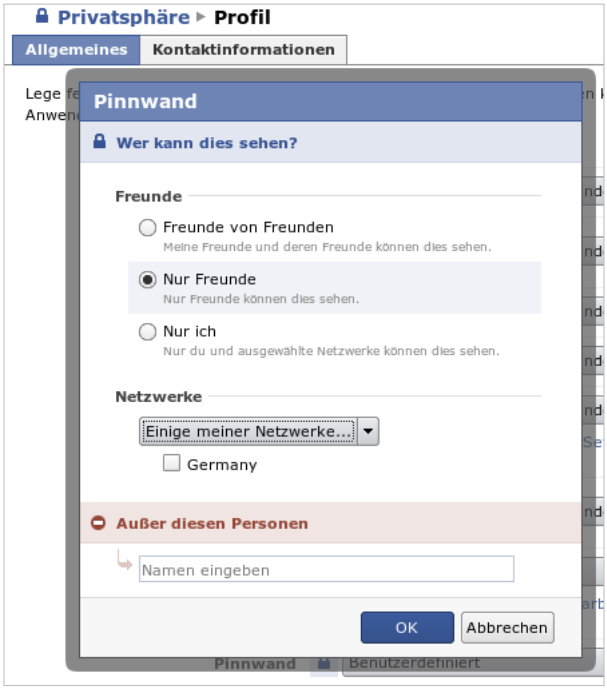


Abbildung 7.5: Erweiterte Zugriffskontrolle bei facebook (Quelle: facebook.com)

Ingesamt bietet Facebook die umfangreichsten Zugriffskontrollen bei den getesteten Plattformen für Privatnutzer: Bis auf wenige Ausnahmen (Name, Netzwerk) können alle Daten geschützt werden. Die zur Verfügung stehende Gruppenaufteilung war die Vielfältigste im Test.

Kritisch ist nur die Gruppe der Netzwerkmitglieder zu sehen, da ein Angreifer unter bestimmten Umständen Mitglied eines Netzwerkes werden kann, dem sein »Angriffsziel« angehört. Vereinfacht wird ein solches Vorgehen dadurch, dass der Angreifer stets die Netzwerke des Opfers sehen kann.

Abmildernd wirkt, dass der Zugang zu einigen Netzwerken limitiert ist. So kann z. B. bei bestimmten Hochschulnetzwerken die Mitgliedschaft nur erlangt werden, wenn eine E-Mail-Adresse bei der jeweiligen Institution vorhanden ist. An diese E-Mail-Adresse wird vor Netzwerkbeitritt ein Bestätigungslink geschickt. Ohne dessen Aktivierung ist kein Beitritt möglich.

Tabelle 7.6: Zugriffskontrolle facebook

	Gruppen				
	Internet	Plattform-mitglieder	Netzwerk-mitglieder	Kontakte 2. Grades	Kontakte 1. Grades [1]
lesender Zugriff					
Name	🔓	🔓	🔓	🔓	🔓
Profilfoto	🔓	🔓	🔓	🔓	🔓
Netzwerke	🔒	🔓	🔓	🔓	🔓
Weitere Daten [2]	🔒	🔒	🔑	🔑	🔓
E-Mail-Adresse [3]	🔒	🔒	🔒	🔑	🔑
Kontaktliste	🔒	🔑	🔑	🔑	🔓
Fotos [4]	🔒	🔒	🔑	🔑	🔑
Videos [4]	🔒	🔒	🔑	🔑	🔑
Neuigkeiten [5]	🔒	🔒	🔑	🔑	🔑
Status	🔒	🔒	🔑	🔑	🔑
Gruppen	🔒	🔒	🔑	🔑	🔑
Kontaktdaten	🔒	🔒	🔑	🔑	🔑
Gästebuch	🔒	🔒	🔑	🔑	🔑
verknüpfte Fotos/ Videos	🔒	🔒	🔑	🔑	🔑
schreibender Zugriff					
Gästebucheintrag [6]	🔒	🔒	🔒	🔒	🔑
Foto-/Videoverknüpfung [7]	🔒	🔒	🔒	🔒	🔑

Anmerkung: Die Standardkonfiguration der Zugriffskontrolle schwächt sich automatisch ab, wenn der Nutzer nach der Anmeldung einem Netzwerk beitritt.

[1] Einige Einstellungen in dieser Spalte lassen sich noch feiner vornehmen (siehe auch Abbildung 7.5).

[2] z. B. politische Einstellung, Beziehungsstatus, Arbeitsstelle

[3] E-Mail-Adresse ist suchbar.

[4] Einstellung ist für jedes Album separat vorzunehmen.

[5] Neuigkeiten werden auch an Kontakte gesendet.

[6] Pinnwand ist vollständig abschaltbar, Einträge können aber nur nachträglich entfernt werden (nachgelagertes Veto).

[7] Können immer nur nachträglich entfernt werden (nur nachgelagertes Veto möglich).

Standardkonfiguration (⊖)

In der Standardkonfiguration sind die Zugriffskontrollen bei facebook bereits restriktiv eingestellt. Abgesehen vom Namen, Profilfoto und Netzwerkzugehörigkeit sind viele Daten nur für Kontakte ersten Grades sichtbar (vergleiche auch Abbildung 7.7).

Es konnte aus den folgenden Gründen dennoch nur eine negative Bewertung vergeben werden:

Sobald der Nutzer einem facebook-Netzwerk beitritt, werden die Beschränkungen der Zugriffskontrolle automatisch auf die Stufe »Meine Netzwerke und Freunde« abgeschwächt, ohne dass er darüber informiert wird. Ein solcher Netzwerkbeitritt unmittelbar nach der Anmeldung bei facebook ist ein üblicher Vorgang, der sogar von der Plattform empfohlen wird. Man kann deshalb bei den automatisch neu gesetzten Einstellungen noch von einer Standardkonfiguration sprechen.

Weiterhin ist selbst in der initalen Standardkonfiguration die Kontaktliste vollständig sichtbar. Zwar ist die entsprechende Option in den Privatsphäre-Einstellungen für das Profil analog zu den anderen Parametern deaktiviert. Allerdings existiert eine weitere Einstellmöglichkeiten unter Menüpunkt »Privatsphäre«, Unterpunkt »Suche« mit der Bezeichnung »Wie kannst du kontaktiert werden? - Deine Freundesliste anzeigen«. Diese ist standardmäßig aktiv.

Die Kontaktliste erlaubt Einblicke in die Beziehungen des Nutzers zu anderen Personen. Hinzu kommt, dass bei Kenntnis des Umfelds einer Person auch Rückschlüsse auf Persönlichkeitsmerkmale möglich sind. Aus diesem Grund handelt es sich bei der Kontaktliste um ein privatsphärenrelevantes Datum, welches im Falle von facebook nicht standardmäßig geschützt wird.

Externer Zugriff auf Multimediadaten (⊖)

Fotos und Videos können von der Plattform facebook allein über die Kenntnis der URL abgerufen werden. Eine vorherige Anmeldung an der Plattform ist nicht erforderlich.

Suchfunktion (⊕)

Wenngleich die facebook-Suchmaschine umfangreiche Suchkriterien, insbesondere auch nach privatsphärenrelevanten Daten (wie z. B. Beziehungsstatus, religiöse Ansichten) bietet, werden die vom Nutzer gesetzten Zugriffsrechte respektiert. Ist also z. B. die Religion nicht sichtbar, dann erscheint der Nutzer nicht in entsprechenden Suchabfragen.

Einziger Wermutstropfen: Man kann auch nach der E-Mail-Adresse suchen. An für sich ist das kein kritischer Punkt. Allerdings kann diese Funktion zur Depseudonymisierung missbraucht werden, wenn eine pseudonyme E-Mail-Adresse, wie z. B. `glitzerfee@emailprovider.de` auch in anderen Kontexten, z. B. einem beliebigen Internetforum, verwendet wird.

Abbildung 7.6: Separate Zugriffskontrolle für die Suchmaschine bei facebook (Quelle: facebook.com)

Ansonsten ist positiv hervorzuheben, dass separate Einstellmöglichkeiten für die Suche existieren (siehe Abbildung 7.6) . Damit kann die Auffindbarkeit in der Plattform weiter reduziert werden. Diese Funktion wird so ausführlich bei keiner anderen Plattform angeboten.

Zugriffsprotokollierung (○)

Die Plattform bietet keine Zugriffsprotokollierung.

Abmelden bei der Plattform (⊖) / Löschumfang (⊕)

Sich bei facebook abzumelden ist ein aufwendigeres Unterfangen: Zwar gibt es in den Konto-Einstellungen eine Funktion »Konto deaktivieren«, dabei handelt es sich jedoch nicht um ein Löschen des Zugangs, sondern nur um ein zeitweises Deaktivieren. Allerdings kann der Nutzer bestimmen, wie lange das Profil deaktiviert ist. Diese Prozedur wird bei facebook als die übliche dargestellt.

Löschen kann man nur, indem man in der Hilfe unter »Privatsphäre und Sicherheit«, Unterpunkt »Privatsphäre« den Hilfetext »Ich möchte meinen Zugang dauerhaft löschen« aufruft und dort dem Link zu einem speziellen Formular folgt. Beim Absenden des Formulares wird offenbar im Hintergrund eine Meldung an den Kundendienst von facebook ausgelöst, da man von diesem eine persönliche E-Mail mit der Löschbestätigung an die eigene E-Mail-Adresse zugeschickt bekommt.

Somit ist zwar im Grunde eine Löschfunktion vorhanden, aber sie ist zum einen schwer auffindbar und zum anderen wird über die »Konto deaktivieren«-Funktion suggeriert, dass diese der normale Weg sei. Diese Dienstgestaltung ist sehr nutzerunfreundlich und wird deshalb negativ bewertet.

Der Löschumfang ist wiederum gut: Gästebuch- und Foreneinträge, Fotoverknüpfungen und Kommentare zu einem Blog werden vollständig entfernt. Diese Gründlichkeit lässt nur bei der Albumübersicht bei anderen Nutzern zu wünschen übrig. Dort wird der Name des gelöschten Nutzers noch angezeigt, wenn er zuvor auf einem der Fotos verknüpft war. Allerdings findet sich kein Hinweis, auf welchem Foto die Verknüpfung erfolgte. Trotz dieses Mankos bleibt der positive Gesamteindruck.

Nutzerführung (◯)

Die Nutzerschnittstelle von facebook macht zunächst einen strukturierten und aufgeräumten Eindruck. Unmittelbar auf der Startseite befindet sich eine Schaltfläche »Privatsphäre«, die alle notwendigen Optionen anzeigt. Das Setzen der Zugriffsrechte für einzelne Daten wird in einer tabellenartigen Anzeige vorgenommen (siehe Abbildung 7.7). Der Nutzer erhält so einen schnellen Überblick, ohne viel Text lesen zu müssen. Neben jedem Auswahlfeld ist ein Schalter vorhanden, der einen passenden Erklärungstext einblendet. Zusätzlich ist eine umfangreiche Hilfe verfügbar. Diese ist allerdings nur teilweise ins Deutsche übersetzt.

Es existiert jedoch zumindest eine Inkonsistenz: Die Sichtbarkeit der Kontaktliste kann nur wirksam eingeschränkt werden, wenn der Nutzer zwei völlig verschiedene Parameter gleichzeitig bearbeitet. Zum einen unter Menüpunkt »Privatsphäre«, Unterpunkt »Profil«, Auswahlfeld »Freunde«. Zum anderen beim Unterpunkt »Suche«, Option »Wie kannst du kontaktiert werden? - Deine Freundesliste anzeigen«.

Weiterhin sind einige Optionen an ungewöhnlicher Stelle positioniert: Die Sichtbarkeit der Gruppen wird so beispielsweise über Menüpunkt »Anwendungen« unter »Privatsphäre«, Link »Seite 'Anwendungen bearbeiten'«, Option »Gruppen: Einstellungen bearbeiten« angepasst.

Zudem gibt es (erwünschte) Seiteneffekte bestimmter Parametrisierungen, die entweder besser zu dokumentieren sind, oder die einen eigenen Menüpunkt erhalten sollten. So kann das Erscheinen in der Kontaktliste anderer Nutzer z.B. durch Verändern der »Such-Sichtbarkeit« eingeschränkt werden.

Abbildung 7.7: Die Zugriffskontrollen bei facebook in der Standardeinstellung (Quelle: www.facebook.de, verkürzte Abbildung)

7.2.3 studiVZ

Geforderte Daten bei der Anmeldung (◯)

Für die Anmeldung an StudiVZ muss der Nutzer den vollständigen Namen, das vollständige Geburtsdatum, das Geschlecht, die besuchte Hochschule und eine E-Mail-Adresse eingeben. Die Angabe der Hochschule wird unter anderem für die Zugriffskontrolle benötigt.

Pseudonyme Nutzung (⊖)

Die Plattform unterstützt keine pseudonyme Nutzung.

Einsatz von Verschlüsselung (◯)

Die Plattform nutzt ausschließlich für den Anmeldevorgang verschlüsselte Datenübertragungen.

Funktionsumfang der Zugriffskontrollen (◯)

Die Benutzereinstellungen bei studiVZ machten einen zweckmäßigen Eindruck. Alle privatsphärenrelevanten Daten können vom Nutzer geschützt werden. Dazu stehen vier Gruppen für die Zugriffskontrolle zur Verfügung:

- Plattformmitglieder,
- Personen einer Hochschule,
- Freundesfreunde, und
- Freunde.

Die Schutzmöglichkeiten sind allerdings sehr grob. Es werden zwei Blöcke gebildet: ein »vollständiges Profil« und ein »eingeschränktes Profil«. Ausgehend von allen Daten werden dann beim »eingeschränkten Profil« Daten schrittweise ausgeschlossen, wie z. B. Fotoverknüpfungen oder Kontaktlisten. Anschließend wird festgelegt, welcher Nutzerkreis das »vollständige Profil« sehen darf. Alle anderen sehen ausschließlich das »eingeschränkte Profil«.

Differenziertere Einstellungen sind nicht möglich. So kann z. B. das Profil nicht so konfiguriert werden, dass nur Kontakte ersten und zweiten Grades auf die Kontaktliste zugreifen können, aber gleichzeitig die Hobbys ausschließlich für Kontakte ersten Grades sichtbar sind.

Für Fotoalben können jeweils individuelle Einstellungen vorgenommen werden. Allerdings kann dabei der Anwender nur die Gruppen »Freunde« oder »alle Plattformmitglieder« auswählen.

Nicht geschützt wird der Name, das Profilfoto und die besuchte Hochschule. Aus diesem Grund ist bei den Zugriffskontrollen die Stufe »Personen einer Hochschule« ungeeignet, da ein potentieller Angreifer selbst die Hochschule

seines »Angriffsziels« auswählen kann. Allerdings kann ein »Hochschulwechsel« nur in bestimmten Zeitabständen erfolgen. Durch Anlegen eines neuen Profils kann diese Einschränkung jedoch leicht umgangen werden.

Weiterhin findet sich bei den Zugriffskontrollen eine Vermischung mit denen der Plattform »meinVZ«. Dabei handelt es sich um einen Ableger von studiVZ. Diese Funktionen wurden hier nicht weiter betrachtet.

Ein Freigabe von Profil- oder anderen Nutzerdaten für Nichtplattformmitglieder existiert nicht.

Tabelle 7.7: Zugriffskontrolle studiVZ

	Gruppen			
	Plattform-mitglieder	Hochschul-angehörige	Kontakte 2. Grades	Kontakte 1. Grades
lesender Zugriff				
Name	🔓	🔓	🔓	🔓
Profilfoto	🔓	🔓	🔓	🔓
weitere Daten [1]	🔑	🔑	🔑	🔓
Kontaktliste	🔑	🔑	🔑	🔓
Fotos [2]	🔑	🔑	🔑	🔑
Status	🔑	🔑	🔑	🔑
Gruppen	🔑	🔑	🔑	🔑
Hochschule	🔓	🔓	🔓	🔓
Kontaktdaten	🔒	🔒	🔒	🔓
Gästebuch	🔑	🔑	🔑	🔑
verknüpfte Fotos	🔑	🔑	🔑	🔓
schreibender Zugriff				
Gästebucheintrag [3]	🔓	🔓	🔓	🔓
Fotoverknüpfung [4]	🔒	🔒	🔒	🔑

[1] z. B. Studiengang, Heimatort, Interessen
[2] Sichtbarkeit ist für jedes Album einzeln einstellbar, dann können aber nur die Gruppen »Kontakte 1. Grades« und »Plattformmitglieder« ausgewählt werden.
[3] für Gästebucheinträge nachgelagertes Veto
[4] Fotoverknüpfungen sind komplett ausschaltbar (Standardeinstellung: nachgelagertes Veto). Außerdem ist eine vorgelagerte Autorisierung möglich.

Standardkonfiguration (⊖)

In der Standardkonfiguration sind privatsphärenrelevante Daten wie z. B. Gruppenzugehörigkeiten, politische Orientierung, Fotoalben und Fotoverknüpfungen für alle Plattformmitglieder lesbar. Im studiVZ-Jargon ist also das »vollständige Profil« für jeden sichtbar. Ein »eingeschränktes Profil« existiert nach der Anmeldung noch nicht.

Externer Zugriff auf Multimediadaten (⊖)

Mit Kenntnis der URL kann auf Bilder in studiVZ beliebig aus dem Internet zugegriffen werden.

Während des Testzeitraums traten bei studiVZ auch Sicherheitslücken bei der Zugriffskontrolle der Fotoalben auf. So waren Fotoalben bei Kenntnis der zugehörigen URL abrufbar, wenn diese nicht indivduell geschützt waren, sondern nur über die Einstellmöglichkeiten des »eingeschränkten Profils«.

In Kenntnis der URL eines geschützten Albums konnte man beispielsweise gelangen, indem man Fotoverknüpfungen auf dieses Album verfolgte. Dazu untersuchte man die Fotoverknüpfungen der Freunde eines Nutzers, da bei diesen die Wahrscheinlichkeit hoch ist, in einem geschützten Album des »Opfers« zu erscheinen.

Diese Schwachstelle wurde bei einer Überarbeitung der Fotoalben-Funktion im August 2008 weiter ausgeweitet. Zwischenzeitlich waren auch geschützte Alben ohne Fotoverknüpfungen zugänglich [7]. Zum Stand Ende August 2008 wurden die aufgefundenen Fehler augenscheinlich behoben.

Suchfunktion (⊖)

Die Suchfunktion bietet eine Standardsuche, die ausschließlich nach dem Namen und Schule oder Hochschule suchen lässt. Zusätzlich existiert eine sogenannte »Super-Suche«, die der Anwender für sein Profil deaktivieren kann.

Die »Super-Suche« erlaubt die Nutzung umfangreicher Suchkriterien, wie z. B. Beziehungsstatus oder politische Auffassung. Zur negativen Bewertung der Suchfunktion führte die Tatsache, dass zuvor gesetzte Zugriffskontrollen nicht auf die Suche einwirken:

Es ist z. B. ohne weiteres möglich, eine bestimmte politische Orientierung in der Suche anzugeben (z. B. »Kommunist«) und in der Ergebnismenge Personen zu erhalten, die dieses Datum nicht für ihr »vollständiges Profil«, also für die Allgemeinheit, freigegeben haben.

Umgekehrt lässt sich mit dieser Lücke der Wert eines verdeckten Datums ermitteln. Die genaue Erläuterung dafür findet sich in 3.7.

Zugriffsprotokollierung (○)

Die Plattform generiert eine Besucherliste. Diese enthält Hyperlinks zu den Profilen der Besucher des eigenen Profils. Ein Datum oder eine Uhrzeit wird nicht angegeben, allerdings ist die Reihenfolge des Abrufs erkennbar.

Die Anwender können allerdings selbst entscheiden, ob sie in der Besucherliste anderer Nutzer erscheinen möchten. Es erfolgte deshalb eine neutrale Bewertung.

Abmelden bei der Plattform (⊕) / Löschumfang (○)

Die Abmeldung bei studiVZ ist unkompliziert: Auf der Seite »mein Account« wird einfach die Funktion »Meinen Account löschen« ausgewählt. Weitere Maßnahmen sind nicht erforderlich.

Positiv ist ebenfalls anzumerken, dass die Allgemeinen Geschäftsbedingungen von studiVZ eine Klausel enthalten nach der mit der Abmeldung »der Account des Nutzers und alle personenbezogenen Daten des Nutzers dauerhaft gelöscht«[18] werden. Es wird auch darauf aufmerksam gemacht, dass bestimmte Daten technisch bedingt weiterhin in der Plattform gespeichert bleiben (z. B. Gästebucheinträge bei anderen Nutzern).

Nach dem Löschen wird bei Foren- und Gästebucheinträgen der Nutzername durch den Text »Gelöschte Person« ersetzt. Die Einträge selbst bleiben erhalten. Das Ersetzen des Personennamens garantiert aber keine vollständige Anonymisierung, da nicht auszuschließen ist, dass der Personenbezug über den Textinhalt bestehen bleibt. Das ist z. B. dann der Fall, wenn der Autor im Text seinen Namen vermerkt hat.

Fotoverlinkungen werden vollständig entfernt.

Nutzerführung (○)

Die Nutzerführung in studiVZ macht prinzipiell einen guten Eindruck. Die Hilfe beantwortet die wichtigsten Fragen. Sie ist in Kategorien, wie z.B. »Meine Seite« oder »Meine Privatsphäre« untergliedert, so dass der Nutzer Hinweise schnell finden kann.

Die Privatsphäre-Einstellungen sind, ebenso wie die Hilfe, mit einem Mausklick über die Startseite erreichbar. Die Aufteilung der Optionen erfolgt zweckmäßig in die Blöcke »Mein Profil«, »Nachrichten & Gruscheln«, »Suche« und »Verschiedenes«. Die einzelnen Funktion sind mit einer Frage überschrieben, wie z. B. »Wie soll mein Geburtstag angezeigt werden?«.

Im Detail existieren jedoch Schwächen:

Ein Problem ist die Vermischung mit Optionen der Plattform »meinVZ«, welche störend wirkt. Aufgrund dieser Vermischung existieren Konfigurationsmöglichkeiten (siehe Abbildung 7.8), deren Bedeutung und Nutzen sich für einige

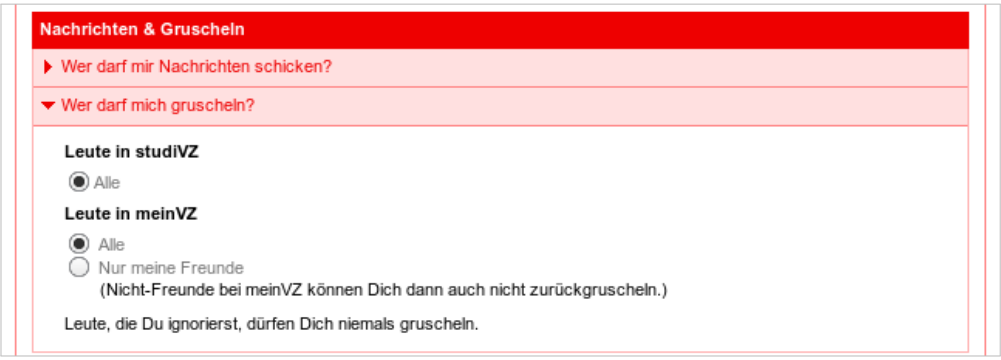


Abbildung 7.8: Vermischen mit Einstellungen für meinVZ bei der Plattform studiVZ (Quelle: studivz.de)

Anwender nicht unmittelbar erschließen wird. Die Verständlichkeit ist damit merklich verschlechtert.

Für den Nutzer ist weiterhin hinderlich, dass es einen für ihn schwer erkennbaren aber gewichtigen Unterschied zwischen dem Einschränken der Sichtbarkeit von Fotoalben mithilfe des »eingeschränkten Profils« und dem Einschränken der Sichtbarkeit mithilfe der »Albuminfo bearbeiten«-Seite gibt.

Mit dem Ersteren wird *keine* Zugriffskontrolle aktiviert, die alle möglichen Ausgaben von Fotos aus Fotoalben in der Plattform erfasst. So ist es unter bestimmten Umständen weiterhin möglich, Fotos unerwünscht einzusehen, auch wenn der Nutzer sie mithilfe der »eingeschränkten Profil«-Funktion vermeintlich geschützt hat. Ein solcher Zugriff ist beispielsweise über Fotoverknüpfungen anderer Nutzer und deren Liste »Fotos auf denen ich verlinkt bin« möglich.

Möchte der Nutzer auch diese Anzeige unterdrücken, so muss er die Sichtbarkeit jedes Albums separat einschränken. Es ist keine Funktion vorhanden, die diesen Vorgang mit den selben Auswirkungen global für alle Fotoalben des Nutzers ausführt. Allerdings ist ernsthaft zu befürchten, dass genau diese Funktionalität über das »eingeschränkte Profils« suggeriert wird. Hier sind vor allem technisch unversierte Nutzer benachteiligt. Sie dürften die subtilen Unterschiede in den Konfigurationsmöglichkeiten kaum erkennen.

Die Nutzerführung wird aus diesen Gründen nur mit »neutral« bewertet.

7.2.4 wer-kennt-wen

Geforderte Daten bei der Anmeldung (○)

Zur Anmeldung muss der Name, Vorname, die E-Mail-Adresse, das Geschlecht und das Geburtsjahr (nicht das vollständige Geburtsdatum) angegeben werden. Die Plattform war damit bezüglich der Anmeldedaten die Sparsamste im Test, auch wenn die Anforderungen für eine positive Bewertung nicht erfüllt waren.

Pseudonyme Nutzung (⊖)

Die Plattform unterstützt keine pseudonyme Nutzung.

Einsatz von Verschlüsselung (⊖)

Die Plattform verwendet keine Verschlüsselung.

Funktionsumfang der Zugriffskontrollen (⊖)

Bei der Plattform wer-kennt-wen werden für die Zugriffskontrolle zwei Nutzergruppen unterschieden: alle Plattformmitglieder und Kontakte ersten Grades (als »Leute, die ich kenne« bezeichnet).

Zahlreiche Daten, wie z. B. Beziehungsstatus, Hobbys oder Vorlieben für Filme und Bücher können also für alle Mitglieder oder nur für Freunde freigeschaltet werden. Alternativ kann eingestellt werden, dass niemand diese Daten sehen kann.

Trotz dieses guten Ansatzes konnte für die Plattform jedoch nur eine negative Bewertung vergeben werden, da sowohl die Kontaktliste als auch Gruppenzugehörigkeiten nicht schützbar sind. Beide sind im Kontext der Plattform als privatsphärenrelevant einzuschätzen:

Die Kontaktliste gibt Auskunft über das soziale Umfeld eines Anwenders. Die Gruppen liefern Hinweise auf religiöse, politische, weltanschauliche oder sexuelle Ansichten und Einstellungen. Beispiele dafür sind Gruppen wie »Lesben mit Kinderwunsch«, »FDP-Wähler« oder auch »Alle die Moslems sind« (ein Beispiel dafür, welche Probleme Gruppenangaben auslösen können, ist auch in [27] erläutert).

Während Gruppen an für sich weniger problematisch sind, wenn sie z. B. nur geographische Zugehörigkeiten ausdrücken, so sind sie in jedem Fall schützenswert, wenn sie oben genannte Informationen liefern. Diesen Schutz gewährleistet die Plattform aber nicht.

Tabelle 7.8: Zugriffskontrolle wer-kennt-wen

	Gruppen	
	Plattform-mitglieder	Kontakte 1. Grades
lesender Zugriff		
Name		
Profilfoto		
allgemeine Daten [1]		
persönliche Daten [2]		
Kontaktliste		
Fotos		
Neuigkeiten [3]		
Status		
Gruppen		
Blog		
Gästebuch		
verknüpfte Fotos		
schreibender Zugriff		
Gästebucheintrag [4]		
Fotoverknüpfung [5]		

[1] z. B. Geburtsname, Wohnort
[2] z. B. Beziehungsstatus, Position, Telefonnummer
[3] Neuigkeiten werden nicht im Profil angezeigt, sondern sind von Kontakten abrufbar.
[4] Gästebuch ist optional, aber standardmäßig aktiv, für Einträge nachgelagertes Veto.
[5] Die Verlinkung ist bis zur Bearbeitung aktiv (nachgelagertes Veto).

Standardkonfiguration (⊖)

In der Standardkonfiguration können alle Plattformmitglieder privatsphärenrelevante Daten wie z. B. Beziehungsstatus, Gruppenzugehörigkeit oder Fotoverknüpfungen lesen.

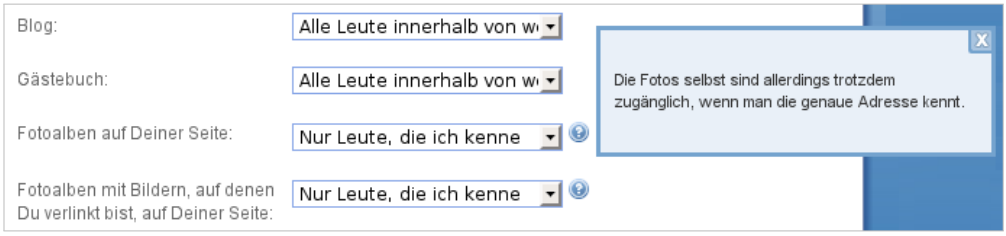


Abbildung 7.9: Hinweis auf externe Erreichbarkeit von Fotos bei wer-kennt-wen (Quelle: wer-kennt-wen.de)

Externer Zugriff auf Multimediadaten (⊖)

Auch bei wer-kennt-wen sind Fotos bei Kenntnis ihrer URL von außen zugänglich. Bemerkenswert ist aber, dass die Plattform selbst per Hilfetext darauf hinweist, wenn man die Einstellungen für die Zugriffskontrolle verändern möchte (siehe Abbildung 7.9). Ein solcher Warnhinweis ist bei den anderen Plattformen nicht vorhanden.

Weiterhin können über die Fotoverknüpfungen anderer Nutzer einzelne Bilder aus einem eigenen geschützten Fotoalbum unerwünscht für alle Plattformmitglieder sichtbar sein.

Suchfunktion (○)

Die Suchfunktion ist bei wer-kennt-wen einfach gehalten. Als Kriterien sind nur der Vorname, Name, das Geschlecht oder ein Ort auswählbar. Diese Daten sind kaum privatsphärenrelevant. Zusätzliche Einstellmöglichkeiten für die Suchbarkeit des eigenen Profils sind nicht vorhanden.

Zugriffsprotokollierung (○)

Es ist eine Protokollierungsfunktion in Form einer Anzeige »Wer war zuletzt auf Deiner Seite?« vorhanden. Der Anwender kann selbst entscheiden, ob er in dieser Liste bei anderen Nutzern erscheinen möchte oder nicht.

Abmelden bei der Plattform (⊕) / Löschumfang (○)

Die Abmeldung des Nutzerzugangs bei wer-kennt-wen ist mit zwei Mausklicks von der Startseite aus möglich. Es wird lediglich die Eingabe des Nutzerkennwortes gefordert.

Foren- und Gästebucheinträge blieben nach Auslösen des Löschvorgangs bestehen. Der Autor wurde aber auf »gelöschter Benutzer« umgeändert. Der Eintrag wird damit aber nicht zwangsläufig vollständig anonymisiert, da über den Textinhalt der Personenbezug erhalten bleiben kann. Bei den Tests konnte außerdem festgestellt werden, dass Fotoverknüpfungen nicht sofort, sondern erst nach zwei Tagen gelöscht wurden. Hierbei könnte es sich aber auch um ein temporäres technisches Problem gehandelt haben.

Nutzerführung (⊕)

Privatsphäre-Einstellungen finden sich übersichtlich auf einer Seite. Sie kann durch Anklicken von »Einstellungen« unmittelbar nach dem Plattform-Login erreicht werden. Der Aufbau ist tabellenartig, ähnlich dem von facebook, allerdings ohne die bei facebook beobachteten Mängel.

Untereinander angeordnet sind die verschiedenen Daten. Rechts daneben befindet sich jeweils eine Auswahlliste für die Einstellung der erlaubten Personenkreise. An geeigneter Stelle sind Hinweistexte verfügbar. Nur die Hilfe, hier als FAQ[1] ausgearbeitet, ist etwas knapp an Erläuterungen im Vergleich zu anderen Plattformen.

Die Ausarbeitung der Privatsphäre-Einstellungen wirkt gut und leicht verständlich. Inkonsistenzen konnten nicht beobachtet werden. Es wird deshalb eine positive Bewertung vergeben.

[1] Häufig gestellte Fragen

7.2.5 lokalisten

Geforderte Daten bei der Anmeldung (◯)

Die Plattform forderte zur Anmeldung die Angabe des Namens, Vornames, E-Mail-Adresse, Geschlechts, Geburtsdatums. Zusätzlich war die Auswahl eines Pseudonyms (Spitzname) notwendig.

Pseudonyme Nutzung (◯)

Die Plattform unterstützt pseudonyme Nutzung. Allerdings kann per Suchfunktion nach vollständigen Nutzernamen gesucht werden. Die Pseudonymisierung ist somit lückenhaft.

Einsatz von Verschlüsselung (⊖)

Die Plattform verwendet keine Verschlüsselung.

Funktionsumfang der Zugriffskontrollen (⊖)

Im Test wiesen die Einstellmöglichkeiten für die Zugriffskontrolle bei lokalisten erhebliche Mängel auf:

Nur Fotoalben und einzelne Einträge im Blog oder Tagebuch kann der Nutzer schützen. Desweiteren gibt es sogenannte »Freundesaktivitäten«, also eine Art Verbreitungskanal für Neuigkeiten, die generell nur für Kontakte ersten Grades sichtbar sind. Interessanterweise erlaubt es die Plattform hier relativ genau einzustellen, welche »Aktivitäten« angezeigt werden sollen.

Gästebucheinträge werden nur nach ausdrücklicher Genehmigung durch den Gästebuchinhaber veröffentlicht. Fotoverknüpfungen können ausschließlich von Kontakten ersten Grades erzeugt werden. Die betroffene Person kann diese aber nur nachträglich wieder entfernen (nachgelagertes Veto).

Tabelle 7.9: Zugriffskontrolle lokalisten

	Gruppen		
	Plattform-mitglieder	Kontakte 2. Grades	Kontakte 1. Grades
lesender Zugriff			
Name [1]	🔒	🔒	🔓
Profilfoto	🔓	🔓	🔓
weitere Daten [2]	🔓	🔓	🔓
E-Mail-Adresse [1]	🔒	🔒	🔒
Kontaktliste	🔓	🔓	🔓
Fotos [3]	🔑🔓	🔑🔓	🔓
Videos	🔓	🔓	🔓
Neuigkeiten [4]	🔒	🔒	🔑🔓
Status	🔓	🔓	🔓
Gruppen	🔓	🔓	🔓
Tagebuch [3]	🔑🔓	🔑🔓	🔓
Blog [3]	🔑🔓	🔑🔓	🔓
Gästebuch	🔓	🔓	🔓
verknüpfte Fotos	🔓	🔓	🔓
schreibender Zugriff			
Gästebucheintrag [5]	🔑🔒	🔑🔒	🔑🔒
Fotoverknüpfung [6]	🔒	🔒	🔓

[1] Name und E-Mail-Adresse sind indirekt über die Suche abfragbar.
[2] z. B. Familienstand, Hobbys, Schule
[3] für jeden Eintrag/jedes Album getrennt einstellbar
[4] Neuigkeiten werden auch im Startfenster der Kontakte angezeigt.
[5] Gästebucheinträgen muss immer zugestimmt werden (nur vorgelagerte Autorisierung).
[6] Verlinkung ist bis zur Bearbeitung aktiv (nur nachgelagertes Veto).

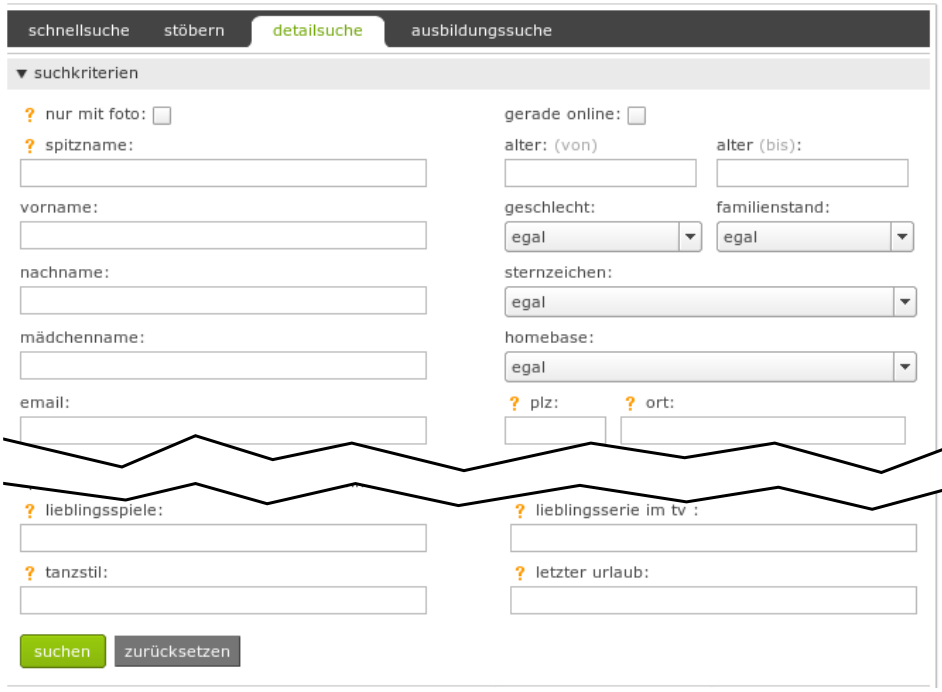


Abbildung 7.10: Sehr umfangreiche Suchkriterien bei der Plattform lokalisten (Quelle: lokalisten.de, verkürzte Darstellung)

Standardkonfiguration (⊖)

Da für eine Vielzahl privatsphärenrelevanter Daten von der Plattform ohnehin keine Zugriffskontrolle vorgesehen wurde, ist die Standardkonfiguration ebenfalls mit »negativ« zu bewerten.

Externer Zugriff auf Multimediadaten (⊖)

Bei lokalisten sind Hyperlinks auf Bilder und Videos auch außerhalb der Plattform gültig.

Suchfunktion (⊖)

Die Suchfunktion bei lokalisten umfasst sehr viele Daten als mögliche Suchkriterien: Hobbys, Alter, E-Mail-Adresse, verschiedene Preferenzen, wie Lieblingsfilme oder Lieblingsbuch und vieles mehr (siehe auch Abbildung 7.10). Diese Daten sind in jedem Fall privatsphärenrelevant. Desweiteren werden sie von keiner vom Nutzer konfigurierbaren Zugriffskontrolle geschützt. Die Suchfunktion wird deshalb negativ bewertet.

Zugriffsprotokollierung (○)

Die Plattform zeigt auf der Startseite Links zu den Profilen der Personen an, die das eigene Profil aufgerufen haben. Die Uhrzeit oder ein Datum des Zugriffs werden nicht geliefert. Der Protokollierte kann die Funktion nicht abschalten.

Allerdings ist aus dem Protokoll die Reihenfolge des Aufrufs abzulesen. Außerdem ist das andere Profil direkt im Protokoll anklickbar. Hier wäre sicher eine weitere Reduzierung der Datensammlung möglich.

Im Sinne der Anforderungen für dieses Kriterium wurde eine neutrale Bewertung vergeben.

Abmelden bei der Plattform (⊖) / Löschumfang (⊕)

Zum Abmelden von lokalisten muss der Nutzer eine E-Mail an den Betreiber schicken. Daraufhin erhält er eine E-Mail mit einem Bestätigungslink zurück. Der Aufruf dieses Links ist erforderlich um das Löschen endgültig zu vollziehen. Die erforderliche E-Mail-Adresse findet der Nutzer in der Hilfe unter dem Menüpunkt »registrierung & account«.

Dieses Prozedere ist umständlich und mit dem Stand der Technik nicht zu rechtfertigen. Deshalb wird eine negative Bewertung vergeben.

»Positiv« ist aber der Umfang des Löschens: Unter anderem werden Gästebucheinträge in fremden Profilen, Nachrichten in Gruppen, Fotoverknüpfungen und Kommentare zu einem Blog gelöscht.

Nutzerführung (○)

Die wenigen Privatsphäre-Optionen die lokalisten bietet, sind vom Anwender leicht über die Startseite (Schaltfläche »Privatsphäre«) zu erreichen. Die Seite wirkt recht übersichtlich. Allerdings ist dieses Gesamtbild der geringen Anzahl an Konfigurationsmöglichkeiten geschuldet.

Die Hilfe ist übersichtlich. Sie enthält aber kaum Informationen zum Privatsphärenschutz. Insgesamt erfolgte deshalb eine Bewertung als »neutral«.

7.3 Einzelbewertungen der Geschäftsnutzer-Plattformen

7.3.1 XING

Geforderte Daten bei der Anmeldung (⊖)

Bei der Anmeldung an XING ist die Eingabe von Stammdaten und sogenannten Businessdaten notwendig. Die Stammdaten umfassen Name, Vorname, E-Mail-Adresse, Geschlecht und Geburtsdatum. Geschäftsdaten sind Berufsstatus, Bezeichnung der Firma, Position innerhalb der Firma, Firmenbranche sowie als Teile der Geschäftsadresse das Land und der Ort.

Es besteht keine rechtliche oder technische Notwendigkeit, warum diese umfangreichen Daten Pflichteingaben sein sollen. Sie sind z.B. für das Vertragsverhältnis mit dem Nutzer in dieser Menge nicht notwendig. Der Zugang ist ohnehin technisch mit weniger Daten realisierbar. Die eingegebenen Daten reichern fast ausschließlich die Profildaten des Nutzers als initialen Zustand an. Sie erfüllen damit auch keine unverzichtbare Funktion in der Plattform, indem sie z.B. eine Datenbasis für spezielle Taxonomien, Gruppensysteme, Zugriffskontrollen etc. bilden. Ein Verzicht auf die Eingabepflicht schränkt deshalb die Plattformfunktionen kaum ein.

Deshalb waren die mit dem Kriterium verknüpften Anforderungen nicht erfüllt und es wurde eine negative Bewertung vergeben.

Einsatz von Verschlüsselung (⊕)

Die Plattform nutzt Verschlüsselung über die gesamte Nutzersitzung hinweg.

Funktionsumfang der Zugriffskontrollen (⊖)

Der Nutzer kann bei XING auf nur wenige Zugriffskontrollen zurückgreifen. Gut ist, dass jegliche Arten von Kontaktdaten (Adressen, Telefonnummern etc.) für jeden anderen Plattformnutzer individuell freigeschaltet werden können. Auch die Kontaktliste kann recht feingranular hinsichtlich der für den Zugriff erlaubten Nutzergruppen (Kontakte bis maximal vierten Grades) konfiguriert werden. Gleiches gilt für die Sichtbarkeit der beigetretenen Gruppen.

Wer Gästebucheinträge erstellen darf, kann ebenfalls eingeschränkt werden. Allerdings ist keine vorgelagerte Autorisierung implementiert sondern nur ein nachgelagertes Veto.

Die sehr umfangreichen »Business Daten« enthalten Angaben über den beruflichen Werdegang, Ausbildung und Interessen (vielfach privater Natur). Diese Daten gehen somit in der Menge als auch hinsichtlich der Privatsphärenrelevanz leicht über die Angaben in einer durchschnittlichen Bewerbungsmappe hinaus. Sie sind also in jedem Fall schützenswert.

Auf der anderen Seite bietet XING keine effektive Zugriffskontrolle. Genauer ausgedrückt, kann die Sichtbarkeit der »Business Daten« zwar gegenüber Nichtplattformmitglieder eingeschränkt werden. Weitere Einstellmöglichkeiten existieren aber nicht.

Ein weiteres Manko ist die Funktion »Zeige alternative Verbindungen«. Sie ist beim Aufruf eines fremden Profils verfügbar (siehe Abbildung 7.11) und dient dazu, Verbindungspfade zwischen der aktuell eingeloggten Person und dem Inhaber des dargestellten Profils aufzuzeigen.

Abbildung 7.11: Aufruf der Funktion »Zeige alternative Verbindungen« (Quelle: xing.com)

Dabei sind die Profile anderer Nutzer die Zwischenstationen auf »dem Weg« zwischen beiden Personen. In der Kontaktliste eines Vorgänger-Profils ist das jeweilige Nachfolger-Profil enthalten. Jeder Pfad stellt also einen Weg vom Startprofil zum Zielprofil durch die Kontaktlisten von Plattformnutzern dar (siehe Abbildung 7.12).

Abbildung 7.12: Anzeige der Verbindungen zwischen zwei Personen (Quelle: xing.com)

Diese Pfade werden auch mithilfe von Profilen gebildet, deren Kontaktliste für den eingeloggten Nutzer nicht sichtbar sind. Da ein Nachfolger in einem Pfad zwingend in der Kontaktliste seines Vorgängers enthalten sein muss, kann auf diese Weise ein Teil der verdeckten Kontaktlisten anderer Plattformanwender rekonstruiert werden. Die Zugriffskontrolle wird somit teilweise unwirksam.

Tabelle 7.10: Zugriffskontrolle XING

	Gruppen			
	Internet	Plattform-mitglieder	Kontakte 2. - 4. Grad.	Kontakte 1. Grades
lesender Zugriff				
Name				
Profilfoto				
Business Daten [1]				
E-Mail-Adresse [2]				
Kontaktliste [3]				
Neuigkeiten [4]				
Gruppen				
Kontaktdaten [2]				
Gästebuch [5]				
schreibender Zugriff				
Gästebucheintrag [5]				

[1] z. B. Berufserfahrung, »Ich biete«, Homepage
[2] Einstellungen zu Kontaktdaten können für jeden Nutzer individuell vorgenommen werden.
[3] zum Teil indirekt über Verbindungen einsehbar, bei Sichtbarkeit im »öffentlichen Profil« wird bei jedem Aufruf ein anderer Ausschnitt (vier Kontakte) aus der Kontaktliste eingeblendet
[4] werden nur im Startfenster der Kontakte angezeigt.
[5] Gästebuch ist optional (Standardeinstellung: aktiv), die Einstellung zu den Einträgen ist an »Nachrichten senden« gekoppelt, für Einträge nachgelagertes Veto.

Standardkonfiguration (⊖)

In der Standardkonfiguration sind privatsphärenrelevante Daten wie z. B. der berufliche Werdegang, Bildungskarriere oder Interessen geschäftlicher und privater Natur für Nichtplattformmitglieder lesbar.

Suchfunktion (⊖)

Als nicht-zahlender XING-Nutzer kann man nach Vorname, Nachname, Branche und Ort aus der Geschäftsadresse suchen. Weitere Suchkriterien sind möglich,

allerdings wird in der Ergebnisliste dann nur das Profilfoto, aber nicht der Name oder Link zu den Nutzerprofilen angegeben. Diese Daten werden nur für zahlende »Premiummitglieder« freigeschaltet.

Solche weiteren Suchkriterien sind beispielsweise Interessen, Hochschulen, Organisationen, Firmenzugehörigkeiten; also im wesentlichen Teile der »Business Daten«. Hier lässt sich z. B. nach politischen Neigungen (z. B. Suchbegriff »CSU« unter Suchkriterium »Interessen«) oder weltanschaulichen Auffassungen (z. B. Suchbegriff »Homöopathie«, »Greenpeace« oder auch »Astrologie« unter Suchkriterium »Interessen«) suchen.

Der Nutzer kann diese Daten innerhalb der Plattform nicht schützen. Sie werden aber offensichtlich von der Suche erfasst. Diese Kombination beeinträchtigt die Privatsphäre des Betroffenen. Es wurde deshalb eine negative Bewertung vergeben.

Zugriffsprotokollierung (◯)

XING bietet auf der Startseite eine Anzeige der »Besucher meines Profils«. Um die Profile der anderen Nutzer öffnen zu können, muss man allerdings ein zahlender »Premiumnutzer« werden. Ansonsten sieht man nur das Profilfoto.

Gut ist, dass für die einzelnen Besucher kein Datum und Uhrzeit des Profilaufrufs angezeigt werden. Weiterhin ist diese Form des automatischen Protokollierens für den Besucher, also den Protokollierten, nicht abschaltbar und damit auch nicht umgehbar.

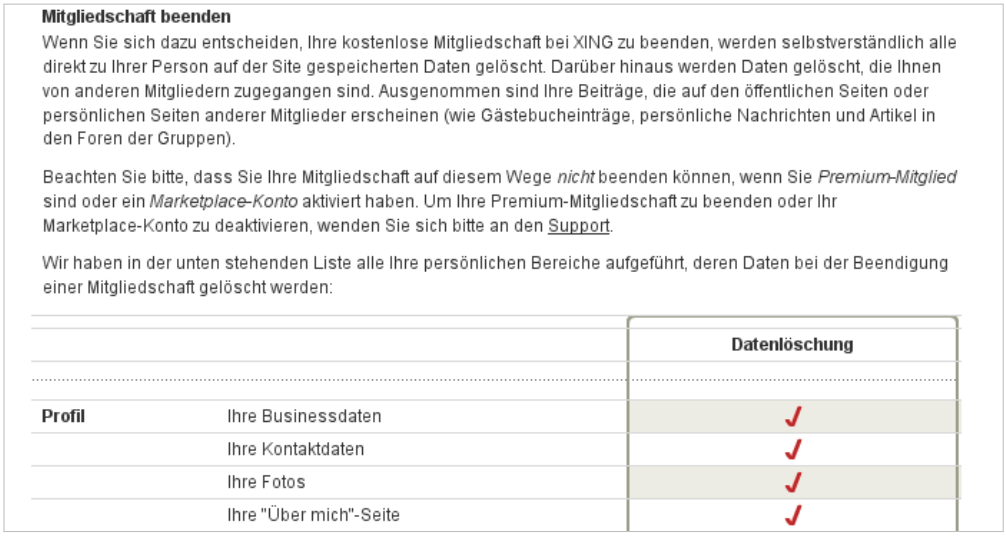
Allerdings ergibt sich aus dem Protokoll die Reihenfolge des Zugriffs. Der Protokollumfang hätte im Plattformkontext auch noch weiter reduziert werden können. Beispielweise hätte die Anzeige der Firma und die Position des Aufrufenden ausgereicht, anstatt dass das Profil des Protokollierten direkt aufgerufen werden kann (vergleiche mit LinkedIn in Abschnitt 7.3.2).

Abmelden bei der Plattform (◯) / Löschumfang (⊖)

Die Schaltfläche zum Abmelden bei der Plattform findet man nur nach einiger Arbeit: Sie befindet sich in der Hilfe unter »Die Funktionen von XING«, Abschnitt »Mitgliedschaft & Rechnung« und Hilfetext »Wie kann ich die kostenlose Mitgliedschaft kündigen/meinen Account löschen?«.

Eine Abmeldefunktion ist somit vorhanden aber umständlich aufzufinden.

Nach dem Löschen erscheint der eigene Name weiterhin bei Einträgen in Gruppenforen und bei Einträgen in Gästebüchern anderer Nutzer. Zu bedenken ist, dass Einträge in Gruppenforen möglicherweise außerhalb der Plattform zugänglich sind, je nachdem, ob das Forum selbst öffentlich ist und wie die Zugriffskontrollen des Nutzers bei der Eintragerzeugung eingestellt waren. Nach dem Stand der Technik ist es dem Plattformbetreiber zuzumuten, mindestens den Klartextnamen durch eine anonyme Kennung zu ersetzen.



Mitgliedschaft beenden

Wenn Sie sich dazu entscheiden, Ihre kostenlose Mitgliedschaft bei XING zu beenden, werden selbstverständlich alle direkt zu Ihrer Person auf der Site gespeicherten Daten gelöscht. Darüber hinaus werden Daten gelöscht, die Ihnen von anderen Mitgliedern zugegangen sind. Ausgenommen sind Ihre Beiträge, die auf den öffentlichen Seiten oder persönlichen Seiten anderer Mitglieder erscheinen (wie Gästebucheinträge, persönliche Nachrichten und Artikel in den Foren der Gruppen).

Beachten Sie bitte, dass Sie Ihre Mitgliedschaft auf diesem Wege *nicht* beenden können, wenn Sie *Premium-Mitglied* sind oder ein *Marketplace-Konto* aktiviert haben. Um Ihre Premium-Mitgliedschaft zu beenden oder Ihr Marketplace-Konto zu deaktivieren, wenden Sie sich bitte an den Support.

Wir haben in der unten stehenden Liste alle Ihre persönlichen Bereiche aufgeführt, deren Daten bei der Beendigung einer Mitgliedschaft gelöscht werden:

		Datenlöschung
Profil	Ihre Businessdaten	✓
	Ihre Kontaktdaten	✓
	Ihre Fotos	✓
	Ihre "Über mich"-Seite	✓

Abbildung 7.13: Ausschnitt aus der Abmeldeseite bei XING (Quelle: xing.com)

Ein Mitarbeiter der XING AG teilte zu diesem Problem dem Fraunhofer SIT mit, dass Beiträge nur bearbeitet werden, wenn der ausgeschiedene Nutzer sich mit einem entsprechenden Wunsch an den Kundendienst der Plattform wendet. Im regulären Abmeldeprozess ist jedoch nicht vorgesehen, Foren- und Gästebucheinträge zu löschen oder zu anonymisieren. Wie schnell und wie sachdienlich eine solche Kundenanfrage bearbeitet wird, konnte im Test nicht festgestellt werden.

Wünschenswert wäre für den privatsphärenbewussten Nutzer ein expliziter Hinweis des Plattformbetreibers auf diesen Service. Zwar zeigt beim Abmelden eine tabellenartige Übersicht die zu löschenden Daten an. Die verbleibenden Daten sind aber in der Tabelle nicht verzeichnet, sondern nur im darüberliegenden Text erwähnt (siehe Abbildung 7.13). Auch in Hinblick auf technisch unversierte Nutzer sollte der Betreiber diesen Überblick entsprechend erweitern und Hinweise zum Kundendienst einblenden.

Auch ist zu überlegen, beim Abmelden den Nutzer selbst entscheiden zu lassen, ob seine Foren- und Gästebucheinträge in der Plattform verbleiben sollen oder nicht. Es könnte dafür eine entsprechende Schaltfläche oder ein Auswahlfeld hinzugefügt werden.

Selbst unter Berücksichtigung der zusätzlichen Informationen von XING, wird für dieses Kriterium dennoch nur eine »negative« Bewertung vergeben: Der *reguläre* Abmeldeprozess sieht keine Lösch- oder Anonymisierungsfunktion für Foren- und Gästebucheinträge vor. Dieses Faktum allein reicht bereits aus, damit die Anforderungen für dieses Kriterium nicht mehr erfüllt werden können. Zudem sind die zusätzlichen Leistungen des Kundendienstes auf den Abmeldeseiten nicht dokumentiert.

Nutzerführung (◯)

Die Einstellungen zur Privatsphäre lassen sich, von der Startseite kommend, unter »Einstellungen« und dem Unterpunkt »Privatsphäre« anpassen. Die Seite

wirkt übersichtlich. Allerdings wird die Sichtbarkeit einiger Komponenten (Gruppenzugehörigkeit, Aktivitätsindex, Skype-Online-Status) im Unterpunkt »Profileinstellungen« angezeigt, obwohl diese Konfigurationsmöglichkeiten eher auf Privatsphäre abzielen.

Ein weiteres Problem ist, dass XING zwar erlaubt für andere Plattformmitglieder individuell den Zugang zu Kontaktdaten (Telefonnummern, Adressen etc.) freizugeben, dafür aber eine zentrale Übersicht fehlt. Der Nutzer hat somit keinen gesamtheitlichen Überblick, wer alles seine Kontaktdaten sehen darf. Hier wäre es wünschenswert, diese prinzipiell gute Idee weiter zu verbessern.

Die Hilfe gibt Hinweise zu den wichtigsten Themen. Eine Kategorie »Datensicherheit« mit Tipps zum Privatsphärenschutz ist vorhanden.

7.3.2 LinkedIn

Geforderte Daten bei der Anmeldung (⊖)

Um sich bei LinkedIn anzumelden, muss der Anwender den vollständigen Namen, E-Mail-Adresse, Land und Postleitzahl angeben. Zusätzlich sind Daten über das Arbeitsleben wie Berufsstatus, Firma, Stellung, Branche und, beim Berufsstatus »Student«, Bildungsangaben wie Hochschule und Dauer der Ausbildung anzugeben. Einige Angaben entfallen bei einem bestimmten Berufsstatus.

Ein Grund, weshalb die vollständige Eingabe dieser Daten erzwungen wird, ist nicht ersichtlich. Sie sind aus technischer oder rechtlicher Sicht in ihrer Gesamtheit nicht notwendig. Das Funktionieren des Dienstes wird auch nicht eingeschränkt, wenn man auf die Eingabepflicht verzichtet. Damit ergibt sich auch aufgrund der Menge an Daten ein vergleichbares Problem wie bei der Plattform XING. Es wurde deshalb analog eine negative Bewertung vergeben.

Pseudonyme Nutzung

Auch wenn dieses Kriterium bei den geschäftlichen Plattform nicht geprüft wurde, lohnt es sich an dieser Stelle darauf hinzuweisen, dass LinkedIn eine gute Pseudonymisierungsfunktion vorweisen kann. Wenn der Nutzer diese aktiviert, dann erscheint vom Nachnamen nur noch der erste Buchstaben in der Plattform (siehe Abbildung 7.14). Dies wirkt auch auf die Suche, d.h. man kann eine Person nicht mehr finden, wenn man nach dem vollständigen Namen sucht.

Einsatz von Verschlüsselung (◯)

Die Plattform nutzt Verschlüsselung nur für die Anmeldung und die Veränderung der Nutzereinstellungen.

Funktionsumfang der Zugriffskontrollen (⊖)

Die Zugriffskontrollen von LinkedIn ähneln denen von XING:

Die umfangreichen Geschäftsdaten (Bildung, beruflicher Werdegang, berufliche und private Interessen) können nur gegen Zugriffe von Nicht-Plattformmitgliedern geschützt werden. Innerhalb der Plattform sind sie unbegrenzt verfügbar.

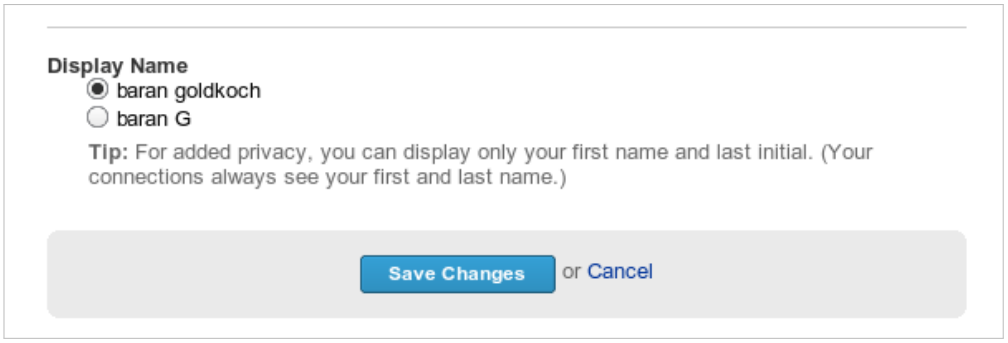


Abbildung 7.14: Pseudonymisierung bei LinkedIn (Quelle: linkedin.com)

Weiter eingeschränkt werden kann der Zugriff auf die Kontaktliste, auf den eigenen Status, die Gruppenzugehörigkeiten und auf das Profilfoto. (Die Kontaktliste kann aber sowieso nur von Kontakten ersten Grades eingesehen werden.)

Ein Teil dieser Daten sind aber beim Aufruf eines Nutzerprofils nur sichtbar, wenn der Aufrufer einen Bezahlzugang zur Plattform hat.

Die Situation ist hier vergleichbar mit der bei XING: Die Geschäftsdaten sind sehr umfangreich und teilweise mit privaten Informationen vermischt. Auf der anderen Seite können sie nicht effektiv geschützt werden. Diese Kombination führte zur Abwertung.

Tabelle 7.11: Zugriffskontrolle LinkedIn

	Gruppen			
	Internet	Plattform-mitglieder	Netzwerk	Kontakte 1. Grades
lesender Zugriff				
Name [1]	🔓	🔓	🔓	🔓
Profilfoto	🔓	🔓	🔓	🔓
Business Daten [2]	🔓	🔓	🔓	🔓
E-Mail-Adresse	🔒	🔒	🔒	🔓
Kontaktliste	🔒	🔒	🔒	🔓
Neuigkeiten [3]	🔒	🔒	🔒	🔓
Status	🔒	🔓	🔓	🔓
Gruppen	🔓	🔓	🔓	🔓
Empfehlung [4]	🔓	🔓	🔓	🔓
schreibender Zugriff				
Empfehlung [5]	🔒	🔒	🔒	🔓

[1] einfache Pseudonymisierung (Abschneiden des Nachnamens) kann aktiviert werden.
[2] z. B. Empfehlungen, Erfahrung, Ausbildung
[3] Neuigkeiten erscheinen nur im Homefenster der Kontakte.
[4] Details einer Empfehlung sind nur Kontakten sichtbar.
[5] vorgelagerte Autorisierung

Standardkonfiguration (⊖)

In der Standardkonfiguration sind privatsphärenrelevante Daten wie z. B. beruflicher Werdegang, Ausbildung und Interessen für Nichtplattformmitglieder lesbar.

Suchfunktion (◯)

Die Suche funktioniert bei LinkedIn hauptsächlich über Schlagworte (»keywords«), die verschiedenartig in den gefundenen Profilen vorkommen (z. B. in den Interessen). Daneben kann unter anderem auch der Name, die Firma, Branchenzugehörigkeit und der Ort angegeben werden.

Die Suchfunktion ähnelt damit der von XING. Allerdings erlangte LinkedIn eine bessere Bewertung, da die Plattform, eine Pseudonymisierungsfunktion besitzt, die auch auf die Suche wirkt. Eine Person kann damit über den Namen nicht-mehr in der Plattform gefunden werden. Erscheint das Profil über ein anderes Suchkriterium, wie z. B. dem Firmennamen, in den Suchergebnissen, dann wird zumindest der Name der Person nicht ausgeben. Das erschwert die Identifizierung und schützt damit teilweise die Privatsphäre.

Zugriffsprotokollierung (◯)

Bei LinkedIn existiert ein Zugriffsprotokoll in Form einer »Who's viewed my profile«-Liste. Interessant ist, dass der Protokollierte sein Erscheinen in dieser Liste dreistufig einstellen kann: Mit Name und Überschrift, als Anzeige ohne Name sondern nur mit Geschäftsfeld und Position oder gar keine Anzeige.

Wäre die Funktion nicht komplett abschaltbar, hätte sie eine gute Lösung hinsichtlich der Abwägung der Interessen des Profilinhabers und des Profilaufrufenden sein können. Der Aufrufende könnte den Informationabfluss in das Protokoll einschränken. Allerdings könnte er sich andererseits auch nicht völlig aus dem Protokoll herausnehmen.

Im Ansatz bietet LinkedIn das beste Konzept bei den getesteten Plattformen. Da die Protokollierung aber dennoch komplett abschaltbar ist, wurde nur eine neutrale Bewertung vergeben.

Abmelden bei der Plattform (⊕) / Löschumfang (⊕)

Zum Abmelden von LinkedIn kann die Funktion »Close Your Account« unter »Account & Settings« verwendet werden. Nach optionaler Angabe eines Grundes und mehrmaligen Bestätigen wird der Zugang gelöscht.

Da es bei LinkedIn keine Foren gibt, fällt damit schon ein Teil der Löschproblematik weg. Bleiben die Empfehlungen (»Recommendations«) bei anderen Nutzern, wie auch Antworten im sogenannten »Answer«-Werkzeug (hier können Fragen an andere Mitglieder gestellt werden). Bei beiden werden die vollständigen Einträge gelöscht. Deshalb wird der Löschumfang mit »positiv« bewertet.

Nutzerführung (◯)

Die Nutzerführung machte bei LinkedIn einen zweckmäßigen Eindruck. Die Einstellungen waren unter »Account & Settings« zentral zusammengefasst. Sehr gut ist, dass die momentane Einstellung mit einem kurzen Aussagesatz beim jeweiligen Menüpunkt wiedergegeben wird, z. B. bei »My Profile Photo« mit

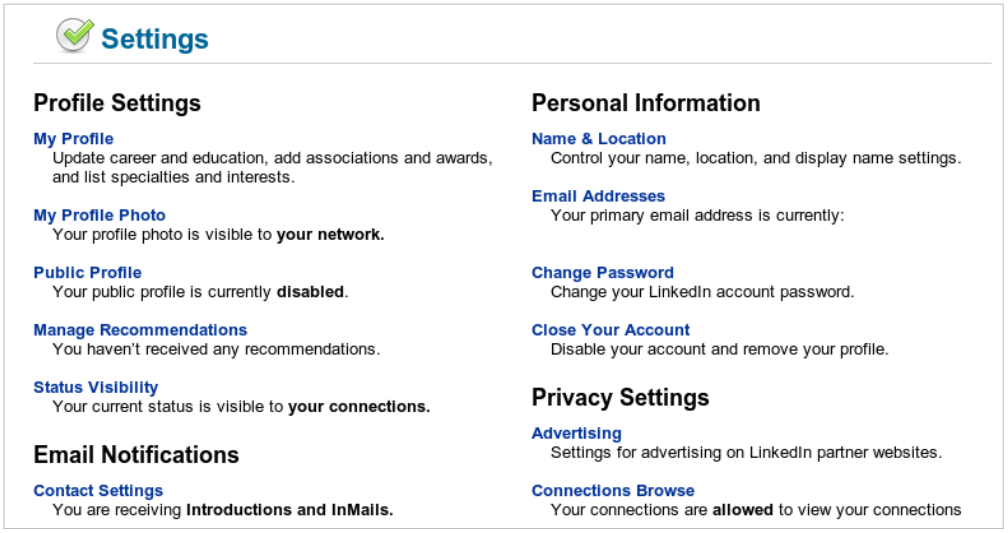


Abbildung 7.15: Einstellmöglichkeiten bei LinkedIn (Quelle: linkedin.com)

»Your profile photo is visible to your network« (siehe auch Abbildung 7.15). Damit wird auch klarer, welche Funktion unter einem Menüpunkt zu erwarten ist.

Etwas ungewöhnlich ist, dass »Status Visibility« und »Public Profile« nicht unter den »Privacy Settings« erscheint. Auf der anderen Seite befindet sich unter den »Privacy Settings« eine Option mit der die Sichtbarkeit der Profilfotos *anderer* Plattformmitglieder eingeschränkt werden kann.

Ungünstig ist auch, dass die Pseudonymisierungsfunktion (vergleiche Abbildung 7.14) im Unterpunkt »Name & Location« unter »Personal Information« platziert ist. Es wäre nutzerfreundlicher gewesen, diese in die Privatsphäre-Einstellungen einzubinden.

Die Hilfe ist in Form von FAQ[2] vorhanden.

[2] Häufig gestellte Fragen

8 Ratgeber für Nutzer

Dieses Kapitel soll einige Regeln und Tipps für privatsphärenbewusste Nutzer von Soziale-Netzwerke-Plattformen liefern. Diese Hinweise haben sich unmittelbar aus den Prüfergebnissen für die einzelnen Plattformen ergeben. Sie sollen keine übertriebene Paranoia schüren. Allerdings werden keine auch Probleme ausklammert, auch wenn sie nur in einigen Anwendungsfällen relevant sind.

8.1 Nutzung in öffentlichen oder fremdadministrierten Netzwerken

Mit Ausnahme von XING ist keine der getesten Plattformen dazu geeignet, in einem öffentlichen drahtlosen Netzwerk (sogenannter Hotspot) in Intercafés, Bahnhöfen oder anderen Einrichtungen genutzt zu werden. Angreifer können leicht den Datenverkehr im Klartext mitlesen und sich in die laufende Nutzersitzung »einklinken«.

Bei den Plattformen myspace, wer-kennt-wen und lokalisten ist sogar das Nutzerkennwort gefährdet, da es unverschlüsselt übertragen wird. Wird dieses Kennwort auch für andere Dienste verwendet (z. B. für das E-Mail-Postfach) entsteht ein noch größeres Gefährdungspotential.

Problematisch kann auch die Nutzung in einem fremdadministrierten Netzwerk, wie z. B. am Arbeitsplatz in einer Firma sein.

Von der Nutzung in privaten, unverschlüsselten Drahtlosnetzwerken wird generell abgeraten.

8.2 Trennung von Geschäftlichem und Privatem

Geschäftlich genutzte Plattformen wie XING oder LinkedIn sind »offener« konzipiert als die für den Privatgebrauch. Es ist häufig Teil der Plattformphilosophie, dass Daten hier zur Präsentation der eigenen Person vollständig für alle anderen Plattformmitglieder zur Verfügung stehen. Entsprechend sind weniger Schutzmechanismen vorhanden um die Sichtbarkeit von Daten einzuschränken.

Dieser Umstand stellt die Nutzung dieser Plattformen nicht prinzipiell infrage. Es empfiehlt sich aber, bei der Profilerzeugung private Angaben außen vor zu lassen, auch wenn sie zunächst banal erscheinen. Beispielsweise kann allein die Angabe einer bestimmten Sportart (z. B. Motorsport) erhöhte gesundheitliche

Risiken implizieren, von den Problemen mit politischen oder weltanschaulich-religiösen Themen ganz abgesehen. Diese Hinweise gelten auch für die weitere Plattformnutzung, z. B. hinsichtlich der Diskussion von Privatem in Foren oder ähnlichem. Für solche Zwecke wird empfohlen eine andere Plattform zu nutzen.

Es ist außerdem sinnvoll, bei dem Erzeugen des Profils die Interessen des Arbeitgebers mit zu berücksichtigen. So können bestimmte Tätigkeitsfelder innerhalb der Firma Betriebsgeheimnisse sein und haben demzufolge nichts in öffentlichen Datenspeichern zu suchen.

8.3 Depseudonymisierung von E-Mail-Adressen

Die Plattformen myspace, facebook und lokalisten erlauben die Suche eines Nutzers anhand der E-Mail-Adresse. Der Nutzer sollte hier berücksichtigen, dass diese Funktion E-Mail-Adressen depseudonymisieren kann: Verwendet man z. B. in einem politischen Forum ein Pseudonym `Hase123` mit der E-Mail-Adresse `hase123@emailprovider.de`, dann sollte man diese Adresse nicht bei facebook oder myspace angeben. Andernfalls kann ein Angreifer mit der jeweiligen Plattformsuche leicht herausfinden, welche Person sich hinter der E-Mail-Adresse `hase123@emailprovider.de` verbirgt.

8.4 Nach der Neuanmeldung

Mit Ausnahme von facebook, war bei allen Plattformen im Test die Standardkonfiguration für den Schutz privater Daten völlig ungeeignet. Deshalb sollte der Nutzer nach der Neuanmeldung unbedingt die Privatsphäre-Einstellungen anpassen. Erschwert wird dieses Unterfangen dadurch, dass die entsprechenden Optionen teilweise über die Plattformen verteilt sind, wie z. B. bei myspace. Es ist sinnvoll, nicht nur unter »Privatsphäre« nachzuschauen, sondern auch unter anderen Menüpunkten.

Um ganz sicher zu gehen, kann man auch andere, bekannte Plattformnutzer fragen, wieviel sie aus dem eigenen Nutzerprofil sehen können. Das kann unangenehme Überraschungen vermeiden.

8.5 Dateneingabe und Privatsphärenschutz

Grundsätzlich gilt: *Erst Zugriffskontrollen konfigurieren, dann Daten eingeben.* Der umgekehrte Weg führt häufig dazu, dass man beim Eingeben zwar schnell, beim Konfigurieren aber dann doch weniger konsequent ist.

Nutzer die sich privatsphärenbewusst verhalten, gehen zudem immer von den niedrigsten erforderlichen Privilegien aus. Wenn z. B. nur die Freunde wissen

sollen, dass man katholisch ist, dann sollte eben nur dieser Personenkreis diese Daten sehen.

Bietet eine Plattform für bestimmte Daten keinen Schutz, dann sollte der Anwender kritisch abwägen, ob die Angabe wirklich soviel Nutzen bringt und wie privatsphärenrelevant sie ist. Das ist in der Praxis nicht immer einfach. Im Zweifelsfall kann deshalb Verzicht die bessere Wahl sein.

8.6 Soziale Rollen und Soziale-Netzwerke-Plattformen

In unterschiedlichen sozialen Rollen sind unterschiedliche Daten relevant oder implizieren gar jeweils andere Informationen: Mögen es die Kommilitonen zwar »cool« finden, wenn man in seinem Profil angibt »Ich schlafe in jeder Mathevorlesung«, so machen sich vielleicht die Eltern des Studenten Sorgen, ob ihre Studienbeihilfe richtig investiert ist. Andererseits muss der (zukünftige) Chef nicht unbedingt wissen, in welchen Nachtclubs ein Profilinhaber seine Wochenendnächte verbringt.

Problematisch ist an dieser Stelle, dass aktuelle Soziale-Netzwerke-Plattformen weitestgehend nur zur Abbildung *einer* sozialen Rolle geeignet sind, also z. B. »Student«, »Sohn/Tochter«, »Arbeitskollege«, »Familienvater/-mutter« oder »ehemaliger Schulfreund«.

Eine Nutzung mit verschiedenen sozialen Rollen ist grundsätzlich immer möglich. Man sollte aber beachten, dass entstehende Vermischungen im Nachhinein schwer zu entflechten sind und die Plattform für einen Nutzer deshalb an Wert verlieren kann.

Ein Beispiel: Man möchte auf einer Plattform Fotos des letzten Urlaubs verbreiten. Man will aber nicht, dass die eigenen Arbeitskollegen diese sehen können. Wenn man allerdings einige Arbeitskollegen neben z. B. Kommilitonen, Vereinsfreunden und Schulfreunden bereits als Kontakte ersten Grades zum Profil hinzugefügt hat, dann wird es bei den getesteten Plattformen schwierig, speziell für ein Fotoalbum diesen Personenkreis im Nachhinein wieder einzuschränken. Vielleicht kann man dieses Problem jetzt nur lösen, indem man für die Urlaubsfotos einen anderen Dienst nutzt oder eben doch hinnimmt, dass einige Arbeitskollegen die Fotos sehen.

Ähnliches gilt für die Trennung zwischen Privatem und Geschäftlichem wie in 8.2 beschrieben.

Prinzipiell ist es für den Nutzer ratsam, sich selbst bei der Verwendung *einer* Plattform auf möglichst *eine* Rolle zu beschränken und diese vorher selbst zu definieren (also z. B. »Student«). Für eine andere Rolle kann eine andere Plattform genutzt werden. Alternativ kann ein weiteres Profil mit anderem Pseudonym bei derselben Plattform angelegt werden, wenn dies möglich und vom Betreiber erlaubt ist. Bei der Beschränkung auf eine Rolle, sollten dann ausschließlich die für diese Rolle gewünschten Daten eingegeben werden. Zugriff

auf die Daten erhalten nur die mit dieser Rolle unmittelbar verbundenen Personen (z. B. ausschließlich Kommilitonen bei der Rolle »Student«).

Der strikte Einsatz von Zugriffskontrollen ist zusätzlich immer erforderlich. Andernfalls verhindert die beschriebene Vorgehensweise nicht, dass Daten über mehrere Plattformen zu einem gesamten Persönlichkeitsprofil zusammengeführt werden können.

In der Praxis ist diese strikte Trennung nicht immer realisierbar. Es ist trotzdem zweckmäßig, diese Zusammenhänge zumindest zu kennen und sich als Nutzer vorher für die Plattformnutzung bewusst Ziele zu setzen.

8.7 Suchmaschinen und Soziale-Netzwerke-Plattformen

Die Plattformen myspace, facebook, XING und LinkedIn erlauben in der Standardkonfiguration Personen, die nicht Mitglieder der Plattform sind, den Zugriff auf bestimmte Profildaten. Im Fall von XING sind teilweise auch Diskussionsforen betroffen. Die Daten sind dann allein durch Aufruf einer Internetverknüpfung wie z. B. `http://www.soziale.netzwerke.plattform/profil=12345678` abrufbar.

Suchmaschinen können Profile damit auch lesen und indizieren. Zwar kann die Zugriffskontrolle zu einem späteren Zeitpunkt vom Nutzer so angepasst werden, dass dieser öffentliche Zugang nicht mehr möglich ist. Allerdings können Daten trotzdem noch eine gewisse Zeit im Zwischenspeicher von Suchmaschinen verbleiben. Ein Abruf von beliebigen Personen ist dann weiterhin möglich. Allerdings können die Daten mittlerweile veraltet sein, was je nach Szenario gut oder schlecht sein kann.

Aus diesen Gründen sollte man gänzlich darauf verzichten, jegliche private Daten frei im Internet zu veröffentlichen. Erlaubt eine Soziale-Netzwerke-Plattform solche Freigaben, so sollten diese direkt nach dem Anlegen des Nutzerkontos deaktiviert werden.

8.8 Hinweise für ausgewählte Plattformen

facebook

Die Plattform facebook ist intern in separate Netzwerke organisiert. Einigen dieser Netzwerke können beliebige Personen ohne eine vorherige Prüfung beitreten. Bei anderen Netzwerken, z. B. bestimmten Firmen-, oder Hochschulnetzwerken ist zum Beitritt eine E-Mail-Adresse an der jeweiligen Institution erforderlich.

Will man Daten für Mitglieder eines Netzwerkes freigeben (z. B. jeder im Netzwerk »TU Darmstadt« darf die persönlichen Hobbys lesen), dann sollte man das

nur für die Netzwerke tun, die eine oben beschriebene Prüfung mithilfe der E-Mail-Adresse nutzen. Andernfalls kann ein Angreifer leicht dem Netzwerk selbst beitreten. (Die Anzeige der Netzwerkzughörigkeit kann nicht unterdrückt werden.)

Die Zugriffskontrollen für die Anzeige der Gruppen und Fotoalben befindet sich separat unter »Privatsphäre«, Menüpunkt »Anwendungen«, Link »Seite 'Anwendungen bearbeiten'«.

Soll der Zugriff auf die Kontaktliste eingeschränkt werden, dann ist auch die Option »Wie kannst du kontaktiert werden? - Deine Freundesliste anzeigen« unter Menüpünkt »Suche« zu deaktivieren.

studiVZ

Der Nutzer sollte den Zugriff auf Fotoalben für jedes Album immer separat mithilfe der Funktion »Albuminfo bearbeiten« einschränken. Die Funktion »Was ist auf meinem eingeschränkten Profil zu sehen?« leistet für (alle) Fotoalben nicht den selben Zugriffsschutz. Ohne individuelle Konfiguration für jedes Fotoalbum ist es z.B. weiterhin möglich, dass unerwünschte Personen Fotos über Fotoverknüpfungen in bestimmten Situationen auslesen können.

Desweiteren verhindert bei studiVZ das Aktivieren des »eingeschränkten Profils« nicht, dass über geschickte Nutzung der Suchfunktion bestimmte, geschützte Daten wie z. B. die politische Orientierung oder der Beziehungsstatus aufgedeckt werden können. Im Zweifelsfall ist es besser die sogenannte »Supersuche« für das eigene Profil auszuschalten.

Ebenfalls ist es nicht sinnvoll für das »eingeschränkte Profil« die Personengruppe »Alle Leute an meiner Hochschule, meine Freunde und deren Freunde« einzustellen. Ein Angreifer kann leicht in studiVZ einer Hochschule »beitreten«.

Weitere Hinweise zur Nutzung von studiVZ und schülerVZ finden sich unter anderem in einer Informationsbroschüre der Organisation ServiceBureau Jugendinformationen, Bremen [36].

lokalisten

Die Zugriffskontrolle von lokalisten wurde im Test für mangelhaft befunden. Privatsphärenbewusste Anwender können die Plattform deshalb nur sehr eingeschränkt nutzen. Von der Eingabe privatsphärenrelevanter Daten wird abgeraten.

XING

Bei der Nutzung von XING bietet es sich an, in irgendeiner Form eine Liste über andere XING-Nutzer zu führen, denen man Zugriff auf die eigenen Kontaktdaten gewährt hat. Verändert sich z. B. die berufliche Situation, dann benötigen vielleicht einige dieser Nutzer die Kontaktdaten nichtmehr. Die Liste ist dann

hilfreich, um Nutzer zu identifizieren, denen man die Autorisierung entziehen möchte.

Um Mitglieder zu markieren, für die Kontaktdaten freigegeben wurden, kann der Nutzer die XING-eigene »Tagging«-Funktion verwenden. Diese findet sich im »Adressbuch« bei denen einzelnen Kontakten im Textfeld »Persönliche Tags«.

Beim regulären Abmelden von XING werden Foren- und Gästebucheinträge nicht gelöscht oder anonymisiert. Es ist dennoch möglich auch diese Daten löschen zu lassen. Dazu wendet man sich mit einer entsprechenden Bitte an den Kundendienst.

8.9 Zusammenfassung

Die wichtigsten Regeln aus den vorhergehenden Abschnitten sind in folgender Liste kurz zusammengefasst:

❶ Keine Nutzung in öffentlichen WLAN-Netzen oder fremdadministrierten Netzwerken (z. B. in Firmen). Von dieser Einschränkung ist XING ausgenommen.

❷ In Geschäftsplattformen keinerlei Daten aus dem Privatleben hinterlegen; Dienste nicht zum »Privatvergnügen« nutzen. Bei der Eingabe von Geschäftsdaten vom Arbeitgeber auferlegte Geheimhaltungspflichten beachten.

❸ Für die Plattformen keine E-Mail-Adressen nutzen, die in anderen Kontexten als Pseudonym verwendet werden (z. B. in einem politischem Forum).

❹ Unmittelbar nach der Neuanmeldung an einer Plattform die Privatsphäre-Optionen restriktiv einstellen.

❺ Freigabe jeglicher Daten im Internet (sogenanntes »öffentliches Profil«) unmittelbar nach der Anmeldung deaktivieren (betrifft myspace, facebook, XING und LinkedIn).

❻ Vor der Eingabe neuer privater Daten zunächst immer die Zugriffskontrollen prüfen und gegebenenfalls anpassen. Ist keine Zugriffskontrolle vorhanden unter Umständen auf die Eingabe verzichten.

❼ Für *eine* Plattform genau *eine* Rolle festlegen, z. B. »Student« oder »Angestellter bei Firma XY«. Nur die für diese Rolle benötigten Daten eingeben. Zugriff auf diese Daten nur gegenüber den Personen freigeben, die mit dieser Rolle verknüpft sind, also z. B. für Kommilitonen oder Arbeitskollegen. Für weitere Rollen andere Plattform wählen oder wenn möglich weiteres Nutzerkonto anlegen.

❽ Plattformspezifische Hinweise:

- **facebook**: Private Daten nur für Netzwerke mit beschränktem Zugang (z. B. Authentifizierung per E-Mail-Adresse bei Hochschulnetzwerken) freigeben. Sichtbarkeit von Gruppen und Fotoalben wird über die »Privatsphäre« - »Anwendungen« eingeschränkt; für die Kontaktliste ist ein Deaktivieren von »Wie kannst du kontaktiert werden? - Deine Freundesliste anzeigen« unter »Suche« notwendig.
- **studiVZ**: Zugriffsschutz für jedes Fotoalbum immer separat konfigurieren. »Super-Suche« abschalten. Daten nicht für »Alle Leute meiner Hochschule« freigeben.
- **lokalisten**: Private Daten nur so weit dringend notwendig eingeben.
- **XING**: Liste über Nutzer führen (z.B. mit »Tagging«-Funktion), für die Kontaktinformationen freigegeben wurden. Bei Änderung der beruflichen Situation, z.B. Wechsel zu einer neuen Firma, anhand der Liste Zugriff wieder einschränken. Löschen von Foren- und Gästebucheinträgen nach dem Abmelden über Kundendienst möglich.

9 Fazit

Hinsichtlich des Privatsphärenschutzes konnte keiner der getesteten Dienste überzeugen. Viele Plattformen sind nur in einigen wenigen Punkten gut oder zeigen nur teilweise gute Ansätze.

Die meisten guten Bewertungen erhielt facebook. Insbesondere die Zugriffskontrolle, welche ein wichtiges Mittel für den Privatsphärenschutz ist, verfügt bei facebook über umfangreiche Funktionen und Konfigurationsmöglichkeiten. Bei facebook kann der Nutzer deshalb viele Daten gegenüber anderen Plattformmitgliedern schützen, insbesondere auch privatsphärenrelevante. Dennoch ist facebook, wie die anderen Plattformen auch, mit zahlreichen Mängeln behaftet.

Das Mittelfeld bei den privaten Plattformen bilden myspace, studiVZ und wer-kennt-wen, die unterschiedliche Schwächen bei verschiedenen Testkriterien zeigen. So bieten beispielsweise myspace und studiVZ gegenüber wer-kennt-wen die besseren Konfigurationsmöglichkeiten für die Zugriffskontrolle. Allerdings wirkt bei beiden Plattformen eben genau diese Zugriffskontrolle nicht vollständig auf die Suchfunktion. Dadurch wird der erreichte Schutz teilweise konterkariert, da ein Angreifer private Daten dennoch unberechtigt auslesen kann. Dieses Problem weist wer-kennt-wen nicht auf, wenngleich diese Plattform nicht so ausgefeilte Zugriffskontrollen wie die anderen beiden bereitstellt.

Den schlechtesten Eindruck bei den Privatplattformen machten die lokalisten. Der Internetdienst zeigte die meisten Defizite, welche für den privatsphärenbewussten Nutzer erhebliche Nachteile bezüglich der Plattformnutzung implizieren. Besonders schwerwiegend sind die weitestgehend fehlenden Zugriffskontrollen.

Die Gestaltung von Schutzmaßnahmen für die Privatsphäre ist bei den beiden Geschäftsplattformen XING und LinkedIn ähnlich. Im Detailvergleich schneidet aber LinkedIn besser ab. Das liegt an mehreren Faktoren:

Nutzer können ihre Mitgliedschaft bei LinkedIn leichter aufgeben als bei XING. Außerdem werden die Anwenderdaten dann gründlicher aus der Plattform gelöscht als beim Konkurrenten. Ebenso bietet nur LinkedIn eine einfache Pseudonymisierungsfunktion, die auch auf die Suche innerhalb der Plattform wirkt. Damit wird dem Anwender ein einfaches aber wirksames Mittel gegeben, seinen Klartextnamen und die Auffindbarkeit in der Plattform zu unterdrücken.

Zusätzlich kann bei LinkedIn die Anzeige im Zugriffsprotokoll anderer Nutzer dreistufig eingeschränkt werden. Auf Wunsch wird dann anstatt des vollen Nutzernamens nur das Geschäftsfeld und die Position angezeigt.

Nur die Verschlüsselung der Datenkommunikation zwischen dem Webbrowser des Nutzers und dem Dienst war bei XING besser. XING war im Übrigen auch der einzige Dienst im Test, der vollständig verschlüsselte. Bei drei getesteten Plattformen war überhaupt kein kryptografischer Schutz vorhanden.

Insgesamt ergibt sich eine lange Liste typischer Mängel, die bei den getesteten Plattformen teilweise vorgefunden wurden:

- zu umfangreiche Pflichtdaten bei der Anmeldung
- kein Unterstützen von Pseudonymen
- fehlendes oder unzureichendes Verschlüsseln des Kommunikationskanals zum Plattform-Server
- konzeptionell nicht gewollter Schutz bestimmter privatsphärenrelevanter Daten
- Fehlen von Mechanismen, die den Zugriff auf Datenobjekte gemäß den vom Nutzer gesetzten Regeln erlauben oder verweigern (z.B. für die Suchfunktion oder Fotoverknüpfungen)
- Abruf vertraulicher Multimediadaten außerhalb der Plattform
- schwer auffindbare Abmeldefunktionen oder umständlicher Abmeldeprozess
- unvollständiges Löschen privater Daten nach dem Abmelden an der Plattform
- eigenwilliges Konzept für die Nutzerführung oder Inkonsistenzen bei den Privatsphäre-Optionen

Tabelle 9.1 liefert abschließend einen Gesamtüberblick über die wichtigsten Eigenschaften der getesteten Plattformen.

Zusammenfassend lässt sich feststellen, dass die Prüfung ein sehr ambivalentes Bild über die konzeptionelle und technische Ausgestaltung der Plattformen liefert. Einzelne Schwächen der einen Plattform decken sich vielfach genau mit den einzelnen Stärken einer anderen. Gesamtheitliche, konsistente und klare Konzepte zum Privatsphärenschutz sind deshalb häufig nur begrenzt auszumachen. Würde man die einzelnen guten Ansätze der geprüften Plattformen weiterführen und in einem einzigen Konzept vereinen, hätte man mit wenigen Einschränkungen die Idealplattform im Sinne dieser Studie.

Plattform	Pro	Contra
myspace	⊕ Unterstützung von Pseudonymen ⊕ einfaches Abmelden; umfassendes Löschen der Nutzerdaten	⊖ eigenwillige Nutzerführung
facebook	⊕ Zugriffskontrolle vielseitig konfigurierbar ⊕ Zugriffskontrolle wirkt auf Suchfunktion und Fotoverknüpfungen, gute Zugriffsautorisierung	⊖ umständliches Abmelden
studiVZ	⊕ einfaches Abmelden	⊖ Aushebeln von Teilen der Zugriffskontrolle über die Suchfunktion
wer-kennt-wen	⊕ wenig Daten zur Anmeldung erforderlich ⊕ einfaches Abmelden ⊕ übersichtliche Konfiguration der Zugriffskontrollen	⊖ Zugriffskontrolle schützt nicht die Anzeige der eigenen Kontakte und der Gruppenzugehörigkeit
lokalisten	⊕ Unterstützung von Pseudonymen ⊕ umfangreiches Löschen der Nutzerdaten nach Abmelden	⊖ mangelhafte Zugriffskontrolle ⊖ Abmelden nur per E-Mail möglich ⊖ Suchfunktion sehr umfangreich bei wenigen Schutzmechanismen für den Nutzer
XING	⊕ Nutzersitzung komplett verschlüsselt	⊖ Foren- und Gästebucheinträge werden nach regulärem Abmelden weder gelöscht noch anonymisiert ⊖ Zugriffskontrolle schließt nur wenige Daten ein ⊖ Suchfunktion sehr umfangreich bei wenigen Schutzmechanismen für den Nutzer
LinkedIn	⊕ Unterstützung von Pseudonymen ⊕ guter Ansatz für das Protokollieren von Profilzugriffen durch schrittweises Einschränken der Daten des Protokollierten ⊕ einfaches Abmelden	⊖ Zugriffskontrolle schließt nur wenige Daten ein

Tabelle 9.1: Zusammenfassung der wichtigsten Plattformeigenschaften

Literaturverzeichnis

[1] *About LinkedIn*. http://www.linkedin.com/static?key=company_info&trk=hb_ft_abtli, letzter Zugriff 07. April 2008. 63

[2] *Alexa Top 100 Sites Germany*. http://www.alexa.com/site/ds/top_sites?cc=DE&ts_mode=country&lang=none, letzter Zugriff 18. Juli 2008. 59

[3] *Anlage zu §9 Satz 1 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970)*. 25

[4] *Artikel 8 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*. 16

[5] *Facebook Factsheet*. http://www.facebook.com/press/info.php?factsheet, letzter Zugriff 07. April 2008. 60

[6] *Fakten zu wer-kennt-wen.de*. http://static.wer-kennt-wen.de/presse/wkw_fakten.pdf, letzter Zugriff 07. April 2008. 61

[7] *heise Security - Zugriff auf gesperrte StudiVZ-Fotoalben möglich*. http://www.heise.de/security/Zugriff-auf-gesperrte-StudiVZ-Fotoalben-moeglich-Update--/news/meldung/114974, letzter Zugriff 27. August 2008. 87

[8] *lokalisten.de - Pressemitteilung: ProSiebenSat1 stockt Anteile des Freundesnetzwerks www.lokalisten.de auf*. http://images.lokalisten.de/press/01-06-08-mehrheitsbeteiligung.pdf, letzter Zugriff 26. Juni 2008. 62

[9] *lokalisten.de: Allgemeines*. http://www.lokalisten.de/press/open/showPress.do, letzter Zugriff 07. April 2008. 62

[10] *lokalisten.de in Zahlen*. http://www.lokalisten.de/press/showPress.do?method=facts&nf=1, letzter Zugriff 07. April 2008. 62

[11] *Polar Rose*. http://www.polarrose.com/, letzter Zugriff 07. April 2008. 34

[12] *Pressemitteilung - RTL interactive und wer-kennt-wen.de gehen Partnerschaft ein*. http://static.wer-kennt-wen.de/presse/wkw_presseinfo_2008_02.pdf, letzter Zugriff 07. April 2008. 61

[13] *Pressemitteilung - studiVZ und schülerVZ behaupten ihre Doppelführung im IVW-Ranking*. http://www.studivz.net/l/press/28, letzter Zugriff 07. April 2008. 61

[14] *§3 Absatz 9 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970)*. 16

[15] *SPIEGEL ONLINE - Auch MySpace öffnet sich*. http://www.spiegel.de/netzwelt/web/0,1518,512164,00.html, letzter Zugriff 07. April 2008. 59

[16] *SPIEGEL ONLINE - »OpenBC hat den Weg für uns bereitet«*. http://www.spiegel.de/wirtschaft/0,1518,453066,00.html, letzter Zugriff 07. April 2008. 63

[17] *SPIEGEL ONLINE - »Regionale Netzwerke sind unpraktisch« - Interview mit facebook-Manager Javier Olivan*. http://www.spiegel.de/netzwelt/web/0,1518,538718,00.html, letzter Zugriff 07. April 2008. 60

[18] *studiVZ - Allgemeine Geschäftsbedingungen*. http://www.studivz.net/l/terms, letzter Zugriff 07. Mai 2008. 88

[19] *studiVZ - Über uns*. http://www.studivz.net/l/press/, letzter Zugriff 07. April 2008. 61

[20] *wer-kennt-wen.de: Wer sind wir?* http://www.wer-kennt-wen.de/wer_sind_wir.html, letzter Zugriff 07. April 2008. 61

[21] *XING AG - Annual Report 2007*. http://corporate.xing.com/fileadmin/image_archive/XING_AG_full_year_results_results_2007.pdf, letzter Zugriff 07. April 2008. 62

[22] *XING Corporate Information - Fakten und Zahlen*. http://corporate.xing.com/german/investor-relations/basic-information/facts-figures/, letzter Zugriff 07. Juni 2008. 62

[23] *XING Corporate Information - Über uns*. http://corporate.xing.com/german/company/about-us/, letzter Zugriff 07. Juni 2008. 62

[24] *Wirtschaftsspionage in Baden-Württemberg und Bayern - Daten-Fakten-Hintergründe*. Landesamt für Verfassungsschutz Baden-Württemberg und Bayerisches Landesamt für Verfassungsschutz, 2006. 67

[25] *Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten - »Rom Memorandum«*. Verabschiedet auf der 43. Sitzung der International Working Group on Data Protection in Telecommunications, 3.-4. März 2008 in Rom (Italien), März 2008. http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf,letzter Zugriff 26. Juni 2008. 26

[26] *BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. 77 ff., Automatisierte Kennzeichenerfassung*, März 2008. http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html, letzter Zugriff 26. Mai 2008. 16

[27] *Internet-Affäre: »Nach Frankreich fahr ich nur auf Ketten«*. ZEIT online, Mai 2008. http://www.zeit.de/news/artikel/2008/05/26/2538091.xml, letzter Zugriff 26. Mai 2008. 90

[28] Bielefeldt, Heiner: *»Ich habe nichts zu verbergen« - ein gedankenloser Spruch*. Datenschutz Nachrichten, 31(1):8–10, 2008. 15

[29] Birk, Dominik, Felix Gröbert und Christoph Wegener: *Social Hacking - Wie Web 2.0 den automatisierten Missbrauch ermöglicht*. iX - Magazin für professionelle Informationstechnik, (9):44–52, August 2008. 67

[30] DiMicco, Joan Morris und David R. Millen: *Identity management: multiple presentations of self in facebook*. In: *GROUP '07: Proceedings of the 2007 international ACM conference on Supporting group work*, Seiten 383–386, New York, NY, USA, 2007. ACM. 13

[31] Düsseldorfer Kreis (Oberste Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich): *Beschluss: Datenschutzkonforme Gestaltung sozialer Netzwerke*, April 2008. http://www.bfdi.bund.de/cln_027/nn_531946/DE/Oeffentlichkeitsarbeit/Entschliessungssammlung/DuesseldorferKreis/170408DatenschutzkonformeGestaltungSozNetzwerke,property=publicationFile.pdf, letzter Zugriff 10. Mai 2008. 26

[32] Gross, Ralph, Alessandro Acquisti und John H. Heinz: *Information revelation and privacy in online social networks*. In: *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, Seiten 71–80, New York, NY, USA, 2005. ACM Press. 14

[33] Hansen, Marit und Sebastian Meissner (Herausgeber): *Verkettung digitaler Identitäten*. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2007. Forschungsbericht im Auftrag und unter Förderung des Bundesministeriums für Bildung und Forschung. 16

[34] Jones, Harvey und José Hiram Soltren: *Facebook: Threats to Privacy*. Technischer Bericht, Massachusetts Institute of Technology, Dezember 2005. 13

[35] Schmidt, Jan: *Social Software: Onlinegestütztes Informations-, Identitäts- und Beziehungsmanagement*. In: *Forschungsjournal Neue Soziale Bewegungen*, Nummer 2/2006, Seiten 37–47. Lucius & Lucius Verlagsgesellschaft mbH, 2006. 9

[36] Siggelkow, Tanja: *Wofür werden noch Spione gebraucht, wenn es doch das Schüler- und StudiVZ gibt? – Big Brother is watching you!* ServiceBureau Int. Jugendkontakte Bremen, 2007. http://jugendinfo.de/toleranz/admin/attachviewer.php?typ=Thema&dateiorig=SchuelerVZ.pdf&dateiverzeichnis=35833&dateiname=1be6654909ad594560a85878046d84f2, letzter Zugriff 10. Juni 2008. 113

[37] Solove, Daniel J.: *»I've Got Nothing to Hide« and Other Misunderstandings of Privacy*. San Diego Law Review, 44, 2007. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565. 15

[38] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *Kommentare und Hinweise zum ULD-Anforderungskatalog*, 2003. https://www.datenschutzzentrum.de/download/hinwanf.pdf, letzter Zugriff 10. Mai 2008. 25

[39] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH*, 2005. https://www.datenschutzzentrum.de/download/anford.pdf, letzter Zugriff 10. Mai 2008. 25

Ansprechpartner

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
D-64295 Darmstadt

Tel.: +49 (0)6151-869-0
Fax: +49 (0)6151-869-224

http://www.sit.fraunhofer.de
http://testlab.sit.fraunhofer.de

Planung und Durchführung dieser Studie

Andreas Poller
Tel.: +49 (0)6151-869-60048
andreas.poller@sit.fraunhofer.de

Forschungsbereich „Sichere Prozesse und Infrastrukturen“

Dr. Thorsten Henkel
Tel.: +49 (0)6151-869-4271
thorsten.henkel@sit.fraunhofer.de

Presse- und Öffentlichkeitsarbeit

Oliver Küch
Tel.: +49 (0)6151-869-213
oliver.kuech@sit.fraunhofer.de

Stand dieser Studie: Ende August 2008

Grafiken erzeugt mit Inkscape und Open Clip Art Library.
Gesetzt mit LaTeX.