

**SIT TECHNICAL REPORTS**

**SOZIALE NETZWERKE BEWUSST NUTZEN**

**EIN DOSSIER ZU DATENSCHUTZ, PRIVATSPHÄRENSCHUTZ  
UND UNTERNEHMENS SICHERHEIT**

08/2013



## **Soziale Netzwerke bewusst nutzen**

**Ein Dossier zu Datenschutz, Privatsphärenschutz und Unternehmenssicherheit**

Andreas Poller und Ulrich Waldmann

Hrsg. Michael Waidner

SIT Technical Reports  
SIT-TR-2013-02

August 2013

Fraunhofer-Institut für Sichere  
Informationstechnologie SIT  
Rheinstraße 75  
64295 Darmstadt

Dieser Bericht wurde gefördert vom  
Hessischen Ministerium des Innern und für Sport.



FRAUNHOFER VERLAG

## IMPRESSUM

### **Kontaktadresse:**

Fraunhofer-Institut für  
Sichere Informationstechnologie SIT  
Rheinstraße 75  
64295 Darmstadt  
Telefon 06151 869-213  
Telefax 06151 869-224  
E-Mail [info@sit.fraunhofer.de](mailto:info@sit.fraunhofer.de)  
URL [www.sit.fraunhofer.de](http://www.sit.fraunhofer.de)

### **Bibliografische Information der Deutschen Nationalbibliothek**

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Hrsg. Michael Waidner  
SIT Technical Reports  
Soziale Netzwerke bewusst nutzen  
Ein Dossier zu Datenschutz, Privatsphärenschutz und Unternehmenssicherheit  
SIT-TR-2013-02  
Andreas Poller und Ulrich Waldmann  
ISBN 978-3-8396-0595-0  
ISSN 2192-8169

Druck und Weiterverarbeitung:  
IRB Mediendienstleistungen  
Fraunhofer-Informationszentrum Raum und Bau IRB, Stuttgart

Für den Druck des Buches wurde chlor- und säurefreies Papier verwendet.

© by **FRAUNHOFER VERLAG**, 2013  
Fraunhofer-Informationszentrum Raum und Bau IRB  
Postfach 800469, 70504 Stuttgart  
Nobelstraße 12, 70569 Stuttgart  
Telefon 0711 970-2500  
Telefax 0711 970-2508  
E-Mail [verlag@fraunhofer.de](mailto:verlag@fraunhofer.de)  
URL <http://verlag.fraunhofer.de>

Alle Rechte vorbehalten  
Copyright Titelbild: Sergey Nivens/fotolia.com

Dieses Werk ist einschließlich aller seiner Teile urheberrechtlich geschützt. Jede Verwertung, die über die engen Grenzen des Urheberrechtsgesetzes hinausgeht, ist ohne schriftliche Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen sowie die Speicherung in elektronischen Systemen. Die Wiedergabe von Warenbezeichnungen und Handelsnamen in diesem Buch berechtigt nicht zu der Annahme, dass solche Bezeichnungen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und deshalb von jedermann benutzt werden dürften. Soweit in diesem Werk direkt oder indirekt auf Gesetze, Vorschriften oder Richtlinien (z.B. DIN, VDI) Bezug genommen oder aus ihnen zitiert worden ist, kann der Verlag keine Gewähr für Richtigkeit, Vollständigkeit oder Aktualität übernehmen.

# Soziale Netzwerke bewusst nutzen

Ein Dossier zu Datenschutz, Privatsphärenschutz und Unternehmenssicherheit

---

Soziale Netzwerke wie Facebook, Google+ oder LinkedIn interessieren eine immer größere Anzahl von Nutzern, zunehmend auch Personenkreise, welche eher zurückhaltend neue Technologie adaptieren. Auch Unternehmen und Institutionen nutzen soziale Netzwerke mehr und mehr für ihre Zwecke wie Personalanwerbung, Marketing und interne Unternehmenskommunikation. Neben dem positiven Nutzen, den die Anwender aus diesen Softwareangeboten ziehen, treten immer häufiger auch Nachteile der Dienste in den Vordergrund und werden in Medien, Wissenschaft und Politik kritisch diskutiert.

Dieses Dossier dokumentiert und kategorisiert aus öffentlich verfügbaren Quellen Szenarien, in denen Nutzer von sozialen Netzwerken oder Unternehmen, welche diese Dienste selbst oder über ihre Mitarbeiter nutzen, Opfer von Angriffen auf die Privatsphäre oder IT-Sicherheit werden können. Das Dossier ist entlang der vier Hauptkategorien "Gestaltungsspielräume zwischen Nutzer und Dienstanbieter", "Gestaltungsspielräume zwischen privaten Nutzern", "Nutzer als Ziel professioneller Angriffe" und "Auswirkungen auf die Unternehmenssicherheit" strukturiert und gibt zu jedem Abschnitt Empfehlungen für private Nutzer und Unternehmen. Ergänzt wird diese Sammlung durch Aufarbeitungen ausgewählter wissenschaftlicher Arbeiten zu den jeweiligen Befunden.

Key Words: Soziale Netzwerke, Datenschutz, Privatsphäre, Identitätsfälschung, Identitätsdiebstahl, Facebook

---

## **Hinweis der Autoren**

Die in dieser Studie enthaltenen Informationen wurden mit großer Sorgfalt erstellt. Eine Haftung und Garantie für die Aktualität, Richtigkeit und Vollständigkeit der zur Verfügung gestellten Informationen kann jedoch nicht übernommen werden.



## INHALTSVERZEICHNIS

<b>Zusammenfassung für den eiligen Leser</b>	<b>7</b>
Die Dienstbetreiber der Netzwerke: Segen und Risiko zugleich . . . . .	7
Privatsphärenschutz zwischen Nutzern . . . . .	8
Professionelle Angreifer und sonstige Risiken . . . . .	9
Aspekte der Unternehmenssicherheit . . . . .	10
<b>1 Hinweise für den Leser</b>	<b>11</b>
<b>2 Gestaltungsspielräume zwischen Nutzer und Dienstanbieter</b>	<b>13</b>
2.1 Zum Umgang mit dem Datenschutz . . . . .	13
2.1.1 Unrechtmäßige Datensammlung . . . . .	13
2.1.2 Mögliche Auswirkungen der Datensammlung . . . . .	17
2.2 Nutzungsrechte und Datenschutzbestimmungen . . . . .	17
2.2.1 Nutzungsrechte von Facebook . . . . .	18
2.2.2 Unklare Datenschutzbestimmungen . . . . .	18
2.3 Zusatzprogramme zu Werbe- und Marketingzwecken . . . . .	19
2.3.1 Facebook “Like”-Button . . . . .	20
2.3.2 Mögliche Auswirkungen der Social-Plugins . . . . .	21
2.4 Integrierte Drittanbieter-Anwendungen . . . . .	22
2.4.1 Mögliche Auswirkungen der App-Zugriffrechte . . . . .	24
2.5 Gesichts- und Bilderkennungsverfahren . . . . .	25
2.5.1 Tagging von Bildern in Facebook . . . . .	26
2.6 Bestimmung des aktuellen Standorts . . . . .	27
<b>3 Gestaltungsspielräume zwischen privaten Nutzern</b>	<b>29</b>
3.1 Ungewollte Veröffentlichungen . . . . .	29
3.1.1 Mangelnde Nutzerfreundlichkeit der sozialen Netzwerke . . . . .	30
3.1.2 Gegenmaßnahme: Beachtung von sozialen Rollen . . . . .	30
3.1.3 Gegenmaßnahme: Schutz der eigenen Privatsphäre . . . . .	31
3.2 Urheberrechte und Impressum . . . . .	31
3.2.1 Veröffentlichung von Fotos oder Abbildungen anderer Personen . . . . .	32
3.2.2 Verwendung von fremden Bildern und Texten . . . . .	32
3.2.3 Verwendung von Zitaten und Links . . . . .	33
3.2.4 Wann ein Impressum notwendig wird . . . . .	33
3.3 Cybermobbing . . . . .	34
<b>4 Nutzer als Ziel professioneller Angriffe</b>	<b>37</b>
4.1 Cross-Site Scripting, Viren und Würmer . . . . .	37
4.1.1 Wie ein Schadprogramm auf einen Heim-PC gelangt . . . . .	38
4.1.2 Gegenmaßnahme 1: Programme auf dem neuesten Stand halten . . . . .	38
4.1.3 Gegenmaßnahme 2: Virenschutz-Programm installieren und auf dem neuesten Stand halten . . . . .	39
4.1.4 Gegenmaßnahme 3: Firewall-Programm installieren und auf dem neuesten Stand halten . . . . .	39
4.1.5 Gegenmaßnahme 4: Auf dem Heim-PC nur mit eingeschränkten Rechten arbeiten . . . . .	40

4.2	Man-in-the-Middle-Attacken . . . . .	40
4.2.1	Warum FITM-Angriffe so erfolgreich sein können . . . . .	41
4.2.2	Gegenmaßnahme: Sichern der Kommunikation mit HTTPS . . . . .	42
4.3	Aggregation und Quervernetzung von Profildaten . . . . .	42
4.4	Hintergrund- und Risikoprüfungen . . . . .	43
4.5	Automatisierter Identitätsdiebstahl . . . . .	44
4.5.1	Wie das Klonen von Identitäten funktioniert . . . . .	44
4.6	Mögliche Gegenmaßnahmen auf Seiten der Betreiber . . . . .	45
4.7	Automatisierte Informationssammlung . . . . .	45
<b>5</b>	<b>Auswirkungen auf die Unternehmenssicherheit</b>	<b>49</b>
5.1	Vorbereitung gezielter Hacker-Angriffe . . . . .	49
5.1.1	Suchmaschinen und Daten in sozialen Netzwerken . . . . .	50
5.2	Gezielte Identitätsfälschung . . . . .	50
5.2.1	Mögliche Auswirkungen gefälschter Identitäten . . . . .	52
5.2.2	Mangelnde Identitätsprüfung auf Seiten der Anbieter . . . . .	52
5.2.3	Klarnamenzwang und pseudonyme Nutzung . . . . .	53
5.3	Rekonstruktion von Unternehmensinterna . . . . .	54
5.3.1	Unerwünschte Informationsabflüsse durch Mitarbeiter . . . . .	54
5.3.2	Gegenmaßnahme: Trennung von Geschäftlichem und Privatem . . . . .	55
5.4	Missbrauch für Marketing oder Bashing . . . . .	56
5.4.1	Mangelnde Strategien bei Unternehmen . . . . .	57
<b>6</b>	<b>Leitfaden für Unternehmen und Mitarbeiter</b>	<b>59</b>
6.1	Erstellung einer Unternehmensrichtlinie . . . . .	59
6.2	Fragen und Antworten für Mitarbeiter und Unternehmen . . . . .	60
<b>7</b>	<b>Plattformspezifische Besonderheiten</b>	<b>69</b>
7.1	Facebook . . . . .	69
7.2	Google+ . . . . .	73
7.3	Twitter . . . . .	75
7.4	XING . . . . .	77
7.5	LinkedIn . . . . .	80
	<b>Danksagung</b>	<b>83</b>
	<b>Literatur</b>	<b>84</b>

## ZUSAMMENFASSUNG FÜR DEN EILIGEN LESER

Soziale Netzwerke wie Facebook, Google+ oder LinkedIn interessieren eine immer größere Anzahl von Nutzern, zunehmend auch Personenkreise, welche eher zurückhaltend neue Technologie adaptieren. Dabei sind die Anwendungsszenarien individuell sehr verschieden und reichen von der Organisation beruflicher Kontakte, über das Teilen privater Informationen wie Fotos und Videos mit Freunden, das Arrangieren von Veranstaltungen, bis hin zum einfachen Chatten auf mobilen Endgeräten wie Smartphones und Tablets.

Eine Technologie wie soziale Netzwerke, welche zunehmend viele Lebensbereiche von Menschen durchdringt, macht auch vor den Türen von Wirtschaftsunternehmen nicht halt: Firmen entdecken diese Internetangebote mehr und mehr für Personalanwerbung, Marketing und interne Unternehmenskommunikation.

Neben dem positiven Nutzen, den die Anwender aus diesen Softwareangeboten ziehen, treten immer häufiger auch Nachteile der Dienste in den Vordergrund und werden in Medien, Wissenschaft und Politik kritisch diskutiert. Dieses Dossier möchte einen Beitrag zu dieser Diskussion liefern, indem es Informationen für verschiedene Spannungsfelder zusammenstellt, kategorisiert und mit Hinweisen für private Nutzer und Unternehmen anreichert.

### Die Dienstbetreiber der Netzwerke: Segen und Risiko zugleich

#### FTC versus Facebook

Viele Nutzer übersehen, dass sie mit dem Hochladen von Daten dem Dienstbetreiber Facebook umfangreiche, teilweise unwiderrufliche Nutzungsrechte für vielfältige Anwendungszwecke einräumen. Dieses Problem findet sich auch bei vielen anderen Diensten. Im Jahr 2009 eröffnete die US-Handelsbehörde (Federal Trade Commission – FTC) gegen Facebook ein Verfahren wegen “möglicher unfairer Verhaltensweisen” gegenüber seinen Nutzern. Im Raum standen beispielsweise Vorwürfe zu irreführenden Privatsphäreinstellungen, unfairen Änderungen dieser Funktionen, und Veröffentlichung von Nutzerfotos und -videos. 2011 schloß die FTC das Verfahren mit einem Vergleich gegen Auflagen ab.

#### Beurteilung

Betreiber sozialer Netzwerke bieten umfangreiche Datenverarbeitungsdienste gebührenfrei an. Um diese Dienste finanzieren zu können, versuchen die Betreiber aber gleichzeitig die Daten ihrer Nutzer gewinnbringend in Dienstleistungen für ihre Geschäftskunden einzusetzen, z. B. für gezielte Werbeschaltungen oder Markt- und Meinungsforschung. Die Betreiber präsentieren ihren Nutzern zudem häufig neue Informationsverknüpfungen und -sammlungen, um das Interesse der Nutzer am Dienst zu stärken, z. B. automatische Gesichtserkennung in Fotos und Funktionen zur Geolokalisierung.

Wenngleich Nutzer eine gebührenfreie Dienstbereitstellung erwarten, bestärkt die Nutzung persönlicher Daten durch den Dienstbetreiber den Eindruck, dass dieser Privatsphärenbedürfnisse der Nutzer missachtet. Dieses Spannungsfeld lässt sich schwer auflösen. Nutzer sollten jedoch prüfen, ob sie optionale, problematische Funktionen deaktivieren können.



### Wir raten Ihnen

- *Verzichten Sie auf pauschale Datenabgleiche*  
Achten Sie darauf, dass Sie nicht versehentlich Daten aus Adressbüchern und anderen E-Mail-Konten zum sozialen Netzwerk übermitteln.
- *Beschränken Sie den Zugriff durch Dritte*  
Prüfen Sie angebotene Konfigurationsmöglichkeiten für personalisierte Werbung.
- *Seien Sie vorsichtig gegenüber Drittanwendungen*  
Schränken Sie die Datenübertragung an die Betreiber zusätzlicher Dienste so weit wie möglich ein. Das betrifft sowohl Ihre Daten als auch die Daten der Personen, mit denen Sie über Facebook in Kontakt stehen.

## Privatsphärenschutz zwischen Nutzern

### Zwischenmenschliche Konflikte

Herabwürdigende, öffentlich sichtbare Äußerungen über den Arbeitgeber in sozialen Netzwerken können ungewollte Folgen haben: So verlor ein Mitarbeiter einer Basketballmannschaft in Pittsburgh seinen Job, nachdem er sich auf Facebook öffentlich negativ über die Leistungen der Spieler geäußert hatte. Aus einer privaten Einladung zu einer privaten Geburtstagsfeier einer Jugendlichen aus Hamburg wurde durch fehlerhafte Privatsphäreinstellungen bei Facebook ungewollt eine öffentliche Veranstaltung. Mehr als tausend Partygäste zogen zum Haus der Eltern des Mädchens, welches von einem Aufgebot an Polizisten vor Randalierern geschützt werden musste.

### Beurteilung

Soziale Netzwerke erweitern die Interaktionsmöglichkeiten zwischen Menschen um neue Formen, die unabhängig von räumlichen und zeitlichen Einschränkungen sind. Insbesondere die Möglichkeit mit entfernteren Bekannten (so genannte “weak ties”) in Verbindung zu stehen als auch das unmittelbare Teilen von Informationen mit engeren Freunden machen den Reiz dieser Dienste aus. Trotz dieser Vorteile haben Nutzer auch negative Erlebnisse. So werden gelegentlich Informationen versehentlich und ungewollt mit zu vielen Personen geteilt, werden durch Verknüpfungen von Informationen in den Diensten, z. B. Fotos und Markierungen von Gesichtern, ungewollt Informationen offengelegt, oder Nutzer werden Opfer von Online-Schikanen. Umgangsformen für soziale Netzwerke müssen sich vielfach erst zwischen den Nutzern entwickeln.

### Wir raten Ihnen

- *Achten Sie stets auf die Privatsphäreneinstellungen*  
Legen Sie mit ihren Privatsphäreneinstellungen fest, wer persönliche Informationen zu Ihrer Person sehen darf. Konfigurieren Sie dabei Ihr Profil lieber restriktiv.
- *Gruppieren Sie Ihre Kontakte*  
Überlegen Sie sich genau, wen Sie als Kontakt hinzufügen möchten. Wenn Sie die Arbeit nicht scheuen, können Sie Ihre Kontakte auch gruppieren, um bestimmten Personenkreisen bewusst Informationen vorzuenthalten.

- *Überprüfen Sie die Rechte Ihrer Kontakte*  
Prüfen Sie besonders kritisch Funktionen, die Ihren Freunden erlauben, Informationen zu Ihrer Person einzugeben, z. B. durch das Markieren Ihres Gesichtes in Fotos, oder durch Kommentieren von Einträgen auf Ihrer Nachrichtenseite.
- *Achten Sie die Privatsphäre anderer Nutzer*  
Vergewissern Sie sich bevor Sie Bilder hochladen, Personen in Bildern markieren, oder Nachrichten auf Pinnwänden hinterlassen, dass Sie andere Personen nicht verletzen oder beleidigen.

## Professionelle Angreifer und sonstige Risiken

### Firesheep - Demonstration eines Angriffs auf Nutzer von sozialen Netzwerken

Mit seiner Software Firesheep demonstrierte der Softwareentwickler Eric Butler, wie leicht sich Datenverbindungen mit sozialen Netzwerken in ungeschützten WLANs kapern lassen. Sein Rechner, auf dem er das Programm Firesheep installierte, schnitt den Netzwerkverkehr mit und entwendete die Sitzungscookies von anderen Nutzern, die im gleichen WLAN Facebook und Co. nutzten. In einem von Butler weiterentwickelten Internetbrowser reichten wenige Mausklicks, um als ein anderer Nutzer aus dem WLAN bei Facebook eingeloggt zu sein. Butler konnte so testweise fremde Nachrichten lesen und mit "fremden Freunden" interagieren.

### Missbrauch zur Bonitäts- und Risikoprüfung

2012 starteten die Schufa und das Hasso-Plattner-Institut (HPI) ein gemeinsames Forschungsprojekt um u. a. Daten aus sozialen Netzwerken zur Bonitätsprüfung zu nutzen. Nach heftigen Protesten von Datenschützern kündigte das HPI den Forschungsvertrag und stellte das Projekt ein. Es gibt aber auch andere Ideen, um von veröffentlichten Nutzerdaten zu profitieren: In den USA setzen beispielsweise Versicherungsfirmer Daten der Nutzer als Beweismittel in Gerichtsprozessen ein.

### Beurteilung

In und um soziale Netzwerke tummeln sich Personen und Gruppen, welche den Nutzern Schaden zufügen wollen, indem sie sich beispielsweise Zugang zu vertraulichen, privaten Daten verschaffen, Spam-Nachrichten versenden, oder Viren und Würmer verbreiten. Solche Angreifer können einerseits selbst in den Plattformen als Nutzer aktiv sein, andererseits aber auch klassische Angriffe wie z. B. Abhören von Netzwerkverbindungen mit Spezialisierung auf soziale Netzwerke durchführen.

### Wir raten Ihnen

- *Achten Sie auf eine sichere Kommunikation*  
Achten Sie auf Verschlüsselung der Verbindung zum Dienstanbieter (HTTPS), insbesondere in öffentlichen WLAN-Netzwerken, Internetcafés oder Hotels.
- *Führen Sie regelmäßig Updates durch*  
Aktualisieren Sie regelmäßig Webbrowser und andere Software auf Ihrem Rechner.

- *Nutzen Sie sichere Passwörter*

Wählen Sie ausreichend lange Passwörter für Ihren Dienstzugang, am besten für jeden Dienst ein anderes.

## Aspekte der Unternehmenssicherheit

### Folgenreicher Angriff auf RSA

Bei einem Angriff auf die Sicherheitsfirma RSA im Jahr 2011 nutzten Hacker Daten aus sozialen Netzwerken für sogenannte Spear-Phishing-Attacks, also gezielte Angriffe mit gefälschten E-Mails auf ausgewählte Mitarbeiter des Unternehmens. Ihnen gelang es damit, Schadsoftware in die Firma einzuschleusen und anschließend hoch vertrauliche Unternehmensinformationen zu stehlen.

### Die falsche Robin Sage

2010 konnte der Sicherheitsberater Thomas Ryan mittels gefälschter Facebook- und LinkedIn-Profiles einer fiktiven Cybersecurity-Spezialistin annähernd 300 "virtuelle" Kontakte zu Pentagon-Mitarbeitern aufbauen. Einige dieser Mitarbeiter vertrauten ihm sensible persönliche und dienstliche Informationen an. Das Pentagon musste nach Bekanntwerden einräumen, dass interne Richtlinien zu unzureichend waren, um den Informationsabfluss zu verhindern.

### Beurteilung

Unternehmen begreifen soziale Netzwerke als Chance zur Gewinnung neuer Kunden und Mitarbeiter. Gleichzeitig können Mitarbeiter, welche soziale Netzwerke nutzen, ein großer Risikofaktor für die Unternehmenssicherheit sein, wenn sie vertrauliche Informationen – meist ungewollt – preisgeben oder durch ungeschickte Aktionen den Ruf des Unternehmens schädigen. Die unbemerkte Vermischung von Privatem und Dienstlichem spielt dabei eine besondere Rolle. So erkennen Mitarbeiter manchmal nicht, dass sie dienstlich agieren, z. B. wenn sie sich mit anderen Mitarbeitern des Unternehmens in einer eigenen Mitarbeitergruppe in einem sozialen Netzwerk zu dienstnahen Themen austauschen.

### Wir raten Ihnen

- *Benennen Sie Ansprechpartner*

Bieten Sie Ihren Mitarbeitern Ansprechpartner für alle Fragen im Umgang mit sozialen Netzwerken und anderen Social-Media-Diensten.

- *Entwickeln Sie Social-Media-Richtlinien*

Erläutern Sie verbindlich Ihren Mitarbeitern, was das Unternehmen von ihnen beim Umgang mit den Diensten erwartet. Unterstützen Sie Ihre Mitarbeiter, richtig mit sozialen Netzwerken umzugehen, anstatt willkürlich Verbote auszusprechen.

- *Betrachten Sie die Risiken*

Berücksichtigen Sie im Risikomanagement mögliche Schadensfälle.

## 1. HINWEISE FÜR DEN LESER

Dieses Dossier wurde auf Grundlage von Informationen erstellt, die aus verschiedenen öffentlich verfügbaren Quellen stammen, wie beispielsweise

- Wissenschaftliche Artikel, wie Journal- oder Konferenzbeiträge
- “Graue Literatur”, also in wissenschaftlichen Institutionen entstandene Berichte und Artikel, die nicht von wissenschaftlichen Gremien evaluiert wurden
- Berichte staatlicher Institutionen, wie beispielsweise offiziell veröffentlichte Dokumente von Behörden
- Beiträge aus Medien (Zeitungen, Fachzeitschriften, Nachrichtenagenturen)
- Veröffentlichungen von Interessenverbänden, wie gemeinnützige Einrichtungen oder Institutionen
- Informationsschriften und Stellungnahmen aus Unternehmen

Die Beiträge zum aktuellen Wissensstand über soziale Netzwerke, denen diese Quellen entnommen sind, ordnet der Bericht entlang der betroffenen Beziehungen zwischen Dienstleistern, Nutzern und Unternehmen in vier Hauptkategorien:

*Gestaltungsspielräume Nutzer-Dienstleister.* Diese Kategorie umfasst Szenarien, in denen Wünsche der Dienstleister zur Verarbeitung und Weiterverwendung der privaten Nutzerdaten zu Konfliktsituationen zwischen Dienstleistern und Nutzern führen können. Häufig beeinträchtigen die Verarbeitungswünsche des Dienstleisters dabei die Privatsphärenwünsche der Nutzer. (Abschnitt 2)

*Gestaltungsspielräume zwischen privaten Nutzern.* Nutzer können durch soziale Netzwerke auch Nachteile in ihrem sozialen Umfeld erleiden, wenn sich Konfliktsituationen zu anderen Nutzern einer Plattform ergeben. Der Dienstleister spielt hier nur eine mittelbare Rolle. (Abschnitt 3)

*Nutzer als Ziel professioneller Angriffe.* Nutzer sind in sozialen Netzwerken auch Risiken durch professionelle Angreifer ausgesetzt, welche sich Lücken in der IT-Sicherheit zunutze machen, oder spezialisierte Techniken und Werkzeuge für großflächige oder gezielte Attacken einsetzen. (Abschnitt 4)

*Auswirkungen auf die Unternehmenssicherheit.* Herausgelöst sind Szenarien, in denen nicht allein einzelne Nutzer von Risiken betroffen sind, sondern auch Unternehmen, in denen diese Nutzer arbeiten, oder mit denen diese Nutzer in Kontakt stehen. (Abschnitt 5)

Diese Zuordnung soll dem Leser helfen, leichter Zugang zum zusammengestellten Material zu finden. Überschneidungen sind dort möglich, wo beschriebene Erkenntnisse eine Bewertung aus mehreren Perspektiven erforderlich machen, z. B. wenn beschriebene Attacken professioneller Angreifer auf Einzelnutzer auch die Sicherheit in Unternehmen betreffen können. Speziell für Mitarbeiter und Unternehmen befindet sich in diesem Dossier ein Leitfaden mit Hinweisen zur Erstellung einer Unternehmensrichtlinie für soziale Netzwerke und zu häufigen wiederkehrenden Fragen bezüglich der Nutzung dieser Dienste (Abschnitt 6). Im abschließenden Kapitel sind plattformspezifische Besonderheiten zusammengestellt (Abschnitt 7). Diese sollen dem Nutzer helfen, die angebotenen Dienste wie Facebook, Google+ oder Twitter besser zu verstehen und möglichen Risiken bei der Dienstnutzung selbst auszuweichen.

Dieses Dossier hat den Anspruch, den Wissensstand zum Thema möglichst vollständig darzustellen. Wenngleich die Autoren für viele Beiträge eine kurze, zusammenfassende Beurteilung abgeben konnten, ist aufgrund der Fülle an Informationen und Quellen keine tiefgreifende Prüfung und damit auch keine abschließende Einschätzung möglich gewesen. Das Dossier ist deshalb primär als Einstiegspunkt für weitergehende Recherchen zum Thema zu verstehen; es kann selbst keine Abschätzung zu der Qualität und Validität der zusammengestellten Informationen und Vertrauenswürdigkeit zitierter Quellen liefern.

#### **Hinweis zur Gestaltung dieses Berichtes**

Bei den meisten Abschnitten in diesem Dossier fasst eine kurzer grau hinterlegter Abschnitt zu Beginn die wichtigsten Informationen zusammen. Am Ende findet sich ein weiterer grau hinterlegter Text, welcher Hinweise für Unternehmen, Mitarbeiter oder Nutzer hervorhebt, die im Zusammenhang mit den zuvor erläuterten Problemen stehen.

## 2. GESTALTUNGSSPIELRÄUME ZWISCHEN NUTZER UND DIENSTANBIETER

Im Spannungsfeld Nutzer-Dienstleister stehen solche Szenarien, in denen Wünsche der Dienstleister zur Verarbeitung und Weiterverwendung der privaten Nutzerdaten zu Konfliktsituationen zwischen Dienstleistern und Nutzern führen können. Häufig beeinträchtigen die Verarbeitungswünsche des Dienstleisters dabei die Privatsphärenwünsche der Nutzer.

### 2.1 Zum Umgang mit dem Datenschutz

Soziale Netzwerke sammeln und verarbeiten sehr umfangreiche Daten zu Nutzungsvorgängen zur Realisierung ihres Geschäftsmodells. Dies kann im Widerspruch zu Datenschutzbestimmungen und zu den Interessen der Nutzer stehen.

#### 2.1.1 Unrechtmäßige Datensammlung

Die Dienstleister der sozialen Netzwerke haben ein Interesse daran, aus den Profildaten und sekundären Nutzungsdaten der Plattformmitglieder (z. B. Zeit und Zeitlänge von Kommunikationsverbindungen, IP-Adressen zur Ortsbestimmung, besuchte Seiten und Werbebanner, Kommentare auf anderen Seiten, versendete und empfangene Nachrichten) wirtschaftliche Vorteile zu ziehen. Ein Weg dazu ist das "Targeted Advertising" mit dem Dienstleister Dritten kundenspezifische Werbung zugänglich machen.

Facebook agiert hier beispielsweise zum einen als Publisher, welcher Werbung veröffentlicht, andererseits aber auch im Bereich der Datenanalyse ("Data Measurement and Site Analytics") um gezielte Werbung zu ermöglichen. Daneben kann Facebook als privatwirtschaftlicher Informations- bzw. Nachrichtendienst<sup>1</sup> auftreten, oder Daten an solche Dienste liefern.<sup>2</sup>

Dabei stützen sich die Dienstleister auf ihre umfangreichen Datenschutzerklärungen, welche häufig sehr unspezifische Angaben zu möglichen Verarbeitungszwecken für personenbezogene Daten machen. Zuweilen monieren Datenschützer den verschleiern Charakter dieser Datenschutzerklärungen und die Unklarheit der möglichen Datenverarbeitung als eine Missachtung des informationellen Selbstbestimmungsrechts der Nutzer.<sup>3</sup>

Die US-Handelsbehörde Federal Trade Commission (FTC) hat diesbezüglich im Jahr 2009 ein Verfahren gegen das US-Unternehmen Facebook eingeleitet [LRRB11], welches beide Parteien im November 2011 mit einem Vergleich abgeschlossen haben. Im Speziellen hat die FTC Facebook folgende "unfaire Verhaltensweisen" gegen seine Nutzer und Datenschutzverstöße vorgeworfen:

<sup>1</sup>Gemeint sind so genannte "Intelligence Companies", für die keine adäquate deutsche Bezeichnung existiert. Die Begriffe beziehen sich nicht auf staatliche Geheimdienste.

<sup>2</sup>Eine Datenweitergabe von Facebook an das Nachrichtenmagazin Politico löste bereits Diskussionen über die Rechtmäßigkeit solcher Aktivitäten aus, siehe <http://futurezone.at/netzpolitik/6925-facebook-datamining-ohne-zustimmung-der-user.php>

<sup>3</sup>Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (2011), siehe <https://www.datenschutzzentrum.de/internet/20111208-DK-B-Soziale-Netzwerke.html>

- **Irreführende Privatsphäreneinstellungen** Selbst wenn Nutzer ihre Privatsphäreneinstellungen auf “Nur Freunde” oder “Freunde der Freunde” gesetzt haben, macht Facebook deren Profildaten auch den Anwendungen zugänglich, die von den Freunden genutzt werden.
- **Unfaire Privatsphäre-Änderungen** Seit Ende 2009 änderte Facebook mehrere Male seine Datenschutzerklärung und die Default-Einstellungen, so dass viele Privatsphäreneinstellungen der Nutzer überschrieben wurden. Daten wie Profildaten, Freundeslisten und Seiten wurden im Internet frei zugänglich und können teilweise nicht mehr zugriffsbegrenzt werden.<sup>4</sup>
- **Zugriff auf Nutzerdaten durch Anwendungen** Entgegen offiziellen Verlautbarungen gewährt Facebook den Anwendungen Zugang zu persönlichen Nutzerdaten, welche für die Anwendungen weder erforderlich noch zweckgebunden sind.
- **Veröffentlichung von Nutzerdaten gegenüber Werbekunden** Entgegen offiziellen Verlautbarungen gibt Facebook die Kennungen der Nutzer, die auf Werbung geklickt haben, an seine Werbekunden weiter, die mittels Nutzerkennung an die persönlichen Nutzerdaten gelangen.
- **Irreführendes Programm zur Anwendungsprüfung** Entgegen offiziellen Verlautbarungen hat Facebook an den als “Verified Applications” markierten Anwendungen keine Sicherheitsprüfungen durchgeführt, welche über die der anderen Anwendungen hinausgingen.
- **Veröffentlichung von Nutzerfotos und -Videos** Facebook-Nutzer und Anwendungen können Fotos und Videos anderer Nutzer per URL im Internet jedem zugänglich machen, selbst dann, wenn die betreffenden Nutzer ihre Accounts gelöscht oder deaktiviert haben.
- **Verstoß gegen EU Safe Harbor-Bestimmungen** Facebook hat in vielen Fällen gegen einschlägige Datenschutzprinzipien verstoßen.

In Europa ist das Unternehmen Facebook Ireland mit Anzeigen konkreter Datenschutzverstöße konfrontiert<sup>5</sup>:

- (1) **Pokes (Anstupsen)** Die Daten werden nach dem “Entfernen” von Facebook weiter gespeichert und nie wieder gelöscht.
- (2) **Schattenprofile** Facebook sammelt im Hintergrund Daten von Personen, ohne dass der Betroffene dies bemerkt oder dem zustimmt. Betrifft vor allem Personen ohne Facebook.
- (3) **Markieren** Markierungen werden ohne Zustimmung des Users (Opt-In) aktiviert. Der User muss die Daten dann entfernen (Opt-Out).
- (4) **Synchronisieren** Facebook saugt persönliche Daten z.B. mittels iPhone-App oder E-Mail-Import ab und verwendet diese Daten für seine eigenen Zwecke – ohne die Zustimmung des Betroffenen.
- (5) **Gelöschte Postings** Postings auf den Seiten der Facebooknutzer werden auch nach dem “Entfernen” weiter gespeichert.
- (6) **Postings auf fremden Seiten** Der User kann nicht herausfinden, wer seine auf fremden Seiten hinterlassenen Daten sehen kann.

<sup>4</sup>Vgl. Matt McKeon (2010): The Evolution of Privacy on Facebook, siehe <http://mattmckeeon.com/facebook-privacy>

<sup>5</sup>Europe versus Facebook (2012), siehe <http://europe-v-facebook.org/DE/Anzeigen/anzeigen.html>

- (7) **Messages** Nachrichten (inkl. Chat-Nachrichten) werden auch nach dem “Löschen” weiter gespeichert. Damit wird die gesamte direkte Kommunikation auf Facebook dauerhaft unlöslichbar.
- (8) **Datenschutzbestimmungen und Zustimmung** Die Datenschutzbestimmungen sind vage, unklar und widersprüchlich. Nach europäischen Standards ist die Zustimmung ungültig.
- (9) **Gesichtserkennung** Die neue Gesichtserkennung ist ein unverhältnismäßiger Eingriff in die Privatsphäre der Nutzer. Außerdem fehlen Hinweise und die Zustimmung.
- (10) **Auskunft mangelhaft** Die Auskunft, zu welcher Facebook gesetzlich verpflichtet ist, ist in vielen Punkten mangelhaft. Viele Daten und Informationen fehlen.
- (11) **Löschen von Markierungen** Markierungen (z. B. in Fotos), die “Entfernt” werden, werden von Facebook nur deaktiviert.
- (12) **Datensicherheit** Facebook sagt in seinen Nutzungsbedingungen, dass es nicht sicherstellen kann, dass Daten sicher sind.
- (13) **Anwendungen** Anwendungen von Freunden können auf die Daten des Nutzers zugreifen. Es gibt keine entsprechenden Sicherheiten, dass die Anwendungen europäischen Datenschutzstandards entsprechen.
- (14) **Gelöschte Freunde** Freunde, die gelöscht werden, bleiben weiter auf Facebook gespeichert.
- (15) **Exzessive Datennutzung** Facebook sammelt unglaubliche Datenmengen als “Host”, die eigene Nutzung ist unlimitiert.
- (16) **Opt-Out** Die Verwendung der Daten auf Facebook ist faktisch “Opt-Out” statt “Opt-In”, das widerspricht den europäischen Gesetzen.
- (17) **Like Button** Der von Facebook derzeit angebotene “Like Button” ist nicht datenschutzkonform und kann zum Ausspionieren der Nutzer verwendet werden.
- (18) **Pflichten als Auftragsverarbeiter** Facebook hat gegenüber den Nutzern die Pflicht die vom Nutzer auf Facebook hinterlegten Daten nicht für eigene Zwecke zu missbrauchen.
- (19) **Privatsphäreneinstellungen bei Bildern** Die User können nur steuern, wer den Link zu einem Bild sehen kann. Das Bild selbst ist für jeden abrufbar, der den Link kennt. Es gibt keine wirkliche Steuerung über Zugriffsrechte.
- (20) **Gelöschte Bilder** Gelöschte Bilder sind weiter abrufbar und werden erst mit großer Verzögerung gelöscht. Nur der Link zum Bild auf facebook.com wird unsichtbar.
- (21) **Gruppenmitgliedschaft** Nutzer können ohne deren Zustimmung zu Gruppen hinzugefügt werden und müssen dann aktiv wieder austreten.
- (22) **Änderung der Datenschutzrichtlinien** Datenschutzbestimmungen werden regelmäßig, ohne entsprechende Information und Zustimmung der User, geändert.

Die Anzeigen stellen juristisch betrachtet eine Rechtsansicht dar, über deren Berechtigung die irische Datenschutzbehörde entscheiden muss. Es liegen aber viele Hinweise vor, dass Facebook gegen nationale und internationale Datenschutzprinzipien verstößt, insbesondere gegen die OECD-Datenschutzprinzipien der begrenzten Datenerhebung, Nutzungsbegrenzung und Offenheit [JW12].

Im Sommer 2013 geraten Facebook und weitere US-amerikanische Internet- und Softwareanbieter (Google mit YouTube, Apple, Microsoft mit Skype, Yahoo, Paltalk, AOL) in die Kritik, dem US-Geheimdienst NSA im Rahmen des PRISM-Überwachungsprogramms



Zugriff auf den gesamten Datenverkehr zu gewähren. “Europe versus Facebook” und andere Nutzergruppen haben gegen die europäischen Tochterunternehmen einiger Anbieter bei den zuständigen Datenschutzbehörden Beschwerden gegen den Transfer von Nutzerdaten in die USA eingelegt.<sup>6,7</sup>

#### **Hinweis für Nutzer**

Das Hochladen von Adressbüchern oder der Zugriff auf E-Mail-Konten durch Anbieter sozialer Netzwerke ist sehr bedenklich und in der Regel vom Arbeitgeber nicht gestattet. Diese Funktionen sollten Sie daher weder privat noch mit Adressbüchern oder E-Mail-Konten ihres Arbeitgebers verwenden. Besonders auf Smartphones und Tablets (z. B. iPhone, iPad, Xoom) kann ein einziger Klick bereits den Upload des Adressbuches an den Dienstanbieter auslösen. Daher sollten Sie besonders auf mobilen Geräten darauf achten, keine Synchronisation von Kontakten zu verwenden.

#### **Hinweis für Nutzer**

Facebook informiert die Nutzer relativ wenig bzw. eher indirekt mittels Web-Seiten über neue Funktionen und Änderungen der Default-Einstellungen. Wer von Facebook rechtzeitig informiert werden möchte, sollte auf der offiziellen Web-Seite “Facebook Site Government”, siehe <https://www.facebook.com/fbsitegovernance>, den “Gefällt mir”-Button anklicken. In vielen Fällen ist es allerdings schwierig abzuschätzen, wie sich die geplanten Neuerungen mit den eigenen Vorstellungen und den eingestellten Privatsphäreoptionen vertragen.

Ein weiteres Beispiel unklarer Datenschutzbestimmungen ist das Recht auf “Vergessenwerden” [KS12]: Selbst wenn Nutzer ihre Mitgliedschaft im sozialen Netzwerk dauerhaft beenden, so räumen Dienstbetreiber ihren Nutzern selten ein Recht auf vollständiges Löschen der gespeicherten persönlichen Daten ein. Facebook hat inzwischen immerhin zugesagt, dass die direkten Links auf gelöschte Bilder nach spätestens 30 Tagen wirklich gelöscht sind.<sup>8</sup>

Vermutlich wird es weitere Anzeigen gegen Facebook geben. Denn Facebook hat die Funktion “Gesehen von” eingeführt, mit der jedes Mitglied einer Gruppe sehen kann, wer sich wann welche Nachricht angesehen hat. Die Funktion lässt sich nicht abschalten. Somit kann kein Nutzer unbeobachtet online sein und sich etwas anschauen. Dass zur Freischaltung offenbar nur eine kleine technische Änderung nötig war, scheint darauf hinzudeuten, dass Facebook generell intern viel mehr speichert als nach außen sichtbar wird.<sup>9</sup>

#### **Hinweis für Nutzer**

Bevor Sie Daten in den Dienst eingeben, prüfen Sie zunächst immer wie die Pri-

<sup>6</sup>unwatched.org: [www.unwatched.org/20130626\\_Nach\\_PRISM-Skandal\\_0esterreicher\\_zeigen\\_Facebook\\_Apple\\_Microsoft\\_Skype\\_und\\_Yahoo\\_an](http://www.unwatched.org/20130626_Nach_PRISM-Skandal_0esterreicher_zeigen_Facebook_Apple_Microsoft_Skype_und_Yahoo_an)

<sup>7</sup>Complaint against Facebook Ireland Ltd – 23 “PRISM”: <http://www.europe-v-facebook.org/prism/facebook.pdf>

<sup>8</sup>Jacqui Cheng: Three years later, deleting your photos on Facebook now actually works, siehe <http://arstechnica.com/business/2012/08/facebook-finally-changes-photo-deletion-policy-after-3-years-of-reporting>

<sup>9</sup>Siehe <http://www.heise.de/newsticker/meldung/Facebook-zeigt-Nutzeraktivitaeten-in-Gruppen-an-1662810.html>

vatsphäreoptionen für diese Daten funktionieren und konfigurieren Sie diese nach Ihren Wünschen. Möchten Sie beispielsweise in Facebook, dass Ihre Profildaten zumindest nicht außerhalb von Facebook sichtbar sind, dann sollten Sie die Voreinstellung “Öffentliche Suche aktivieren” entfernen. Möchten Sie, dass niemand auf Basis Ihrer Netzwerk-Aktivitäten Werbeanzeigen von Drittanbietern erhält, dann sollten Sie das unter “Einstellungen für soziale Werbeanzeigen bearbeiten” eintragen. Fehlen gewünschte Einstellmöglichkeiten, dann überlegen Sie genau, ob das Teilen bestimmter Informationen mit anderen für Sie wirklich so wichtig ist.

### 2.1.2 Mögliche Auswirkungen der Datensammlung

Profildaten und sekundäre Daten sollten als persönliche Daten betrachtet werden. Denn darunter fallen gemäß der europäischen Richtlinie 95/46/EG “Alle Informationen über eine bestimmte oder bestimmbare natürliche Person” [Art07].<sup>10</sup> Zumeist ist den Nutzern unklar, welche Daten die Dienstanbieter langfristig speichern, aggregieren und verwerten, insbesondere wenn der Nutzer sein Profil deaktiviert oder gelöscht hat. Da die sozialen Netzwerke immer mehr Dienste und Anwendungen in sich vereinen, können in nie gekanntem Ausmaß persönliche Daten gesammelt und an Dritte weiterverkauft werden. Das grundlegende Recht der Nutzer, alleinige Kontrolle über ihre persönlichen Daten auszuüben, ist damit stark gefährdet.

#### **Hinweis für Nutzer**

Schalten Sie in Ihren Privatsphäreinstellungen die Sichtbarkeit Ihrer persönlichen Daten für Nichtmitglieder ab. So können Sie wenigstens verhindern, dass Suchmaschinen Ihre Daten indizieren.

## 2.2 Nutzungsrechte und Datenschutzbestimmungen

Betreiber von sozialen Netzwerken besitzen zumeist Nutzungsrechte an den veröffentlichten Inhalten der Nutzer. Auch schließen die meisten Anbieter die Haftung, Gewährleistung oder Verfügbarkeit aus. Dabei sind die Datenschutzhinweise oder Einstellmöglichkeiten häufig unklar.

Betreiber von überwiegend kostenfreien Diensten der sozialen Netzwerke lassen sich zumeist Nutzungsrechte zur Vermarktung und Weitergabe der eingestellten und veröffentlichten Inhalte einräumen. Dies ist teilweise Voraussetzung dafür, dass ein Nutzer die Inhalte überhaupt bearbeiten oder darstellen kann. Die Inhalte werden dann veräußert oder anderweitig zur Gewinnerzeugung genutzt, u. a. zur Gewinnung neuer Interessenten und Nutzer (“Leadgenerierung”) oder für Werbeanzeigen.

<sup>10</sup>Richtlinie 95/46/EG (1995), siehe <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html>

### 2.2.1 Nutzungsrechte von Facebook

Facebook lässt sich ein einfaches Nutzungsrecht an Fotos und Videos einräumen (so genannte “Intellectual Properties (IP)”, d. h. “IP-Inhalte” und “IP-Lizenzen”). Dieses wird unwiderruflich, sobald diese mit anderen Nutzern geteilt wurden. Faktisch bedeutet dies, dass Facebook immer ein unwiderrufliches Nutzungsrecht an Fotos und Videos erhält.<sup>11</sup>

Facebook hat bereits Profildaten für Werbezwecke verwendet. Das Landesgericht Berlin hat aber in einer Entscheidung<sup>12</sup> die Verwendung des Freundfinders und die Vertragsklauseln zu Werbung, Datenschutz und den IP-Inhalten als rechtswidrig erklärt. Die weitere Entwicklung bleibt abzuwarten.

### 2.2.2 Unklare Datenschutzbestimmungen

Die Nutzungsbedingungen und Datenschutzhinweise (AGB) von Diensten sozialer Netzwerke können für private Nutzer und für Unternehmen nachteilige Regelungen enthalten. Typische nachteilige Regelungen sind etwa: Der Diensteanbieter lässt sich Nutzungsrechte an den bei ihm veröffentlichten Inhalten einräumen, v. a. bzgl. Bildern und Videos, so z. B. bei YouTube und Picasa, d. h. der Nutzer verliert die alleinige Verfügungsgewalt über die Inhalte. Bei patentrelevanten Inhalten kann eine Veröffentlichung zudem neuheitsschädlich sein und eine spätere Patentierbarkeit verhindern.

Mit der Rechtseinräumung an den Dienst gehen oftmals die fehlende Möglichkeit einher zu kontrollieren, wo eingestellte Inhalte veröffentlicht werden und die fehlende Möglichkeit, Inhalte zu löschen, auch wenn der Account selbst gelöscht wird. Da viele Dienste kostenlos sind, ist in der Regel jegliche Haftung ausgeschlossen, etwa auch wenn Daten unabsichtlich veröffentlicht oder Accounts gehackt werden. Letztlich behalten sich Dienste oftmals vor, den Betrieb unangekündigt einzustellen, ohne dass ein Anspruch auf Herausgabe der eigenen Daten besteht.

Selbst wenn der Dienst seinen Nutzern Rechte einräumt, sind diese gegenüber Anbietern im Ausland regelmäßig kaum praktisch durchsetzbar. Bei der Nutzung sollte man daher davon ausgehen, im Zweifel gar keine Rechte gegen den Dienst zu haben oder durchsetzen zu können. Zudem ist es nach anderen Rechtsordnungen möglich, dass Behörden oder Dritte aufgrund gerichtlicher Verfügungen oder staatlichen Geheimdienstprogrammen (siehe US-Geheimdienstprogramm PRISM) Einsicht in die von Nutzern gespeicherten Daten bekommen.

#### **Hinweis für Nutzer**

Es ist wichtig, dass man vor der Nutzung eines Dienstes zunächst die Nutzungsbedingungen und Datenschutzhinweise (AGB) des Dienstes liest, bevor man ihnen zustimmt. AGB können für private Nutzer und für Unternehmen nachteilige Regelungen enthalten, die eine sinnvolle Nutzung des Dienstes im Einzelfall in Frage stellen oder alternative Dienste attraktiver machen.

<sup>11</sup>Siehe <http://www.facebook.com/legal/terms?ref=pf>

<sup>12</sup>LG Berlin: Az.: 16 O 551 /10 vom 06.03.2012

## 2.3 Zusatzprogramme zu Werbe- und Marketingzwecken

Andere Web-Seiten integrieren Zusatzprogramme der Anbieter sozialer Netzwerke für Werbe- und Marketingzwecke. Dies ermöglicht den Anbietern sozialer Netzwerke personenbezogene Daten der Nutzer zu sammeln und beispielsweise mehr über die Surf-Gewohnheiten der Nutzer zu erfahren.

Soziale Netzwerke stellen Zusatzprogramme, sogenannte Social-Plugins, für Marketingzwecke zur Verfügung. So führte Facebook Ende 2007 zusammen mit 44 Partner-Online-Shops das “Beacon”-Programm ein, das die Werbung mittels Mund-zu-Mund-Propaganda revolutionieren sollte. Sobald ein Nutzer auf einer Partnerseite etwas kaufte, wurden alle Freunde darüber mittels einer Statusmeldung informiert.<sup>13</sup> Das Programm wurde standardmäßig freigeschaltet, ohne dass die meisten Nutzer davon wussten und ohne die Einwilligung der Nutzer einzuholen. Mittels Cookies wurden Informationen an Facebook übertragen, selbst dann, wenn ein Besucher der Partnerseite gar kein Facebook-Account besaß.

Massive Proteste entzündeten sich nicht nur an verpatzten Weihnachtsüberraschungen, sondern generell an der Verletzung der Privatsphäre und dem fehlenden Opt-In (statt Opt-Out). Nach mehreren Verbesserungsversuchen<sup>14</sup> zog Facebook aufgrund einer Sammelklage wenige Monate später das Programm zurück.<sup>15</sup>

Seit Ende 2008 können Web-Seiten “Facebook Connect” in ihre Seiten einbinden. Dies ermöglicht es Facebook-Nutzern, sich mit ihren Facebook-Zugangsdaten auf anderen Web-Seiten, Anwendungen, mobilen Geräten usw. einzuloggen, sich dort mit anderen Freunden zu verbinden und sogar ihre Privatsphären-Einstellungen mitzunehmen. Facebook bewies mit der Connect-API<sup>16</sup> offenbar mehr Umsicht und stößt bei anderen Internetdiensten, die sich dadurch mehr Kommunikation auf ihren Seiten erhoffen, auf Interesse.<sup>17</sup> Eine solche “Einmalanmeldung” ermöglicht es dem Netzwerk aber ebenso, das Surfverhalten des Nutzers auf anderen Seiten zu verfolgen (“Tracking”).

Außerdem arbeitet Facebook an einem neuen Verfahren für ein so genanntes “Optimized CPM” (“Optimized Costs per 1,000 ad impressions”), mit dem das Nutzerverhalten und der Erfolg von Werbeanzeigen besser bestimmt werden kann. Dazu wird die so genannte Konversion der Anzeigen gemessen, d. h. festgestellt, ob die Nutzer, die auf eine Anzeige geklickt haben, auch die weiteren damit verbundene Aktionen durchführen, z. B. wirklich das Produkt kaufen. Möglich wird dies durch ein Zusatzprogramm, das ohne Cookies auskommt und selbst über verschiedene Browser und Geräte (Smartphones, Notebooks und Tablets,...) hinweg die aufgerufenen Web-Seiten einem aktiven Nutzer-Login zuordnet und verarbeitet.<sup>18</sup>

### Hinweis für Nutzer

Den Betreibern von sozialen Netzwerken kann die Analyse des Nutzer-Verhaltens er-

<sup>13</sup>Siehe <http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503.html>

<sup>14</sup>Siehe <http://bits.blogs.nytimes.com/2007/11/29/the-evolution-of-facebooks-beacon>

<sup>15</sup>Siehe <http://mashable.com/2009/09/19/facebook-beacon-rip>

<sup>16</sup>API = Application Programming Interface, Schnittstelle zur Anwendungsprogrammierung

<sup>17</sup>Siehe <http://www.nytimes.com/2008/12/01/technology/internet/01facebook.html>

<sup>18</sup>Zach Rodgers: Product Manager David Baser on Facebook’s Attribution Roadmap (23.1.2013), siehe <http://www.adexchanger.com/social-media/product-manager-david-baser-on-facebooks-attribution-roadmap/>

schwert werden, indem man sich konsequent vor dem Besuch anderer Webseiten und der Nutzung anderer Geräte aus dem Netzwerk ausloggt. Die Zuordnung der Nutzeraktivitäten zur jeweiligen Facebook-ID wird zumindest schwieriger, wenn man nicht dauerhaft im Hintergrund (Facebook-Tab im Browser) eingeloggt bleibt.

### 2.3.1 Facebook “Like”-Button

Social-Plugins werfen aber weiterhin datenschutzrechtliche Bedenken auf, wie am Beispiel des Facebook “Like”-Buttons ersichtlich ist,<sup>19</sup> den Facebook als vermeintlich harmlosen Beacon-Nachfolger im April 2010 einführte.<sup>20</sup> Die deutschen Diskussionen beziehen sich vor allem darauf, inwieweit solche Plugins im Widerspruch zum deutschen Datenschutzrecht stehen.<sup>21</sup> Insbesondere steht hierbei die Frage im Raum, ob die Einbindung der Social-Plugins durch Betreiber in ihre eigenen Web-Seiten zulässig ist.

Selbst wenn der Code zur Einbettung der Social-Plugins in das Web-Angebot von Facebook/Twitter/Google+ zur Verfügung gestellt wird, laufen Anbieter deutscher Web-Seiten Gefahr, selbst datenschutzrechtliche Verstöße zu begehen, wenn sie den Code in ihre Web-Seiten integrieren.<sup>22</sup> Bei jedem Aufruf einer Seite, in welche ein Social-Plugin-Button integriert ist, wird der Button von einem Server des entsprechenden sozialen Netzwerks geladen, so dass das soziale Netzwerk im Rahmen einer Reichweitenanalyse Einblicke in das Internetnutzungsverhalten des Web-Seitenbesuchers erhalten kann. Bei einer Reichweitenanalyse werden Informationen über die Nutzung einer Web-Seite sowie das Verhalten der Web-Seitenbesucher gesammelt und gemeldet. Unabhängig davon, ob der jeweilige Social-Plugin-Button gedrückt wird, werden personenbezogene Daten erhoben und verarbeitet (unter anderem IP-Adressen und Cookies), sobald der Nutzer eines sozialen Netzwerks eine Web-Seite mit integriertem Social-Plugin-Button lädt.

Dieser Vorgang ist für den Nutzer weder erkennbar, noch hat er die Möglichkeit, sich diesem Vorgang ohne weiteres zu entziehen. Zudem findet die Verarbeitung der personenbezogenen Daten durch die sozialen Netzwerke in der Regel außerhalb Deutschlands und der EU statt. Nutzer sozialer Netzwerke könnten durch das Senden von IP-Adresse und Cookies an den jeweiligen Betreiber des sozialen Netzwerks individualisiert werden. Das geschieht beim Besuchen einer Web-Seite automatisch während des Ladens des Social-Plugin-Buttons. Bei diesem Vorgang wird zusätzlich die Adresse (URL) der besuchten Seite, das Datum und die Uhrzeit übermittelt. Der Betreiber kann aus den empfangenen Daten einen direkten Personenbezug herstellen.

#### **Hinweis für Nutzer**

Für die Internet-Browser Chrome, Safari und Firefox gibt es die Extension “Facebook Disconnect”, die alle Aufrufe von anderen Web-Seiten aus zu Facebook blockiert. Bei der Benutzung eines anderen Browsers sollte man darauf achten, sich regelmäßig beim

<sup>19</sup>siehe z. B. <http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html>

<sup>20</sup>Der Facebook “Like”-Button wird im deutschsprachigen Raum als “Gefällt mir”-Button bezeichnet. Weitere Social-Plugins von Facebook sind etwa der “Empfehlen” und der “Teilen”-Button. Die Social-Plugins von Twitter und Google+ heißen unter anderem “Tweet” und “+1”.

<sup>21</sup>Siehe z. B. <https://www.datenschutzzentrum.de/presse/20110819-facebook.htm>

<sup>22</sup>Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (2011), siehe <https://www.datenschutzzentrum.de/internet/20111208-DK-B-Soziale-Netzwerke.html>

Verlassen von Facebook abzumelden und keinen Facebook-Tab im Browser geöffnet zu lassen. Facebook erhält dann zwar trotzdem Daten, kann diese aber nicht mehr einem Facebook-Profil zuordnen.

### 2.3.2 Mögliche Auswirkungen der Social-Plugins

Die Verwendung von Social-Plugins wie den Like-Button hat zur Folge, dass soziale Netzwerke erfahren können, auf welchen anderen Webseiten sich der jeweilige Nutzer aufhält, ohne dass der Nutzer dies ohne Weiteres unterbinden kann. Das soziale Netzwerk kann zudem erfahren, welche einzelnen Seiten und Artikel sich der Nutzer ansieht. Auf einem Online-Shopping-Portal, welches ein Social-Plugin auf einzelnen Produktseiten integriert hat, kann das soziale Netzwerk dem Nutzer demnach beim Einkaufen über die Schulter schauen, bei einer Online-Zeitung, welche Social-Plugins integriert hat, ist es dem sozialen Netzwerk möglich zu erfahren, welche einzelnen Artikel der Nutzer liest. Auf diese Weise können umfangreiche Persönlichkeitsprofile erstellt werden.

Eine aktuelle Studie [KSG13] mit rund 58.000 Facebook-Nutzern hat gezeigt, dass sich sensible Persönlichkeitsmerkmale wie z. B. das Geschlecht, die sexuelle Orientierung, Religionszugehörigkeit, ethnische Zugehörigkeit und politische Überzeugungen der Nutzer anhand der vom jeweiligen Nutzer angeklickten Plugin-Buttons sehr gut durch automatische Analysen bestimmen lassen. Die Analysen ermöglichten auch Aussagen zu Charakter, Intelligenz und Drogenmissbrauch des Nutzers – in einer Genauigkeit wie sie in herkömmlichen Persönlichkeitstests erreicht wird. Die Analyseergebnisse sind zudem durch die eigentlichen Profildaten und die vielen unfreiwilligen digitalen Spuren im Internet beliebig erweiterbar.

Beim Klicken auf ein Social-Plugin erfolgt die Datenerhebung nicht durch den Webseitenbetreiber, der das Social-Plugin auf seiner Web-Seite integriert hat, sondern über eine direkte Kommunikationsverbindung zwischen dem Computer des Nutzers und dem sozialen Netzwerk. Der Webseitenbetreiber erhebt somit zwar keine Daten, die er an das soziale Netzwerk übermittelt, der HTML-Code sorgt jedoch dafür, dass der Rechner des Nutzers eine Verbindung zu dem sozialen Netzwerk aufbaut. Webseitenbetreibern, die Social-Plugins in ihre Web-Seiten integrieren, drohen daher hohe Bußgelder wegen Datenschutzverstößen.<sup>23</sup>

Es existieren inzwischen datenschutzfreundliche Lösungen,<sup>24</sup> bei denen die Social-Plugins auf der Anbieterseite so lange ersetzt werden, bis der Nutzer über die anstehende Datenübermittlung an das jeweilige soziale Netzwerk aufgeklärt wurde und in diese eingewilligt hat. Eine Datenübermittlung an die sozialen Netzwerke vor der Einwilligung wird somit unterbunden.

#### **Hinweis für Nutzer und Unternehmen**

Die Verwendung von Social-Plugins wie dem Facebook Like-Button ist datenschutzrechtlich kritisch zu sehen. Durch das Einbinden werden, ohne dass der Besucher der Webseite dies verhindern kann, Daten an den Anbieter übermittelt. Daher sollten Social-Plugins nicht direkt in die Webseiten eingebunden werden. Den Nutzern wird empfohlen, auf das Anklicken von Buttons weitgehend zu verzichten, solange sich nicht datenschutzfreundliche Lösungen durchgesetzt haben.

<sup>23</sup>Siehe <https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf>

<sup>24</sup>Siehe z. B. WordPress.org: 2 Click Social Media Buttons, <http://wordpress.org/extend/plugins/2-click-socialmedia-buttons>

## 2.4 Integrierte Drittanbieter-Anwendungen

Drittanbieter integrieren eigene Software wie z. B. Computerspiele in soziale Netzwerke. Diese Zusatzanwendungen verfügen häufig über weitgehende Zugriffsrechte auf die persönlichen Daten der Nutzer – unter Umständen viel mehr als die Anwendung selbst benötigt.

Nutzer können Drittanwendungen in ihre Profile integrieren, um die Attraktivität des sozialen Netzwerks zu erhöhen. Inzwischen gibt es über 82.000 Facebook-Anwendungen,<sup>25</sup> die durchweg kostenlos sind. Etwa zwei Drittel aller Anwendungen können im Betrieb auf bestimmte Nutzerdaten zugreifen. Facebook verwendet das OAuth 2.0-Authentisierungsprotokoll<sup>26</sup> für die Kommunikation zwischen einer Drittanwendung, dem Nutzer und Facebook, siehe Abbildung 1.

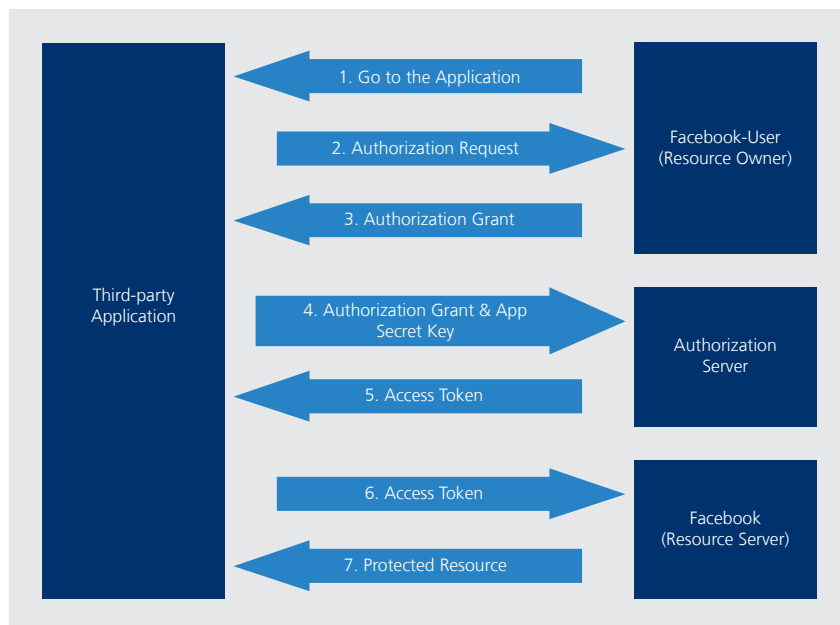


Abbildung 1. Nutzung des OAuth 2.0-Protokolls bei Facebook

Dies ermöglicht eine Rechtedelegierung vom Nutzer an die Anwendung, damit die Anwendung auf geschützte Nutzerdaten zugreifen kann, ohne die Zugangsdaten des Nutzers zu benötigen.<sup>27</sup> Wenn der Nutzer eine Anwendung autorisiert hat, dann erhält die Anwendung von Facebook neben der Nutzererkennung (“User-ID”) ein so genanntes “Access Token”. Beides dient dazu, über das “Open Graph Protocol” gezielte Datenabfragen an Facebook zu senden. Das “Open Graph Protocol” bietet eine Sicht auf das von Facebook aufgezeichnete Beziehungsgeflecht (“Social Graph” u. a. mit Personen, Fotos, Ereignissen, Seiten einschließlich all ihrer Verbindungen). Diese Datenbasis macht es für viele Drittanbieter attraktiv, von Nutzern möglichst umfangreiche Berechtigungen zu erhalten. Die zugrunde liegenden

<sup>25</sup>Siehe <http://www.socialbakers.com/facebook-applications>

<sup>26</sup>Siehe <http://tools.ietf.org/pdf/draft-ietf-oauth-v2-12.pdf>

<sup>27</sup>Siehe <http://developers.facebook.com/docs/facebook-login>



technischen Protokolle lassen selbst keine Gefährdungen erkennen, auch wenn fehlerhafte Implementierungen ein Sicherheitsrisiko darstellen können.<sup>28</sup>

Vor allem aber scheinen der Umfang der zu vergebenden Berechtigungen und die damit verbundenen Datenabfragen der Anwendungen bedenklich. So wird die Rechtedelegation vom Nutzer an die Anwendung nicht zentral von Facebook, sondern dezentral durch die Anbieter der Anwendungen kontrolliert. Grundsätzlich ignorieren aber Anwendungen die globalen Privatsphäreneinstellungen der Nutzer [WXG11]. Viele Anwendungen versuchen den Nutzern immer mehr Zugeständnisse abzurufen und verkaufen die gewonnenen Nutzerdaten an andere Werbeunternehmen weiter.<sup>29</sup>

Insgesamt gibt es über 60 Facebook-Berechtigungen in 23 verschiedenen Kategorien, die lesend, schreibend und ordnend auf Nutzerdaten zugreifen können. Sieht man die Berechtigungen als potentiell gefährlich an, die den Zugriff auf sensitive persönliche Daten freigeben, so kann jede Facebook-Berechtigung gefährlich werden. 67% aller Anwendungen möchten auf Daten zugreifen und erfragen dazu mindestens die Berechtigung “Access my basic information” (Name, Foto, Geschlecht, Gruppe, Nutzerkennung, Freundesliste, gemeinsame Daten). Die bedenklichsten Berechtigungen sind vermutlich “Access my data any time”, und “Access information people share with me” – letztere berechtigt zum Zugriff auf persönliche Daten der Freunde.

#### Hinweis für Nutzer

Leider kann man nicht kontrollieren, welche Drittanbieter-Anwendungen von Facebook über Seiten der Freunde auf die eigenen persönlichen Daten zugreifen können. Man kann aber die Datenübertragung an Drittanbieter unter den Einstellungen “Wie Nutzer deine Informationen an Anwendungen weitergeben, die sie nutzen” einschränken. Ganz verhindern lässt sie sich nur dadurch, dass man alle Anwendungen deaktiviert.

Generell werden folgende datenschutzrelevante Punkte an den Drittanbieter-Anwendungen kritisiert [CYA12; WXG11]:

- **Umfangreiche Datenanforderungen der Anwendungen** Gerade die beliebten Anwendungen erfragen überdurchschnittlich viele Berechtigungen, deren Zweck für die Anwendung nicht offensichtlich ist. Für Anwendungsentwickler gibt es keine Anreize, auf Berechtigungen zu verzichten.
- **Mangelnde Sicherheitskontrolle** Da Drittanwendungen nicht auf Facebook.com bereit gestellt werden, kann Facebook nicht sicherstellen, dass die Anwendungen unkritisch sind.
- **Mangelnde Transparenz** Der Berechtigungsdialog zeigt keine Informationen darüber, wozu eine Anwendung bestimmte Daten benötigt.
- **Unzureichende Berechtigungsanzeige** Der Berechtigungsdialog zeigt nicht vollständig die mit einer Berechtigung verbundenen Datenzugriffe an. “Photos uploaded by me” sagt z. B. nicht, dass auch alle damit verbundenen Objekte (Beschreibung, Kommentare, Zeitangaben, Links, Tags etc.) zugreifbar werden.
- **Fehlende Warnungen** Die Dialoge spiegeln nicht die globalen Privatsphäreneinstellungen des Nutzers wider. Es gibt keine Meldungen, die auf Risiken hinweisen, z. B. auf

<sup>28</sup>Vgl. Nir Goldshlager: “How I Hacked Facebook OAuth To Get Full Permission On Any Facebook Account (Without App “Allow” Interaction)”, siehe <http://www.nirgoldshlager.com/2013/02/how-i-hacked-facebook-oauth-to-get-full.html>

<sup>29</sup>Vgl. <http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html>



Widersprüche zu den Privatsphäreneinstellungen. Erhältliche Nutzerkommentare (z. B. WOT Services<sup>30</sup>) werden an dieser Stelle nicht genutzt.

- **Missachtung der Privatsphäreneinstellungen** Die Facebook APIs ermöglichen es den Anwendungen, Nutzereinstellungen zu ignorieren. Hat ein Nutzer z. B. in seinen globalen Einstellungen den Zugriff auf das Geburtsdatum untersagt, fügt dann aber seinem Profil eine Kalender-App hinzu und lässt dort unbemerkt den Zugriff auf das Geburtsdatum zu, so ignoriert die Anwendung die globale Einschränkung. Damit werden anderen Nutzern Daten sichtbar, die sie direkt nicht ansehen dürfen.
- **Mangelnde Kontrolle durch den Nutzer** Nach der Installation einer Anwendung kann der Nutzer nur einige der Berechtigungen wieder entfernen. “Send me email”, “Access my profile information”, “Access my friends’ information” und “Access my photos and videos” können nicht entfernt werden.
- **Bewusste Täuschung** Erfolgreiche Anwendungen werden oft in Funktion und Namen nachgeahmt (z. B. Namenszusatz “2”, “Plus” oder “Free”), um fremden Erfolg auszunutzen und mehr Nutzerdaten zu sammeln. Ein Bewertungssystem auf Basis von Nutzer- und Expertenmeinungen, das davor warnen könnte, existiert nicht.

Facebook ist zudem mit der Gestaltung seines neuen App-Zentrums in die Kritik deutscher Verbraucherschützer geraten. Nach Auffassung des Verbraucherzentrale Bundesverbandes verstößt Facebook damit sowohl gegen das Telemediengesetz als auch gegen das Gesetz gegen den unlauteren Wettbewerb.<sup>31</sup> Denn Facebook gibt persönliche Daten an die App-Anbieter weiter, ohne vor der Installation einer Anwendung eine explizite Zustimmung der Nutzer einzufordern.

Facebook hat inzwischen Neuerungen in die Verwaltung der Privatsphäreneinstellungen eingeführt, die für mehr Klarheit sorgen können, aber an der grundlegenden Problematik der App-Zugriffsrechte wenig ändern. Beispielsweise fragen jetzt viele Apps (aber nicht Spiele-Apps) in separaten Anfragen beim Nutzer nach, um Zugriff auf die öffentlichen Daten wie Freundeslisten und E-Mail-Adresse und dem Recht zum Posten auf der Pinnwand von Freunden zu bekommen.<sup>32</sup> So genannte “Privacy Shortcuts” über eine Toolbar ermöglichen das direkte Kontrollieren und Ändern von Privatsphäreneinstellungen, ohne dass der Nutzer die aktuell aufgerufene Seite verlassen muss.

#### 2.4.1 Mögliche Auswirkungen der App-Zugriffrechte

Facebooks “Open Graph Protocol” ermöglicht den von den Nutzern autorisierten Anwendungen, umfangreiche Datenabfragen zu stellen, so dass sie u. U. auch auf solche Daten schließen können, zu denen die Nutzer keinen direkten Zugriff gewähren (“Inference Attack”) [AAF11]. Die Ursachen dafür liegen darin, dass die Beziehungen zwischen den zugänglichen und nicht-zugänglichen Nutzerdaten durch das einfache Berechtigungsschema nicht erfasst werden und Facebooks Datenschnittstelle nicht auf Datenvermeidung optimiert wurde, sondern zusätzlich viele Metadaten (Zeitangaben, Kommentare, verlinkte Daten anderer Nutzer etc.) preisgibt.

Eine Anwendung könnte z. B. auf den von einem Nutzer verborgenen Geburtstag schließen, indem sie ein Jahr lang den Strom an Nachrichten und Statusmeldungen auf Glück-

<sup>30</sup>Siehe <http://www.mywot.com>

<sup>31</sup>vzby legt erneut Klage gegen Facebook ein (6.12.2012), siehe [http://www.surfer-haben-rechte.de/cps/rde/xchg/digitalrechte/hs.xsl/75\\_2404.htm?back=index.htm&backtitle=Startseite](http://www.surfer-haben-rechte.de/cps/rde/xchg/digitalrechte/hs.xsl/75_2404.htm?back=index.htm&backtitle=Startseite)

<sup>32</sup>Facebook developers: Providing People Greater Clarity and Control (12.12.2012), siehe <https://developers.facebook.com/blog/post/2012/12/12/providing-people-greater-clarity-and-control/>

wünsche analysiert, da Facebook jede Nachricht mit Datum versieht. Vermutlich gleichen nur wenige Nutzer die selbst erzeugten Informationen laufend mit ihren Privatsphäreinstellungen ab. Sie können mittels Berechtigungsvergabe ohnehin nicht kontrollieren, was andere Nutzer über sie preisgeben. So sind die konkreten Auswirkungen der Privatsphäreinstellungen auf sich und andere Nutzer ohne geeignete technische Metriken zumeist nicht überschaubar.

Interessant ist aber, dass Facebook das “Open Graph Protocol” in Form einer intelligenten Suchfunktion namens “Graph search” auch seinen privaten Nutzern zur Verfügung stellt,<sup>33</sup> so dass die Nutzer auch Antworten auf semantische Fragen wie “Restaurants in Berlin, die meine Freunde besucht haben” bekommen können. Facebook betont, dass nur solche Informationen sichtbar werden, welche mit den Privatsphäreinstellungen der einzelnen Nutzer übereinstimmen. Zudem würden die Nutzer auf neue vereinfachte Kontrollmöglichkeiten der Privatsphäreinstellungen hingewiesen.

#### **Hinweis für Nutzer**

Haben Sie ein Auge auf Drittanbieter-Anwendungen, die Sie Ihrem Profil hinzufügen können. Häufig möchten diese Anwendungen unnötigerweise auf viele Ihrer persönlichen Daten zugreifen, und auch auf die Ihrer Kontakte. Auch Anwendungen bei Ihren Kontakten können unter Umständen Ihre Daten auslesen. Prüfen Sie Ihre Privatsphäre-Einstellungen in diesem Punkt besonders genau. Ändern Sie die Voreinstellungen oder deaktivieren Sie die Anwendungen, wenn sie sich und ihre Kontakte vor einer unerwünschten Datenweitergabe schützen möchten.

## 2.5 Gesichts- und Bilderkennungsverfahren

Bildverarbeitungssoftware kann beinahe beliebige Bildinhalte mit anderen persönlichen Inhalten in sozialen Netzwerken verknüpfen. Dies könnte Informationen enthüllen, welche die Nutzer nicht mitteilen möchten.

Bei der Fülle von digitalen Fotoalben und Videos in sozialen Netzwerken und auf anderen Webseiten (z. B. YouTube) spielen die Verfahren der biometrischen Gesichtserkennung und des “Content-based Image Retrieval” (CBIR) aus der Forensik eine zunehmende Rolle bei der externen Auswertung von Profildaten. Bilder erlauben nämlich, Nutzerprofile untereinander und auch zwischen verschiedenen Diensten in Beziehung zu setzen, um weitere Informationen über Personen zu gewinnen. Persönliche Fotos können dabei als eine Art Pseudonym dienen, um beispielsweise verschiedene Nutzerprofile als zu einer Person gehörig zu identifizieren. Mittels CBIR können zudem weitere Bildmerkmale wie Hintergrund oder sichtbare Gegenstände mittels großer Datenbanken identifiziert werden, um z. B. den Aufnahmeort zu bestimmen, Personen zu deanonymisieren und kompromittierende Informationen zu sammeln [Hog07]. Dies ist nicht nur für die automatischen erkennungsdienstlichen Verfahren der Strafverfolgung interessant,<sup>34</sup> sondern auch für andere Betreiber und Angrei-

<sup>33</sup>Facebook – Expanding Graph Search Beta, siehe <http://newsroom.fb.com/News/660/expanding-Graph-Search-Beta>

<sup>34</sup> Siehe <http://www.heise.de/newsticker/meldung/FBI-will-Gesichtserkennung-zum-Abgleich-mit-oeffentlichen-Daten-nutzen-1660162.html>

fer, die sich mit unerwünschter Werbung, Veröffentlichung, Stalking oder Erpressung gegen die Nutzer richten. Eine zentrale Speicherung biometrischer Daten ist an sich schon ein Sicherheitsrisiko, da es ein attraktives Ziel für Hackerangriffe darstellt.<sup>35</sup>

### 2.5.1 Tagging von Bildern in Facebook

Facebook hat die Gesichtserkennung in Bildern der Nutzer Mitte 2011 zunächst standardmäßig aktiviert, was selbst in den USA umstritten ist.<sup>36</sup> Mit dieser Funktion ist es Nutzern möglich, Freunde auf hochgeladenen Fotos zu markieren und zu identifizieren, Metadaten wie Personennamen, Profil-Links und E-Mail-Adressen in die Bilder einzufügen, selbst dann, wenn die Bilder nicht zu ihrem Profil gehören. Es können auch Daten über Personen eingefügt werden, welche nicht Nutzer von Facebook sind. Zudem transportieren die Foto-Tags Informationen, die Dritte zum Nachteil der Nutzer verwenden können. So existieren bereits Verfahren, welche die Tags auswerten können, um persönliche Eigenschaften und Vorlieben der Nutzer zu bestimmen [PCRA12].

Nach heftiger Kritik europäischer Datenschützer hat Facebook seine Gesichtserkennungsfunktion für Europa im September 2012 deaktiviert.<sup>37</sup> Datenschützer hatten u. a. kritisiert, dass eine Datenbank mit biometrischen Merkmalen von Millionen Nutzern ein immenses Risiko- und Missbrauchspotenzial berge.

Facebook betont jedoch weiterhin, dass die Funktion aus Sicht des Unternehmens konform mit europäischen Datenschutzbestimmungen sei und macht auch kein Geheimnis daraus, die in der geplanten europäischen Datenschutzverordnung vorgesehenen Bestimmungen wie etwa das “Recht auf Vergessen” und “Privacy by Default” durchweg abzulehnen.<sup>38</sup> Mit der Deaktivierung in Europa ist das Problem also nicht aus der Welt geschafft. Es ist nicht auszuschließen, dass künftig die Gesichtserkennungsfunktion in Europa unter abgeänderten Bedingungen wieder angeboten wird.

#### **Hinweis für Nutzer**

Wer die Kontrolle darüber behalten möchte, ob er auf Bildern identifiziert werden kann, sollte sich das Hochladen seiner Fotos in soziale Netzwerke gut überlegen. Zudem ist das Hochladen von Fotos, die Dritte abbilden, ohne deren Einwilligung unzulässig. Um Verstöße gegen das Persönlichkeitsrecht zu vermeiden, muss daher eine Einwilligung vorliegen, bevor ein Foto, das Dritte abbildet, in ein soziales Netzwerk hochgeladen wird.

<sup>35</sup>Vgl. das BSI-Register aktueller Gefährdungen, siehe [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS\\_001.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS_001.pdf)

<sup>36</sup>Siehe <http://www.heise.de/newsticker/meldung/US-Senator-will-gesetzliche-Regelung-fuer-Gesichtserkennung-1649167.html>

<sup>37</sup>Office of the Data Protection Commissioner, Ireland: Facebook Ireland Ltd – Report of Re-Audit, siehe [http://dataprotection.ie/documents/press/Facebook\\_Ireland\\_Audit\\_Review\\_Report\\_21\\_Sept\\_2012.pdf](http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf)

<sup>38</sup>Facebook’s views on the EU Data Protection Regulation – 30th March 2012 (von Europe versus Facebook kommentierte Version), siehe [http://www.europe-v-facebook.org/FOI\\_Facebook\\_Lobbying.pdf](http://www.europe-v-facebook.org/FOI_Facebook_Lobbying.pdf)

## 2.6 Bestimmung des aktuellen Standorts

Soziale Netzwerke verarbeiten und verteilen Informationen über den Standort ihrer Nutzer.

Geo-soziale Netzwerke bieten ortsabhängige Dienste an, die reale Orts- und Zeitangaben mit Nutzern und Nutzerdaten verknüpfen und auswerten. Beispiele von geo-sozialen Diensten sind Foursquare, Google Places, Google Latitude, Facebook Orte und die mobile Anwendung von Twitter. Beispielsweise können Nutzer über eine Anwendung auf ihrem Mobiltelefon ihre Position melden (“user tagging”) und auf Interessantes hinweisen (“geotagging“), Fotos hochladen oder Freunde in ihrer Nähe auffinden. Gemäß ihren Privatsphäreneinstellungen werden diese Informationen dann für andere Nutzer des Netzwerks sichtbar.

Facebook zeichnet standardmäßig die GPS-Daten von Nutzern auf, die mit ihrem Smartphone Statusmeldungen oder Fotos posten oder anderen Nutzern ihren Standort mitteilen. Zudem arbeitet Facebook offensichtlich an einer App, welche auch ungeöffnet im Hintergrund den aktuellen Standort der Nutzer bestimmt, um besondere Dienste zu bieten (z. B. Lokalisierung von Freunden in der Nähe, insbesondere aber auch ortsbezogene Werbung).<sup>39</sup>

Nutzer könnten also auch gegen ihren Willen von sozialen Netzwerken und anderen Nutzern überwacht und verfolgt werden, wenn die entsprechenden Privatsphäreneinstellungen fehlen bzw. gar nicht gesetzt werden können. Auf Basis von automatisch oder willentlich erhobenen Daten können Bewegungsprofile erstellt und daraus Wohnort, Arbeitsplatz, Freizeit- und Reiseaufenthalte bestimmt werden.<sup>40</sup> Informationen über den Aufenthaltsort einer Person sind personenbezogene Daten, unterliegen damit dem BDSG und erfordern das Einverständnis des Benutzers [Ver12].

Anwendungen verstoßen gegen die Privatsphäre der Nutzer durch die unkontrollierte Auskunft über den Standort eines Nutzers zu einem spezifischen Zeitpunkt (Verletzung der “location privacy“), über die Abwesenheit eines Nutzers von einem spezifischen Standort (“absence privacy“), über die gleichzeitige Anwesenheit von Nutzern an einem Ort (“co-location privacy“) und über die aus den Angaben gefolgerte Identität des Nutzers (“identity privacy“). Daher könnten Personen selbst dann, wenn sie in geo-sozialen Netzwerken anonym auftreten, mittels Analyseprogramme oftmals doch erkannt werden. Um dies zu verhindern, müssen teilweise erst geeignete Lösungsansätze gefunden werden.[VFBJ11]

Leicht lassen sich alltägliche Beispiele konstruieren, in denen Personen anderen gegenüber nicht offenlegen möchten, dass sie an einem bestimmten Ort oder mit bestimmten Menschen zusammen gerade nicht am Arbeitsplatz oder in ihrer Wohnung sind.<sup>41</sup>

### Hinweis für Nutzer

Bei Google und Facebook kann die Ortserfassung deaktiviert werden, bei Diensten wie

<sup>39</sup>Douglas MacMillan: Facebook Is Said to Create Mobile Location-Tracking App (4.2.2013), siehe <http://www.bloomberg.com/news/2013-02-04/facebook-is-said-to-create-mobile-location-tracking-app.html>

<sup>40</sup>Grimme-Institut: Im Blickpunkt: Hier und jetzt im Netz, siehe <http://www.grimme-institut.de/imblickpunkt/pdf/imblickpunkt-hier-und-jetzt-im-netz.pdf>

<sup>41</sup>Vgl. den inzwischen eingestellten Dienst “Please Rob me“, der Twitter- und Foursquare-Meldungen automatisch scannte, um anzuzeigen, wann eine Person nicht zu Hause ist, siehe <http://techcrunch.com/2010/02/17/please-rob-me-makes-foursquare-super-useful-for-burglars>

Foursquare, die genau darauf beruhen, verständlicherweise nicht. Es besteht immer die Möglichkeit, dass andere Personen durch Statusmeldungen oder z. B. durch kommentierte Foto-Uploads (plus Metadaten) die Privatsphäre anderer verletzen. Keine der bekannten Anwendungen kann so konfiguriert werden, dass de-anonymisierende Informationen in jedem Fall vermieden werden.

### 3. GESTALTUNGSSPIELRÄUME ZWISCHEN PRIVATEN NUTZERN

Nutzer können durch soziale Netzwerke auch Nachteile in ihrem sozialen Umfeld erleiden, wenn sich Konfliktsituationen zu anderen Nutzern einer Plattform ergeben. Der Dienstanbieter spielt hier zunächst eine zweitrangige Rolle.

#### 3.1 Ungewollte Veröffentlichungen

Nutzer veröffentlichen unter Umständen Inhalte, welche ihnen später Nachteile bereiten.

Felduntersuchungen dokumentieren unterschiedliche Szenarien, in denen Nutzer durch das ungewollte Veröffentlichen persönlicher Daten, z. B. Fotos oder Kurzmitteilungen, Nachteile erlitten haben. [WNK<sup>+</sup>11; Boy08; MB10] Häufige Gründe für negative Ergebnisse von Veröffentlichungen sind das falsche Konfigurieren von Empfängerkreisen, fehlerhaftes Einschätzen möglicher Wirkungen von Äußerungen, oder fehlendes Verständnis für die Verarbeitung und Verbreitung innerhalb und außerhalb der Plattform.

Als ausgewählte Beispiele seien hier erwähnt [WNK<sup>+</sup>11]:

- herabwürdigende Äußerungen gegenüber dem Arbeitgeber oder aus dem Arbeitsumfeld heraus, deren Folgen bis zur Kündigung reichen können<sup>42</sup>
- politische, religiöse oder weltanschauliche Äußerungen, welche unerwünschte Kritik oder Debatten auslösen, oder zwischenmenschliche Beziehungen beschädigen
- Veröffentlichen privater, sexueller Inhalte wie z. B. Fotos
- Inhalte, welche den persönlichen Konsum illegaler Rauschmittel und Alkohol zeigen
- negative, unangemessene, oder auch beleidigende Kommentare als Reaktion auf Veröffentlichungen anderer Nutzer
- ungewolltes Aufdecken von Verheimlichungen

Nach einer Studie der Landesanstalt für Medien NRW<sup>43</sup> haben 10 bis 20% der Jugendlichen zwischen 12 bis 24 Jahren sehr offene Privatsphäreneinstellungen und geben sehr viel von sich preis, insbesondere die jüngeren und formal niedriger gebildeten unter ihnen. Probleme im Bereich der Privatsphäre entstehen insbesondere dann, wenn Nutzer Daten über andere Nutzer veröffentlichen, ohne die Betroffenen um Erlaubnis gefragt zu haben. Gefordert wird neben einem stärkeren Engagement für den Jugendschutz durch die Betreiber auch eine größere “Medienproduzentenkompetenz” der Nutzer,<sup>44</sup> da man durch unachtsam eingestellte Inhalte sich selbst und andere in Gefahr bringen kann, siehe Abschnitt 3.3 über Cybermobbing.

<sup>42</sup>Beispielhaft sei hier der im Magazin “NY Daily News” dokumentierte Fall eines Mitarbeiters einer Baseball-Mannschaft erwähnt, siehe <http://www.nydailynews.com/news/national/pittsburgh-pirate-pierogi-mascot-fired-bashing-team-facebook-page-article-1.180649>

<sup>43</sup>Zusammenfassung der Studie “Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen” siehe [http://www.lfm-nrw.de/fileadmin/lfm-nrw/Forschung/Kurzzusammenfassung\\_Bd-71.pdf](http://www.lfm-nrw.de/fileadmin/lfm-nrw/Forschung/Kurzzusammenfassung_Bd-71.pdf)

<sup>44</sup>Beispielsweise von Seiten der Kommission für Jugendmedienschutz (KJM), siehe [http://www.kjm-online.de/de/pub/aktuelles/pressemitteilungen/pressemitteilungen\\_2012/pm\\_152012.cfm](http://www.kjm-online.de/de/pub/aktuelles/pressemitteilungen/pressemitteilungen_2012/pm_152012.cfm)

### 3.1.1 Mangelnde Nutzerfreundlichkeit der sozialen Netzwerke

Auch wenn die beschriebenen Probleme nicht spezifisch für die Nutzung von sozialen Netzwerken sind und auch in der physischen, zwischenmenschlichen Alltagskommunikation auftreten, so gibt es vermehrt Hinweise, dass sie durch die technische Ausgestaltung der sozialen Netzwerke befördert werden. So bemängeln Nutzer in Feldstudien die mangelnde Nutzerfreundlichkeit der Bedienoberfläche, oder die schwierig zu überschauende Verbreitung ihrer Daten auf Basis der gewählten Privatsphärekonfiguration. [WNK<sup>+</sup>11] Die in der Öffentlichkeit breit diskutierte Fälle von Einladungen zu privaten Veranstaltungen, welche versehentlich öffentlich zugänglich waren, sind in der Regel auf Softwarebedienfehler zurückzuführen<sup>45</sup>.

Andere empirische Untersuchungen üben fundamentalere Kritik an den technischen Konzepten sozialer Netzwerke. So wird beispielsweise die prinzipielle Eignung der gruppenbasierten Zugriffskontrollen vieler Plattformen in Frage gestellt. [KBM<sup>+</sup>11]

### 3.1.2 Gegenmaßnahme: Beachtung von sozialen Rollen

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 eines Studenten Sorgen, ob ihre Studienbeihilfe richtig investiert ist. Auch muss der (zukünftige) Chef nicht unbedingt wissen, in welchen Nachtclubs ein Profilinehaber seine Wochenendnächte verbringt.

Problematisch ist an dieser Stelle, dass aktuelle soziale Netzwerke mit wenig Aufwand nur *eine* soziale Rolle abbilden können, also z. B. “Student”, “Sohn/Tochter”, “Arbeitskollege”, “Familienvater/-mutter” oder “ehemaliger Schulfreund”.

Ein Beispiel: Ein Nutzer möchte auf einer Plattform Fotos seines letzten Urlaubs verbreiten. Er möchte aber nicht, dass die eigenen Arbeitskollegen diese sehen können. Wenn er allerdings einige Arbeitskollegen neben z. B. Kommilitonen, Vereinsfreunden und Schulfreunden bereits zu seiner Kontaktliste hinzugefügt hat, dann muss er einigen Aufwand betreiben speziell für sein neues Urlaubsfotoalbum diesen Personenkreis wieder einzuschränken.

Jeder Nutzer sollte darüber nachdenken, sich selbst bei der Verwendung *einer* Plattform auf möglichst *eine* Rolle zu beschränken und diese vorher selbst zu definieren. Für eine andere Rolle kann beispielsweise ein anderer Dienst genutzt werden.

#### **Hinweis für Nutzer**

Wählen Sie für einen Dienst immer nur eine Rolle, in der Sie diesen nutzen möchten. Geben Sie nur entsprechend dieser Rolle Daten preis und wählen Sie entsprechend Ihre Kontakte aus, die Zugriff auf Ihre privaten Daten haben sollen. Alternativ können Sie auf die Rollenwahl verzichten und insgesamt nur wenig Daten in den Diensten preisgeben.

<sup>45</sup>Der unter <http://www.ftd.de/panorama/kultur/:fehler-bei-facebook-thessas-unvergessliche-party-die-sie-nie-wollte/60061061.html> einsehbare Artikel der Financial Times Deutschland beschreibt z. B. die Ursache der sog. “Thessa-Geburtstagsparty”

### 3.1.3 Gegenmaßnahme: Schutz der eigenen Privatsphäre

Nach der Neuanmeldung ist ein Plattformprofil in der Regel sehr offen konfiguriert. Daher sollte man als Nutzer grundsätzlich erst die Privatsphäreneinstellungen konfigurieren und erst danach private 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, sollte man kritisch abwägen, ob eine Angabe einem wirklich soviel Nutzen bringt und wie privatsphärenrelevant sie ist.

#### **Hinweis für Nutzer**

Überprüfen Sie nach einer Neuanmeldung zunächst die Privatsphäreneinstellungen und passen Sie diese umgehend nach den eigenen Bedürfnissen an. Unklare Einstellmöglichkeiten sollten möglichst restriktiv konfiguriert werden. Um sicher zu gehen, dass die eigene Konfiguration korrekt ist, können Bekannte, Freunde oder Arbeitskollegen gefragt werden, wie viel sie von den persönlichen Daten sehen können. Damit können Fehler frühzeitig erkannt und unangenehme Überraschungen vermieden werden.

Zur Kontrolle der eigenen Einstellungen, besteht auch die Möglichkeit, die eigene Chronik aus der Sicht eines Freundes anzusehen. Dazu muss man in der Chronik unter "Aktivitätenprotokoll" die Funktion "Anzeigen aus der Sicht von" anklicken. Anschließend erscheint ein Freifeld, in welches der Name eines Freundes eingegeben werden kann.

## 3.2 Urheberrechte und Impressum

Nutzer können in sozialen Netzwerken leicht gegen das Urheberrecht verstoßen. Persönlichkeitsrechte Dritter dürfen aber auch in sozialen Netzwerken nicht beeinträchtigt werden.

Das Teilen fremder Inhalte in sozialen Netzwerken kann teuer werden, wenn der User dadurch fremde Rechte verletzt. So machte im Jahr 2012 eine Abmahnung, die ein Nutzer erhielt, weil ein Freund ein Gummienten-Foto auf seine Facebook-Pinnwand hochgeladen hatte, Schlagzeilen.<sup>46</sup>

Urheberrechtsverstöße können entstehen, wenn man fremde Grafiken, Fotos, Videos, Musik oder Texte ohne die Erlaubnis des Rechteinhabers teilt. Ob ein Verstoß vorliegt, hängt u. a. davon ab, wie man fremden Inhalt präsentiert. Wer z. B. ein Foto einscannt oder aus dem Internet kopiert und ohne die Erlaubnis des Rechteinhabers auf der eigenen Webseite (z. B. im Blog oder in einem sozialen Netzwerk) postet, hat damit eine unzulässige Vervielfältigung und öffentliche Zugänglichmachung begangen. Dies gilt auch für Vorschaubilder neben Hyperlinks, außer der Zielseitenbetreiber erklärt sich durch "Share Buttons" einverstanden. Auch durch "Embedding" bzw. "Framing" werden Inhalte beim Anklicken

<sup>46</sup>Benedikt Fuest: Abmahnung wegen Ente auf Facebook-Pinnwand, siehe <http://www.welt.de/wirtschaft/webwelt/article106168945/Abmahnung-wegen-Ente-auf-Facebook-Pinnwand.html>



von externen Servern aufgerufen und in die eigene Webseite integriert. So wird der Inhalt zwar nicht kopiert, aber evtl. unzulässig öffentlich zugänglich gemacht.

#### **Hinweis für Nutzer**

Unproblematisch ist das Setzen eines Hyperlinks zum Wechsel auf eine fremde Webseite, sofern diese Seite keinen rechtswidrigen Inhalt enthält. Fragwürdigen Inhalt sollte man sicherheitshalber nicht verlinken oder sich zumindest ausdrücklich davon distanzieren.

### 3.2.1 Veröffentlichung von Fotos oder Abbildungen anderer Personen

Persönlichkeitsrechte Dritter dürfen durch Nutzeraktivitäten in sozialen Netzwerken nicht beeinträchtigt werden. Fotos von Personen sollten niemals veröffentlicht werden, ohne die Einwilligung der abgebildeten Personen einzuholen.<sup>47</sup> Hierbei muss die abgebildete Person nicht direkt zu erkennen sein. Es genügt, wenn sich die Erkennbarkeit der abgebildeten Personen durch eindeutige Merkmale ergibt. Im Einzelfall kann auch das Setzen eines Links auf Privatfotos in einem geschäftlichen Zusammenhang gegen Persönlichkeitsrechte des Abgebildeten verstoßen.<sup>48</sup>

#### **Hinweis für Nutzer**

Ist die betroffene Person nur Beiwerk auf einem Foto, z. B. läuft diese in Entfernung vor einem zu fotografierenden Gebäude vorbei oder ist Teil einer großen Menschenmenge, ist gemäß § 23 KunstUrhG eine Veröffentlichung erlaubt. Auf öffentlichen Veranstaltungen ist eher anzunehmen, dass Fotos von Personen im Rahmen der Berichterstattung veröffentlicht werden dürfen. Hier müssen die Gäste damit rechnen, fotografiert zu werden, z. B. auf einer Messe. Tagungen und Seminare sind jedoch keine öffentlichen Veranstaltungen. Die Teilnehmer sollten daher vor Veröffentlichung von Bildern um Ihre Einwilligung gebeten werden.

### 3.2.2 Verwendung von fremden Bildern und Texten

Grundsätzlich darf man Bilder nur dann veröffentlichen, wenn man auch die Rechte an ihnen besitzt. Ebenso ist sogenannte “Open Source Software”, “Shareware” oder “Freeware” nicht frei verwendbar. Das Fehlen eines Copyright-Zeichens bedeutet nicht, dass ein Werk frei benutzt werden darf, da es für den urheberrechtlichen Schutz an sich keine Rolle spielt.

Grundsätzlich dürfen gemäß § 62 UrhG keine Änderungen an Werken Dritter vorgenommen werden. Insbesondere ist die Entstellung eines Werkes nicht gestattet (§ 14 UrhG). Handelt es sich nicht um eine Entstellung, sondern um eine zulässige Veränderung oder sonstige Umgestaltung, so ist es nur dem Urheber erlaubt, diese Umgestaltung zu verwenden oder zu veröffentlichen (§ 23 UrhG). Eine zulässige Umgestaltung kann z. B. auch das Vergrößern von Lichtbildern zur besseren Wahrnehmbarkeit darstellen.

Es steht jeder Person aber offen, geschützte Werke als Vorlage zu wählen und daraus neue Werke zu erschaffen und zu veröffentlichen. Wichtig hierbei ist, dass aus dem alten Werk ein neues, selbstständiges Werk geschaffen wird und das Original dabei in den Hintergrund tritt (§ 24 I UrhG]. Dies erfordert allerdings wesentliche Änderungen.

<sup>47</sup>Vgl. § 22 KunstUrhG: “Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. [...]”, siehe [http://www.gesetze-im-internet.de/kunsturhg/\\_23.html](http://www.gesetze-im-internet.de/kunsturhg/_23.html)

<sup>48</sup>Vgl. die Urteile des LG Frankfurt/Main, 2/03 O 468/05 und des OLG München, 18 U 2076/07

**Hinweis für Nutzer**

Dokumente und Bilder enthalten oftmals zusätzliche Informationen (“Metadaten”), die man auf den ersten Blick nicht wahrnimmt. Bilder enthalten Informationen über die Kamera, den Zeitpunkt der Aufnahme, möglicherweise den Standort und vieles mehr. Dokumente beinhalten oft Namen von Personen, Abteilungen, Bearbeiter, Zeitpunkt der letzten Änderungen usw. Angreifer könnten diese Daten für Social Engineering Angriffe verwenden. Daher sollten unnötige Informationen aus Dokumenten entfernt werden.

**3.2.3 Verwendung von Zitaten und Links**

Bilder und Texte anderer können gemäß § 51 UrhG in Form von Zitaten verwendet werden. Ein Zitat bildet eine Schranke des Urheberrechts und gestattet es, ein Bild ohne Einwilligung des Rechteinhabers zu vervielfältigen, zu verbreiten oder öffentlich wiederzugeben. Voraussetzung hierfür ist, dass die Nutzung in ihrem Umfang durch einen besonderen Zweck gerechtfertigt ist. Das Urhebergesetz nennt hier als eine Möglichkeit die Verwendung von Bildern in einem eigenen, wissenschaftlichen Werk. Voraussetzung ist, dass es als Grundlage für selbstständige Ausführungen dient. Auch Textzitate fallen wie Bildzitate unter die Regelungen des § 51 UrhG. Texte dürfen in Teilen zum Zwecke der Berichterstattung oder zur Verwendung in einem eigenständigen Sprachwerk verwendet werden.

Wenn bei Veröffentlichungen im Internet Hyperlinks verwendet werden, um auf fremde Inhalte zu verweisen, sollte deutlich sein, dass der Inhalt nicht der eigene ist. Wird Inhalt dagegen “zu eigen gemacht”, beispielsweise durch einen umschreibenden Text oder eine grafische Einbettung in der Web-Seite (“Framing”), dann kann das Verlinken so interpretiert werden, als handele es sich um eigenen Inhalt. Dazu braucht man jedoch die Zustimmung des Rechteinhabers. Es sollte also jede Verlinkung vermieden werden, die den Eindruck erweckt, der referenzierte Inhalt sei der eigene.

**Hinweis für Nutzer**

Handelt es sich bei der gewünschten Veröffentlichung nicht um eigene Inhalte, dann muss man vor der Verwendung die Zustimmung des Rechteinhabers einholen (z.B. von Verlagen, Fotografen, Autoren). Wenn möglich sollte man die Zustimmung des Rechteinhabers dokumentieren.

Bei Zitaten sollte immer auf eine korrekte Zitierweise unter Nennung des Autors und der Quelle geachtet werden. Soweit möglich sollte man Links zu den gewünschten Inhalten verwenden.

**3.2.4 Wann ein Impressum notwendig wird**

Unter einem Impressum versteht man eine rechtlich vorgeschriebene Herkunftsangabe in Publikationen. Ursprünglich bezogen sich diese Herkunftsangaben auf Printmedien wie zum Beispiel Bücher, Zeitungen und Zeitschriften. Mittlerweile bezieht sich die Impressumspflicht aber auch auf Veröffentlichungen im Internet, so dass “geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien” einen Herkunftshinweis enthalten müssen. Von der Impressumspflicht ausgenommen sind nach herrschender Meinung nur diejenigen Web-Auftritte, die ausschließlich privaten und/oder familiären Zwecken dienen.

Die allgemeinen Informationspflichten, die bei einem Web-Auftritt zu nennen sind, enthält § 5 TMG.<sup>49</sup> Darin heißt es, dass Unternehmen die wichtigsten Informationen wie vollständige Unternehmensbezeichnung, Registereinträge, Anschrift, verantwortliche Stellen, Kontaktmöglichkeiten und weiteres ständig verfügbar bereithalten müssen. Dies gilt auch in Diensten von sozialen Netzwerken wie Facebook, in denen das Unternehmen vertreten ist. Soweit möglich sollte die Haftung für Hyperlinks im Impressum ausgeschlossen werden.

Im August 2011 bestätigte das Landgericht Aschaffenburg die Impressumspflicht auch für nicht zu ausschließlich privaten und/oder familiären Zwecken genutzten Social Media-Auftritte. Im konkreten Fall bestätigte das Landgericht Aschaffenburg die Notwendigkeit eines Impressums für eine zu Marketingzwecken genutzten Facebook-Seite. Wie genau das Impressum wirksam in der Facebook-Seite einzubringen ist, hat das Landgericht Aschaffenburg nicht ausgeführt. Jedoch vertritt es die Meinung, dass sich das Impressum nicht direkt auf der Facebook-Seite befinden muss. Eine Verlinkung auf das Impressum der eigenen Web-Seite reicht aus, darf sich aber auf der Facebook-Seite laut des Landgerichts Aschaffenburg nicht unter “Info” befinden.

Wie aktuell das Thema ist, zeigt die Abmahnwelle gegen Betreiber von Facebook-Seiten, deren Impressum in der mobilen Version des Sozialen Netzwerks nicht deutlich genug zu erkennen ist.<sup>50</sup>

Seit dem Urteil des Landgerichts Aschaffenburg werden einige Impressum-Apps angeboten, mit denen man ein Impressum auf Facebook leicht erkennbar einbinden kann. Diese Apps können daher sehr hilfreich sein. Es sollte aber dennoch überprüft werden, ob durch die Nutzung einer solchen Anwendung alle an das Impressum gestellten Voraussetzungen erfüllt werden.

#### **Impressum bei der beruflichen Nutzung**

Ein Impressum ist bei beruflicher Nutzung einer Seite in einem sozialen Netzwerk immer notwendig. Das Impressum oder ein direkter Link auf das Impressum muss leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein. Die Anzeige von Inhalten auf mobilen Endgeräten kann von der normalen Anzeigeform abweichen. Bitte überprüfen Sie Ihre Lösung daher auch darauf, ob die Voraussetzungen an das Impressum auch auf mobilen Endgeräten erfüllt sind.

### 3.3 Cybermobbing

Nutzer können durch Inhalte anderer Nutzer in sozialen Netzwerken bewusst herabgewürdigt, belästigt, bedroht oder bloßgestellt werden.

Soziale Netzwerke sind ein beliebtes Werkzeug für Cybermobbing (eng. Cyberbullying), also dem gezielten Herabwürdigen, Verleumden und Diffamieren, Bloßstellen oder gar Be-

<sup>49</sup>§ 5 “Allgemeine Informationspflichten” Telemediengesetz, siehe [http://www.gesetze-im-internet.de/tmg/\\_5.html](http://www.gesetze-im-internet.de/tmg/_5.html)

<sup>50</sup>Zeit Online: 3.000 Euro Strafe für verstecktes Impressum, siehe <http://www.zeit.de/digital/internet/2013-07/abmahnung-facebook-impressum-mobil>

drohen von Personen im Web 2.0.<sup>51</sup> So lassen sich viele Funktionen sozialer Netzwerke zu diesem Zweck missbrauchen, wie z. B. Fotoalben, Gruppenfunktionen und Benachrichtigungsfunktionen. Täter können dabei weitestgehend aus der Anonymität heraus agieren. Als Beispiel sei hier das Bilden von so genannten “Hassgruppen” erwähnt, in denen ein Personenkreis gemeinschaftlich Einzelpersonen mobbt, oder auch das vom Betroffenen ungewollte Veröffentlichen herabwürdigender Videos oder Fotos. [Kat11] Nach vorsichtigen Schätzungen werden etwa 10 bis 15% der deutschen Jugendlichen wiederholt Opfer von Cybermobbing. [SMKM12]

Neuere Untersuchungen zeigen allerdings, dass Cybermobbing seltener vorkommt als Mobbing in der realen Welt und von den Betroffenen auch nicht unbedingt als schlimmer empfunden wird. Bei den Tätern handelt es sich häufig um dieselben aus dem persönlichen Umfeld bekannten Personen, wobei das Medium (Online vs. Physische Welt) keine so große Rolle spielt wie die Art und Weise des Mobbing: Anonyme Täter und hohe Sichtbarkeit der Auswirkungen werden als verletzender empfunden als persönliche private Schikanierungen. [SP12b], [SRAP13]

Relativ harmlos erscheinen die Spotted-Seiten auf Facebook (von engl. “to spot”: bemerken, erkennen), die besonders an Universitäten beliebt sind. Sie dienen dazu, anonyme Nachrichten und Anfragen zu posten bzw. diese zu kommentieren, z. B. um eine beobachtete Person kennenzulernen oder diese zumindest zu identifizieren. Jeder kann Hinweise geben und die gesuchte Person outen, auch ohne deren Wissen oder Einwilligung. Unklar ist noch, wie hoch das Missbrauchspotential solcher neuen Funktionen ist, und wie überhaupt die bestehende Datenschutzbestimmungen darauf angewandt werden könnten.<sup>52</sup>

Facebook startete Mitte Januar 2013 eine Initiative gegen Mobbing, auf deren Plattform sich die Nutzer austauschen und zu Gruppen zusammenschließen können.<sup>53</sup> Der EU-Initiative “klicksafe” geht das nicht weit genug. Sie erwartet von den Betreibern sozialer Netzwerke benutzerfreundliche Meldefunktionen, um Cyber-Mobbing-Vorfälle zu melden, und das Löschen beleidigender und regelwidriger Inhalte.<sup>54</sup>

### Hinweis für Nutzer

Online, genauso wie offline, gelten gesetzliche Regelungen, die ein friedliches Miteinander regeln. Beleidigungen, üble Nachreden, Verleumdung sind gleichfalls strafbar (vgl. §§ 185, 186, 187 StGB). Achten Sie daher auf einen respektvollen Umgang und unterlassen Sie möglicherweise strafbare Handlungen und Aussagen, z. B. auch Verlinkung auf strafbare Inhalte, auch dann, wenn Sie einen anonymen Account haben.

<sup>51</sup>Das Deutsche Institut für Internationale Pädagogische Forschung bietet dazu eine umfangreiche Literaturliste unter [http://www.wiki.bildung-schadet-nicht.de/images/archive/f/f7/20100414061437!Literaturliste\\_zum\\_Thema\\_Cyber-Bullying.pdf](http://www.wiki.bildung-schadet-nicht.de/images/archive/f/f7/20100414061437!Literaturliste_zum_Thema_Cyber-Bullying.pdf) an.

<sup>52</sup>Andrea Jenewein: Datenschutzbeauftragter warnt vor “Spotted”-Seiten (30.1.2013), siehe <http://www.stuttgarter-nachrichten.de/inhalt.trend-im-internet-datenschutzbeauftragter-warnt-vor-spotted-seiten.f5ab906b-1a66-496b-9299-3c200b984bd4.html>

<sup>53</sup>Facebook: Sei mutig. Stopp Mobbing. Siehe <https://www.facebook.com/seimutigstoppmobbing>

<sup>54</sup>klicksafe: Cybermobbing, siehe <http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/wie-kontaktiere-ich-service-anbieter>



## 4. NUTZER ALS ZIEL PROFESSIONELLER ANGRIFFE

Nutzer sind in sozialen Netzwerken auch Risiken durch professionelle Angreifer ausgesetzt, welche sich Lücken in der IT-Sicherheit zunutze machen, oder spezialisierte Techniken und Werkzeuge für großflächige oder gezielte Attacken einsetzen.

### 4.1 Cross-Site Scripting, Viren und Würmer

Schwachstellen in den Web-Anwendungen erlauben Angreifern die Verbreitung von Schadcode auf den Geräten, die Nutzer für den Zugang zu sozialen Netzen verwenden.

Die Nutzer rufen die Web-Dienste der sozialen Netzwerke über einen Webbrowser auf, der den Bedrohungen durch Malware ausgesetzt ist. So stellen Varianten herkömmlicher Angriffe für die Sicherheit sozialer Netzwerke eine Herausforderung dar. Besonders gilt dies für Cross-Site Scripting (XSS) Würmer — auch bekannt als Cross-Site Scripting Viren. Hierbei wird auf dem Zielsystem, z. B. im eigenen Profil oder anderen öffentlichen Bereichen, Schadcode eingebunden, der sämtliche Betrachter infiziert, sich selbständig auf deren Seiten repliziert und von dort wiederum weitere Besucher infiziert. Die Verbreitung kann aber ebenso über interne Kommunikationsfunktionen erfolgen.

Wie die Autoren in [FS09] feststellen, ist die Ausbreitungsrate herkömmlicher Würmer, insbesondere durch Überlastung von Routern und Plattformabhängigkeit, im Allgemeinen wesentlich geringer als bei XSS-Würmern. Studien zufolge sind etwa 80% aller Web-Anwendungen für XSS-Angriffe anfällig. [FS09] Auch im Umfeld sozialer Netzwerke lassen sich hierfür genügend Beispiele finden wie der MySpace-Wurm Samy, der bereits im Jahr 2005 aufgetreten ist und binnen 20 Stunden über eine Million Profile infiziert hat, oder der Wurm Koobface, der sich 2008 in Facebook ausgebreitet hat.

Überdies sind soziale Netzwerke auch Bedrohungen durch Malware ausgesetzt, wie ein “Malvertising-Angriff” Ende 2011 in Facebook demonstriert. Bei einem solchen Angriff werden auf Drittanbieter-Anwendungen bösartige Werbebanner platziert, die den Nutzer mehrfach über verschiedene Banner hinweg weiterleitet und ihn schließlich auf eine Seite führt, die gängige Schwachstellen z. B. in Java, ActiveX, PDF oder Flash ausnutzt. [Con11]

Die starke Verbreitung von XSS-Schwachstellen hängt damit zusammen, dass die meisten Web-Anwendungen Eingaben von Sonderzeichen nur unzureichend validieren und Angreifer somit das Einbinden von Schadcode ermöglichen. Die zuverlässige Filterung aller Eingaben ist aus dem Grund eine so anspruchsvolle Aufgabe, da es eine nahezu unbegrenzte Menge gefährlicher Eingabevarianten gibt<sup>55</sup> und die meisten Web-Sprachen außerdem keine ausgereiften Filterfunktionen anbieten. [FS09]

XSS Würmer können die Ausgangsbasis verschiedenster Angriffsszenarien sein. So können Angreifer unbemerkt auf vertrauliche Inhalte wie persönliche Nachrichten und Bilder zugreifen, Kontaktlisten der Opfer einsehen, Profileinstellungen ändern oder sämtliche Tastatureingaben protokollieren. [acu12] Ferner können Session Token für “Session Hijacking” gesammelt, “DDoS-Angriffe” initiiert oder auch Browser-Schwachstellen ausgenutzt werden.

<sup>55</sup>Siehe <http://hackers.org/xss.html> demonstriert die Vielfalt möglicher Eingabevarianten

**Hinweis für Nutzer**

Klicken Sie nicht ohne nachzudenken auf jeden Link, den Sie in E-Mails oder sonstigen Anfragen erhalten. Immer häufiger werden soziale Netze dazu verwendet, über Phishing an Zugangsdaten zu kommen oder Malware zu verbreiten. Malware kann bereits beim Aufrufen von manipulierten Webseiten über den Browser auf Ihren Computer gelangen.

**4.1.1 Wie ein Schadprogramm auf einen Heim-PC gelangt**

Ein Schadprogramm muss sich erst einmal auf dem Heim-PC einnisten, bevor es Schaden verursachen kann. Dazu lassen sich die Autoren solcher Programme allerlei Tricks einfallen.

Eine beliebte Vorgehensweise ist das Versenden von E-Mails, die einen Anhang mit dem Schädling enthalten. Um kein Misstrauen zu erwecken, sind diese E-Mails oft als persönliche Nachrichten oder als nützliche Programme getarnt. Das Ziel ist, den Nutzer dazu zu verleiten, das Programm im Anhang herunterzuladen und auszuführen. Schädlinge, die sich selbst tarnen und als harmloses oder gar nützliches Programm ausgeben, werden auch Trojanische Pferde oder kurz Trojaner genannt. Oft sind in den E-Mail-Anhängen keine ausführbaren Programme hinterlegt, sondern scheinbar harmlose PowerPoint- oder PDF-Dateien. Oft wird vorgegeben, es handele sich um Scherze oder wichtige Informationen. Beim Öffnen der Dokumente wird dann oft sogar Text angezeigt, im Hintergrund wird gleichzeitig der Schädling ausgeführt. Im Gegensatz zu einem Diebstahl auf öffentlichen Plätzen ist ein Angriff durch einen Schädling meistens keine gezielte Attacke auf Ihren Heim-PC, vielmehr wird versucht, möglichst viele PCs in kurzer Zeit anzugreifen.

Die meisten Nutzer haben das gleiche Betriebssystem (z. B. Windows) installiert. Es werden außerdem für bestimmte Aktivitäten nur eine Handvoll Programme auf sehr vielen Heim-PCs verwendet (z. B. der Adobe Acrobat Reader zum Anzeigen von PDF-Dateien und Microsoft PowerPoint für Bildschirmpräsentationen). Wenn ein Betriebssystem oder ein Programm einen Fehler hat, sind daher automatisch alle PCs betroffen, auf denen sie installiert sind. Zur Verbreitung von Schädlingen werden daher oft Fehler eines Programms ausgenutzt. Die PowerPoint- oder PDF-Dateien, die per E-Mail versendet werden, versuchen so, einen Schädling auf den PC einzuschleusen.

Nach diesem Prinzip arbeiten auch andere gefährliche Angriffe. Beispielsweise werden häufig Fehler in Browsern ausgenutzt, um Schädlinge in den PC einzuschleusen. Es genügt schon, eine präparierte Internetseite zu besuchen, die einen Fehler ausnutzt und der PC ist von einem Schädling befallen. Im Gegensatz zur Verbreitung per E-Mail ist hier keine Aktion des Nutzers nötig. Die Infektion geschieht quasi "im Vorbeigehen" und wird in Anlehnung dessen auch "Drive-by-Download" genannt. Seit einiger Zeit ist diese Verbreitungsmethode für Schädlinge die häufigste.

Wie man seinen PC gegen Angriffe schützt, kann man beispielsweise auf den Seiten der EU-Initiative "clicksafe"<sup>56</sup> und des BSI [https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/BasisschutzComputer/basisschutzComputer\\_node.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/BasisschutzComputer/basisschutzComputer_node.html) erfahren. Die folgenden Abschnitte beschreiben einige Grundregeln zum Schutz gegen Angriffe aus dem Internet.

**4.1.2 Gegenmaßnahme 1: Programme auf dem neuesten Stand halten**

Schadprogramme nutzen oft einen Fehler in einem bereits installierten Programm aus, um sich im Heim-PC einzunisten. Die Hersteller der Programme geben sich große Mühe, Fehler

<sup>56</sup>Siehe <http://www.klicksafe.de/themen/technische-schutzmassnahmen/den-pc-schuetzen>

in ihren Programmen zu finden und anschließend zu beheben. Regelmäßig erscheinen Aktualisierungen für Ihre Programme, die meistens neben der Fehlerbehebung das Programm auch gleich schneller und stabiler machen. Es ist also eine gute Idee, darauf zu achten, möglichst schnell Aktualisierungen für Ihre Programme zu installieren.

Die auf Heim-PCs gängigen Betriebssysteme Windows, Mac OS X und Linux haben bereits Programme eingebaut, die selbständig nach Aktualisierungen suchen und diese auch installieren. Da diese Betriebssysteme jedoch sehr umfangreich sind, dauert das Herunterladen und das anschließende Installieren der verfügbaren Aktualisierungen manchmal sehr lange, vor allem, wenn Ihre Internetverbindung nicht so schnell ist. Für den Schutz vor Schädlingen sind die Aktualisierungen aber sehr wichtig. Wenn Sie den Heim-PC gerade nicht benötigen, können Sie die Installation der Aktualisierungen starten und werden nicht davon gestört.

Generell ist es wichtig, dass Sie alle Internet-Programme immer auf dem neuesten Stand halten. Da diese Programme mit dem Internet kommunizieren, können Schädlinge bestimmte Fehler in diesen Programmen am leichtesten für eine Infizierung Ihres Heim-PCs benutzen. Zu diesen Programmen gehören zum Beispiel Adobe Flash, Adobe Acrobat Reader, ihr E-Mail-Programm usw.

Für die Aktivitäten in sozialen Netzwerken ist es besonders wichtig, dass der verwendete Browser auf dem neuesten Stand ist. Es empfiehlt sich, verfügbare Aktualisierungen für Ihren Browser sofort zu installieren. Das gilt auch für die installierten Programme der sozialen Netzwerke: Meist werden in regelmäßigen Abständen Fehlerbehebungen für diese Programme veröffentlicht.

#### **4.1.3 Gegenmaßnahme 2: Virenschutz-Programm installieren und auf dem neuesten Stand halten**

Durch Aktualisierungen beheben die Hersteller zwar bekannte Fehler, aber zwischen dem Bekanntwerden eines Fehlers und der Aktualisierung vergeht oft etwas Zeit, in der ein Schädling diesen Fehler ausnutzen kann. Aus diesem Grund ist es wichtig, dass ein Virenschutzprogramm auf dem PC installiert ist. Dieses Programm hat die Aufgabe, Schädlinge aufzuspüren und vom PC zu entfernen. Es läuft im Hintergrund und überprüft selbständig das Betriebssystem, die Programme und sogar die Anhänge von E-Mails.

Wie für alle anderen Programme gilt auch für Viren-Schutzprogramme, dass Sie es regelmäßig aktualisieren sollten. Die Hersteller der Viren-Schutzprogramme aktualisieren inzwischen in sehr kurzen Abständen ihre Programme, um neue Schädlinge aufzuspüren zu können. Wie bei den Betriebssystemen haben Viren-Schutzprogramme bereits die Möglichkeit eingebaut, selbständig Aktualisierungen herunterzuladen und zu installieren.

#### **4.1.4 Gegenmaßnahme 3: Firewall-Programm installieren und auf dem neuesten Stand halten**

Viele Schädlinge versuchen, sich über das Internet weiter zu verbreiten oder senden die eingesammelten Daten von befallenen Heim-PCs über das Internet zurück zum Angreifer. Für beide Fälle empfiehlt es sich, eine Firewall zu installieren. Ein Firewall-Programm ist dafür zuständig, alle Kommunikationsverbindungen zwischen dem PC und dem Internet zu überwachen. Normalerweise schottet das Programm den PC von allen von außen eingehenden Kommunikationsverbindungen ab. Deshalb können Schädlinge nicht mehr ohne Weiteres einen Fehler in einem Internet-Programm ausnutzen und so auf den PC gelangen.



Wenn auf dem PC mit einem Programm eine Verbindung in das Internet aufgebaut wird – beispielsweise durch das Aufrufen einer Internetseite mit einem Browser – prüft die Firewall diese Verbindung. Firewall-Programme arbeiten dabei nach festgelegten Regeln: Zum Beispiel ist dem Programm nach der Installation bekannt, dass ein bestimmter Browser Internetseiten ansteuern darf. Die meisten Firewalls können aber auch dazulernen. Wird ein neues Programm installiert und damit eine Verbindung in das Internet geöffnet, wird der Nutzer gefragt, ob er dies zulassen möchte. Erlaubt er es, werden auch alle zukünftigen Verbindungsversuche zugelassen.

Versucht ein Schädling jetzt, seine gesammelten Daten über das Internet zu versenden, geschieht das nicht mehr unbemerkt. Entweder, das Firewall-Programm blockiert die Verbindung sofort oder fragt den Nutzer, ob er/sie diese Verbindung zulassen will. Aus diesem Grund sollte sorgfältig bedacht werden, welchem Programm Zugang zum Internet gewährt wird.

#### 4.1.5 Gegenmaßnahme 4: Auf dem Heim-PC nur mit eingeschränkten Rechten arbeiten

Betriebssysteme bieten generell die Möglichkeit, mehrere Benutzerkonten einzurichten. Dies lässt sich zum Beispiel dazu verwenden, jedem Familienmitglied ein eigenes Benutzerkonto einzurichten, das jeder dann nach den eigenen Wünschen verwendet. Das Einrichten von Benutzerkonten wird mit Hilfe eines Benutzers erledigt, der auf dem Heim-PC alles darf: Der Administrator. Er darf Programme installieren, deinstallieren und generell auf alle Daten des Heim-PCs zugreifen. Nistet sich ein Schädling auf dem PC ein, während Sie als Administrator arbeiten, hat der Schädling die gleichen Rechte, das heißt, er darf praktisch alles.

Im Gegensatz zum Administrator darf ein Benutzerkonto mit eingeschränkten Rechten deutlich weniger: Er darf keine Programme installieren und deinstallieren. Außerdem ist nur ein Zugriff auf die eigenen Dateien erlaubt. Die Nutzung eines eingeschränkten Benutzerkontos hilft dabei, Schädlingen das Einnisten auf den Heim-PC und das anschließende Ausspionieren von Daten schwerer zu machen, da der Schädling oft gar nicht erst die nötigen Berechtigungen dazu besitzt.

#### **Checkliste für die wichtigsten Maßnahmen zum Schutz eines PC**

- Betriebssystem und die genutzten Programme (z. B. Browser) auf dem neuesten Stand?
- Programm der sozialen Netzwerke auf dem neuesten Stand?
- Viren-Schutzprogramm installiert, eingeschaltet und auf dem neuesten Stand?
- Firewall installiert, eingeschaltet und auf dem neuesten Stand?
- Nutzung eines Benutzerkontos mit eingeschränkten Rechten?

## 4.2 Man-in-the-Middle-Attacken

Die technischen Sitzungen zwischen Nutzer und Anbieter des sozialen Netzwerks sind aufgrund von Sicherheitsmängeln auf dem Übertragungsweg kompromittierbar, so dass

Angrifer die Profilinhalte der rechtmäßigen Nutzer ausspähen oder in deren Namen Aktionen durchführen können.

Die meisten sozialen Netzwerke sind anfällig gegen “Man-in-the-Middle”-Attacken auf Ebene des Datentransports, da die Kommunikation zwischen Nutzer und Dienstanbieter auf dieser technischen Ebene unterhalb der Anwendung meist nicht ausreichend gesichert ist [HMW<sup>+</sup>11]. Diese Angriffe werden im Kontext sozialer Netzwerke meist “Friend-in-the-Middle Attacks (FITM)” genannt und starten mit dem aktiven Abhören (“Eavesdropping”) des sozialen Netzwerks. Angreifer können dazu verschiedene Angriffsvektoren nutzen, z. B. “HTTP Hijacking”, “DNS Poisoning”, “Cross-Site Request Forgery (CSRF)”, Abhören eines ungeschützten WLAN und weitere [HMW<sup>+</sup>11]. Recht populär ist z. B. das Werkzeug “Firesheep”, welches das Übernehmen von Nutzersitzungen in ungeschützten WLAN-Netzwerken erlaubt, siehe Abbildung 2.

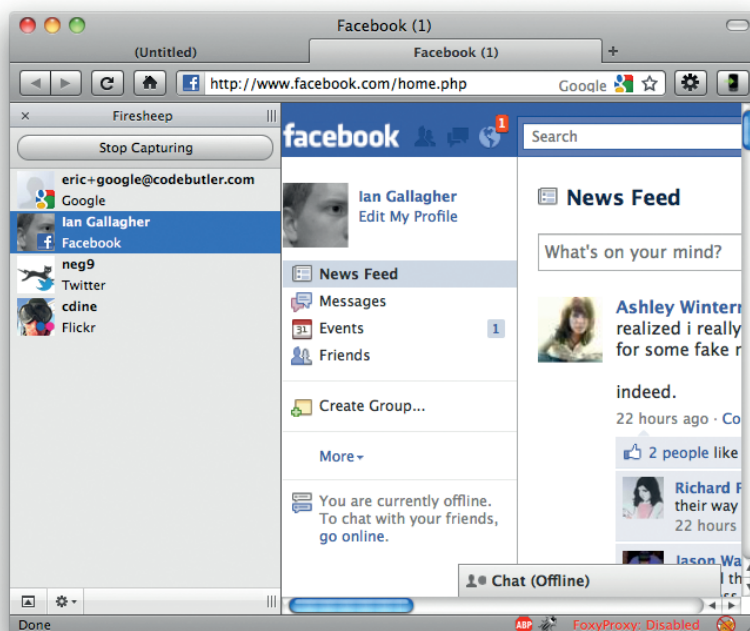


Abbildung 2. Nutzeroberfläche von Firesheep (Quelle: <http://codebutler.com/firesheep>)

Das Ziel des Abhörens ist das Stehlen von Sitzungsparametern (“Session Credentials”) einer bestehenden Kommunikationsverbindung zwischen Nutzer und Dienstleister. Der Angreifer verwendet anschließend diese Parameter als gültige Authentisierungstoken gegenüber dem Dienstanbieter und führt im Namen des rechtmäßigen Nutzers Aktionen durch.

#### 4.2.1 Warum FITM-Angriffe so erfolgreich sein können

Solche Angriffe sind vor allem deshalb erfolgreich, weil die meisten sozialen Netzwerke nicht durchgängig das sichere Internet-Kommunikationsprotokoll HTTPS einsetzen, sondern nur das ungeschützte HTTP. Ungeschützte HTTP-Sitzungen sind noch immer die Regel. So

verwenden Facebook, Orkut und LinkedIn das sichere HTTPS bisher standardmäßig nur zur Übertragung der Login-Daten, nicht für die anschließende Kommunikation. Facebook ermöglicht inzwischen HTTPS auch in der weiteren Kommunikation, standardmäßig allerdings nur in Nordamerika, in der übrigen Welt nur auf ausdrücklichen Wunsch des Nutzers (Opt-In). Ausschließlich XING, Twitter und Google+ unterstützen HTTPS vollständig.

Außerdem bieten die meisten sozialen Netzwerke einschließlich Facebook eine relativ einfache Registrierung für Drittanwendungen an, um in der Konkurrenz um neue attraktive Anwendungen keine zusätzlichen Hürden zu schaffen. Diese Drittanwendungen werden kaum einer Sicherheitsprüfung unterzogen.

FITM-Attacken ebnet den Weg für weitere Angriffsszenarien, z. B. das Eindringen in ein geschlossenes Netzwerk im Namen des Opfers (“Friend Injection”), das Extrahieren von Profilinghalten mittels einer Drittapplikation, z. B. einem Spiel mit verborgener Malware (“Application Injection”) und den Missbrauch der gewonnenen Informationen in Angriffen des “Social Engineering” wie etwa kontextbezogener Spam oder “Spear Phishing”.

#### 4.2.2 Gegenmaßnahme: Sichern der Kommunikation mit HTTPS

Als wichtigste Sicherheitsmaßnahme gegen FITM-Attacken sollte jegliche Kommunikation in sozialen Netzwerken mit HTTPS gesichert werden, was für die Dienstanbieter allerdings keine triviale Aufgabe darstellt, da sich hinter den Diensten meist komplexe über viele Domänen verteilte Web-Services verbergen. Der Nutzer könnte bis dahin bestimmte Browser-Erweiterungen einsetzen, die HTTPS zu erzwingen versuchen.<sup>57</sup> Mittels Datenschutzverstärkender Drittanwendungen (z. B. “FlyByNight”) kann die Kommunikation zwischen Nutzern kryptographisch gesichert werden. Umfassenden Schutz gegen FITM-Angriffe würde aber vermutlich nur eine neuartige technische Konzeption der sozialen Netzwerke auf Basis von “Privacy-by-Design” bringen. Die Dienstanbieter sehen bisher offenbar wenig wirtschaftlichen Anreiz für eine solche Verbesserung.

##### **Hinweis für Nutzer**

Nutzer sollten darauf achten, dass in allen Kommunikationsverbindungen zu sozialen Netzwerken durchgehend das verschlüsselte Web-Protokoll HTTPS verwendet wird, insbesondere bei der Dienstnutzung in öffentlichen, fremdadministrierten Netzwerken (Internetcafés, Bahnhöfen, Hotels oder anderen Einrichtungen). Bei den Plattformen LinkedIn und Facebook muss die HTTPS-Verschlüsselung separat im Profil aktiviert werden. Grundsätzlich sichert HTTPS ausschließlich die Kommunikationsverbindungen zwischen Nutzer und Dienstanbieter, schützt jedoch nicht gegen eine unrechtmäßige Datennutzung auf Seiten des Dienstanbieters, vgl. die Abschnitte 2.1 und 2.2.

### 4.3 Aggregation und Quervernetzung von Profildaten

Unternehmen nutzen Daten in sozialen Netzwerken für Personenauskünfte oder Statistiken.

<sup>57</sup>Siehe z. B. “HTTPS Everywhere” der Electronic Frontier Foundation, <https://www.eff.org/https-everywhere>

Nutzerprofile von sozialen Netzwerken können von Dritten durchsucht, heruntergeladen und für Zwecke verwendet werden, die vom Nutzer meist nicht vorgesehen sind. Arbeitgeber durchsuchen soziale Netzwerke nach potentiellen neuen Mitarbeitern oder zum Aussortieren von Bewerbern nach unliebsamen Eigenschaften [LK10]. Zwar können die Nutzer ihre Profile zumindest teilweise ändern oder löschen, sie können jedoch nicht wirksam verhindern, dass ihre Daten anderswo, z. B. bei einem potentiellen Arbeitgeber gespeichert und aufgehoben werden. Das Entfernen von personenbezogenen Daten auf fremden Webseiten gestaltet sich meist als sehr schwierig.<sup>58</sup>

Zunehmend versuchen Unternehmen den Markt, die Wirksamkeit ihrer Werbung oder ihr Image in der Bevölkerung mit Hilfe des “Social Media Monitoring” zu beobachten. Dazu werden Drittanbieter beauftragt, mit Hilfe von so genannten “Crawler”-Programmen soziale Netzwerke und andere Online-Quellen auf definierte Fragestellungen hin zu durchsuchen und die Ergebnisse in Form von Grafiken und Ergebnislisten bis hin zu Handlungsempfehlungen aufzubereiten.<sup>59</sup> Kritik bekommen weniger die Privatunternehmen, sondern diejenigen staatlichen Stellen, die solche “Überwachungssoftware” selbst nutzen möchten, “um auf Krisen und auf Besorgnisse der Bürger schnell und sachgerecht reagieren zu können”, als ginge es ausschließlich um “abstrakte Meinungsbilder ohne Personenbezug”.<sup>60</sup>

#### 4.4 Hintergrund- und Risikoprüfungen

Auskunfteien und Versicherungen nutzen Daten in sozialen Netzwerken für ihre Geschäftszwecke.

Daten in sozialen Netzwerken können Versicherungen und Kreditauskunfteien mit Informationen zu Versicherungs- und Kreditrisiken, oder auch nützliche Hintergrundinformationen zu tatsächlichen Versicherungsfällen liefern. Beispielhaft seien hier zwei Fälle kurz erläutert:

Das Hasso-Plattner-Institut (HPI) initiierte im Juni 2006 mit der SCHUFA das Forschungsprojekt “SCHUFALab@HPI”. Ziel war die Erforschung von Methoden zur “Validierung [...] und [...] Gewinnung von Daten” aus dem “Web” um “langfristig die Qualitätsführerschaft unter den Auskunfteien in Deutschland [zu] sichern”.<sup>61</sup> Das HPI hat das Projekt nach eigenen Angaben aufgrund umfangreicher Kritik durch Externe eingestellt.<sup>62</sup>

In den Vereinigten Staaten sind Daten aus sozialen Netzwerken ein zumindest teilweise akzeptiertes Beweismittel um Forderungen aus Versicherungsfällen durchzusetzen oder abzuwehren. Bekannt ist ein Fall vor einem Bundesgericht im US-Staat New Jersey bei dem der Versicherer anhand von MySpace- und Facebook-Nachrichten seiner Versicherungsnehmern nachweisen wollte, dass er nicht für Gesundheitsleistungen zum Kurieren einer Essstörung aufkommen muss. [Gal08]

<sup>58</sup>S. Gilbertson: Delete your bad web reputation, [www.wired.com/science/discoveries/news/2006/11/72063](http://www.wired.com/science/discoveries/news/2006/11/72063)

<sup>59</sup>Siehe <http://t3n.de/magazin/social-media-monitoring-deutschland-denn-wissen-nicht-226126>

<sup>60</sup>Siehe <http://www.heise.de/newsticker/meldung/Sachsen-will-Software-zur-Beobachtung-sozialer-Netze-einsetzen-1663567.html>

<sup>61</sup>Pressemitteilung des HPI zum Projektbeginn unter <http://www.hpi.uni-potsdam.de/presse/mitteilung/beitrag/hpi-und-schufa-starten-gemeinsames-web-forschungsprojekt.html>

<sup>62</sup>Pressemitteilung des HPI zur Projektkündigung unter <http://www.hpi.uni-potsdam.de/presse/mitteilung/beitrag/schufa-forschungsprojekt-gekuendigt.html>

## 4.5 Automatisierter Identitätsdiebstahl

Angriffsverfahren und großflächige Zugriffe auf private Daten der Nutzer von sozialen Netzwerken lassen sich automatisieren.

Arbeiten im französischen Forschungszentrum EURECOM haben gezeigt [BSBK09], dass sich Identitäten in sozialen Netzwerken in großem Maßstab kopieren oder imitieren lassen. Mit Hilfe des automatisch arbeitenden iCloner-Systems wurden in XING, StudiVZ, MeinVZ, Facebook und LinkedIn Profile geklont (“Profile Cloning”) und auch fiktive Profile registriert. Von den gefälschten Profilen wurden Freundschaftsanfragen versendet, die bei den geklonten Profilen in Facebook in den meisten Fällen (60%) angenommen wurden, auch wenn die Kontakte zum echten Profil bereits vorher bestanden hatten. Bei den Freundschaftsanfragen der fiktiven Profile betrug die Akzeptanzrate immerhin noch 30%. Von den gefälschten Profilen wurden anschließend unpersönliche Nachrichten mit undurchsichtigen Links an die Freunde versendet. Diese Links wurden zu 50% auch angeklickt. Dabei machte es kaum einen Unterschied, ob diese Nachrichten von den geklonten oder den fiktiven Profilen versendet worden waren.

Ein weiterer Angriffsmechanismus identifizierte Nutzer, welche nur bei XING und nicht bei LinkedIn registriert waren, nahm die Identitäten der Opfer und registrierte sie in LinkedIn (“Cross-Site Profile Cloning”). Anschließend wurden Freundschaftsanfragen an solche LinkedIn-Nutzer gesendet, die in XING als Freunde des Opfers identifiziert worden waren. 56% der Freundschaftsanfragen wurden akzeptiert, wohl auch deshalb, weil die neuen Nutzer noch nicht in der Kontaktliste standen. Selbst in den Fällen, wo Nutzer die Besitzer der Original-Profile warnten, dass etwas Merkwürdiges vor sich ging, geschah das meist erst nach Annahme der Freundschaftsanfrage und ließ dem Angreifer genug Zeit, um persönliche Daten auszulesen. Die meisten Nutzer begannen, an die gefälschten Identitäten Nachrichten und Postings zu senden, als ob es sich um echte Profile handelte. Bis zum Abbruch des Experiments wurden durch das automatisierte Verfahren ca. 5 Mio. öffentliche Profile ausgewertet und ca. 1,2 Mio. bestehende Profile komplett erfasst.

### 4.5.1 Wie das Klonen von Identitäten funktioniert

Die oben erwähnte iCloner-Architektur besteht aus Komponenten, die öffentliche Profile und Kontaktlisten sammeln, die gewonnenen Informationen in einer Datenbank analysieren, Profile duplizieren (mit Namen und Bild des Originals) oder Profile neu generieren, Freundschaftsanfragen und Nachrichten versenden. Die in vielen Netzwerken gebräuchlichen Captcha-Mechanismen<sup>63</sup> konnten mittels Open Source-Tools automatisch analysiert und zu einem hohen Anteil gebrochen werden.

Das Klonen von Identitäten ist relativ leicht, da die Vor- und Nachnamen von Nutzern in den sozialen Netzwerken nicht eindeutig sind und bei der Registrierung ohnehin keine sichere Identitätsprüfung stattfindet. Der hohe Anteil an erfolgreichen Freundschaftsanfragen zeigt, dass zumindest zum Zeitpunkt der Untersuchung in sozialen Netzwerken ein hoher Grad an Vertrauen vorhanden war und Nutzer gegenüber den Nachrichten ihrer “Freunde” wenig Vorsicht walten ließen.

<sup>63</sup>CAPTCHA ist das Akronym für “Completely Automated Public Turing test to tell Computers and Humans Apart”, d. h. ein Test zur Unterscheidung von Computern und Menschen.

Mit Hilfe solcher automatisierten Tools können Angreifer in großem Maßstab persönliche Daten von Nutzern auswerten und die gewonnenen Kontakte zum gezielten “Social Engineering” (z. B. “Spear Phishing”) und zur Verbreitung von Malware nutzen. Immer häufiger wird versucht, durch Phishing direkt an Login-Daten, Passwörter, PINs oder sonstige Daten zu kommen.

#### **Hinweis für Nutzer**

Bei seltsamen E-Mails oder Freundschaftsanfragen über soziale Netzwerke sollte erhöhte Wachsamkeit herrschen. Enthalten Freundschaftsanfragen oder E-Mails Links auf eine Webseite, sollten diese nicht angeklickt werden. Oftmals werden Links maskiert und führen nicht auf die genannte Webseite, sondern auf nachgeahmte Seiten. Soll die scheinbar verlinkte Webseite trotzdem aufgerufen werden, wird die Adresse zur Sicherheit besser von Hand in die Adresszeile des Browsers eingegeben.

## 4.6 Mögliche Gegenmaßnahmen auf Seiten der Betreiber

Die Experimente zeigten, dass sich die Erfolgsrate von Angriffen durch das Klonen realer Nutzerprofile steigern lässt. Mittels der Freundschaftsanfragen lassen sich dann auch viele nicht öffentliche Profile erreichen und auswerten. Die Autoren des Papers [BSBK09] geben den Dienst Anbietern von sozialen Netzwerken einige Empfehlungen. So sollten die Freundschaftsanfragen mit zusätzlichen Informationen versehen werden, damit der Empfänger die Echtheit besser einschätzen kann, z. B. Länderinformation auf Grundlage der IP-Adresse und das Erstellungsdatum des Profils.

Die Autoren in [BSBK09] empfehlen, unbedingt die Captcha-Mechanismen zu verbessern. Dabei sind die Facebook-Captchas bereits sehr viel schwieriger zu brechen, da sie Wortbilder von Buch-Digitalisierungsprojekten verwendet, die von Programmen des “Optical Character Recognition” (OCR) nicht erkannt werden konnten. Weiter wird den Dienst Anbietern die Einführung oder Verbesserung von verhaltensbasierten Anomalieerkennungsmechanismen empfohlen, so dass beispielsweise das automatische Durchsuchen von Profilen oder das serienmäßige Versenden von Freundschaftsanfragen besser erkannt werden können. Nicht zuletzt sollte das Problembewusstsein der Nutzer in Bezug auf Datenschutz und Sicherheitsrisiken in sozialen Netzwerken geschärft werden.

Gegen das Klonen realer Nutzerprofile ließen sich Techniken des “Digital Right Managements” (DRM) einsetzen, z. B. Verschlüsselung und digitale Signatur der Daten, eindeutige Zeitstempel oder digitale Wasserzeichen, die vom Dienstleister beim erstmaligen Hochladen eingefügt werden und nur durch den Dienstleister (mittels eines geheimen Schlüssels) ausgelesen werden können. Enthielten solche Wasserzeichen beispielsweise eine eindeutige Nutzer-ID und einen Hashwert des Bildes, so könnte die Herkunft und Echtheit der Bilder leicht überprüft werden [KS12].

## 4.7 Automatisierte Informationssammlung

Angreifer sammeln Informationen in sozialen Netzwerken für weitere Angriffe des “Social Engineering”.

In der ersten Phase von “Social Engineering”-Angriffen werden aus verschiedensten Quellen Informationen über ein Opfer zusammengetragen, mit denen im weiteren Verlauf sensible Information ausgehorcht werden sollen. Hierfür kann der Angreifer entweder selbst eine Vertrauensbeziehung mit dem Opfer aufbauen oder durch Identitätsdiebstahl z. B. als Autoritäts- oder Vertrauensperson auftreten. Herkömmliche “Social Engineering”-Angriffe sind jedoch sehr zeitintensiv, da sämtliche Informationen manuell recherchiert, zusammengeführt und verwertet werden müssen.

Soziale Netzwerke eröffnen die Möglichkeit automatisierter “Social Engineering”-Angriffe, die weitaus effizienter und günstiger durchführbar sind. In [HKNT09] wird ein Angriffsszenario beschrieben, bei dem Profilinformatoren des Opfers sowie dessen Umfeld als Informationsbasis dienen. Diese Informationen liegen in maschinenlesbarer Form vor und können daher einfach durch so genannte “Crawler”-Programme extrahiert und gespeichert werden. Die starke Verknüpfung von Daten entlang der in den Plattformen abgebildeten Beziehungen zwischen den Nutzern ermöglichen das Extrahieren neuer Informationen über den Informationsgehalt einzelner Datenobjekte hinaus [Pol08; JK11]. Beispielsweise kommen automatische Tools zum Einsatz, welche die Profildaten und eingestellten Daten auf bestimmte Stichworte und Namen durchsuchen, um die Verknüpfungen von Personen, Unternehmen und Aktivitäten im Sinne eines späteren Social-Engineering-Angriffs auszuwerten [BGW08].

Bei nicht öffentlichen Profilen geht diesem Schritt das Senden von Freundschaftsanfragen voraus. Im Anschluss an die Recherchephase kann eine automatisiert geführte Konversation mit dem Opfer gestartet werden, für die zuvor eine geeignete Chat-Logik definiert wird. Im Gespräch wird das Opfer bspw. über einen Link mit Malware attackiert oder nach sensiblen Informationen befragt, die die Grundlage späterer automatisierter Angriffe bilden können. In [HKNT09] wird davon ausgegangen, dass nur wenige Nachrichten ausgetauscht werden müssen und das Opfer deswegen nicht anzweifelt, mit einer realen Person zu kommunizieren. Angreifer können solch automatisierte Chats weiter perfektionieren, indem sie sich nach Art des “Man-in-the-Middle” zwischen mehrere Nutzer schalten und automatisiert Konversationsbrocken zwischen den Nutzern zielgerichtet querversenden, fallenlassen, einschieben oder modifizieren. Weil dabei ausschließlich menschliche Kommunikationsfragmente eingesetzt werden, ist die Erkennungsrate, dass es sich um einen automatisierten Angriff handelt, stark vermindert [LPBK10].

Weitere Forschungsexperimente zeigen, dass in sozialen Netzwerken Sicherheitslücken existieren, durch die in großem Umfang Nutzerdaten für “Social Engineering”-Angriffe extrahiert werden können. So akzeptierten noch Anfang 2010 viele Netzwerke automatische Abfragen zur Prüfung von E-Mail-Adresslisten. Da viele Nutzer über verschiedene Netzwerke hinweg dieselbe E-Mail-Adresse verwenden, konnten Profile, die zu einer Person gehören, leicht identifiziert und aggregiert werden. Dabei fielen auch Diskrepanzen in den Datensätzen vieler Nutzer auf bzgl. Namen, Geschlecht, Alter, Familien- und Beziehungsstand. Diese würden sich vermutlich gut für “Social Engineering” oder herkömmliche Erpressungsversuche eignen [BPH<sup>+</sup>10]. Andere Arbeiten nutzen öffentlich zugängliche Informationen über existierende Gruppen in Netzwerken, um Nutzer über ihre Gruppenmitgliedschaft zu deanonymisieren. Die Arbeiten deuten darauf hin, dass viele Netzwerke der Gruppenmitgliedschaft der Nutzer generell keinen hohen Schutz beimessen [WHKK10].

Für “Social Engineering”-Angriffe mit Hilfe von Identitätsdiebstahl ist auch das in [Ver12] vorgestellte Java-Tool “Facebook Pwn”<sup>64</sup> geeignet. Der Angreifer muss nur ein Opfer auswählen, woraufhin das Tool Freundschaftsanfragen an alle Kontakte des Opfers schickt.

<sup>64</sup>Siehe <http://code.google.com/p/fbawn>

Anschließend bietet es eine Funktion zum “Profile Cloning” derjenigen Profile an, die der Freundschaftsanfrage zugestimmt haben. Danach wird eine Freundschaftsanfrage an das Opfer gerichtet, bei dessen Zustimmung sämtliche Profilinformatio­nen lokal gespeichert werden. Das hierdurch erschlichene Vertrauen bildet die Ausgangsbasis für weitere “Social Engineering”-Aktivitäten.

**Hinweis für Nutzer**

Als Passwort für Ihr Netzwerk-Konto sollten Sie ein ausreichend langes Passwort mit Ziffern und Sonderzeichen wählen (mindestens 10 Zeichen Länge). Zudem sollten Sie Passwörter nicht mehrfach verwenden, sondern für jedes soziale Netzwerk und jeden Webdienst ein eigenes Passwort erstellen, möglichst auch eine eigene E-Mail-Adresse. Gelangt nämlich ein Angreifer ansonsten an irgendeiner Stelle an Ihre Zugangsdaten, erlangt er Zugriff auf viele Konten und womöglich auch auf Ihre E-Mail. Haben Angreifer Zugriff auf Ihre E-Mail, können sie sich zudem die Passwörter von weiteren Diensten schicken lassen, bei denen Sie registriert sind.

Seien Sie bei Freundschaftsanfragen generell vorsichtig.





## 5. AUSWIRKUNGEN AUF DIE UNTERNEHMENS SICHERHEIT

In diesem Kapitel werden einige Szenarien beschrieben, in denen nicht allein einzelne Nutzer von Risiken betroffen sind, sondern auch Unternehmen in denen diese Nutzer arbeiten, oder mit denen diese Nutzer in Kontakt stehen.

Eine gute Einführung zu Auswirkungen und Risiken sozialer Netzwerke für Unternehmen bietet [LK10]. Beispiele von Risiken einer ungeordneten internen Nutzung sozialer Netzwerke sind die Überwachung von Mitarbeitern, Belästigungen und Mobbing, Verbreitung von Viren und Malware und den Verlust von Arbeitszeit und Produktivität [Ver12]. Externe und interne Angriffe über soziale Netzwerke und das Exponieren von Unternehmensaktivitäten in sozialen Netzwerken können leicht zum Verlust von Ansehen und Geschäftsgeheimnissen führen oder professionellen Hackern neue Angriffsmöglichkeiten bieten. Die folgenden Kapitel zeigen exemplarisch einige typische Angriffsverläufe.

### 5.1 Vorbereitung gezielter Hacker-Angriffe

Angreifer verwenden die in sozialen Netzwerken gesammelten Informationen, um in Unternehmen einzusteigen.

Soziale Netzwerke können Angreifern detaillierte Informationen über bestimmte Personengruppen in Unternehmen liefern, siehe Abschnitt 4.7. Die Datensuche in sozialen Netzwerken ersetzt immer mehr das herkömmliche “Dumpster Diving” (Suche nach Informationen in Müllcontainern), um sich Kontaktlisten, Organigramme, Hierarchien, Zuliefererlisten, Dienstpläne usw. zu beschaffen. Mittels Daten sozialer Netzwerke können Angreifer Details des Privat- und Geschäftslebens und des Persönlichkeitsbildes einer Person rekonstruieren. Die Innentäter eines Unternehmens können nun auch online in sozialen Netzwerken aktiv werden. Dabei können die gesammelten Daten weitere Angriffe vorbereiten und unterstützen, z. B. Eingriffe in das Privatleben der Opfer oder professionelle Hackerangriffe auf das IT-System des Unternehmens.

Gewonnene Informationen lassen sich beispielsweise in gezielten Phishing-E-Mails verwenden, um Mitarbeiter des Unternehmens bösartig zu täuschen (sog. “Spear Phishing”). Der Erfolg einer solchen gezielten Phishing-Attacke ist relativ hoch, da die Phishing-E-Mail z. B. durch eine persönliche Anrede, Insider-Informationen, oder Hinweise auf spezielle Aufgaben oder Vorlieben des Empfängers einen persönlichen Bezug suggeriert und je nach Art des “Social Engineering” dem Empfänger authentisch, unauffällig oder besonders relevant vorkommt. Die Phishing-E-Mails bilden dabei eine weitere Stufe zur Vorbereitung ernstere Angriffe, indem sie z. B. Dateien mit Schadcode oder bösartige Links transportieren.

Ein herausragendes Beispiel für eine solche Vorgehensweise ist der Angriff auf die US-amerikanische Sicherheitsfirma RSA im März 2011. [Ash11] Angreifer schleusten mithilfe gezielter Phishing-E-Mails Schadcode in die Firma ein, und erlangten damit weiterführenden Zugang zu IT-Netzwerken und -Systemen (siehe Abbildung 3). Anschließend konnten sie hoch-sensitive Unternehmensdaten stehlen. Die für das Phishing benötigten Informationen über RSA-Mitarbeiter stammen vermutlich aus offen zugänglichen Daten sozialer Netzwerke [Riv11].

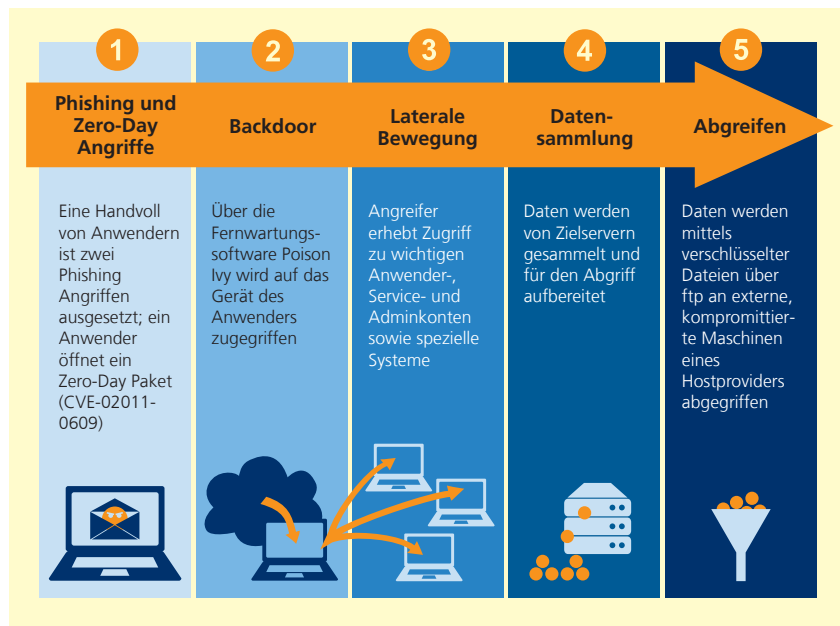


Abbildung 3. Angriff auf die Sicherheitsfirma RSA, siehe [Riv11]

### 5.1.1 Suchmaschinen und Daten in sozialen Netzwerken

Facebook, XING und LinkedIn erlauben in der Standardkonfiguration Personen, die nicht Mitglieder der Plattform sind, auf Ihre Profildaten zuzugreifen. Im Fall von XING sind teilweise auch Diskussionsforen betroffen. Externe können Forenbeiträge gelegentlich allein durch den Aufruf einer Internetverknüpfung wie z. B. <http://www.soziale.netzwerke.plattform/profil=12345678> abrufen. Derart öffentlich verfügbare Daten können auch von Internet-Suchmaschinen gelesen und indiziert werden. Zwar können die Privatsphäreinstellungen zu einem späteren Zeitpunkt so angepasst werden, dass dieser öffentliche Zugang nicht mehr möglich ist, allerdings können die Daten noch eine gewisse Zeit im Zwischenspeicher von Suchmaschinen verbleiben. Ein Abruf von Externen ist dann weiterhin möglich.

#### Hinweis für Mitarbeiter in Unternehmen

Um eine unrechtmäßige Informationsbeschaffung über Unternehmen aus sozialen Netzwerken zu beschränken, sollten Mitarbeiter gänzlich darauf verzichten, jegliche Daten des Unternehmens frei im Internet zu veröffentlichen. Erlaubt ein soziales Netzwerk solche Freigaben, so sollten diese direkt nach dem Anlegen des Nutzerkontos deaktiviert werden.

## 5.2 Gezielte Identitätsfälschung

Mit gestohlenen oder gefälschten Identitäten können Angreifer unberechtigten Zugang zu Unternehmen, Organisationen und Nutzergruppen erhalten.

Soziale Netzwerke bieten – wenn auch aus Sicht vieler Betreiber unerwünschte – Möglichkeiten für die Registrierung fiktiver Identitäten. Angreifer können fiktive Identitäten nutzen, um Unternehmen und Organisationen anzugreifen oder zu unterwandern. So berichtete die Washington Times im Juli 2010 vom Facebook-Account einer vermeintlichen Nutzerin, der 25-jährigen Robin Sage, die binnen eines Monats annähernd 300 teils hochrangige Verbindungen zu Sicherheitsabteilungen von Unternehmen, Militär, Geheimdiensten und Rüstungsindustrie aufgebaut hatte (Sage-Affäre). In Wirklichkeit handelte es sich um ein fiktives Profil, das der Sicherheitsberater Thomas Ryan geschaffen hatte, um Schwachstellen in US-Verteidigung und US-Geheimdienst aufzuzeigen [Wat10]. Das LinkedIn-Profil der Robin Sage spricht von 10-jähriger Hacker-Erfahrung gegen Global 500-Unternehmen und Regierungen, siehe Abbildung 4.

Current	• N8 at Naval Network Warfare Command
Past	• Intern at Government Agency
Education	• Massachusetts Institute of Technology • St. Paul's School
Recommendations	1 person has recommended Robin
Connections	177 connections
Websites	• Where I Work • Dark Side of Security • My Facebook
Twitter	• robinsage
Public Profile	<a href="http://www.linkedin.com/in/robinsage">http://www.linkedin.com/in/robinsage</a>

### Summary

I have been in the computer hacking scene for over ten years. During this time I have penetrated hundreds of networks as a professionally contracted hacker and was empowered by the adrenaline rush of breaking into secured facilities of Global 500 companies and various governments. Because of my style and diverse areas of expertise, many of my friends refer to me as the real life Abby Scuito of NCIS.

Abbildung 4. LinkedIn-Profil der fiktiven Robin Sage, siehe auch [Rya10]

Robin Sage bekam Job-Angebote und Einladungen zu Sicherheitskonferenzen und Reviews. Sie bekam vertrauliche persönliche und sicherheitskritische Daten zugesendet. Obwohl einige Personen nachforschten und die Echtheit des Profils anzweifelten, wusste niemand, an welche Stelle man sich wenden konnte, um andere zu warnen. Die sozialen Netzwerke selbst sahen keine entsprechende Meldestelle vor. Eine Stellungnahme des Pentagon räumte ein, dass bis zu 20% des Netzverkehrs des Verteidigungsministeriums mit öffentlichen Social Media-Seiten in Verbindung stehen und die bestehenden Richtlinien völlig unzureichend sind.

Ein weiteres Beispiel für die Gefahren, die mit ungeprüften Identitäten verbunden sein können, zeigt ein Bericht über das Verhalten israelischer Soldaten in Facebook. Die israel-

lische Armee sah sich im Juli 2010 mit den Vorwürfen konfrontiert, die Soldaten hätten eine Facebook-Gruppe gegründet, in der ein Journalist Mitglied werden konnte, ohne dass dessen reale militärische Zugehörigkeit gegegenprüft worden war [The10]. Die Existenz der Facebook-Gruppe war sogar öffentlich sichtbar, d. h. jeder konnte sich um einen Beitritt bewerben, ohne auf eine Einladung des Gruppenadministrators angewiesen zu sein. Nach eigenen Angaben wurde die Zeitung von der israelischen Zensurbehörde an der Veröffentlichung von Personennamen und Orten gehindert. Stellungnahmen aus der israelischen Armee räumten mögliche Sicherheitslücken durch die verbreiteten Online-Aktivitäten ein und erwähnten vermeintliche Freundschaftsangebote der Hisbollah unter gefälschten Identitäten in Facebook. Als Gegenmaßnahmen wurden Aufklärung und Stärkung des Problembewusstseins bei den Soldaten genannt.

### 5.2.1 Mögliche Auswirkungen gefälschter Identitäten

Gefälschte Identitäten stellen ein neues Risiko für den persönlichen Datenschutz und die Sicherheit von Unternehmen dar. Spionage in Unternehmen und Communities wird für Angreifer einfacher durch die Vielzahl an personenbezogenen Daten der Mitglieder, die vermeintliche Authentizität der anderen Netzwerkmitglieder und die fehlenden Sicherheitsmechanismen beim Netzerkanbieter. Ein Identitätsdiebstahl (Evil-Twin) kann z. B. das Entlocken von geheimen Informationen der echten möglicherweise prominenten Person ermöglichen und eine Rufschädigung der Person, der betroffenen Community oder eines gesamten Unternehmens nach sich ziehen. Ähnliche Auswirkungen kann ein Angreifer mit Hilfe eines fiktiven Profils wie das von Robin Sage erreichen, auf das sich Nutzer der betreffenden Community vertrauensvoll einlassen. Das Fälschen von Identitäten stellt zudem einen möglichen Weg für das Einspeisen von Schadcode über Social Engineering dar, vgl. Abschnitt 4.7.

Zudem lassen sich mit der Angabe fremder Profildaten u. U. persönliche Daten anderer Nutzer ausspionieren. Beispielsweise überprüft Facebook bei der Eröffnung eines neuen Facebook-Kontos nicht sofort die Rechtmäßigkeit der vom neuen Nutzer eingegebenen E-Mail-Adresse. Hat sich der Nutzer mit einer fremden E-Mail-Adresse angemeldet, kann er über die Funktion "Freunde finden" die Namen von Personen sehen, die nach dem Besitzer des E-Mail-Kontos gefragt haben. Grundsätzlich können sämtliche eingestellten Daten für die öffentliche Suche im Internet freigegeben werden, was einem Missbrauch von persönlichen Daten für falsche Identitäten Vorschub leistet.

### 5.2.2 Mangelnde Identitätsprüfung auf Seiten der Anbieter

Obwohl die meisten Netzwerke die Nutzer dazu verpflichten, sich mit echten Identitätsdaten, also zumindest mit dem Vornamen, Nachnamen und dem Geburtsdatum anzumelden ("Klarnamenzwang") und eine explizite pseudonyme Nutzung nicht vorsehen, können neue Nutzer bei der Anmeldung absichtlich falsche Angaben machen. Die Identifikation und Authentisierung beim Registrieren und Einloggen in soziale Netzwerke finden nur online auf Systemebene statt. Bei der Registrierung wird kein zweiter sicherer Kommunikationskanal geöffnet, um "Out-of-Band" die Identität der real anwesenden Person zu überprüfen [BGW08].

Derartige Identitätsprüfungen wären zwar hilfreich, sind aber sehr aufwändig und nur gegenüber einem Teil der Nutzer überhaupt anwendbar, z. B. das Versenden einer SMS des Anbieters an das Handy des sich registrierenden Nutzers mit Abgleich der Telefonnummer oder eine persönliche Nachfrage von Seiten des Anbieters. Zudem sind international agierende soziale Netzwerke generell nicht bereit, in die Integration nationaler Sicherheitslösungen wie das deutsche PostIdent-Verfahren oder die Nutzung der eID-Funktion des neuen Per-

sonalausweises zu investieren. Das Senden von Zugangsdaten an die vom neuen Nutzer angegebene E-Mail-Adresse impliziert jedenfalls keine zuverlässige Identitätsprüfung, sondern nur die korrekte Zuordnung einer Nutzeradresse, die möglicherweise unter ähnlich einfachen Bedingungen eingerichtet wurde.

Die sichere Unterscheidung von echten und gefälschten Identitäten ist eine ungelöste Aufgabe für die einzelnen Nutzer, für die Technik (Anonymisierungsdienste, usw.) und für die Gesetzgebung (BDSG, europäische Datenschutzgesetzgebung) [BGW08]. Facebook vermutet, dass von den 955 Mio. registrierten Accounts 83 Mio. (8,7 Prozent) keine echten Identitäten sind, sondern Mehrfach-Accounts oder falsch klassifizierte Accounts z. B. zum Versenden von Spam.<sup>65</sup>

### 5.2.3 Klarnamenzwang und pseudonyme Nutzung

Gegen den Klarnamenzwang und die vermeintliche Sicherheit von Klarnamen fordert das Unabhängige Datenschutzzentrum Schleswig-Holstein (ULD) seit längerem von Facebook eine offizielle Zulassung pseudonymer Accounts und begründet dies mit dem deutschen Telemediengesetz, wonach “der Dienstanbieter [...] die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen [hat], soweit dies technisch möglich und zumutbar ist.”<sup>66</sup> Allerdings haben das zuständige Verwaltungsgericht und Oberverwaltungsgericht dem Klarnamenzwang von Facebook recht gegeben. Gemäß Europäischer Datenschutzrichtlinie finde nicht das deutsche Telemediengesetz, sondern die irische Datenschutzrecht Anwendung, da die Verarbeitung persönlicher Nutzerdaten bei Facebook Irland bzw. in rechtmäßiger Auftragsdatenverarbeitung auf US-amerikanischen Servern erfolgt.<sup>67</sup> <sup>68</sup> Somit sind auch die deutschen Facebook-Nutzer weiterhin verpflichtet, sich mit ihren richtigem Namen zu registrieren.

Die Empfehlung an die Dienstanbieter bleibt bestehen: Neben allgemeiner gebotener Datensparsamkeit auf Seiten der Nutzer, sollten die Dienstanbieter auch offiziell eine pseudonyme Nutzung der Online-Dienste zulassen, um Bedürfnissen der Nutzer nach Anonymität entgegen zu kommen. Die verwendeten Pseudonyme sollten dabei aber eindeutig als solche gekennzeichnet sein, vgl. die pseudonyme Nutzung von De-Mail mittels Präfix `pn_` im Nutzernamen.

#### Hinweis für Unternehmen

Zur Abwehr von Angriffen auf Basis gefälschter Identitäten sollten zumindest folgende Sicherheitsmaßnahmen eingesetzt werden:

- Die Berücksichtigung von Risiken der sozialen Netzwerke im Risikomanagement
- Eine umfassende Aufklärung der Mitarbeiter (“Dein Privatleben – unsere Firmengeheimnisse”)
- Die Nennung eines Ansprechpartners zur Meldung von verdächtigen Vorkommnissen (Hinweisgebersystem)

<sup>65</sup>Siehe <http://www.heise.de/newsticker/meldung/Facebook-vermutet-83-Millionen-Fake-Accounts-1658492.html>

<sup>66</sup>Telemediengesetz § 13 “Pflichten des Diensteanbieters”, siehe [http://www.gesetze-im-internet.de/tmg/\\_13.html](http://www.gesetze-im-internet.de/tmg/_13.html)

<sup>67</sup>Schleswig-Holsteinisches Verwaltungsgericht: Beschluss 8 B61/12, siehe <https://www.datenschutzzentrum.de/facebook/Facebook-Inc-vs-ULD-Beschluss.pdf>

<sup>68</sup>Oberverwaltungsgericht Schleswig-Holstein: [http://www.schleswig-holstein.de/OVG/DE/Service/Presse/Pressemitteilungen/230420130VG\\_Facebook\\_Klarnamen.html](http://www.schleswig-holstein.de/OVG/DE/Service/Presse/Pressemitteilungen/230420130VG_Facebook_Klarnamen.html)

- Die generelle Einschränkung des Zugangs und der Datenübermittlung an soziale Netzwerke mittels einer Richtlinie, welche auch eine sichere Erkennung der berechtigten Kommunikationspartner vorsieht, vgl. Abschnitt 6.1.

### 5.3 Rekonstruktion von Unternehmensinterna

Angreifer sammeln und korrelieren Daten aus sozialen Netzwerken, um vertrauliche unternehmensinterne Informationen zu rekonstruieren.

Auf der RSA Conference 2011 wurden Forschungsarbeiten präsentiert, die zeigen wie Angreifer detailliert Einblicke in die Interna von Unternehmen über soziale Netzwerke erhalten können (im Englischen spricht man häufig von der "DNA einer Organisation", siehe Abbildung 5). [Son11] Dazu wurden die Profile und Aktivitäten in sozialen Netzwerken der Mitarbeiter von 20 Unternehmen analysiert. Aus den gefundenen Daten konnten reale Entscheidungswege, Informationsflüsse, Motivationslage und Strukturen innerhalb der Unternehmen rekonstruiert werden. Bei über 50% der Unternehmen konnten die Strukturen und Hierarchien identifiziert und Motivatoren (z. B. drohende Insolvenz, Unzufriedenheit, psychologische Profile) skizziert werden.

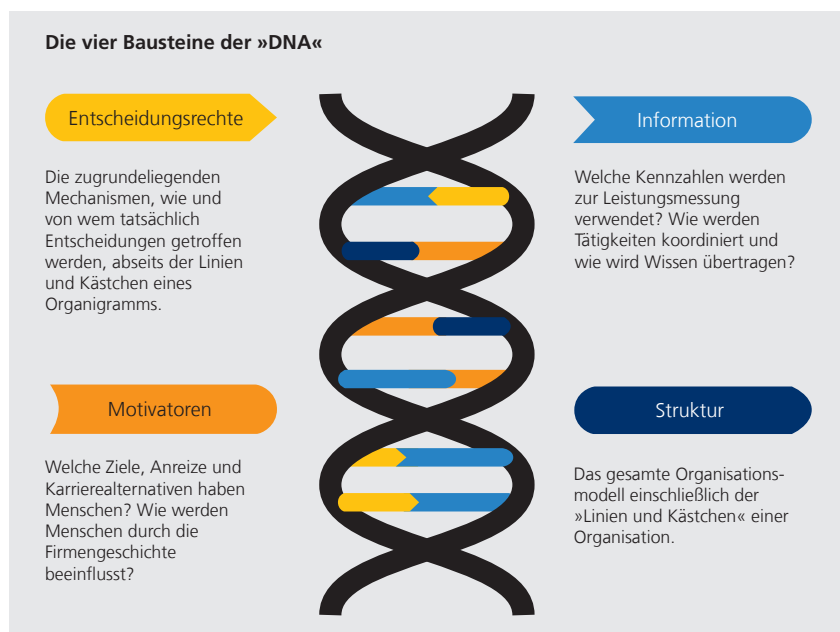


Abbildung 5. "DNA-Bausteine" einer Organisation, Quelle: [Son11]

#### 5.3.1 Unerwünschte Informationsabflüsse durch Mitarbeiter

Die intensive Marketingpräsenz von Unternehmen in sozialen Netzwerken hat die Kehrseite, dass u. U. wichtige Unternehmensvorgänge ungewollt enthüllt werden und vertrauliche Daten durchsickern können oder marktrelevante Informationen z. B. zu Produkteinführungen,

Jahresberichten oder finanziellen Details verfrüht an die Öffentlichkeit kommen. Mitarbeiter, die von ihren privaten Facebook- und Twitter-Accounts private und geschäftliche Details kundtun, können zu einem negativen Bild des Unternehmens in der Öffentlichkeit beitragen. Zumeist unterschätzen die Teilnehmer der sozialen Netzwerke die Möglichkeiten, die sich dem Angreifer aus dem Zusammenführen von Daten aus verschiedenen Quellen ergeben. So wurden im ersten Schritt der in [Son11] präsentierten Analyse so viele Mitarbeiter eines Unternehmens wie möglich über LinkedIn-Profile identifiziert. Anschließend wurden die Twitter- und Facebook-Profile der Mitarbeiter untersucht und deren Feeds überwacht. Auf diese Weise konnten die Entscheidungsträger identifiziert und die Stimmungslage im Unternehmen leicht bestimmt werden.

Gefährdet sind sowohl die immateriellen Unternehmenswerte wie Unternehmensphilosophie, Entscheidungshierarchien, interne Kommunikationsformen, Geschäftsumfeld und die Unternehmensethik als auch die Sachvermögen wie geistiges Eigentum, Finanzinformationen und Betriebsgeheimnisse.

### 5.3.2 Gegenmaßnahme: Trennung von Geschäftlichem und Privatem

In der Praxis sind die Übergänge von offiziell dienstlichen (Betreiben des offiziellen Twitterkanals eines Unternehmens), persönlichen-beruflichen (z. B. Kommunikation in XING über das Profil als Mitarbeiter eines Unternehmens mit beruflicher E-Mail-Adresse) und rein privaten Aktivitäten (z. B. Facebook Profil mit privater E-Mail-Adresse) häufig fließend. Daher ist es umso wichtiger, dass sich Mitarbeiter der unterschiedlichen Rollen, die sie in sozialen Netzwerken einnehmen, bewusst sind und ihre Aktivitäten und Äußerungen entsprechend überprüfen.

Grundsätzlich sollten Mitarbeiter von Unternehmen bei ihren Aktivitäten in sozialen Netzwerken Arbeit und Privates möglichst vollständig trennen. Dabei sind geschäftlich genutzte Plattformen wie XING oder LinkedIn offener konzipiert als die für den Privatgebrauch, wie z. B. Facebook. Bei XING oder LinkedIn ist es eher Teil der Plattformphilosophie, dass Daten zur Präsentation der eigenen Person vollständig allen anderen Plattformmitgliedern angezeigt werden. Entsprechend sind weniger Schutzmechanismen vorhanden, um die Sichtbarkeit von Daten einzuschränken.

Mitarbeiter eines Unternehmens sollten deshalb überlegen, ob sie bei der Profilgestaltung private Angaben besser ganz außen vor lassen, auch wenn solche Angaben 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. Dies sollte bedacht werden, bevor man in Foren "Privates" diskutiert.

Für alle Plattformen gilt: Als Mitarbeiter eines Unternehmens sollte man beim Erstellen des Profils auch an die Interessen des Arbeitgebers denken. So können bestimmte Tätigkeitsfelder und eingesetzte Techniken innerhalb eines Unternehmens Betriebsgeheimnisse berühren und haben demzufolge nichts in den Plattformen sozialer Netzwerke zu suchen. Gleiches kann auch für Informationen zu Terminen, aktuellen Aufenthaltsorten oder Kunden gelten.

#### **Hinweis für Mitarbeiter in Unternehmen**

Hinterlegen Sie in Geschäftsplattformen keine Informationen aus Ihrem Privatleben. Hinterlegen Sie in keinem der Dienste vertraulichen Informationen zu Projekten in Ihrem Unternehmen. Denken Sie dabei auch an Angaben, die indirekt vertrauliche Infor-



mationen enthüllen können, z. B. wenn Sie in Ihre Pinnwand schreiben, dass Sie “heute einen großen Autohersteller in Stuttgart besuchen”.

## 5.4 Missbrauch für Marketing oder Bashing

Unternehmen missbrauchen bewusst oder unbewusst soziale Netzwerke für Marketing oder werden selbst Opfer von Kritiken oder Schmähungen durch die Nutzer.

Viele Unternehmen nutzen soziale Netzwerke und insbesondere Microblogging-Services wie Twitter zum kostenlosen Marketing. Dabei kann sich ein Unternehmen durch eine unprofessionelle oder ethisch bedenkliche Nutzung leicht selbst schädigen wie das Verhalten des britischen Möbelhauses Habitat 2009 in Twitter zeigt: Habitat hatte bestimmte Schlagworte, so genannte Hashtags, verschiedener Twitter-Trends in den eigenen Tweets verwendet, um seine eigene Bekanntheit zu erhöhen und in den “Trending Topics” zu erscheinen. Verwendet wurden neben kommerziellen Hashtags wie #iphone oder #apple in der Zeit der Einführung des neuen iPhones 3GS auch Hashtags aus sensiblen politischen Tweets wie #mousavi und #iranelection in der Zeit der iranischen Wahlen, siehe Abbildung 6. Daraufhin sah sich Habitat in kurzer Zeit online mit zahlreichen Beschwerden und heftiger Kritik konfrontiert. Viele Nutzer sahen im Verhalten Habitats eine verletzende Störung wichtiger politischer Ereignisse und allgemein ein unlauteres Aufspringen auf fremde Trends. Dies schädigte den Ruf des Unternehmens – nicht zuletzt auch dadurch, dass Habitat in Diskussionen um soziale Netzwerke bis heute als schlechtes Beispiel genannt wird.

Ein weiteres Beispiel zeigt, wie eine kommerzielle Nutzung eigener Hashtags ebenfalls einen beabsichtigten Effekt ins Gegenteil verkehren kann. Im Januar 2012 rief McDonalds den Hashtag #McDStories ins Leben, um seiner Kundschaft den Austausch positiver Restaurantenerlebnisse zu ermöglichen. Diese Marketingaktion wurde allerdings nach nur zwei Stunden wieder eingestellt, da McDonalds statt der erwarteten Geschichten zahlreiche Beschwerde-Tweets erhielt. Privatnutzer der sozialen Netzwerke verwenden generell Hashtags gegenüber großen Unternehmen, um beispielsweise den schlechten Kundenservice von Unternehmen zu brandmarken. Während diese so genannten “Bashtags” gegen Unternehmen nicht unbedingt in negativer Absicht verwendet werden, können sie großen persönlichen Schaden anrichten, wenn sie in negativer Absicht gegen Privatpersonen, Prominente oder Minderheiten gerichtet sind.



Abbildung 6. Missbrauch von Twitter-Hashtags durch ein Unternehmen

### Hinweis für Unternehmen

Bei offiziellen oder gemeinschaftlich genutzten Accounts (z. B. PR-Abteilung) sollten die Zugangsdaten für Notfälle ggf. bei der IT-Administration oder der Pressestelle hinterlegt werden. Passwörter sollten für Notfälle immer hinterlegt werden, da ein Unternehmen in dringenden Fällen auf Vorfälle entsprechend vorhandener Notfallregelungen reagieren muss.

#### 5.4.1 Mangelnde Strategien bei Unternehmen

Durch eine Analyse der Hashtags kann festgestellt werden, welche Twitter-Themen besonders beliebt sind. Diese werden in den so genannten “Trending Topics” auf der Twitter-Startseite angezeigt. Die kommerzielle Verwendung von Hashtags durch Unternehmen wie Habitat und McDonalds zeigt, wie schnell Unternehmen teilweise auf neue Medien aufspringen, um von einer Echtzeit-Kommunikation mit Kunden zu profitieren, dabei aber offenbar über keine solide Marketingstrategie verfügen: Unternehmen werden oftmals von den negativen Auswirkungen überrascht und verlieren darüber vollends die Kontrolle.<sup>69</sup>

Dies wird auch durch die unprofessionellen Reaktionen von Habitat auf den Vorfall bestätigt. Das Unternehmen entschuldigte sich zwar, übernahm aber nicht die Verantwortung, sondern sprach davon, dass die Twitter “Top 10 Trending Topics” inhaltlich ungeprüft und vom Management nicht autorisiert verwendet worden waren.<sup>70</sup> Andere Meinungen sprechen davon, dass viele Unternehmen mit dem Versuch, über die sozialen Netzwerke Kontakt zu Kunden aufzunehmen, schlicht überfordert sind. Es seien oftmals bloße Experimente, die womöglich auf Studentenjobs zurückzuführen sind.<sup>71</sup>

### Hinweis für Unternehmen

Die Verwendung von Hashtags für kommerzielle Werbung durch Unternehmen wird von vielen Nutzern sozialer Netzwerke als primitives Spamming gewertet und ist daher für Marketingzwecke weitgehend ungeeignet. Die negativen Reaktionen auf unsensibles Verhalten von Unternehmen in sozialen Netzwerken erscheint vielen Nutzern als gerechtfertigt und können sehr schnell negative Folgen für das Unternehmen nach sich ziehen.

<sup>69</sup>Search & More (2012): You are what you tweet, why businesses should think twice before tweeting, siehe <http://www.searchandmore.co.uk/social-media/tweet-businesses-tweeting>

<sup>70</sup>360innovate, The Social Media Diaries (2009): Habitat getting it wrong, siehe <http://www.360innovate.co.uk/blog/2009/06/the-social-media-diaries-habitat-getting-it-wrong>

<sup>71</sup>The Telegraph (2009): Habitat apologises for Twitter ‘hashtag spam’, siehe <http://www.telegraph.co.uk/technology/twitter/5621970/Habitat-apologises-for-Twitter-hashtag-spam.html>



## 6. LEITFADEN FÜR UNTERNEHMEN UND MITARBEITER

### 6.1 Erstellung einer Unternehmensrichtlinie

Ein Unternehmen sollte als Präventionsmaßnahme gegen Angriffe auf die Unternehmenssicherheit und als Orientierung für die Mitarbeiter eine Richtlinie für die Unternehmensaktivitäten in sozialen Netzwerken erstellen und diese in regelmäßigen Abständen überprüfen und aktualisieren.

Folgende Fragen können bei der Erstellung einer Richtlinie hilfreich sein:

- Welche firmenbezogenen Daten dürfen in sozialen Netzwerken veröffentlicht werden?
- Wie sind für ausgewählte Daten Zugriffskontrollen zu konfigurieren?
- Welche Daten dürfen aus Netzwerken empfangen werden? (Beschränkung möglich, soweit Nutzung auf Dienstrechnern)
- Welche dienstlichen Vorgänge dürfen über Netzwerke abgewickelt werden?
- Welche netzwerkspezifischen Einschränkungen sollen gelten?
- Wie kann die Authentizität der Kommunikationspartner verifiziert werden?

Die Richtlinie sollte klar definieren, welche Mitarbeiter im Namen des Unternehmens in welchen sozialen Netzwerken aktiv sein dürfen. Blogs und Tweets im Namen des Unternehmens bleiben dabei am besten nur wenigen autorisierten Personen vorbehalten, z. B. ausschließlich den offiziellen Sprechern für Twitter und Facebook. Die Sprecher sollten genau wissen, was sie kommunizieren dürfen, und alle Verlautbarungen dokumentieren.

#### **Hinweis für Unternehmen**

Alle offiziellen Aktivitäten, die in sozialen Netzwerken vorgenommen werden, sollten, soweit möglich, dokumentiert werden. Dies kann ausnahmsweise Fälle betreffen, in denen rechtlich relevante Erklärungen oder Statements abgegeben werden. Eine Sicherung ist in den Diensten der sozialen Netzwerke meist nur schwer möglich, zur Not kann aber ein Screenshot oder Papierausdruck genügen.

Teil der Richtlinie könnten auch detaillierte Vorgaben für die Eingabebeschränkung und Bedingungen für Zugriffskontrollen sein. Der Empfang bestimmter Daten könnte ganz untersagt werden, beispielsweise die Weitergabe von projektspezifischen Informationen oder Firmeninterna, die Weitergabe via 1:1 Kommunikationskanälen, das Überspielen des dienstlichen Adressbuches in die Plattform oder das Organisieren von dienstlichen Terminen über die Plattform. Als eine Bedingung für Zugriffskontrollen sollte gelten, dass bei der Eingabe von Projektkontakten diese maximal für das eigene Netzwerk sichtbar sein dürfen. Eine weitere Grundregel sollte lauten, keine Dokumente und andere Dateien über die Plattform zu senden und auch keine Absprachen zum Datenempfang über die Plattform zu versenden. Die Mitarbeiter können anhand solcher konkreter Vorgaben durch Aufklärungsmaßnahmen in angemessenem Online-Verhalten geschult werden. Die Richtlinie könnte schließlich der PR-Abteilung eines Unternehmens vorschreiben, parallel zu Verlautbarungen in sozialen Netzwerken immer auch die direkten Kontakte zu Analysten und Börsenmaklern zu nutzen und Pressemitteilungen zu veröffentlichen.

Beispiele von aktuellen Richtlinien bekannter Unternehmen sind im Internet zu finden.<sup>72</sup> Darunter sind die Policies von IBM und der Daimler AG hervorzuheben, die prägnante Regeln für das Verhalten der Mitarbeiter in sozialen Netzwerken definieren. Die Richtlinie sollte schließlich in Form einer Betriebsvereinbarung oder als Dienstanweisung einen verbindlichen Stellenwert im Unternehmen bekommen [HK12].

Die Risiken einer unkontrollierten Nutzung von Webdiensten bezüglich der Informationssicherheit und der Erfüllung rechtlicher Anforderungen werden in [SP12a] untersucht. Darin werden auch Wege aufgezeigt, wie die Risiken durch bestimmte Maßnahmen vermindert werden können.

#### **Hinweis für Unternehmen**

Alle in sozialen Netzwerken verbreiteten Informationen sollten zeitnah auch auf den offiziellen Webseiten des Unternehmens erscheinen, um Gerüchten vorzubeugen und Inkonsistenzen zu vermeiden. Die Unternehmen sollten in jedem Fall ihren Aktivitäten in sozialen Netzwerken ggf. einen ähnlich hohen Stellenwert einräumen wie den herkömmlichen Kommunikationskanälen.

## 6.2 Fragen und Antworten für Mitarbeiter und Unternehmen

Die folgenden Fragen und Antworten sind für Mitarbeiter gedacht, die gemäß einer Unternehmensrichtlinie im Namen des Unternehmens in sozialen Netzwerken aktiv sein dürfen. Die Antworten und Hinweise sind unverbindlich, stellen insbesondere keine Rechtsberatung dar und ersetzen keine Unternehmensrichtlinie. Wenn Sie die Empfehlungen in Erwägung ziehen möchten, sollten Sie sich wegen Ihres Anliegens zunächst an die Rechtsabteilung Ihres Unternehmens, an einen Anwalt oder an eine Beratungsstelle wenden.

**Frage 1: Kann ich meine berufliche E-Mail-Adresse zur Anmeldung in sozialen Netzwerken verwenden?**

Möchte ein Mitarbeiter ein Konto bei einem sozialen Netzwerk erstellen, um als Funktionsträger bzw. Mitarbeiter eines Unternehmens aufzutreten, und dazu die persönliche, dienstliche E-Mail-Adresse zur Anmeldung und als Kontaktadresse verwenden, dann sollte auch der Name des Arbeitgebers und die vollständige Adresse in das Profil eingetragen werden.

#### **Hinweis für Nutzer**

Handelt es sich um einen privaten Account, der überwiegend privat genutzt wird (mit Angabe des Arbeitgebers), sollten Sie für die Anmeldung eine private E-Mail-Adresse verwenden und die dienstliche E-Mail-Adresse als weitere Kontaktadresse Ihrem Konto hinzufügen.

<sup>72</sup>Chris Boudreaux: Social Media Governance – Policy Database (2012), siehe <http://socialmediagovernance.com/policies.php>

## Frage 2: Darf ich Namen oder Adressen von Kollegen über soziale Netzwerke veröffentlichen oder dort in Kontakten einpflegen?

Sollen Inhalte mit personenbezogenen Daten in sozialen Netzwerken veröffentlicht werden, so müssen die Datenschutzvorschriften eingehalten werden. Datenschutzvorschriften sind in verschiedenen Gesetzen enthalten, z. B. dem Telemediengesetz (TMG) für die bei deren Nutzung anfallenden Daten. Greifen die Vorschriften solcher spezieller Gesetze nicht, gelten die allgemeinen Vorschriften des Bundesdatenschutzgesetzes (BDSG).

Personenbezogene oder -beziehbare Daten wie Namen, Adressen, Telefonnummern u. a. dürfen gemäß allen Datenschutzgesetzen nur verwendet werden, wenn eine Rechtsnorm es erlaubt oder der Betroffene eingewilligt hat. Dies gilt auch für Daten, die in Dokumenten oder Präsentationen enthalten sind.

### Hinweis für Nutzer

Hat Ihnen jemand seine Kontaktdaten gegeben, ist im Einzelfall abzuwägen, ob er auch damit einverstanden ist, diese in einem sozialen Netzwerk zu veröffentlichen, da die meisten Dienste auch auf die Kontaktdaten ihrer Nutzer zugreifen. Im Zweifel sollte die betreffende Person daher um Erlaubnis gefragt werden.

## Frage 3: Was ist mit öffentlich verfügbaren Daten, z. B. aus Unternehmensverzeichnissen oder Telefonbüchern?

Auch wenn meist Telefonnummern und Adressen in Unternehmensverzeichnissen oder öffentlich zugänglichen Verzeichnissen bereitgehalten werden, dürfen diese nicht ohne Einwilligung des Unternehmens oder des Betroffenen in andere Systeme und Datenbanken eingebracht werden. Der Betroffene hat nur in die Veröffentlichung im jeweiligen Verzeichnis eingewilligt und weiß auch nur, dass seine Daten dort geführt werden.

Zudem sind die Datenbanken selbst meist urheberrechtlich geschützt, auch wenn sie öffentlich zugänglich sind. Das Auslesen von Teilen der Datenbanken und Erstellen einer neuen Datenbank bräuchte daher zusätzlich eine Zustimmung des Verzeichnisanbieters.

### Hinweis für Nutzer

Nur weil ein Verzeichnis möglicherweise öffentlich zugänglich ist, bedeutet dies nicht, dass seine Daten ohne Einwilligung in andere Verzeichnisse, neue Datenbanken oder Dienste sozialer Netzwerke übertragen oder veröffentlicht werden dürfen.

## Frage 4: Kann ich einen Adressbuchabgleich durchführen, um Kollegen in sozialen Netzwerken zu finden?

Viele Zusatzprogramme ("Add-ons") für dienstlich genutzte Programme stellen zwischen internen IT-Systemen und Drittanbietern (z. B. dem Betreiber eines sozialen Netzwerks) eine Verbindung her. Oftmals sollen diese Add-ons durch die Kombination von bestehender Software und Webdiensten die Handhabung erleichtern oder erweiterte Funktionen wie z. B. den Adressbuchabgleich zur Verfügung stellen.

Doch können durch falsche Bedienung, sei es wegen schlecht oder fehlerhaft programmierter Software oder nur wegen eines falschen Klicks, Kontaktdaten oder Projektdaten veröffentlicht oder an Dritte gesendet werden. Einmal veröffentlicht oder versendet kann es unmöglich sein, solche Fehler zu korrigieren.

Programme und Add-ons laden zudem oftmals ohne Rückfrage automatisch Adressbücher und Adressverzeichnisse zum Anbieter hoch, um Kontakte zu finden, die beim gleichen Anbieter angemeldet sind. Automatische Synchronisierungen von Daten über das Internet sollten daher überhaupt nicht verwendet, sondern abgeschaltet werden.

**Hinweis für Nutzer**

Der Zugriff auf E-Mail-Konten durch Dritte sollte nicht zugelassen werden. Auch sollten keine Adressbücher/Kontaktdaten an Dritte übermittelt oder hochgeladen werden. Falls Sie ihre Kollegen in sozialen Netzwerken finden möchten, sollten sie die dafür vorgesehenen Suchfunktionen der Dienste verwenden oder sich mit den Kollegen absprechen.

**Frage 5: Darf ich soziale Netzwerke zum Austausch von Dokumenten verwenden?**

Soziale Netzwerke bieten oftmals schnelle und einfache Online-Kommunikation. Mit wenigen Klicks und geringem Zeitaufwand können Informationen und Dokumente ausgetauscht werden. Der Versand der Daten läuft hierbei über die Server des Diensteanbieters. Dieser sitzt oftmals im Ausland und unterliegt anderen Rechtsordnungen. Es kann daher nicht ausgeschlossen werden, dass der Anbieter oder staatliche Behörden Zugriff auf die Daten und Dokumente der Nutzer haben und diesen auch gebrauchen. Daher sollte möglichst keine unternehmensinterne Kommunikation über soziale Netzwerke abgewickelt und keine Dokumente darüber ausgetauscht werden.

**Hinweis für Nutzer**

Vor allem Daten mit personenbezogenen Inhalten dürfen nur unter ganz bestimmten Umständen an Dritte übermittelt werden. Dokumente die der Geheimhaltung unterliegen (VS-NfD), sollten niemals über soziale Netzwerke versendet werden. Hierfür sollten herkömmliche Kommunikationswege verwendet werden, wie z. B. verschlüsselte E-Mail.

**Frage 6: Darf ich Yammer, Facebook oder andere Dienste zur internen Kommunikation verwenden?**

Dienste wie Facebook, Yammer und andere sollten für die interne Kommunikation zwischen Mitarbeitern in der Regel nicht verwendet werden. Durch die Verwendung von Diensten Dritter zur Nachrichtenübermittlung können unternehmensinterne Informationen an die Anbieter übermittelt werden.

**Hinweis für Nutzer**

Mit dem Anbieter des Netzwerks schließt man als Privatperson einen Vertrag zur Nutzung des Dienstes ab. Werden dann anschließend betriebliche Informationen über bzw. an den Anbieter versendet, kann dies gegen arbeitsvertragliche Pflichten verstoßen. Dies gilt gleichermaßen für alle Dokumente, Protokolle, Berichte etc., die nicht zur Veröffentlichung vorgesehen sind.

### Frage 7: Darf ich über Projekte berichten oder mich mit anderen darüber austauschen?

Im Rahmen von Projekten können einzelne Dokumente oder Informationen dem Geheimschutz oder Vertraulichkeitsvereinbarungen unterliegen. Teils wünschen Projektpartner auch Geheimhaltung bezüglich des ganzen Projektes bis zum Erreichen eines bestimmten Projektziels oder Zeitpunktes.

Die Geheimhaltungspflichten aus dem Arbeitsvertrag gelten auch für die Online-Kommunikation in sozialen Netzwerken. Betriebs- und Geschäftsgeheimnisse sind auch in privat genutzten Diensten vertraulich zu behandeln. Hierzu gehören Informationen zu geplanten oder aktuellen Projekten, Kundenbeziehungen, Arbeitsabläufen, IT-Strukturen oder Ähnliches.

#### **Hinweis für Nutzer**

Um nicht gegen solche Verschwiegenheitsvereinbarungen zu verstoßen, sollten Sie Rücksprache mit den Vorgesetzten oder Projektleitern halten, welche Informationen veröffentlicht und welche Kontakte preisgegeben werden dürfen.

### Frage 8: Welche Äußerungen in sozialen Netzwerken sollte ich als Mitarbeiterin/Mitarbeiter unbedingt vermeiden?

Als Grundsatz gilt, dass die arbeitsvertraglichen Regelungen auch in der virtuellen Welt wie den sozialen Netzwerken Bestand haben. Bei der Nutzung sozialer Netzwerke sind daher die allgemeinen Rücksichtnahme- und Loyalitätspflichten, die gegenüber dem Arbeitgeber bestehen, zu beachten. Wichtig sind in diesem Zusammenhang insbesondere die Wahrung von Betriebs- und Geschäftsgeheimnissen und das Verbot, unternehmensschädliche Äußerungen zu tätigen.

Nach gängiger Definition sind Betriebs- und Geschäftsgeheimnisse alle auf ein Geschäft oder einen Betrieb bezogenen Tatsachen, die nur ein begrenzter Personenkreis kennt, die der Geschäfts- oder Betriebsinhaber erkennbar und berechtigt geheim halten will und die anderen Personen nicht einfach zugänglich sind.

Alle Mitarbeiterinnen und Mitarbeiter sollten daher darauf achten, dass Informationen zu aktuellen oder geplanten Projekten, Akquisitionen, Kundenbeziehungen und anderen marktrelevanten Interna vertraulich sind. Stimmen Sie sich in Zweifelsfällen mit Ihrem/Ihrer Vorgesetzten darüber ab, welche Informationen veröffentlicht werden dürfen. Der Verrat von Geschäfts- oder Betriebsgeheimnissen kann arbeitsrechtliche Maßnahmen bis hin zur außerordentlichen Kündigung rechtfertigen.

Ob eine konkrete Äußerung der Verschwiegenheitspflicht unterfällt, hängt vom jeweiligen Einzelfall ab. Eine Verschwiegenheitspflicht besteht immer dann, wenn von einem berechtigten betrieblichen Interesse des Arbeitgebers an der Geheimhaltung ausgegangen werden kann.

#### **Hinweis für Nutzer**

Jeder Mitarbeiter/jede Mitarbeiterin ist im Rahmen der arbeitsvertraglichen Rücksichtnahmepflicht verpflichtet, Betriebs- und Geschäftsgeheimnisse des Arbeitgebers zu wahren. Die Verschwiegenheitspflicht gilt in der Regel auch über das Ende des Arbeitsverhältnisses hinaus. Soweit nichts anderes vereinbart ist, gilt sie gegenüber jedermann auf unbestimmte Zeit.



Aufgrund der allgemeinen Loyalitätspflicht gegenüber dem Arbeitgeber ist grundsätzlich jeder Mitarbeiter/jede Mitarbeiterin verpflichtet, den Ruf des Arbeitgebers nicht durch ehrenrührige Äußerungen (z. B. über Vorgesetzte, Arbeitsbedingungen etc.) herabzusetzen. Hier sind private, vom Grundrecht auf freie Meinungsäußerung gedeckte Aussagen von solchen, die vom Arbeitgeber sanktioniert werden können, abzugrenzen. Die Abgrenzung ist insbesondere schwierig bei Äußerungen, die keine betrieblichen Auswirkungen haben, aber im Widerspruch zur Kommunikationsstrategie des Unternehmens stehen.

#### **Hinweis für Nutzer**

Unzulässig sind u. a. bewusste Geschäfts- oder Rufschädigungen, Drohungen, Diskriminierungen, Beleidigungen, falsche Tatsachenbehauptungen sowie Äußerungen, die den Betriebsfrieden ernstlich gefährden und die Zusammenarbeit im Unternehmen mit den übrigen Mitarbeiterinnen und Mitarbeitern, aber auch mit dem Arbeitgeber selbst unzumutbar machen. Die Grenze, ob eine Äußerung noch als zulässig angesehen werden kann, ist fließend. Entscheidend ist immer der Einzelfall.

#### **Frage 9: Wie lange gelten Verschwiegenheitsvereinbarungen?**

Die Dauer von Geheimhaltungs- oder Verschwiegenheitserklärungen wird in der Erklärung selbst festgeschrieben. Ist keine automatische Beendigung vereinbart, gilt die nachvertragliche Schweigepflicht gegenüber jeder Person auf unbestimmte Zeit. Dies gilt auch für Verschwiegenheitserklärungen im Rahmen von Arbeitsverträgen. So gilt beispielsweise bei Verträgen nach TVöD eine Verschwiegenheitspflicht über die Beendigung des Arbeitsverhältnisses hinaus, siehe § 3 I TVöD.

#### **Hinweis für Nutzer**

Verarbeiten Sie im Rahmen ihrer Tätigkeit personenbezogene Daten, so gelten besondere Vorschriften. Endet Ihre Verschwiegenheitserklärung zu einem bestimmten Zeitpunkt, bleibt dennoch gemäß § 5 BDSG die Vertraulichkeit von personenbezogenen Daten bestehen.

#### **Frage 10: Soll ich flüchtige geschäftliche Kommunikation sichern?**

Unmittelbar rechtlich relevante Erklärungen wie beispielsweise Vertragsabschlüsse aber auch Mängelrügen oder finanzielle Erklärungen sollten überhaupt nicht über soziale Netzwerke abgegeben werden, da die konvergente Kommunikation aus Mail, Chat und Postings meistens flüchtig ist.

#### **Hinweis für Nutzer**

Verwenden Sie für rechtlich relevante Erklärungen weniger flüchtige elektronische Medien oder Ausdrucke auf Papier. Für herkömmliche E-Mails bestehen zumindest lokale Archivierungen und Rechtsprechung zur Beweiseignung. Im Einzelfall können relevante Erklärungen auch mit einem Screenshot fixiert werden.

### Frage 11: Gibt es Situationen, in denen der Betriebsrat zu kontaktieren ist?

Die Aktivitäten in sozialen Netzwerken könnten auch betriebliche Regelungen zur Mitbestimmung des Betriebsrats betreffen. Teilweise ist der Betriebsrat vor Nutzung bestimmter Dienste zu konsultieren, da ihm Mitwirkungs- oder Mitbestimmungsrechte zustehen. Dies betrifft v. a. Dienste sozialer Netzwerke mit Datenschutz-Relevanz, bei denen der Betriebsrat Informations- und Anhörungsrechte hat, beispielsweise wenn größere Kontaktdatenbestände an einen Dienst übermittelt werden sollen. Ein Mitbestimmungsrecht kann auch dann vorliegen, wenn über einen Dienst Leistungs- oder Verhaltenskontrollen möglich sind, beispielsweise bei Kollaborations-Diensten.

#### **Hinweis für Nutzer**

Wenden Sie sich in Zweifelsfällen an den Betriebsrat und die Unternehmensleitung. Grundsätzliche Zulässigkeitsregelungen zur allgemeinen Internetnutzung ergeben sich ggf. aus einer Betriebsvereinbarung. Teilweise bestehen auch spezielle Betriebsvereinbarungen wie beispielsweise zu Online-Umfragen.

### Frage 12: Ist die Nutzung von sozialen Netzwerken auch während der Arbeitszeit erlaubt?

Viele Unternehmen empfehlen ihren Mitarbeitern ausdrücklich die dienstliche Nutzung von sozialen Netzwerken und fördern entsprechende Aktivitäten. Von einer dienstlichen Nutzung ist auszugehen, wenn Mitarbeiter offiziell im Namen des Unternehmens unter Verwendung der offiziellen E-Mail-Adresse als Kontaktadresse tätig werden. Generell gilt: Für die Nutzung von IT-Systemen eines Unternehmens gelten für alle Mitarbeiterinnen und Mitarbeiter ggf. Regelungen der Betriebsvereinbarung oder der IT-Benutzungsordnung.

#### **Hinweis für Nutzer**

Die private Mitnutzung der IT-Systeme während der Arbeitszeit ist meist in einer Betriebsvereinbarung geregelt, beispielsweise zeitlich beschränkt. Bitte beachten Sie, dass durch die private Nutzung die Erfüllung betrieblicher Aufgaben nicht beeinträchtigt werden darf und dass die beruflichen E-Mail-Adressen meist nicht als Kontaktdaten für private Kommunikation dienen dürfen.

### Frage 13: Darf ich mich über Facebook krank melden?

Von einer Krankmeldung über Facebook ist dringend abzuraten. Jede Mitarbeiterin/jeder Mitarbeiter ist verpflichtet, dem Arbeitgeber die Arbeitsunfähigkeit und deren voraussichtliche Dauer unverzüglich mitzuteilen (vgl. § 5 Abs.1 S.1 Entgeltfortzahlungsgesetz). Auf welche Art die Mitteilung erfolgt, ist zwar im Gesetz nicht festgelegt. Es muss jedoch sichergestellt sein, dass die Krankmeldung die zuständige Stelle rechtzeitig erreicht.

#### **Hinweis für Nutzer**

In den meisten Unternehmen erfolgen Krankmeldungen telefonisch. Diese Gepflogenheit sollte nicht durch Benachrichtigungen mittels sozialer Netzwerke ersetzt werden, da diese die Adressaten nicht unbedingt in der gewünschten Zeit erreichen und zudem nicht in jedem Fall datenschutzfreundlich sind.

#### Frage 14: Darf ich in sozialen Netzwerken Informationen über Bewerberinnen und Bewerber recherchieren?

Das Datenschutzrecht schützt nicht nur die personenbezogenen Daten von Arbeitnehmern, sondern auch von Bewerbern. Um in sozialen Netzwerken Daten eines Bewerbers zu erheben, benötigt ein Arbeitgeber daher in der Regel die ausdrückliche Einwilligung des Bewerbers. Eine Ausnahme liegt nach herrschender Meinung dann vor, wenn die Daten des Bewerbers allgemein, zum Beispiel durch eine Recherche mit Hilfe einer Suchmaschine, zugänglich sind und der Datenerhebung zudem keine schutzwürdigen Interessen des Bewerbers entgegenstehen. Um die schutzwürdigen Interessen des Bewerbers zu achten, sollten Daten nicht in solchen sozialen Netzwerken erhoben werden, die ausschließlich oder teilweise privat genutzt werden.

Die Frage ist allerdings derzeit noch nicht abschließend geklärt, hier sind insbesondere datenschutzrechtliche Aspekte zu beachten. Der Gesetzgeber erarbeitet aktuell das "Gesetz zur Regelung des Beschäftigtendatenschutzes", das u. a. diese Frage regeln soll. Der aktuelle Gesetzentwurf sieht eine Differenzierung zwischen Daten aus freizeitorientierten und beruflich orientierten Netzwerken vor. Soweit soziale Netzwerke der Kommunikation dienen (z. B. Facebook), soll sich der Arbeitgeber nicht über Bewerberinnen und Bewerber informieren dürfen. Im zweiten Fall soll ein Zugriff möglich sein, da diese Netzwerke zur Darstellung der beruflichen Qualifikation der Nutzer bestimmt sind (z. B. XING, LinkedIn).

Die Abgrenzung zwischen freizeitorientierten und berufsorientierten Netzwerken ist jedoch fließend. Facebook wird z. B. zunehmend zur Darstellung von Fertigkeiten und beruflichen Qualifikationen genutzt, indem der Arbeitgeber, die Ausbildung und der berufliche Werdegang dargestellt wird. Auf der anderen Seite werden Netzwerke wie XING häufig auch zur Pflege sozialer Kontakte genutzt, z. B. indem auch Freunde und Bekannte aus dem privaten Bereich aufgenommen werden. Bis zur endgültigen Klärung der Rechtslage sollte daher eine Recherche in sozialen Netzwerken grundsätzlich vermieden werden.

#### **Hinweis für Unternehmen**

Die Suche nach allgemein zugänglichen Informationen im Internet, z. B. über Suchmaschinen wie Google, ist nach derzeitigem Recht datenschutzrechtlich unbedenklich.

#### Frage 15: Ich habe gesehen, dass sich einige meiner Mitarbeiterinnen und Mitarbeiter im Internet bei XING oder LinkedIn vorstellen und habe die Befürchtung, dass sie abwandern könnten — kann ich verhindern, dass sie von Headhuntern am Arbeitsplatz kontaktiert werden?

Aussagen wie "Suche neue Herausforderung" oder "Biete Perspektive" in Profilen beruflich orientierter Netzwerke können ein Indiz für eine grundsätzlich vorhandene Wechselbereitschaft von Beschäftigten sein. Abwerbeversuche von professionellen Personalberatern kann der Arbeitgeber jedoch grundsätzlich nicht verhindern.

#### **Hinweis für Unternehmen**

Der Bundesgerichtshof hat zur Frage des Headhunting am Arbeitsplatz entschieden, dass Headhunter Beschäftigte sowohl auf ihren privaten Mobiltelefonen als auch über den geschäftlichen Festnetzanschluss anrufen dürfen. Die Direktansprache am Arbeits-

platz ist daher zulässig, sofern es sich um ein erstes, nur der Kontaktaufnahme dienendes Gespräch handelt.

#### Frage 16: Dürfen wir Stellenanzeigen twittern oder auf XING verbreiten?

Ja, die Veröffentlichung von Stellenanzeigen in sozialen Netzwerken ist zulässig. Unternehmen können dadurch einen großen Kreis potentiell Interessierter ansprechen. Es sollte aber darauf geachtet werden, dass auch bei der Nutzung von sozialen Netzwerken die Regelungen von Betriebsvereinbarungen eingehalten werden. Insbesondere ist darauf zu achten, dass in der externen Stellenanzeige keine geringeren Anforderungen an die Bewerberinnen und Bewerber gestellt werden als in der internen Stellenausschreibung.

#### **Hinweis für Unternehmen**

Gerade bei schnelllebigen Medien ist es sehr wichtig, bei Stellenanzeigen auf Konformität mit dem Allgemeinen Gleichbehandlungsgesetz zu achten — vermeiden Sie daher diskriminierende Formulierungen und Präsentationen.

#### Frage 17: Darf ich als Vorgesetzter/als Vorgesetzte Einfluss auf die außerdienstlichen Aktivitäten meiner Mitarbeiterinnen und Mitarbeiter in sozialen Netzwerken nehmen?

Grundsätzlich darf der Arbeitgeber keinen Einfluss darauf nehmen, wie Mitarbeiterinnen und Mitarbeiter sich in ihrer Freizeit verhalten, da das außerdienstliche Verhalten der Regelungsbefugnis des Arbeitgebers prinzipiell entzogen ist. Der/Die Vorgesetzte kann daher nicht die von seinem Mitarbeiter/seiner Mitarbeiterin im Internet außerhalb der Arbeitszeit unternommenen Aktivitäten einschränken, untersagen oder sanktionieren.

#### **Hinweis für Unternehmen**

Ausnahmen von diesem Grundsatz, dass sich der Arbeitgeber nicht in die Freizeitaktivitäten der Mitarbeiter einmischen darf, sind nur sehr begrenzt möglich, z. B. falls Betriebs- und Geschäftsgeheimnisse betroffen sind oder sich der Mitarbeiter im Internet unternehmensschädlich äußert.

#### Frage 18: Ein wichtiger Mitarbeiter hat gekündigt. Ich habe die Befürchtung, dass er Kundendaten und -kontakte, die er über soziale Netzwerke geknüpft hat, mitnehmen möchte. Darf er das?

Hier gilt zunächst der Grundsatz, dass ein Arbeitnehmer die Informationen, die bei ordnungsgemäßer Organisation für die Tätigkeit notwendig sind, am Arbeitsplatz hinterlassen muss. Für die Beantwortung der Frage, ob der Arbeitgeber die Herausgabe des gesamten Accounts oder einzelner Kundendaten und -kontakte verlangen kann, kommt es entscheidend darauf an, wem der Account gehört.

Ein rein dienstlicher Account muss vom Mitarbeiter komplett zurückgelassen werden. Etwas schwieriger ist die Abgrenzung bei einem Account, der sowohl privat als auch dienstlich genutzt wird. Hier muss dem Mitarbeiter die Möglichkeit gegeben werden, rein private Kontakte und Korrespondenz zu löschen. Hinsichtlich der dienstlichen Kontakte wird regelmäßig ein Anspruch des Arbeitgebers auf Herausgabe der im Account gespeicherten Kundendaten und entsprechender Korrespondenz bestehen.

**Hinweis für Unternehmen**

Achten Sie beim Ausscheiden des Mitarbeiters darauf, dass alle Passwörter und Zugangscodes von dienstlichen Accounts übergeben werden und der Mitarbeiter keine Kopien der Geschäftskontakte mitnimmt. Bei einem rein privaten Account besteht grundsätzlich keine Herausgabepflicht.

## 7. PLATTFORMSPEZIFISCHE BESONDERHEITEN

### 7.1 Facebook

#### Art des Netzwerks

Facebook ist das größte soziale Netzwerk mit mehr als 1 Milliarde Nutzer weltweit und ca. 22 Millionen deutschlandweit (April 2012). Facebook wird vor allem von Leuten zwischen 18 und 34 Jahren dazu genutzt, um sich zu über Statusnachrichten, Bilder, Videos und Veranstaltungen auszutauschen und sich mit Freunden, Bekannten oder Arbeitskollegen zu vernetzen.

Neben dem privaten Nutzen kann die Plattform auch für Marketing- und Personalmarketingzwecke verwendet werden. Für Recruiting eignet sich diese Plattform nicht, da die Profile und die Suche nicht dafür ausgerichtet sind.

#### Anlegen eines Profils

Zur Registrierung bei Facebook müssen Sie Vorname, Nachname, E-Mail-Adresse, Geschlecht und das vollständige Geburtsdatum angeben. Facebook erlaubt Ihnen keine pseudonyme Nutzung und hat dies in seinen Erklärungen zu Rechten und Pflichten der Nutzer festgeschrieben.

Bei einer dienstlichen Nutzung des Profils sollte der Klurname und eine berufliche individuelle E-Mail-Adresse verwendet werden. Bei gemeinschaftlich genutzten Accounts (z. B. innerhalb einer PR-Abteilung) kann auch eine allgemeine E-Mail-Adresse verwendet werden. Die Sichtbarkeit des Geburtsdatums sollte in den Profileinstellungen ausgeblendet werden.

Facebook fordert jeden neuen Nutzer dazu auf, über die eingetragene E-Mail-Adresse Freunde zu finden. Dieser Schritt ist freiwillig und sollte durch den Link "Diesen Schritt überspringen" ausgeblendet werden. Der Zugriff auf berufliche E-Mail-Konten durch Facebook ist in der Regel nicht gestattet.

#### Einsatz von Verschlüsselung

In der Standardkonfiguration nutzen nur die Anmeldung und das Bearbeiten der Kontoeinstellungen das verschlüsselte Protokoll HTTPS. Sie können jedoch die Option "Sicheres Stöbern" aktivieren, damit Facebook nach Möglichkeit alle Verbindungen zwischen dem Web-Browser und dem Web-Server auf dem Übertragungsweg verschlüsselt.

#### Funktionsumfang der Zugriffskontrollen

Sie können mit einigem Aufwand die Privatsphäreoptionen bei Facebook differenziert und feingranular anpassen. Facebook unterscheidet dazu grundsätzlich folgende Nutzerkreise:

- Nutzer im Internet, die nicht Mitglieder von Facebook sind
- alle Mitglieder von Facebook
- Kontakte zweiten Grades ("Freunde von Freunden")
- Kontakte ersten Grades ("Freunde")
- Kontakte ersten Grades, die nicht als Bekannte markiert wurden ("Freunde ohne Bekannte")
- Benutzerdefinierte Listen, bestehend aus Kontakten ersten Grades, und
- Anwender ("Nur ich")

Anhand dieser Gruppen und Listen können Sie den Zugriff auf nahezu jede bereitgestellte Information schrittweise limitieren. Gästebucheinträge und Fotoverknüpfungen können zudem grundsätzlich nur von Kontakten ersten Grades erzeugt werden. Sie müssen jedoch Bedenken, dass die generellen Privatsphäreneinstellungen von Facebook, also ohne Berücksichtigung von z. B. Fotoalben, über 60 Einzeloptionen bereitstellen. Auch die vordefinierten Einstellungen “Öffentlich” und “Freunde” (siehe Abbildung 7) helfen Ihnen kaum weiter, da sie in einzelnen Optionen sehr unterschiedlich umgesetzt sind.

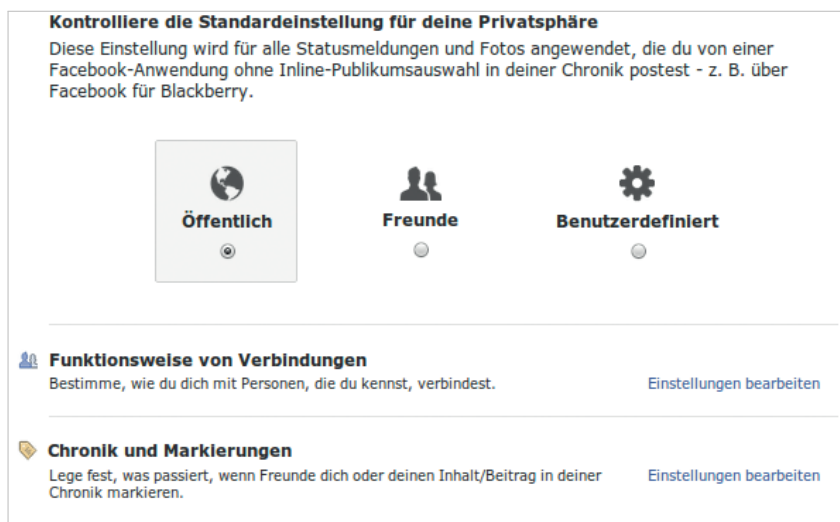


Abbildung 7. Privatsphäreneinstellungen bei Facebook mit vordefinierten Einstellungen

### Standardkonfiguration

In der Standardkonfiguration sind die Privatsphäreneinstellungen bei Facebook als “Öffentlich” eingestellt. Eine eindeutige Aussage über die Sichtbarkeit der Daten eines Nutzers lässt sich daraus jedoch nicht ableiten, lediglich eine Tendenz. So sind Kontaktdaten eines Nutzers auch bei der Standardkonfiguration “Öffentlich” nur für Kontakte ersten Grades sichtbar, wohingegen Informationen zu “Arbeit und Ausbildung” für alle einsehbar sind, ebenso wie die Kontaktliste. Sie sollten also unbedingt die Konfiguration der Privatsphäreneinstellungen nach einer Neuanmeldung prüfen.

### 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.

Einziges Wermutstropfen: Man kann auch nach der E-Mail-Adresse suchen. An für sich ist das kein kritischer Punkt. Allerdings kann diese Funktion zur De-Pseudonymisierung

missbraucht werden, wenn eine pseudonyme E-Mail-Adresse, wie beispielsweise `glitzerfee@emailprovider.de` auch in anderen Kontexten, z. B. einem beliebigen Internetforum, verwendet wird.

### Zugriffsprotokollierung

Facebook zeichnet für Profilbesitzer nicht auf, wer das Profil besucht hat. Allerdings wird von Facebook registriert und an die Gruppenmitglieder veröffentlicht, wann ein Nutzer in sein eigenes Postfach geschaut und eine bestimmte Nachricht gelesen hat. Dieses “Gesehen von” Feature lässt sich in den Einstellungen nicht deaktivieren, kann aber durch inoffizielle Tricks blockiert werden.<sup>73</sup>

### Unternehmensseiten

Um eine Unternehmensseite zu erstellen, müssen Sie bereits bei Facebook registriert sein. Zur Eingruppierung Ihrer Seite können Sie zwischen “Lokales Unternehmen oder Ort”, “Unternehmen, Organisation oder Institution”, Marke oder Produkt, Künstler, Band oder öffentliche Person, Unterhaltung, Anliegen oder Gemeinschaft wählen.

Unternehmensseiten werden immer mit Personen-Profilen verknüpft. Diese als Administratoren eingetragenen Personen können dann im Namen des Unternehmens Beiträge verfassen. Diese Verknüpfung mit eventuell sogar privaten Accounts ist als äußerst kritisch zu bewerten. Sinnvoll erscheint es hier, neue Profile mit E-Mail-Adressen des Unternehmens zu generieren, und diese Profile dann als Seiten-Administratoren einzutragen. Die Zugangsdaten für diese zu diesem Zweck angelegten Profile sollten dann sicher, z. B. bei der IT-Administration oder der zuständigen Pressestelle, hinterlegt werden.

#### **Hinweis für Nutzer und Unternehmen**

Facebook erzeugt zu jeder Unternehmensseite eine E-Mail-Adresse. Inhalte, die an diese E-Mail-Adresse gesendet werden, erscheinen wie normale Beiträge im Profil auf der Unternehmensseite. Diese Beiträge werden vorher nicht geprüft. Jede Person, die in Kenntnis dieser E-Mail-Adresse ist, kann demnach Beiträge im Profil veröffentlichen. Daher muss diese Adresse unbedingt geheim gehalten werden. Um die Gefahr eines Missbrauchs so klein wie möglich zu halten, wird von der Verwendung dieser E-Mail-Adresse abgeraten.

### Sicherheitshinweise

Es wird angenommen, dass ein dienstlicher Facebook-Account angelegt und verwendet wird.

- **Verschlüsselte Übertragung** Grundsätzlich sollte die sichere Übertragung von Daten über HTTPS aktiviert werden. Facebook nennt diese Option “Sicheres Durchstöbern”.
- **Anmeldebenachrichtigungen und Anmeldebestätigungen** sollten zur Erhöhung der Account-Sicherheit aktiviert werden.
- **Verknüpfte Konten** Offizielle Accounts oder dienstliche Mitarbeiter-Accounts sollten nicht mit privaten Konten verknüpft werden. Generell sollten Sie so wenige Konten wie möglich miteinander verknüpfen.

<sup>73</sup>Beispielsweise mittels der Browser Extension “Adblock Plus”, siehe <http://pc.de/web/facebook-deaktivieren-4231>



- **Bekannte Geräte/Aktive Sitzungen** Hier können Sie zwar keine Einstellungen vornehmen, aber Sie können Geräte und Sitzungen erkennen, die mit Ihrem Account verknüpft sind. Geräte und Sitzungen können hier beim Missbrauchsverdacht entfernt werden.
- **Privatsphäreneinstellungen** Im Zweifel sind alle Angaben, die Sie in Facebook einstellen, öffentlich oder können öffentlich werden. Versuchen Sie daher vor der Veröffentlichung abzuschätzen, ob eine mögliche Veröffentlichung von Informationen Schaden für Ihr Unternehmen oder Sie selbst auslösen kann (Rufschädigung, Verstöße gegen Verträge etc.).
- **Nachrichten** Es sollten in der Regel keine unternehmensinternen Dokumente über Facebook versendet werden.
- **Geburtsdatum** Ihr Geburtsdatum sollten Sie nicht öffentlich bekannt geben. Daher sollte die Sichtbarkeit des Geburtsdatums für Dritte deaktiviert werden.
- **Adressbuchabgleich** Der Upload von Adressbüchern oder der Zugriff auf E-Mail-Konten durch Dritte ist in der Regel nicht gestattet. Die Funktion “Freunde Finden” sollten daher nicht in Verbindung mit beruflichen Adressbüchern verwendet werden.
- **Nachrichten** An persönliche Nachrichten an Facebook-Mitglieder können Dateien beliebiger Art angehängt werden. Bitte beachten Sie, dass der Upload von internen Dateien, Berichten, Protokollen usw. an Dritte (hier: Facebook) in der Regel nicht gestattet ist. Jegliche Information, die nicht zur Veröffentlichung bestimmt ist, darf nicht über Facebook versendet werden.
- **Werbeanzeigen** Werbeanzeigen sollten immer deaktiviert werden. Diese Option ist in den Standardeinstellungen aktiviert.
- **Anwendungen und Webseiten** Von Anwendungen auf Facebook ist generell eher abzuraten, denn diese geben ungefragt Daten (Name, Profilbild, Geschlecht, Freundesliste, Nutzerkennnummer, Nutzernamen und Informationen, die mit “Allen” geteilt werden) von Ihnen und Ihren Freunden weiter. Außerdem ist es ratsam, beliebte Anwendungen zu blockieren oder gleich alle zu deaktivieren, damit Sie keine Nachrichten über die Verwendung von Anwendungen durch Freunde bekommen. Ansonsten könnte nämlich schnell Ihre Infowall zugesamt werden.
- **Wie Nutzer Ihre Informationen an Anwendungen weitergeben, die sie nutzen** Auch hier ist zu empfehlen in “Einstellungen bearbeiten” alle Häkchen zu den Informationen zu entfernen, um so wenige Daten wie möglich weiter zu geben.
- **Umgehende Personalisierung** Generell ist auch an dieser Stelle zu empfehlen, die umgehende Personalisierung zu deaktivieren. Allerdings können die Informationen im Einzelfall auch interessant sein, um ähnlich interessierte Personen kennen zu lernen, die z. B. den selben Artikel gelesen haben.
- **Öffentliche Suche** Bei beruflichen Profilen oder Unternehmensseiten ist es zu empfehlen, die öffentliche Suche zu aktivieren, damit Ihr Profil auch über Suchmaschinen gefunden werden kann.
- **Blockierte Personen und Anwendungen** Blockieren heißt, dass das Einsehen Ihrer Informationen und Beiträge und die Interaktion mit Ihnen untersagt werden. Es besteht die Möglichkeit, einzelne Nutzer (diese werden nicht darüber benachrichtigt), Anwendungsanfragen und Veranstaltungseinladungen zu blockieren.

#### **Hinweis für Nutzer und Unternehmen**

Besonders auf Smartphones und Tablets (z.B. iPhone, iPad, Xoom etc.) kann ein einzi-

ger Klick bereits den Upload des Adressbuches an den Dienstanbieter auslösen. Daher sollten Sie bei Verwendung der Facebook-App darauf achten, die Funktion “Freunde finden – Finde Freunde auf deinem Handy” nicht zu benutzen, um Kontakte automatisiert durch Übertragung des Adressbuches zu finden. Zwar bietet Facebook an, hochgeladene Kontaktdaten wieder zu löschen. Ob dies aber wirklich geschieht ist nicht nachvollziehbar.

### Abmelden bei der Plattform/Löschungsumfang

Sich bei Facebook abzumelden ist ein aufwändigeres Unterfangen: Zwar gibt es in den Kontoeinstellungen eine Funktion “Konto deaktivieren”, allerdings können Sie damit Ihr Konto nur zeitweise deaktivieren, aber nicht löschen. Sie können dafür aber festlegen, wie lange das Profil deaktiviert sein soll. Diese Prozedur wird bei Facebook als die übliche dargestellt.

Löschen können Sie Ihr Profil nur, indem Sie im Hilfebereich “Facebook-Grundlagen”, Unterpunkt “Verwalten deines Kontos” und weiter “Einstellungen und Löschen eines Kontos” den Hilfetext “Wie kann ich mein Konto dauerhaft löschen?” aufrufen und dort dem Link zu einem speziellen Formular folgen. Daraufhin wird das Konto für 14 Tage deaktiviert und nach Ablauf dieser Frist automatisch gelöscht. In der Zwischenzeit können Sie sich jederzeit anmelden und damit das Löschen verhindern. Auch die Anmeldung über eine Drittanbieter-Anwendung gilt als Widerruf des Ausstiegswunsches.

Der Löschungsumfang ist gut: Gästebuch- und Foreneinträge, Fotoverknüpfungen und Kommentare zu einem Blog entfernt Facebook vollständig.

## 7.2 Google+

### Art des Netzwerkes

Google+ ist das soziale Netzwerk von Google und dient dazu, die bestehenden Dienste von Google zu verknüpfen und die Inhalte daraus mit anderen zu teilen. Im Allgemeinen ist Google+ weniger dazu geeignet, sich mit etablierten Kontakten in Verbindung zu setzen, da die Verdichtungsrate von Google+ im Gegensatz zu Facebook eher gering ist. Stattdessen ist Google+ sehr gut dafür geeignet, neue Kontakte aufzubauen. Es ist daher wichtig, aktiv nach interessanten Benutzern zu suchen und sie zu den eigenen Kontakten hinzuzufügen. Es wird im Gegensatz zu Facebook im Allgemeinen keine Gegenseitigkeit erwartet – man fügt jemand anderes zu seinen Kreisen hinzu, weil dessen Beiträge einen interessieren, aber das bedeutet nicht, dass dieser sich verpflichtet fühlen muss, dasselbe zu tun.

Kontakte werden auf Google+ in sogenannte “Circles” unterteilt, welche man nach unterschiedlichen Themengebieten und Interessen ordnen kann. Wenn man einen Beitrag auf Google+ setzt, muss man sich entscheiden, ob man diesen öffentlich setzt, oder ob man diesen nur für bestimmte Circles sichtbar macht (z.B. “Arbeitskollegen”, “An Erneuerbare Energien Interessierte”, oder beides auf einmal.)

Diese Circles kann man darüber hinaus auf Google+ veröffentlichen, so dass andere Benutzer sie komplett übernehmen können – wenn zum Beispiel ein Benutzer einen Kreis voller Wissenschaftler erstellt hat, dann kann er diesen veröffentlichen, und seine Leser, die ebenfalls an Wissenschaftlern interessiert sind, können alle Mitglieder des Circles zu ihren Kontakten hinzufügen und deren Beiträge verfolgen. Wird man von einem Google+-

Mitglied mit sehr vielen Lesern in so einem Circle veröffentlicht, so kann es leicht passieren, dass man in einem einzigen Tag mehrere hundert neue Leser dazu bekommt. Daher lohnt es sich, stetig neue und interessante Beiträge auf Google+ zu veröffentlichen, da damit die Anzahl der Leser sehr schnell ansteigen kann.

### Anlegen eines Profils

Bei einer dienstlichen Nutzung des Profils ist in der Regel der Klarname und die berufliche E-Mail-Adresse zu verwenden. Bei gemeinschaftlich genutzten Accounts (z. B. PR) kann auch eine allgemeine berufliche E-Mail-Adresse verwendet werden. Die Sichtbarkeit des Geburtsdatums sollte in den Profileinstellungen ausgeblendet werden.

Unternehmensseiten werden in Google+ immer mit Personen-Profilen verknüpft. Diese als Administratoren eingetragenen Personen können dann im Namen des Unternehmens Beiträge verfassen. Die Ersteller von Unternehmensseiten heißen Eigentümer. Diese Verknüpfung mit evtl. sogar privaten Accounts ist als äußerst kritisch zu bewerten. Sinnvoll erscheint es hier, neue Google-Profile zu generieren, und diese Profile dann als Seiten-Administratoren einzutragen. Die Zugangsdaten für diese zu diesem Zweck angelegten Profile können dann sicher bei einer IT-Administration oder der zuständigen Pressestelle hinterlegt werden.

#### Hinweis für Nutzer und Unternehmen

Google bietet im Dashboard eine Übersicht über alle bei Google gespeicherten Daten an. Hier können Sie zudem auch Einstellungen für verschiedene Google-Dienste ändern.

### Sicherheitshinweise

Seit kurzer Zeit sind (fast) alle Google Dienste miteinander verknüpft. Erstellt man ein Google+ Konto (Profil), wird damit automatisch auch ein Google E-Mail-Konto erstellt, worüber man Zugriff auf andere Google Dienste (z. B. Picasa Webalbum) bekommt. Diese Verknüpfung von Konten ist datenschutzrechtlich und sicherheitstechnisch kritisch zu bewerten. Daher sollte ein Profil so gut wie möglich gegen Zugriffe von Dritten abgesichert werden.

- **Verbundene Konten** Offizielle Accounts oder dienstliche Mitarbeiter-Accounts sollten nicht mit weiteren privaten Konten verknüpft werden. Generell sollten so wenige Konten wie möglich miteinander verknüpft werden.
- **Profil und Datenschutz** Im Zweifel sind alle Angaben, die Sie in Google+ einstellen, öffentlich oder können öffentlich werden. Versuchen Sie daher vor der Veröffentlichung abzuschätzen, ob eine mögliche Veröffentlichung von Informationen Schaden für Ihren Arbeitgeber oder Sie selbst auslösen kann (Rufschädigung, Verstöße gegen Verträge etc.).
- **Geburtsdatum** Ihr Geburtsdatum sollten Sie nicht öffentlich bekannt geben. Daher sollte die Sichtbarkeit des Geburtsdatums für Dritte deaktiviert werden.
- **Fotos** Sie können in den Kontoeinstellungen von Google+ vermerken, ob die von Ihnen veröffentlichten Bilder von Dritten heruntergeladen werden dürfen, und ob diese Bilder geographische Angaben enthalten sollen. Zudem kann die Gesichtserkennung auf Bildern aktiviert werden. Wenn kein expliziter Grund für diese Funktionen spricht, sollten die Optionen deaktiviert werden.

- **+1 auf Websites Dritter** Diese Funktion sollte in der Regel ebenfalls deaktiviert werden. Ist diese Funktion aktiviert, werden +1-Meldungen auf Webseiten Dritter aktiviert. Die +1-Wertungen sind somit auf anderen Webseiten sichtbar. Dies könnte als werbende Maßnahme angesehen werden.

#### **Hinweis für Nutzer und Unternehmen**

Unter “Kontoeinstellungen – Sicherheit” sollte zur Wiederherstellung eines Passwortes eine weitere E-Mail-Adresse eingetragen werden. Im Falle eines Zugriffs durch Dritte kann dann das Passwort zurückgesetzt und ein neues Passwort an die Ersatz-E-Mail-Adresse gesendet werden, um wieder Kontrolle über den Account zu erhalten.

## 7.3 Twitter

### Art des Netzwerkes

Twitter wurde 2006 gegründet und ist eine Microblogging-Plattform. Twitter unterscheidet sich von anderen sozialen Netzwerken durch seinen Kurznachrichten-Charakter und durch die Öffentlichkeit aller Nachrichten. Eine Twitter-Nachricht (oder auch Tweet) ist auf 140 Zeichen beschränkt und kann, einmal getwittert, von jedem Internetnutzer weltweit gesehen werden. Bekannt wurde Twitter vor allem als Nachrichtenkanal, über den sich aktuelle Ereignisse nahezu in Echtzeit verfolgen lassen (z. B. die Notwasserung des US-Airways-Flugs 1549 auf dem Hudson River im Jahr 2009).

Zurzeit nutzen Twitter über 300 Millionen Menschen weltweit, um sich öffentlich zu verschiedenen Themen, Marken oder Personen auszutauschen. 54 Prozent der Twitternden sind weiblich und 46 Prozent männlich und entgegen der gängigen Meinung nutzen ebenso viele der 30 bis 49-Jährigen Twitter wie die Altersgruppe der 18 bis 29-Jährigen.

In Deutschland wird Twitter von ca. 500.000 Menschen genutzt. Die vergleichsweise kleinen Nutzerschaft ist jedoch sehr aktiv: Twitter ist nach Facebook das meistbesuchte Social Network. Auf Twitter finden sich neben Privatpersonen auch Unternehmen, Journalisten, Blogger und weitere Multiplikatoren. Der Kanal eignet sich sowohl für die Direktkommunikation mit dem Kunden (B2C) als auch für Kommunikation zwischen Unternehmen (B2B) sowie für Öffentlichkeitsarbeit (Public Relations).

### Registrieren / Anmelden

Zur Erstellung Ihres Twitter-Profiles registrieren Sie sich mit Ihrem Vornamen, Nachnamen, Ihrer E-Mail-Adresse und einem Passwort auf der Startseite [www.twitter.com](http://www.twitter.com). Wenn Sie ein Unternehmensprofil bei Twitter anlegen, beachten Sie, dass Sie wenn möglich eine allgemeine E-Mail-Adresse verwenden, falls weitere Kollegen den Twitter-Account betreuen sollen. Twitter überprüft Namen, E-Mail-Adresse und die Passwort-Stärke und macht Ihnen Vorschläge für einen verfügbaren Twitter-Benutzernamen (basierend auf Ihren angegebenen Daten).

Der Benutzername besteht aus maximal 9 Zeichen und sollte möglichst aussagekräftig sein. Der Benutzername kann später zwar noch geändert werden, Sie sollten jedoch bedenken, dass dann Follower unter Ihrem alten Namen nicht mehr fündig werden. Sobald Sie ein Konto erstellt haben, ist dieses online und theoretisch im Web sichtbar.

## Anlegen eines persönlichen Profils

Nach der Registrierung öffnet sich das Twitter-Profil, das Sie direkt bearbeiten können. Die Elemente eines Profils sind das Profilbild (oder auch Thumbnail), Name, Standort, die Kurzbiografie und die Verlinkungen.

Für Ihr privates Profil sollten Sie am besten ein Bild von sich wählen, für das Firmenprofil kommen beispielsweise ein eigens entworfenes Social Media Logo oder eine Abbildung des Unternehmensgebäudes in Frage. Der Name sollte seriös gewählt werden, damit Sie bei Twitter auch gefunden werden können. Er repräsentiert Sie in der Twitter-Welt. Auch hier gilt, dass der Name wieder geändert werden kann, was sich wegen der Wiedererkennbarkeit des Kanals jedoch nur begrenzt empfiehlt.

Die Standortangabe ist freiwillig, für Unternehmensprofile aber empfehlenswert. In der Kurzbiografie ("Bio") stellen Sie sich oder Ihr Unternehmen in wenigen Worten vor. Das können z. B. Ihr Arbeitsschwerpunkt, Ihr Geschäftsfeld oder Ihre Berufsbezeichnung aber auch Hobbys oder Interessen sein. Sie haben für Ihre Beschreibung maximal 160 Zeichen zur Verfügung.

Zu den Verlinkungen gehört allen voran Ihre (Unternehmens-)Webseite. Hier können aber auch Blogs oder Social Media Profile verlinkt werden, die das Unternehmen oder die Person näher vorstellen. Weiter können Sie Ihren Twitter-Kanal direkt mit Facebook verbinden, so dass alle Twitter-Nachrichten auch auf Facebook gepostet werden. Twitter könnte außerdem in Ihre Webseite eingebunden werden.

## Einstellungen Konto / Privatsphäre

Zur Personalisierung Ihres Profils können Sie unter dem Reiter "Design" der Profileinstellungen weitere Einstellungen vornehmen, wie beispielsweise die Wahl eines Hintergrundbildes oder der Farbgebung. Twitter bietet hier verschiedene Hintergrundbilder zur Auswahl an, es können aber auch eigene Bilder hochgeladen werden. Für Unternehmensprofile wird der Hintergrund der Webseiten empfohlen.

Unter dem Reiter "Account" verwalten Sie die technischen Einstellungen Ihres Twitter-Kontos wie den Benutzernamen, E-Mail-Adresse für Benachrichtigungen, Sprache, Land und verschiedene Einstellungen für Nachrichten. Wenn Sie Fotos twittern möchten, müssen Sie unter dem Punkt "Medien versenden" Häkchen setzen. Die Verwendung von HTTPS (Tweet Sicherheit) sollte immer aktiviert sein.

### Hinweis für Nutzer und Unternehmen

Der Button "Freunde finden" ermöglicht es, über Googlemail, Yahoo oder Messenger das eigene Adressbuch zu durchsuchen und so weitere Freunde auf Twitter zu finden. Hier sollte man besonders als Unternehmensprofil Vorsicht walten lassen.

## Sicherheitshinweise

Es wird angenommen, dass ein dienstlicher Twitter-Account angelegt und verwendet wird.

- **Name** Bei der Registrierung sind der Klarname und die berufliche E-Mail-Adresse zu verwenden.
- **Adressbuchabgleich** Der Upload von Adressbüchern oder der Zugriff auf E-Mail-Konten durch Dritte ist in der Regel nicht gestattet. Diese Funktionen sollten daher nicht mit Adressbüchern oder E-Mail-Konten Ihres Unternehmens verwendet werden.

- **Sichere Verbindung** In den Einstellungen ist die Einstellung “Nutze immer HTTPS” zu setzen.
- **Apps** Die Verwendung und Verknüpfung von Applikationen (Apps) mit dem Account sollte nur verwendet werden, falls diese für die dienstliche Verwendung sinnvoll erscheinen.

#### **Hinweis für Nutzer und Unternehmen**

Sie sollten insbesondere bei Verwendung der Twitter-App auf Smartphones und Tablets darauf achten, die Funktion “Folge deinen Freunden” nicht zu benutzen, um nicht Kontakte automatisiert durch Übertragung des Adressbuches zu finden. Twitter bietet die Funktion an, einmal bereits hochgeladene Adressen wieder löschen zu können. Ob dies wirklich geschieht ist allerdings nicht ersichtlich.

## 7.4 XING

### Art des Netzwerkes

XING wird vorrangig zum Finden und Unterhalten beruflicher Kontakte genutzt. Nutzer und Unternehmen können z.B. Profile anlegen, Arbeitsstellen suchen oder ausschreiben und sich an Diskussionen in den rund 55.000 Gruppen zu unterschiedlichen Interessengebieten beteiligen. Die kostenpflichtigen XING-Versionen bieten auch interaktive Community-Funktionen.

### Anlegen eines Profils

Wenn Sie bei XING Mitglied werden möchten, dann müssen Sie Ihren Namen, Vornamen, Ihre E-Mail-Adresse, und die “Basisinformationen” Art der Beschäftigung, Stellenbezeichnung, Unternehmen, Arbeitsort, und Branche angeben.

### Einsatz von Verschlüsselung

Die Plattform nutzt die Verschlüsselung über die gesamte Nutzersitzung hinweg.

### Funktionsumfang der Zugriffskontrollen

Sie können bei XING auf nur wenige Zugriffskontrollen zurückgreifen. So können Sie z. B. jegliche Arten von Kontaktdaten (Adressen, Telefonnummern etc.) für andere Plattformnutzer individuell freischalten. Auch Ihre Kontaktliste können Sie feingranular sichtbar machen. Gleiches gilt für die Sichtbarkeit der Gruppen, denen Sie beitreten. Sie können auch konfigurieren, wer Gästebucheinträge erstellen darf. Allerdings können Sie nur im Nachgang ungewollte Einträge wieder löschen. Für andere Daten, z. B. zur Ihrer Ausbildung und beruflichem Werdegang finden Sie jedoch keine Privatsphärenoptionen zum Schutz vor anderen Plattformmitgliedern.

Bedenken Sie, dass die XING-Funktion “Zeige alternative Verbindungen: “Was wäre, wenn diese Person kein direkter Kontakt wäre” anderen Plattformmitgliedern Kontakte aus Ihrer Kontaktliste verraten kann – auch wenn Sie die Kontaktliste explizit verborgen haben. Damit sind bestimmte Einschränkungen in Ihren Privatsphärenoptionen teilweise unwirksam.

## Standardkonfiguration

In der Standardkonfiguration ist ein Großteil Ihrer Daten wie z. B. der berufliche Werdegang, Bildungskarriere oder Interessen geschäftlicher und privater Natur auch für Nichtplattformmitglieder lesbar.

## Suchfunktion

Die Suchfunktion bei XING erlaubt sehr vielfältige Suchkriterien, zumindest für zahlende Plattformmitglieder. Andere XING-Nutzer können Sie beispielsweise über Ihre Interessen, Angebote oder Angaben zu besuchten Hochschulen finden. Die Suche kann dabei sehr unspezifisch, ähnlich einer Rasterfahndung erfolgen. Wenn Sie in solchen Suchanfragen nicht auftauchen wollen, müssen Sie auf bestimmte Angaben in Ihrem Profil verzichten.

Abbildung 8. Die Mitgliedersuche bei XING bietet umfangreiche Suchkriterien für zahlende Mitglieder

## Zugriffsprotokollierung

XING bietet Ihnen auf der Startseite eine Anzeige der “Besucher Ihres Profils”. Um die Profile der anderen Nutzer öffnen zu können, müssen Sie allerdings ein zahlender “Premiumnutzer” werden. Ansonsten sehen Sie nur das Profilfoto.

Sind Sie ein Premiumnutzer, so zeigt XING Ihnen zusätzlich an, über welchen Weg Ihre Besucher auf Ihr Profil gelangt sind. Dies müssen Sie umgekehrt berücksichtigen, wenn Sie andere Profile aufrufen. Wenn Sie nicht möchten, dass andere XING-Nutzer wissen, dass Sie auf einem speziellen Weg zu einem Profil gelangt sind, dann müssen Sie eine andere Variante anwenden das Profil zu öffnen.

Das Datum und die Uhrzeit des Profilaufrufs protokolliert XING nicht, es ist aber die Abfolge der Besucher erkennbar. Das automatische Protokollieren können Sie nicht abschalten.

### 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?” (siehe Abbildung 9 und 10).

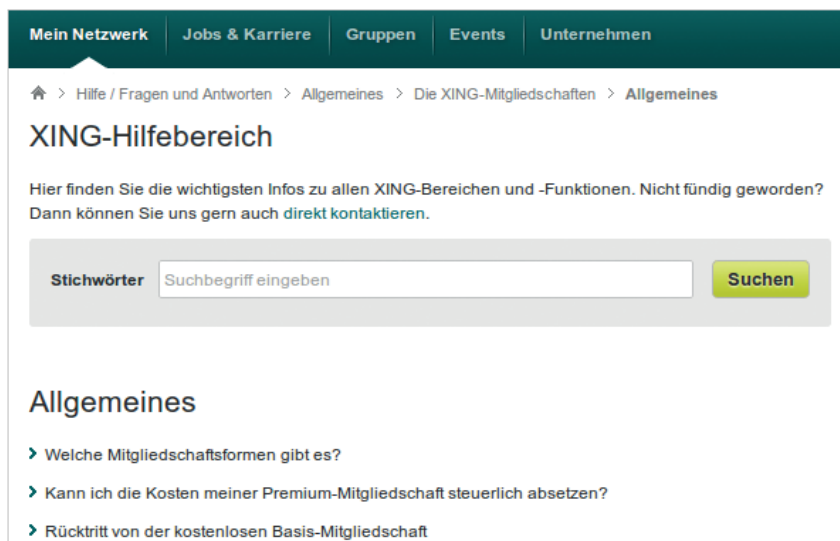


Abbildung 9. Aufruf der Webseite zum Beenden der Mitgliedschaft bei XING

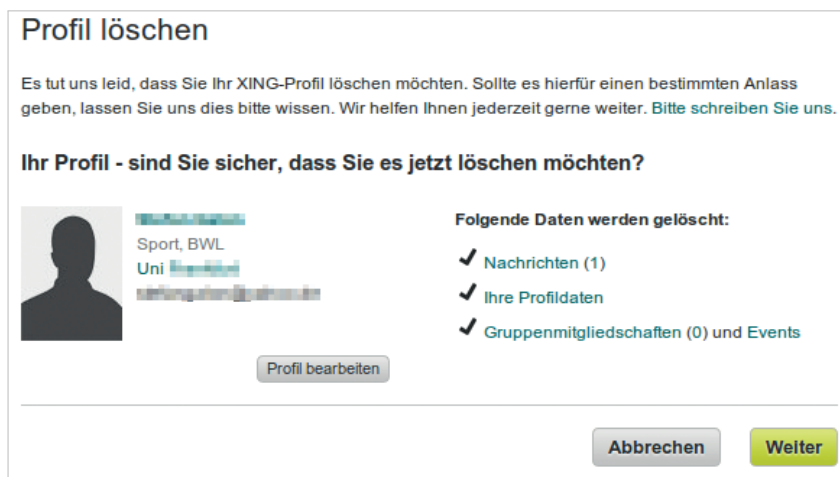


Abbildung 10. Ausschnitt aus der Abmeldeseite bei XING

Nach dem Löschen erscheint Ihr Name weiterhin bei Einträgen in Gruppenforen und bei Einträgen in Gästebüchern anderer Nutzer. Zu bedenken ist, dass Ihre Einträge in



Gruppenforen möglicherweise außerhalb der Plattform zugänglich sind, je nachdem, ob das Forum selbst öffentlich ist und wie Ihre Privatsphärenoptionen bei der Eintragerzeugung eingestellt waren.

## 7.5 LinkedIn

### Art des Netzwerkes

LinkedIn ist das größte soziale Netzwerk für Businesskontakte mit weltweit über 150 Mio. Mitgliedern (Februar 2012) und über 2 Mio. Mitgliedern im deutschsprachigen Raum. Führungskräfte aus allen Fortune-500-Unternehmen sind bei LinkedIn Mitglieder und es existieren mehr als 2 Mio. Unternehmensseiten und mehr als 1 Mio. LinkedIn-Gruppen.

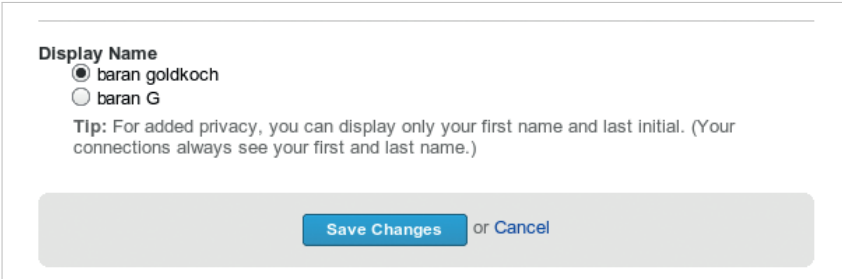
### Anlegen eines Profils

Um sich bei LinkedIn anzumelden, müssen Sie Ihren vollständigen Namen, E-Mail-Adresse, Land und Postleitzahl eingeben. Zusätzlich sind Daten über das Arbeitsleben wie Berufsstatus, Firma, Stellung, Branche und, beim Berufsstatus "Student", Bildungsangaben wie Hochschule und Dauer der Ausbildung Pflichtangaben. Einige Angaben entfallen bei einem bestimmten Berufsstatus.

Sie können auf LinkedIn mehrere E-Mail-Adressen verwenden und Ihr Profil in mehreren Sprachen speichern, um die Kontaktmöglichkeiten zu erhöhen. Die meisten LinkedIn-Mitglieder verfügen über eine geschäftliche und eine persönliche E-Mail-Adresse. Dies ist wichtig für den Fall, dass Sie den Zugang zu Ihrer primären E-Mail-Adresse verlieren (wenn Sie beispielsweise Ihre Arbeitsstelle wechseln und den Zugang zu Ihrer geschäftlichen E-Mail-Adresse verlieren). Wichtig aber ist, eine primäre E-Mail-Adresse zu wählen, denn an diese werden alle LinkedIn-Nachrichten gesendet.

### Pseudonyme Nutzung

LinkedIn bietet eine Pseudonymisierungsfunktion, bei deren Benutzung vom Nachnamen des Nutzers nur noch der erste Buchstabe in der Plattform sichtbar ist (siehe Abbildung 11). Dies wirkt sich auch auf die Suche aus. Zwar kann eine Person bei Suche nach dem vollständigen Namen trotzdem gefunden werden, jedoch erscheint der vollständige Name nicht bei der Suche über andere Suchkriterien, wie z. B. dem Firmennamen, in den Suchergebnissen. Das erschwert die Identifizierung und schützt damit teilweise die Privatsphäre.



**Display Name**

baran goldkoch

baran G

**Tip:** For added privacy, you can display only your first name and last initial. (Your connections always see your first and last name.)

[Save Changes](#) or [Cancel](#)

Abbildung 11. Pseudonymisierung bei LinkedIn

### Einsatz von Verschlüsselung

Die Plattform nutzt Verschlüsselung standardmäßig nur für die Registrierung, den Login und die Veränderung der Nutzereinstellungen. Mithilfe der Konteneinstellungen können Sie allerdings eine durchgängig verschlüsselte Verbindung einschalten (“Einstellungen”–“Konto”–“Sicherheitseinstellungen verwalten”).

### Funktionsumfang der Zugriffskontrollen

Sie können die umfangreichen Geschäftsdaten (Bildung, beruflicher Werdegang, berufliche und private Interessen) nur gegen Zugriffe von Nicht-Plattformmitgliedern schützen, innerhalb der Plattform sind sie unbegrenzt einsehbar.

Weiter einschränken können Sie den Zugriff auf die Kontaktliste, auf den eigenen Status, die Gruppenzugehörigkeiten, auf Ihr Profilfoto sowie die Datenweitergabe an externe Anwendungen. (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.

### 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 Pseudonymisierungsfunktion (siehe oben) wirkt sich auch auf die Suche aus. Zwar kann eine Person bei der Plattformsuche über den Namen gefunden werden, jedoch erscheint der vollständige Name nicht bei der Suche über andere Suchkriterien, wie z. B. dem Firmennamen, in den Suchergebnissen. 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 nur mit Geschäftsfeld und Position, oder gar keine Anzeige.

### Abmelden bei der Plattform/ Löschumfang

Zum Abmelden von LinkedIn können Sie die Funktion “Close Your Account” unter “Account & Settings” verwenden. 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. Empfehlungen (“Recommendations”) bei anderen Nutzern und Antworten im sogenannten “Answer”-Werkzeug (hier können Fragen an andere Mitglieder gestellt werden) werden auch vollständig gelöscht.



## DANKSAGUNG

Die Autoren danken Ulrich Pordesch, Tim Kern und der gesamten Social Media Gruppe der Fraunhofer Gesellschaft für die Erlaubnis, Teile ihrer Schriften mit in die Studie aufzunehmen, außerdem Matthias Enzmann, Michael Herfert, Christopher Schmitz, Markus Schneider und Annika Selzer für ihre Unterstützung und Bereitstellung verschiedener Projektergebnisse. Herzlichen Dank an Mona Bien, Birgit Blume, Sonja Karl, Oliver KÜch, Marion Mayer, Enver Simsek und Sandra Wittrin für ihre Design-Beiträge und Fehlerkorrekturen.

## LITERATUR

- [AAF11] Ahmadinejad, S.H.; Anwar, M. ; Fong, P.W.L.: Inference attacks by third-party extensions to social network systems. In: *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on*, 2011, 282-287
- [acu12] *Exploiting a cross-site scripting vulnerability on Facebook*. <http://www.acunetix.com/websitesecurity/xss-facebook>. Version: 2012
- [Art07] Artikel-29-Datenschutzgruppe: *Stellungnahme 4/2007 zum Begriff "personenbezogene Daten" - 01248/07/DE - WP 136*. Juni 2007
- [Ash11] Ashford, Warwick: *RSA hit by advanced persistent threat attacks*. ComputerWeekly.com. <http://www.computerweekly.com/news/1280095471/RSA-hit-by-advanced-persistent-threat-attacks>. Version: March 2011
- [BGW08] Birk, Dominik; Gröbert, Felix ; Wegener, Christoph: Schnapp mich - Wie Web 2.0 den automatisierten Missbrauch ermöglicht. In: *iX 9* (2008), S. 44-52
- [Boy08] Boyd, Danah: *Taken out of context: American teen sociality in networked publics*. University of California, Berkeley, 2008 <http://www.danah.org/papers/TakenOutOfContext.pdf>. – PhD Thesis
- [BPH<sup>+</sup>10] Balduzzi, Marco; Platzer, Christian; Holz, Thorsten; Kirda, Engin; Balzarotti, Davide ; Kruegel, Christopher: Abusing Social Networks for Automated User Profiling. In: Jha, Somesh (Hrsg.); Sommer, Robin (Hrsg.) ; Kreibich, Christian (Hrsg.): *Recent Advances in Intrusion Detection* Bd. 6307. Springer Berlin / Heidelberg, 2010. – ISBN 978-3-642-15511-6, S. 422-441
- [BSBK09] Bilge, Leyla; Strufe, Thorsten; Balzarotti, Davide ; Kirda, Engin: All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. In: *Proceeding WWW '09 Proceedings of the 18th international conference on World wide web*, 2009
- [Con11] Constantin, Lucian: *Drive-by Download Attack on Facebook Used Malicious Ads*. [http://www.computerworld.com/s/article/9220557/Drive\\_by\\_download\\_attack\\_on\\_Facebook\\_used\\_malicious\\_ads](http://www.computerworld.com/s/article/9220557/Drive_by_download_attack_on_Facebook_used_malicious_ads). Version: 2011
- [CYA12] Chia, Pern H.; Yamamoto, Yusuke ; Asokan, N.: Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals. In: *ACM 978-1-4503-1229-5/12/04*, 2012, S. 311-320
- [FS09] Faghani, M.R.; Saidi, H.: Social Networks' XSS Worms. In: *Computational Science and Engineering, 2009. CSE '09. International Conference on* Bd. 4, 2009, S. 1137-1141
- [Gal08] Gallagher, Mary P.: *MySpace, Facebook Pages Called Key to Dispute Over Insurance Coverage for Eating Disorders*. <http://www.insuranceheadlines.com/Health-Insurance/4479.html>. Version: 2008
- [HK12] Heidrich, Joerg; Kuri, Jürgen: Social Media Guidelines. In: *c't extra – Soziale Netze* Bd. 2. Heise Zeitschriften Verlag, Oktober 2012, S. 176-179
- [HKNT09] Huber, M.; Kowalski, S.; Nohlberg, M. ; Tjoa, S.: Towards Automating Social Engineering Using Social Networking Sites. In: *Computational Science and Engineering, 2009. CSE '09. International Conference on* Bd. 3, 2009, S. 117-124
- [HMW<sup>+</sup>11] Huber, M.; Mulazzani, M.; Weippl, E.; Kitzler, G. ; Goluch, S.: Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam. In: *Internet Computing, IEEE 15* (2011), may-june, Nr. 3, S. 28-34. – ISSN 1089-7801

- [Hog07] Hogben, Giles; Network, European (Hrsg.); Agency, Security (Hrsg.): Security Issues and Recommendations for Online Social Networks / ENISA. Version: 2007. [http://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks/at\\_download/fullReport](http://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks/at_download/fullReport). 2007. – Forschungsbericht
- [JK11] Joshi, P.; Kuo, C.-C.J.: Security and privacy in online social networks: A survey. In: *Multimedia and Expo (ICME), 2011 IEEE International Conference on*, 2011
- [JW12] Johnston, A.; Wilson, S.: Privacy Compliance Risks for Facebook. In: *Technology and Society Magazine, IEEE* 31 (2012), S. 59–64
- [Kat11] Katzer, Catarina: Tatorte im Internet- Cyberbullying im Web2.0. In: *Der niedergelassene Arzt* 2011 (2011), June, Nr. 6, S. 20–24
- [KBM<sup>+</sup>11] Kelley, Patrick; Brewer, Robin; Mayer, Yael; Cranor, Lorrie ; Sadeh, Norman: An Investigation into Facebook Friend Grouping. In: Campos, Pedro (Hrsg.); Graham, Nicholas (Hrsg.); Jorge, Joaquim (Hrsg.); Nunes, Nuno (Hrsg.); Palanque, Philippe (Hrsg.) ; Winckler, Marco (Hrsg.): *Human-Computer Interaction – INTERACT 2011* Bd. 6948, Springer Berlin / Heidelberg, 2011 (Lecture Notes in Computer Science). – ISBN 978–3–642–23764–5, S. 216–233
- [KS12] Kalabis, Lukas; Selzer, Annika: Das Recht auf Vergessenwerden nach der geplanten EU-Verordnung. In: *Datenschutz und Datensicherheit* 9 (2012), S. 670–675
- [KSG13] Kosinski, Michal; Stillwell, David ; Graepel, Thore: *Private traits and attributes are predictable from digital records of human behavior*. PNAS Early Edition. <http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html>. Version: 2013
- [LK10] Langheinrich, Marc; Karjoth, Günter: Social networking and the risk to companies and institutions. In: *Inf. Secur. Tech. Rep.* 15 (2010), Nr. 2, S. 51–56. – ISSN 1363–4127
- [LPBK10] Lauinger, Tobias; Pankakoski, Veikko; Balzarotti, Davide ; Kirda, Engin: Honeybot, your man in the middle for automated social engineering. In: *Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*. Berkeley, CA, USA : USENIX Association, 2010 (LEET’10), 11–11
- [LRRB11] Leibowitz, Jon; Rosch, J. T.; Ramirez, Edith ; Brill, Julie: *United States of America - Federal Trade Commission: In the Matter of Facebook, INC., a corporation*. <http://www.ftc.gov/os/caselist/0923184/index.shtm>. <http://www.ftc.gov/os/caselist/0923184/120810facebookcmpt.pdf>. Version: 2011. – Document Number 0923184
- [MB10] Marwick, Alice E.; Boyd, Danah: I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience. In: *New Media & Society* 13 (2010), 7, Nr. 1, S. 114–133
- [PCRA12] Pesce, João P.; Casas, Diego L.; Rauber, Gustavo ; Almeida, Virgílio: Privacy attacks in social media using photo tagging networks: a case study with Facebook. In: *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*. New York, NY, USA : ACM, 2012 (PSOSM ’12). – ISBN 978–1–4503–1236–3, 4:1–4:8
- [Pol08] Poller, Andreas: Privatsphärenschutz in Soziale-Netzwerke-Plattformen / Fraunhofer Institut für Sichere Informationstechnologie SIT. Version: 2008. [https://www.sit.fraunhofer.de/fileadmin/dokumente/studien\\_und\\_technical\\_reports/Studie\\_Social\\_Networks.pdf](https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Studie_Social_Networks.pdf). 2008. – Forschungsbericht
- [Riv11] Rivner, Uri: *Anatomy of an Attack*. Speaking of Security, The official RSA Pod and Podcast. <http://blogs.rsa.com/rivner/anatomy-of-an-attack/>. Version: April 2011

- [Rya10] Ryan, Thomas: *Getting In Bed with Robin Sage*. <http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf>. Version: 2010
- [SMKM12] Sitzer, Peter; Marth, Julia; Kocik, Caroline ; Müller, Kay N.: Cyberbullying bei Schülerinnen und Schülern / Institut für interdisziplinäre Konflikt- und Gewaltforschung (IKG). Version: 2012. <http://www.uni-bielefeld.de/cyberbullying/downloads/Ergebnisbericht-Cyberbullying.pdf>. 2012. – Forschungsbericht
- [Son11] Sonwane, Abhilash: *Mapping an Organization's DNA using Social Media*. RSA Conference 2011, Session ID: HT1-107, February 2011
- [SP12a] Steidle, Roland; Pordesch, Ulrich: *Wider das anarchistische IT-Outsourcing! Webdienste und Informationssicherheit – Ein Beitrag zu Dropbox & Co. im Unternehmen*. <http://publica.fraunhofer.de/eprints/urn:nbn:de:0011-n-208414-17.pdf>. Version: 2012
- [SP12b] Sticca, Fabio; Perren, Sonja: Is Cyberbullying Worse than Traditional Bullying? Examining the Differential Roles of Medium, Publicity, and Anonymity for the Perceived Severity of Bullying. In: *Journal Youth Adolescence* (2012)
- [SRAP13] Sticca, Fabio; Ruggieri, Sabrina; Alsaker, Françoise ; Perren, Sonja: Longitudinal Risk Factors for Cyberbullying in Adolescence. In: *Journal of Community & Applied Social Psychology* 23 (2013), S. 52–67
- [The10] The Media Line: There are things we'll never know, Top secret IDF base exposed on Facebook. In: *The Jerusalem Post*, *jpost.com* (2010). <http://www.jpost.com/Israel/Article.aspx?id=180838>
- [Ver12] BAYERISCHES LANDESAMT FÜR VERFASSUNGSSCHUTZ: Soziale Netzwerke und ihre Auswirkungen auf die Unternehmenssicherheit. Version: 2012. [http://www.verfassungsschutz.bayern.de/imperia/md/content/lfv\\_internet/service/brosch\\_resozialenetzwkneu.pdf](http://www.verfassungsschutz.bayern.de/imperia/md/content/lfv_internet/service/brosch_resozialenetzwkneu.pdf). 2012. – Forschungsbericht
- [VFBJ11] Vicente, Carmen R.; Freni, Dario; Bettini, Claudio ; Jensen, Christian S.: Location-Related Privacy in Geo-Social Networks. In: *Internet Computing, IEEE* 15 (2011), S. 20–27
- [Wat10] Waterman, Shaun: Fictitious femme fatale fooled cybersecurity. In: *Washington Times* (2010). <http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity/?page=all>
- [WHKK10] Wondracek, Gilbert; Holz, Thorsten; Kirda, Engin ; Kruegel, Christopher: A Practical Attack to De-anonymize Social Network Users. In: *Security and Privacy (SP), 2010 IEEE Symposium on*, 2010. – ISSN 1081–6011, S. 223 –238
- [WNK<sup>+</sup>11] Wang, Yang; Norcie, Gregory; Komanduri, Saranga; Acquisti, Alessandro; Leon, Pedro G. ; Cranor, Lorrie F.: “I regretted the minute I pressed share” A Qualitative Study of Regrets on Facebook. In: *Proceedings of the Seventh Symposium on Usable Privacy and Security*. New York, NY, USA : ACM, 2011 (SOUPS 11). – ISBN 978–1–4503–0911–0, S. 10:1–10:16
- [WXG11] Wang, Na; Xu, Heng ; Grossklags, Jens: Third-party apps on Facebook: privacy and the illusion of control. In: *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*. New York, NY, USA : ACM, 2011 (CHIMIT 11). – ISBN 978–1–4503–0756–7, 4:1–4:10

**ISBN: 978-3-8396-0595-0**

**ISSN: 2192-8169**