Facebook, Twitter & Co.
Aber sicher!

Gefahrlos unterwegs in sozialen Netzwerken

Manuel Ziegler

HANSER

Aus dem Inhalt

- Facebook, Google+, XING, meinVZ, myspace, Twitter: Schützen Sie Ihre persönlichen Daten mit den richtigen Profileinstellungen
- Informationen und Bilder: Was dürfen Freunde von Ihnen wissen, was sollten Fremde auf keinen Fall erfahren
- Wie Sie Ihren Browser sichern und eine neue IP-Adresse erhalten
- Positionsdaten: Vorsicht mit der GPS-Funktion in Ihrem Smartphone

Empfohlen von

VERBRAUCHER SICHER · ONLINE

»Interessant und angenehm zu lesen. Ich denke, dass dieses Buch vielen weiterhilft, die sich über die Sicherheit in sozialen Netzwerken informieren wollen.«

Dr. Kei Ishii, Verbraucher Sicher Online

Ziegler

Facebook, Twitter & Co.
Aber sicher!

Bleiben Sie auf dem Laufenden!

Der Hanser Computerbuch-Newsletter informiert Sie regelmäßig über neue Bücher und Termine aus den verschiedenen Bereichen der IT. Profitieren Sie auch von Gewinnspielen und exklusiven Leseproben. Gleich anmelden unter

www.hanser-fachbuch.de/newsletter

Manuel Ziegler

Facebook, Twitter & Co. Aber sicher!

Gefahrlos unterwegs in sozialen Netzwerken

HANSER

Der Autor:
Manuel Ziegler, Limbach-Krumbach
Kontakt: buch@manuelziegler.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.

Lektorat: Sieglinde Schärl
Herstellung: Irene Weilhart
Copy editing: Rosa Riebl, Böblingen
Umschlagdesign: Marc Müller-Bremer, www.rebranding.de, München
Umschlagrealisation: Stephan Rönigk
Druck und Bindung: Kösel, Krugzell
Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702
Printed in Germany

print-ISBN: 978-3-446-43466-0
e-book-ISBN: 978-3-446-43474-5

Inhalt

Vorwort

Liebe Leser,

mit jedermann in Verbindung treten und das in Echtzeit – die sozialen Netzwerke Facebook, Google+, XING oder Twitter machen es möglich.

Durch die kostenlosen Mitgliedschaften sind Millionen von Nutzern in den verschiedenen Netzen aktiv, gestalten sie und machen sie für immer weitere Personengruppen attraktiv.

Weil es sich kein Anbieter leisten kann, Geld und Arbeit in die technische Bereitstellung kostenloser Dienste zu investieren, muss er sich die zahlenden Kunden an anderer Stelle suchen. Gefunden wurden sie unter Werbetreibenden, denen Präsentationsfläche für Produktanzeigen vermietet wird. Sie kommen in Scharen und zahlen viel dafür, wenn sie wissen, dass ihr Produkt zielgenau den ihren Vorstellungen entsprechenden Kunden angeboten wird oder wenn sie sich die Zielgruppe, die sie ansprechen wollen, sogar selbst zusammenstellen können. Die Voraussetzung dafür ist, dass der Betreiber möglichst umfangreiche und genaue Daten seiner Mitglieder besitzt – die er sich natürlich auf alle erdenklichen Arten besorgt.

Dies ist keineswegs verwerflich, schließlich profitieren alle Nutzer vom kostenlosen Kommunikationsangebot und wollen, dass das so bleibt.

Wer sich von der Werbung belästigt fühlt, kann sich ihr ganz leicht entledigen: Er muss nur das Browserfenster so verkleinern, dass die rechte Spalte der Webseite mit den Anzeigen ausgeblendet wird. Oder er installiert Werbeblocker im Browser, die dafür sorgen, dass die Anzeigen nicht angezeigt werden.

Die große Zahl der Mitglieder, die sich in den Foren tummeln, zieht aber auch Nutznießer an, die man sich unbedingt vom Leib halten muss, weil sie wirklich gefährlich sind: Spione. Wenn es nur die Kollegen von James Bond wären, wären sie eigentlich keiner Erwähnung wert, weil sie nur Ausschau nach ein paar bestimmten Personen halten. Nein, die Spione der digitalen Welt sind aufdringlicher und ihre Arbeit ist viel wirksamer: Sie sammeln persönliche Daten über alle Mitglieder der Netze und wenden die Daten im Ernstfall gegen Sie selbst an. In- und ausländische Geheimdienste, staatliche und halbstaatliche Behörden, Privatpersonen mit kriminellen oder halbkriminellen Absichten – sie alle versuchen, aus den im Netz gespeicherten Informationen den glä-

sernen Bürger zu bauen, seinen Aufenthaltsort zu ermitteln, seine Verhaltensmuster herauszufinden, seine Ansichten über Politik und andere Themen zu erfahren und ihn dabei so transparent zu machen, dass seine Aktionen vorhersagbar und seine Meinungen dokumentiert sind. Und in den modernen Datenbanken ist es schließlich nicht weiter schwierig, all diese Informationen und ihre Verknüpfungen untereinander abzuspeichern und maschinell zu analysieren. Egal, ob man dann in eine polizeiliche Rasterfahndung oder in das Visier eines Einbrechers gerät – in jedem Fall wird man sich wünschen, man wäre deutlich weniger freizügig mit persönlichen Daten gewesen und hätte dadurch den Spionen nicht gewissermaßen freiwillig die „Waffen“ in die Hand gegeben, die sich nun gegen einen selbst richten.

Aber nur wer die Gefahren kennt, kann ihnen auch angemessen begegnen, und nur wer den Gefahren, die von sozialen Netzwerken ausgehen, frühzeitig angemessen begegnet, kann sich Langzeitfolgen ersparen. Meine Intention, dieses Buch zu verfassen, war es, die Leser für die Gefahren zu sensibilisieren und ihnen ein datensparsames Verhalten in den Netzwerken nahezubringen.

Bevor ich Ihnen nun viel Spaß mit diesem Buch wünsche, möchte ich noch ein Wort des Dankes äußern. Ich danke Robin und Sebastian, die mir erlaubt haben, ihre Bilder aus sozialen Netzwerken abzudrucken. Ohne unnötig große Reden zu schwingen, möchte ich mich auch bei allen bedanken, die indirekt zum Gelingen des Buches beigetragen haben, sei es durch Inspiration, sei es durch das Vermitteln neuer Perspektiven oder auch nur durch das Interesse an meiner Arbeit. Besonders die Personen, die mir während der Entstehung dieses Buchs besonders nahe gestanden haben, haben den größten Anteil am Gelingen dieses Werkes. Herzlichen Dank!

Manuel Ziegler

Kontakt: buch@manuelziegler.de

www.facebook.com/SicherImSozialenNetz

Besuchen Sie mich auf meiner Facebook-Page zum Buch. Hier finden Sie regelmäßig Aktualisierungen und weiterführende Beiträge.

1 Soziale Netzwerke

Soziale Netzwerke sind aus dem modernen Internet nicht mehr wegzudenken. Im allgemeinen Sprachgebrauch handelt es sich bei einem sozialen Netzwerk um eine bestimmte Gemeinschaft von Personen, die über einen Webdienst miteinander kommunizieren und in Verbindung stehen. Aus technischer Sicht steht der Begriff stellvertretend für den dieser Gemeinschaft zugrundeliegenden Webdienst, der die Mittel für die Kommunikation der Clients untereinander bereitstellt. Die englische Bezeichnung „Social Network Services" beschreibt den Dienst, der im Deutschen einfach als „soziales Netzwerk" übersetzt wurde, eigentlich wesentlich besser, wobei „social" im ursprünglichen Sinne eine Gemeinschaft, eine Gruppe bedeutet.

1.1 Zielgruppen

Mittlerweile gibt es eine große Fülle sogenannter sozialer Netzwerke, die sich voneinander meist nur sehr geringfügig unterscheiden. Zwar versuchen die einzelnen Betreiber in einem ewigen Wettlauf immer neue Funktionen hinzuzufügen und so die Nutzer für sich zu gewinnen, aber im Grunde beruhen die meisten sozialen Netzwerke auf dem gleichen Konzept und bieten ähnliche Funktionen wie ihre Konkurrenten an. Nur selten stechen einzelne Netzwerke durch ausgefallene, einzigartige Konzepte hervor oder heben sich durch besondere, einmalige Zusatzfunktionen ab. Allerdings bleiben diese meist Nischenprodukte, die nur wenige Anhänger finden. Dies liegt daran, dass die meisten Benutzer keine Lust haben, regelmäßig den Anbieter zu wechseln, sondern einem Anbieter erstaunlich lange treu bleiben. Dies zum Glück der Unternehmen, die als Betreiber hinter dem sozialen Netzwerk stehen. Schließlich sind alle Benutzer enorm wichtig für das Bestehen des Netzwerks, sie bilden quasi aus sich heraus den Dienst und verleihen ihm seinen Charakter. Kein soziales Netzwerk kann ohne eine ausreichende Menge an Benutzern auskommen. Diese Tatsache erschwert es neuen Netzwerken ungemein, über längere Zeit auf dem Markt zu bleiben. Daher kann man die wichtigen sozialen Netzwerke an beiden Händen abzählen.

TABELLE 1.1 Die wichtigsten sozialen Netzwerke, XING und Stay Friends bieten als Besonderheit zusätzlich zu kostenlosen eine Premium-Mitgliedschaft an. Die Mitgliederzahlen differieren teilweise deutlich von Quelle zu Quelle

Name	Web-Adresse	Mitglieder	Zielgruppe
Facebook	http://facebook.com	ca. 900 Mio.	Alle Internetnutzer
Google+	http://plus.google.com	ca. 90 Mio.	Alle Internetnutzer
Twitter	http://twitter.com	ca. 100 Mio.	Alle Internetnutzer
XING	http://www.xing.com	ca. 11 Mio.	Geschäftsleute
VZ-Netzwerke	http://www.meinVZ.net; http://www.StudiVZ.net; http://www.SchuelerVZ.net	Zusammen etwa 4 Mio.*	Schüler, Studenten, junge Erwachsene
myspace	http://www.myspace.com	etwa 50 Mio.	Musiker und Musikinstrumente
Wer kennt wen	http://www.wer-kennt-wen.de	etwa 9,6 Mio.	Vor allem ältere Internetnutzer
StayFriends	http://www.stayfriends.de	ca. 13 Mio.	Alte Schulfreunde
Flickr	http://www.flickr.com	etwa 77 Mio.	Alle, die Fotos teilen möchten

* Die Mitgliederzahlen differieren je nach Quelle erheblich. Bei Drucklegung dieses Buches sind Gerüchte über das Schließen der VZ-Netzwerke wegen eines massiven Mitgliederschwunds und des damit einhergehenden wirtschaftlichen Niedergangs zu lesen, siehe http://www.wuv.de/nachrichten/digital/holtzbrinck_beerdigt_social_media_marke_vz. Danach hat sich die Zahl der Mitglieder von Februar 2011 bis Februar 2012 von 10,8 auf 3,99 Millionen verringert.

Es gibt vermutlich kein soziales Netzwerk, bei dem die Kommunikation zwischen den Benutzern keine Rolle spielt, doch die sozialen Netzwerke können sich bei der Bedeutung der Kommunikation mitunter sehr stark unterscheiden. So gibt es soziale Netzwerke, manchmal auch soziale Medien genannt, die den größten Wert auf öffentliche Inhalte legen, die von Benutzern mit der Gemeinschaft geteilt werden. Bei ihnen steht hauptsächlich das persönliche Profil des einzelnen Benutzers im Vordergrund. Dieses Profil umfasst in den meisten Fällen eine Art Steckbrief sowie eine Art virtuelles Gästebuch. Die Benutzer bringen selbst aktiv Informationen in das Netzwerk ein und teilen sie anderen mit, sie entwickeln das Netz quasi selbst weiter, es lebt von den Eigenschaften und Interessen seiner Mitglieder. Diese Netzwerke sind auf spezielle Aktivitäten der Benutzer angewiesen, um die Interessen anderer Benutzer befriedigen zu können. Die einzelnen Mitglieder müssen gewillt sein, Informationen über sich selbst preiszugeben und mit anderen Benutzern zu teilen. Solche Netze werden in diesem Buch „benutzerprofilbasiert“ genannt.

Kommuniziert wird zwischen den Benutzern in benutzerprofilbasierten Netzwerken hauptsächlich im öffentlichen Bereich. Das bedeutet beispielsweise, dass die Benutzer ihren Freunden innerhalb dieser sozialen Netzwerke mitteilen, wo sie gerade sind, was sie kürzlich machten und was sie demnächst machen werden. Diese Mitteilungen können anschließend in den meisten Fällen von allen Freunden gelesen werden.

Zwar gibt es häufig auch die Möglichkeit, wie in einem Chat auf herkömmliche Weise, also privat durch das Versenden einzelner Textnachrichten in einen Dialog zu treten, allerdings ist diese Kommunikation in benutzerprofilbasierten Netzwerken lediglich als Ergänzung vorgesehen. Die wichtigsten dieser Netzwerke sind Facebook, Google+, XING, myspace und meinVZ.

Anders als bei den benutzerprofilbasierten Netzwerken steht beim zweiten Typ nicht der einzelne Nutzer selbst, sondern vielmehr die Interaktion zwischen den Nutzern im Vordergrund, also die Kommunikation untereinander, wobei die Persönlichkeit des einzelne Benutzers in den Hintergrund tritt. Diese Netzwerke sollen hier als „kommunikativ" bezeichnet werden. Natürlich gibt es auch hier teilweise große Unterschiede in der Art der Umsetzung, aber im Grunde zeichnen sich diese Netzwerke alle dadurch aus, dass die Mitglieder zu Diskussionen angeregt werden, sei dies nun durch eine Struktur wie sie aus Foren bekannt ist oder eher durch Kurznachrichten.

Apropos Forum: Foren sind wohl die häufigste Form der kommunikativen Netzwerke. Hier gibt es mehrere Benutzer, die gewöhnlich unter Pseudonymen und ohne viel Wert auf ihr Profil zu legen, Meinungen austauschen und miteinander diskutieren. Sogar Probleme werden häufig in Foren gelöst. Da aber Foren meist nur recht wenige Benutzer beherbergen (die Mitgliederzahl eines Forums geht nur sehr selten über 100.000 hinaus), sind diese meist zu klein, um im Rahmen dieses Buchs als ernsthaftes soziales Netzwerk gelten zu können.

1.1.1 Mitgliederstruktur

Teilt man die Mitglieder der sozialen Netzwerke in Gruppen ein, ergibt sich in etwa die gleiche Verteilung wie bei den generellen Internetnutzern.

Der weitaus größte Anteil aller Mitglieder wird von den unter Achtzehnjährigen gestellt, gefolgt von den jungen Erwachsenen bis zum Alter von dreißig Jahren. Einen erheblich geringeren Anteil machen die zwischen Dreißig- und Vierzigjährigen aus, allerdings immer noch einen größeren Anteil als die Vierzig- bis Fünfundfünfzigjährigen. Von noch älteren Personen werden soziale Netzwerke nur in Ausnahmefällen genutzt, womit die über Fünfundfünfzigjährigen die kleinste Altersgruppe stellen[1].

Eine ganz ähnliche Verteilung ergibt sich hinsichtlich der Zeit, die einzelne Benutzer täglich beziehungsweise wöchentlich oder monatlich in sozialen Netzwerken verbringen. Logischerweise verbringen Jugendliche den weitaus größten Zeitanteil in sozialen Netzwerken, und Mitglieder mit einem Alter von über 55 Jahren erübrigen selten mehr als eine Stunde pro Monat dafür.

Erklären lässt sich das mit den unterschiedlichen Arten der Nutzung. Während Jugendliche über soziale Netzwerke mit nahezu allen ihren Freunden kommunizieren und dafür durchschnittlich dreißig Minuten, in einigen Fällen sogar bis zu acht Stunden am

[1] Siehe http://www.bitkom.org/files/documents/BITKOM_Publikation_Soziale_Netzwerke_zweite_Befragung.pdf

Tag aufwenden, haben junge Erwachsene wesentlich weniger Freizeit als Jugendliche und halten sich nicht so ausgiebig in sozialen Netzen auf. Allerdings sind ihre Freunde im Vergleich mit den Dreißig- bis Fünfundfünfzigjährigen in den Netzwerken meist recht zahlreich vertreten, so dass prinzipiell die Möglichkeit bestehen würde, mit fast allen Freunden in Kontakt zu treten. Mitglieder, die älter als dreißig Jahre sind, haben meist wesentlich weniger Freunde in den Netzwerken als junge Erwachsene, so dass davon ausgegangen werden kann, dass auch ein Großteil ihrer Freunde dort gar nicht vertreten ist. Das ist natürlich auch der Grund, dass sie soziale Netzwerke in wesentlich geringerem Umfang nutzen. Über Fünfundfünfzigjährige sind wie bereits erwähnt nur sehr sporadisch in sozialen Netzwerken registriert, oft überhaupt nur deshalb, weil sie den Kontakt zu Jüngeren, beispielsweise zu ihren erwachsenen Kindern oder jugendlichen Enkeln halten wollen. Der Freundeskreis dieser Benutzergruppe beschränkt sich meist auf wenige Dutzend Personen, weshalb Angehörige dieser Altersgruppe auch die wenigste Zeit in sozialen Netzwerken verbringen.

1.1.2 Netzwerkauswahl

Welches soziale Netzwerk das jeweils richtige ist, ist eine individuelle Entscheidung. So hängt es im Grunde vollständig von den Interessen des potentiellen Mitglieds ab, welches Netzwerk für ihn in Frage kommt. Nachfolgend wird ein grober Überblick darüber gegeben, welche Zielgruppe von welchem sozialen Netzwerk erreicht wird, wobei die für eine geplante Netzwerkzugehörigkeit maßgeblichen Faktoren hervorgehoben werden. Die Gefahren der einzelnen sozialen Netzwerke werden nur dann berücksichtigt, wenn ein bestimmtes soziales Netzwerk erheblich größere Risiken als ein anderes mitbringt. Die möglichen Gefahren werden in den Kapiteln 2 bis 5 noch genauer erörtert.

Das wichtigste Kriterium bei der Auswahl eines sozialen Netzwerks ist generell die Frage, wo die meisten eigenen Freunde registriert sind. Die Sicherheit der eigenen Daten spielt bei den meisten Anwendern eine untergeordnete Rolle[2]. Dies ist durchaus verständlich, denn schließlich ist das erklärte Ziel eines sozialen Netzwerks üblicherweise die Kontaktaufnahme mit den eigenen Freunden. Dennoch dürfen Aspekte wie Sicherheit und Datenschutz bei einer gewissenhaften Wahl nicht außen vor gelassen werden.

Viele soziale Netzwerke adressieren mit ihrem Angebot nur eine bestimmte Zielgruppe. Das Netzwerk StudiVZ ist ein klassisches Beispiel, weil es lediglich Studenten erreicht; dies geht ja schon aus seinem Namen hervor. Ähnlich ist es mit dem Netzwerk SchülerVZ. Dementsprechend findet man in diesen Netzwerken nahezu ausschließlich Mitglieder, die diesen Zielgruppen angehören.

Andere Netzwerke wie die meisten der hier noch explizit vorgestellten versuchen dagegen, ein möglichst breites Nutzerspektrum anzusprechen. Sie haben daher meist auch mehr Mitglieder und damit steigt automatisch das Risiko des Datenmissbrauchs.

[2] Ebenfalls in der auf der vorigen Seite genannte Bitcom-Studie nachzulesen.

In den letzten Jahren hat sich vor allem ein Netzwerk zum Marktbeherrscher entwickelt: Facebook. Für die meisten Computerbesitzer ist der Begriff „Facebook“ ein Pseudonym für soziale Netzwerke geworden. Wer in sozialen Netzwerken aktiv sein möchte, kommt an ihm meistens nicht vorbei. Das zeigen die Nutzungsstatistiken sozialer Netzwerke, nach denen fünfundvierzig Prozent der Internetnutzer ein aktives Konto bei Facebook besitzen sollen. Auf dem zweiten Platz folgen die Netzwerke StayFriends und Wer kennt Wen, die jedoch nur noch einen Anteil von vierzehn beziehungsweise zwölf Prozent haben.

Im Folgenden soll die Auswahl des richtigen sozialen Netzwerks aus Anwendersicht beispielhaft dargestellt werden. Wir betrachten dazu Tom, Toms Vater Dirk und Toms Schwester Susanne, die alle drei auf der Suche nach einem sozialen Netzwerk sind. Tom wird im weiteren Verlauf des Buchs noch häufiger auftauchen, nämlich immer dann, wenn bestimmte Situationen an einem Beispiel verdeutlicht werden müssen.

Tom ist Student. Er ist an den Wochenenden in der Heimat und hat dort wie auch an seiner Universität eine große Menge Freunde. Er möchte möglichst nur in einem sozialen Netzwerk täglich aktiv sein, kann es sich aber durchaus vorstellen, Benutzerkonten in mehreren zu pflegen. Tom wird bei einer Befragung seiner Freunde feststellen, dass fünfundneunzig Prozent soziale Netzwerke nutzen und Mitglied bei Facebook sind, zehn Prozent seiner Freunde von der Universität zudem bei StudiVZ registriert sind und immerhin fünfzig Prozent der Freunde zusätzlich Google+ nutzen, wenn auch nur sporadisch. Natürlich ist auch Twitter vertreten, zirka weitere fünfzig Prozent der Freunde in sozialen Netzwerken greifen auch auf Twitter zu. meinVZ ist im Grunde nur im Rahmen von StudiVZ vertreten, während myspace vernachlässigt werden kann[3].

Tom würde sich also wohl für drei bis vier Benutzerkonten entscheiden:

- Ein Facebook-Account wäre für Tom das wohl wichtigste Benutzerkonto. Er sucht es aktiv regelmäßig auf.
- Ein Google+-Benutzerkonto würde das Facebook-Benutzerkonto ergänzen, Tom würde es jedoch nicht täglich aufrufen.
- Ähnlich ist es mit dem Twitter-Konto: Es würde das Facebook-Benutzerkonto ergänzen, aber nicht zur alltäglichen Pflichtübung werden.
- Eventuell würde Tom auch noch ein StudiVZ-Benutzerkonto anlegen, um darüber Kontakt zu seinen Mitstudenten an der Universität zu pflegen, allerdings stellt sich die Frage, ob es sich wirklich lohnt, dieses Konto anzulegen.

Toms Schwester Susanne geht im Gegensatz zu ihm noch zur Schule. Ihre Freunde konzentrieren sich auf eine ganz bestimmte Region. Es stört sie aber nicht weiter, wenn sie sich alltäglich in mehrere soziale Netzwerke parallel einloggt, um alle ihre Freunde zu erreichen.

[3] Die hier genannten Zahlen sind willkürlich gewählt, sind jedoch für die Altersklasse, der Tom angehört, charakteristisch. Die Zahlen folgen nicht ganz der weiter oben zitierten Studie vom Dezember 2011. Das liegt daran, dass Google+ in dieser Zeit weiteren Zulauf erfahren hat und dass, nach der Einschätzung des Autors, Google+ in Zukunft das einzige soziale Netzwerk sein wird, das an Facebook herankommen könnte.

Auch von Susannes Freunden sind 95 Prozent in Facebook vertreten, Google+ wird jedoch nur von weniger als 30 Prozent von ihnen genutzt und auch die Twitter-Nutzer sind mit nur knapp 20 Prozent sehr schwach vertreten. Allerdings befinden sich in dem regionalen Netzwerk, das die Wohngegend von Susanne weiträumig abdeckt, insgesamt 70 Prozent ihrer Freunde. Susanne wird höchstwahrscheinlich ein Facebook-Benutzerkonto anlegen sowie ein Konto im Netzwerk ihrer Region und beide relativ intensiv besuchen. Zusätzlich könnte sie auch noch ein Google+- sowie ein Twitter-Konto anlegen, beide wird sie jedoch nur sporadisch aufrufen.

Während sich Tom und Susanne im Grunde für die gleichen sozialen Netzwerke entscheiden werden, wird Toms Vater Dirk höchstwahrscheinlich andere Plattformen bevorzugen. Er sucht eines, in dem er Altersgenossen antrifft und Kontakte aus seiner Schul- und Studienzeit pflegen kann. Zwar wird er in Facebook ebenfalls einige Freunde wiederfinden, allerdings längst nicht so viele wie beispielsweise in *Wer kennt Wen*. Vermutlich wird sich Dirk deshalb für solch ein Nischennetzwerk entscheiden. Zusätzlich möchte er in sozialen Netzwerken auch Geschäftsbeziehungen pflegen und entscheidet sich daher für den Marktführer in diesem Segment, nämlich für XING. Außerdem ist Dirk der Datenschutz wichtiger als seinen Sprösslingen, weshalb er sich entscheidet, von Facebook Abstand zu nehmen.

1.2 Die Netzwerke

Wie man unschwer an den vorangegangenen Beispielen erkennen kann, ist die Auswahl der geeigneten sozialen Netzwerke ein sehr individueller Prozess, bei dem sich jeder seine eigene Plattform auswählen muss. Dabei ist es notwendig, sich ausführlich mit den einzelnen sozialen Netzwerken zu beschäftigen, bevor man sich für eines entscheidet.

Die einzelnen sozialen Netzwerke unterscheiden sich oft nur in Details voneinander, deshalb wird die Auswahl meist primär von der Mitgliederzahl beeinflusst. Besser wäre es, die sicherheitstechnischen Themen sehr viel höher zu gewichten. Die persönlichen Daten sind nämlich bei den meisten sozialen Netzwerken nur unzureichend gesichert. In diesem Buch wird noch detailliert auf die unterschiedlichen Sicherheitsaspekte eingegangen.

1.2.1 Facebook

Facebook ist derzeit das wohl populärste und bekannteste soziale Netzwerk. Es wurde im Jahre 2004 vom damaligen Psychologiestudenten Mark Zuckerberg zusammen mit Dustin Moskovitz, Chris Hughes und Eduardo Saverin gegründet[4]. In den folgenden

[4] Ursprünglich wurde Facebook unter dem Namen thefacebook gegründet. Dieser Name wurde jedoch im August 2005 durch den heute bekannten Namen Facebook ersetzt.

Jahren verbreitete sich Facebook auf der ganzen Welt. Heute hat es nach eigenen Angaben über 900 Millionen aktive Nutzer.[5]

Viele soziale Netzwerke haben mittlerweile das Grundkonzept von Facebook in mehr oder weniger modifizierter Form übernommen, so dass Facebook als Urahn der benutzerprofilbasierten sozialen Netzwerke angesehen werden kann.

Das Motto von Facebook, wie es der Besucher bereits beim ersten Besuch in den Dienst auf der Startseite (Bild 1.1) antrifft – *Facebook ermöglicht es dir, mit den Menschen in deinem Leben in Verbindung zu treten und Inhalte mit diesen zu teilen* –, hat dem Dienst in den vergangenen Jahren immer wieder Kritik eingebracht. Ihm wurde vorgeworfen, die persönlichen Daten seiner Benutzer nicht ausreichend zu schützen. Dabei wurden auch Verstöße gegen deutsche und europäische Datenschutzgesetze bekannt. Die Gruppe Europe vs. Facebook[6] prangert derartige Verstöße an und bringt sie häufig zur Anzeige.

BILD 1.1 Die Startseite von Facebook, auf der rechten Seite können sich neue Benutzer registrieren

[5] Unter der Adresse http://www.facebook.com/press/ stellt Facebook zahlreiche statistische Daten sowie weitere interessante Informationen zusammen. Allerdings sind diese Informationen mit Vorsicht zu genießen. Schließlich werden diese Daten von Facebook selbst zusammengestellt.

[6] Siehe http://europe-v-facebook.org

Registrierung

Weil Facebook eine kommerziell betriebene Plattform ist, muss sich der Nutzer erst registrieren, bevor er die angebotenen Dienste in Anspruch nehmen kann. Dafür müssen einige persönliche Daten im Registrierungs-Formular auf der rechten Seite der Startseite eingetragen werden (Bild 1.1). Facebook erwartet hier von seinen zukünftigen Mitgliedern, dass sie Vor- und Familienname, E-Mailadresse, Geschlecht und Geburtsdatum angeben, wobei Mitglieder, die jünger als 13 Jahre sind, nicht registriert werden. Angeblich gibt es aber sehr viele noch jüngere Nutzer, die ein falsches Geburtsdatum angegeben haben, da es von Facebook bei der Anmeldung nicht kontrolliert wird[7]. Erlaubt ist das eigentlich nicht, Facebook fordert von seinen Mitgliedern, das richtige Geburtsdatum anzugeben (Bild 1.2).

BILD 1.2 Die Angabe des Geburtstags ist Pflicht, vordergründig wegen des Jugendschutzes

Nachdem diese Daten in die entsprechenden Felder eingetragen sind und zusätzlich ein Passwort für das Konto vergeben ist, kann die Anmeldung mit einem Klick auf REGISTRIEREN fortgesetzt werden.

Im nächsten Schritt muss sich das zukünftige Mitglied als Mensch identifizieren und zwei schwer lesbare Wörter aus einem Bild in das darunter befindliche Textfeld schreiben. Dieses Verfahren soll sicherstellen, dass die Registrierung eines neuen Benutzerkontos nicht automatisiert durch einen Computer vorgenommen werden kann. Mit einem weiteren Klick auf REGISTRIEREN wird bestätigt, dass man die Nutzungsbedingungen sowie die Datenschutzrichtlinien gelesen hat und ihnen zustimmt. Man sollte das Lesen übrigens nicht nur blind bestätigen, sondern vorher wirklich die Texte gelesen haben.

Nachdem dies alles bestätigt wurde, erhält man typischerweise zwei E-Mails. Die erste hat den Betreff „Du hast den Registrierungsprozess fast abgeschlossen“ und enthält

[7] Siehe dazu auch http://www.br.de/fernsehen/bayerisches-fernsehen/sendungen/rundschau/facebook-datenschutz-internet100.html

einen Link sowie einen Bestätigungscode. Auf diesen Link sollte man entweder klicken oder ihn in das Adressfeld eines Browsers kopieren, um die Registrierung abzuschließen. Unter Umständen wird man zusätzlich dazu aufgefordert, den ebenfalls in der Mail enthaltenen Bestätigungscode einzutippen; normalerweise wird er aber nicht verlangt.

Die zweite E-Mail mit dem Betreff „Willkommen bei Facebook“ enthält zusätzliche Informationen für den Anwender, die jedoch für die weiteren Schritte nicht benötigt werden.

Nachdem die oben beschriebenen Schritte erfolgreich ausgeführt wurden, ist man als Benutzer bei Facebook registriert. Nun hat man üblicherweise einen Assistenten vor sich, der dabei helfen soll, das Benutzerkonto einzurichten. Dabei wird man aufgefordert, den eigenen E-Mail-Provider auszuwählen.

Anschließend wird das Passwort für das angegebene E-Mailkonto verlangt – weil Facebook auf die Kontaktdaten, die in diesem E-Mailkonto gespeichert sind, zugreifen möchte und so dabei helfen will, Freunde zu finden. Auch wenn Facebook behauptet, dass hierbei keine Passwörter gespeichert werden, ist von der Weitergabe des E-Mail-Passworts dringend abzuraten! Dieses Thema wird in Kapitel 3.2.3 noch ausführlich behandelt. Im Vorgriff auf dieses Kapitel sei aber bereits hier dringend empfohlen, statt der Preisgabe des Passworts des E-Mailkontos auf Diesen Schritt überspringen in der rechten unteren Ecke zu klicken (Bild 1.3).

Nun ist man bei Schritt 3 angelangt. Jetzt wird der Anwender aufgefordert, zusätzliche Profilinformationen anzugeben. Aber bevor man sich dazu entscheidet, hier die Schule, die Hochschule oder den Arbeitgeber mitzuteilen, sollte man Kapitel 2 in diesem Buch

BILD 1.3 Überspringen Sie diesen Schritt!

lesen. Diese Informationen können jederzeit auch später eingegeben werden, weshalb auch bei Schritt 3 zu einem Klick auf ÜBERSPRINGEN geraten wird.

Im letzten Schritt wird man dazu aufgefordert, ein eigenes Profilbild von der Festplatte des Rechners hochzuladen oder mit der Webcam aufzunehmen. Auch hier sollte man besser auf ÜBERSPRINGEN klicken und später in aller Ruhe über ein Profilbild entscheiden.

Nachdem der Einrichtungsassistent beendet ist, gelangt man zur persönlichen Facebook-Startseite (Bild 1.4).

BILD 1.4 Die persönliche Startseite von Facebook direkt nach dem Registrieren

In der Mitte des Fensters sind noch einmal die von Facebook empfohlenen Schritte zur Einrichtung des Benutzerkontos zu sehen. Auch hier ist es wieder sinnvoll, diese Schritte zu ignorieren und auf eigene Faust mit dem Einrichten des Benutzerkontos fortzufahren.

Die Benutzeroberfläche

Bild 1.4 zeigt die Benutzeroberfläche von Facebook. Sie besteht im Prinzip aus einem einfachen dreispaltigen Layout[8]. Im Kopfbereich der Seite befinden sich die wichtigsten

[8] Ein Dreispaltenlayout besteht in der Regel aus einer Kopfzeile, die das Logo der Seite und wichtige Navigationselemente enthalten kann, aus einem in drei Spalten geteilten Hauptanzeigebereich und optional einer Fußzeile. Im Hauptanzeigebereich ist meist der Inhalt der Seite untergebracht: Die linke Spalte enthält die Navigationselemente, die mittlere Spalte den eigentlichen Inhalt der Seite und die rechte Spalte typischerweise Werbung.

Steuerelemente der Seite: Rechts neben dem Facebook-Logo stehen die drei wichtigsten Benachrichtigungsfelder für erhaltene Freundschaftsanfragen, neue Nachrichten und Benachrichtigungen über Pinnwandeinträge sowie Veranstaltungseinladungen, Kommentare und ähnliches.

Rechts von diesen Benachrichtigungsfeldern ist das Feld für Suchen aller Art. Gibt man hier den Namen einer Person ein, kann in Facebook nach ihr gesucht werden. Aber nicht nur Personen, sondern auch Seiten von Unternehmen, Produkten, Vereinen oder auch Bands lassen sich damit finden. Außerdem ist eine Suche nach öffentlichen und geschlossenen Gruppen möglich.

Auf der rechten Seite befindet sich ein Link mit dem Namen des Benutzers, er führt zum Profil des aktuell angemeldeten Benutzers. Mit dem Link Startseite gelangt man zur eigenen Startseite, die alle abonnierten Meldungen in umgekehrter chronologischer Reihenfolge anzeigt.

Ganz rechts ist noch ein dreieckiger Pfeil, wie man ihn beispielsweise von Dateibrowsern wie dem Windows Explorer kennt. Klickt man ihn an, öffnet sich ein Drop-down-Menü, das üblicherweise die Punkte Kontoeinstellungen, Privatsphäre-Einstellungen, Abmelden und Hilfe enthält; die verschiedenen Einstellmöglichkeiten werden später noch genauer erläutert.

Mit einem Klick auf Abmelden wird die aktuelle Facebook-Sitzung beendet. Unter Hilfe findet man die umfangreichen Hilfeoptionen des Systems. Sie sind nach den Themen Grundlagen, Fehlfunktionen, Beschwerden, Sicherheit und weiterhin in kommerzielle Funktionen gegliedert.

In der linken Spalte befinden sich die einzelnen Navigationselemente, mit denen der Benutzer auf die verschiedenen Bereiche von Facebook zugreifen kann. Ganz oben ist ein Verweis auf das Benutzerprofil des aktuell angemeldeten Benutzers. Darunter stehen die Links zu seinen favorisierten Seitenbereichen. Hier befindet sich üblicherweise neben einem Link zur Startseite (hier mit Neuigkeiten benannt) und einem Link zu den Nachrichten des Benutzers auch ein Link auf den Veranstaltungskalender, in dem die Veranstaltungen aufgelistet sind, zu denen der Benutzer geladen ist. Direkt nach dem Einrichten des Benutzerkontos finden sich hier auch Verweise zur Willkommenseite und zum sogenannten Freundefinder.

Unter diesen Punkten sind, falls vorhanden, die Gruppen aufgeführt, in denen der Benutzer aktiv ist, sowie die Listen, in denen er seine Freunde verwalten kann. Zuletzt werden hier noch die Anwendungen angeboten, die von Facebook selbst oder von Drittanbietern in Facebook integriert wurden und die verschiedensten Zwecken dienen. Diese Anwendungen können beispielsweise Zusatzfunktionen wie Umfragen in Facebook integrieren oder auch Spiele damit verknüpfen. Mehr zu Anwendungen ist ab Seite 25 unter dem gleichlautenden Stichwort nachzulesen.

Der mittlere Bereich der Seite enthält die eigentlichen Inhalte der aktuell angezeigten Seite. Hier befinden sich beispielsweise alle neuen Meldungen, wenn der Benutzer gerade auf der Startseite verweilt. Häufig ist im oberen Bereich der Seite eine Statuszeile zu sehen, über die er seinen Status aktualisieren kann, indem er das, was er gerade

macht, in das Textfeld eingibt. Anschließend kann er diesen Status mit Zusatzinformationen versehen und beispielsweise die Personen, die ihn begleiten oder den Ort, an dem er sich gerade befindet, nennen. Er kann auch ein Bild hinzufügen. Außerdem kann er die Sichtbarkeit dieses Beitrags in der rechten unteren Ecke ändern. Je nach Sicherheitseinstellungen des Kontos kann hier eine der folgenden Sicherheitsstufen ausgewählt werden:

- FREUNDE VON FREUNDEN[9] macht den Beitrag für die eigenen Freunde und alle deren Freunde sichtbar. Diese Sichtbarkeitsstufe sollte stets mit Bedacht gewählt werden, denn ein an diese Gruppe gesandter Beitrag kann von einem sehr großen Personenkreis gelesen werden!
- FREUNDE macht den Beitrag für alle Freunde des Benutzers sichtbar. Hier kann die Zahl der Personen, die von diesem Beitrag erreicht werden sollen, über die Anzahl der Freunde exakt bestimmt werden.
- NUR ICH macht den Beitrag ausschließlich für denjenigen, der diesen Beitrag geschrieben hat, sichtbar – jedenfalls in der Theorie. Dass in der Praxis noch jemand ganz anderes mitliest, wird unter anderem Thema von Kapitel 4 sein. Zwar stellt sich hier die Frage, ob es überhaupt sinnvoll ist, solche Beiträge zu schreiben, aber das muss jeder Benutzer für sich selbst entscheiden.
- BENUTZERDEFINIERT schließlich gibt dem Benutzer große Freiheiten zu bestimmen, wer einen Beitrag sehen soll. So können hier einzelne Benutzer sowie Listen oder oben angeführte Sicherheitsstufen ausgewählt werden, die einen Beitrag angezeigt bekommen sollen. Außerdem können bestimmte Personen oder Listen ausgewählt werden, für die der Beitrag nicht sichtbar sein soll.

Zusätzlich zu diesen vordefinierten Sicherheitsstufen kann der Benutzer auch einzelne Listen, in denen der Beitrag veröffentlicht werden soll, auswählen. In solchen Listen werden Freunde gruppiert. Beispielsweise könnte die Liste SCHULKAMERADEN alle Schulkameraden zusammenfassen. Vorgegebene Listen wie ENGE FREUNDE oder FAMILIE gruppieren Personengruppen, die alle Anforderungen dieser jeweiligen Liste erfüllen. Wählt man als Sichtbarkeit für einen Beitrag jedoch eine oder mehrere Listen aus, können die Mitglieder dieser Listen die Namen der anderen sehen und mit wem sie in eine Schublade gesteckt wurden.

Auf diese Art und Weise veröffentlichte Statusmeldungen landen anschließend auf der Startseite aller Abonnenten des Verfassers. Dieser Teil der Benutzerfläche umfasst eigentlich alles Interessante für den Benutzer, doch der Vollständigkeit halber soll noch kurz auf die rechte der drei Spalten eingegangen werden.

---

[9] Man nehme einmal an, man hätte 100 Freunde, die selbst wiederum 100 Freunde haben. Weiter nehme man an, man hätte im Durchschnitt mit jedem der Freunde 30 Freunde gemeinsam, also etwa ein Drittel der Freunde würden sich jeweils untereinander kennen. In diesem Fall würde eine Statusmeldung, die für Freunde von Freunden sichtbar ist, schlimmstenfalls zirka 100 + 100 * 70 = 7100 Personen erreichen. Wenn man bedenkt, dass viele Facebook-Nutzer 200 und mehr Freunde haben und es in bestimmten Kreisen auch Nutzer mit mehr als 500 Freunden gibt, kann man abschätzen, welche Kreise eine solche Statusmeldung ziehen kann. Mehr zu diesem Thema erfahren Sie in Kapitel 2.

In dieser Spalte werden dem Mitglied nämlich Werbeanzeigen eingeblendet, die mit erstaunlicher Präzision auf seine Interessen und Persönlichkeit abgestimmt sind. Es ist beobachtbar, dass die Anzeigen immer zielgenauer werden, je mehr Zeit seit der Registrierung vergangen ist. In Kapitel 3 wird auf dieses Thema näher eingegangen. Man sollte jedoch generell darauf achten, sich von den hier geschalteten Werbeanzeigen nicht manipulieren zu lassen, egal, wie verlockend sie aussehen mögen. Geht man das erste Mal darauf ein, bestätigt man den Eindruck, den Facebook von seinem Mitglied gewonnen hat und ermöglicht damit die Einordnung in bestimmte Kategorien.

Das Benutzerprofil

Das Benutzerprofil ist praktisch ein öffentlicher Steckbrief der eigenen Person unter Facebook. Es besteht aus einem Informationsbereich (INFO), in dem die Informationen zu Ausbildung und Arbeitsstelle, Geburtsdatum und Geschlecht sowie Informationen zur Einstellung der Person und andere Charaktermerkmale gespeichert werden können.

BILD 1.5 Das Benutzerprofil

Zusätzlich zu diesem Informationsbereich enthält das Benutzerprofil eine sogenannte Pinnwand. Auf ihr sind alle Aktivitäten des Benutzers in umgekehrter chronologischer Reihenfolge aufgeführt. Unter diese Aktivitäten fallen beispielsweise Statusmeldungen, GEFÄLLT MIR-Angaben sowie Kommentare zu fremden Beiträgen. Außerdem können auf der Pinnwand andere Benutzer Beiträge hinterlassen, die dann ebenfalls dort angezeigt werden.

Neben der Pinnwand und dem Informationsbereich enthält ein Benutzerprofil typischerweise auch eine Sammlung von Bildern, die vom Benutzer selbst hochgeladen wurden oder auf denen der Benutzer verlinkt wurde.

Abhängig von den Einstellungen enthält ein Benutzerprofil auch die Freundesliste des Benutzers, die der Besucher des Profils sehen kann. Zusätzlich bietet Facebook hier einen weiteren Service, indem es dem Besucher mitteilt, wie viele Freunde er und der Besuchte gemeinsam haben. Auf dieser Basis schlägt Facebook seinen Mitgliedern auch Freunde vor.

Vor kurzem hat Facebook damit begonnen, die Benutzerprofile abzuschaffen und durch die sogenannte Chronik zu ersetzen. Die Chronik (Bild 1.6) fasst die Daten der Benutzer übersichtlich und grafisch aufgewertet zusammen, so dass einerseits ein ästhetisch ansprechender Eindruck entsteht, andererseits aber auch zahlreiche Daten bereits auf den ersten Blick von anderen Nutzern erfasst werden können.

BILD 1.6 Die Chronik

Die Chronik bringt insgesamt nicht viel Neues mit sich, trägt aber durchaus dazu bei, dass die Spionage durch andere Benutzer und vor allem tiefergehende Recherchen vereinfacht werden.

Auch die Chronik ist in verschiedene Bereiche gegliedert. Den Hauptteil bildet die eigentliche Chronik, die die frühere Pinnwand ersetzt. Sie enthält alle Beiträge, die man selbst dort abgelegt hat oder die andere Benutzer dort hinterlassen haben. Hier sind

auch alle sonstigen Aktivitäten des Benutzers zu finden. Geordnet ist die Chronik anhand eines in der Mitte befindlichen Zeitstrahls, der eine tatsächlich chronologische Anordnung der Ereignisse zulässt. Auf der rechten Seite findet der Besucher einer Chronik mehrere Links, über die anhand eines einfachen Mausklick zu einem bestimmten Zeitpunkt gesprungen werden kann. So soll es möglich sein, mehr über das Leben des Benutzers zu einem bestimmten Zeitpunkt zu erfahren.

Neben diesem Bereich sind in der Chronik – wie auch im Benutzerprofil – natürlich noch andere Kategorien enthalten. Die wichtigsten sind INFO, FREUNDE und KARTE. Außer einer grafischen Aufwertung sind diese Kategorien gleich geblieben. Die neu hinzugekommene Karte allerdings hat es in sich. Hier werden alle Orte, die der Benutzer mit dem Wissen von Facebook jemals besucht hat, eingetragen.

Und so entsteht ein Bewegungsprofil des Anwenders.

Einstellungen

Klickt man in der oberen rechten Ecke auf den Pfeil in der Kopfzeile, findet man dort unter anderem die Konto- und die Privatsphäre-Einstellungen. Mit ihnen lassen sich nahezu alle relevanten Einstellungen eines Facebook-Kontos vornehmen. Als Benutzer sollte man sich mit diesen Einstellungsmöglichkeiten gründlich auseinandersetzen, um seine Privatsphäre zu schützen und anderen Ärgernissen aus dem Weg zu gehen.

Kontoeinstellungen

Die Kontoeinstellungen sind in die folgenden Kategorien eingeteilt:

1. Allgemein
2. Sicherheit
3. Benachrichtigungen
4. Abonnenten
5. Anwendungen
6. Handy
7. Zahlungen
8. Facebook-Werbeanzeigen

In ALLGEMEIN sind die grundsätzlichen Benutzerinformationen wie der eigene Name, der Facebook-Benutzername (falls vorhanden) und die E-Mail-Adresse(n) gespeichert. Zusätzlich besteht hier die Möglichkeit, das Passwort zu ändern, Netzwerken beizutreten, andere Konten mit dem eigenen Facebook-Konto zu verknüpfen oder seine Spracheinstellungen zu modifizieren.

Um einen der oben genannten Punkte zu bearbeiten, muss am rechten Rand des entsprechenden Punkts auf BEARBEITEN geklickt werden. Im anschließenden Dialog werden die geforderten Daten eingegeben.

Besonders interessant ist die Funktion LADE EINE KOPIE DEINER FACEBOOK-DATEN HERUNTER. Hier bietet Facebook dem Mitglied die Möglichkeit, alle Beiträge, Aktivitä-

ten, Kommentare und Informationen, die er jemals in Facebook veröffentlicht hat, in einem Archiv herunterzuladen. Zwar sind in diesem Archiv leider nicht die Daten enthalten, die von Facebook selbst zusätzlich ermittelt werden, aber beim Durchstöbern kann man dennoch einen Einblick bekommen, welchen Aufschluss über die eigene Person die Aktivitäten in Facebook ermöglichen.

Die Kategorie SICHERHEIT enthält Einstellungen, die den Zugang zu einem Benutzerkonto schützen sollen. Sofern noch nicht geschehen, hat der Nutzer hier die Möglichkeit, eine Sicherheitsfrage für sein Konto einzurichten. Damit kann er Zugang zum Konto erlangen, auch wenn er sein Kennwort vergessen hat. Hier geht die Sicherheitstechnik von Facebook sogar soweit, dass jemand, der keinen Zugriff zu seinem Mailkonto hat und sich nicht mehr an sein Facebook-Kennwort erinnern kann, das eigene Konto sperren und anschließend wieder Zugriff darauf erlangen kann.

In diesem Zusammenhang kam es bereits vor, dass es Angreifern gelang, die Passwörter von E-Mailkonten zu knacken und so auch Zugang zum Facebook-Benutzerkonto des Opfers erlangten. Die betroffenen Benutzer konnten durch die relativ gute Sicherheitstechnik von Facebook jedoch einen Missbrauch ihres Benutzerkontos verhindern. Hier kam ihnen vor allem zugute, dass sie eine Sicherheitsfrage eingerichtet hatten. Aber auch andere Mechanismen, mit denen Facebook bestimmen kann, ob sich der Benutzer von dem entsprechenden Rechner bereits eingeloggt hat oder ob er sich in der bevorzugten geographischen Region des Facebook-Nutzers aufhält, helfen dabei, den Missbrauch eines Benutzerkontos zu vermeiden. Ohne diese Techniken müsste man wesentlich mehr Zeit aufwenden, um Missbräuche zu verhindern.

Eine Sicherheitsfrage kann nur einmal eingerichtet werden. Damit soll umgangen werden, dass Angreifer, die Zugriff auf das Benutzerkonto haben, durch eine Änderung der Sicherheitsfrage eine schnelle Sperrung des Kontos durch den regulären Benutzer verhindern. Durch eine Änderung der Sicherheitsfrage könnte sich der reguläre Benutzer nämlich nicht mehr ohne weiteres als der rechtmäßige Inhaber des Benutzerkontos ausweisen. Würde er sein Konto dann sperren wollen, müsste er direkten Kontakt mit Facebook aufnehmen.

Neben der optionalen Sicherheitsfrage gibt es noch zahlreiche weitere Sicherheitseinstellungsmöglichkeiten. So kann beispielsweise das sogenannte SICHERE DURCHSTÖBERN aktiviert und deaktiviert werden. Dabei handelt es sich um nichts anderes als das Aktivieren des https[10]-Protokolls anstelle des üblichen http[11]-Protokolls. Mehr dazu in Kapitel 4.

[10] **H**yper**t**ext **T**ransfer **P**rotocol **S**ecure. Dieses Protokoll soll eine abhörsichere Übertragungsmöglichkeit der Daten zwischen dem Rechner des Benutzers (Client) und dem Server bieten. Bekannt ist https beispielsweise aus dem Online-Banking, doch mittlerweile bieten immer mehr Website-Betreiber dieses Protokoll an, wenn es um die Übertragung von Passwörtern und ähnlichem geht. Allerdings gibt es auch beim https-Protokoll Schwachstellen, so dass man sich bei ihm nie auf hundertprozentige Sicherheit verlassen sollte.

[11] Das **H**yper**t**ext **T**ransfer **P**rotocol ist das Standardprotokoll zur Übertragung von Webseiten zwischen dem Server und dem Anwenderrechner. Es wurde dafür entwickelt, sogenannten Hypertext, also beispielsweise HTML (Hypertext Markup Language) oder XHTML (Extensible Hypertext Markup Language) zu übertragen. HTML und XHTML sind Auszeichnungssprachen, mit denen der Aufbau und der Inhalt einer Internetseite definiert wird, sie bilden quasi das layouterische Rückgrat des World Wide Web.

Durch das Einrichten sogenannter Anmeldebenachrichtigungen kann man informiert werden, wenn ein unbekanntes Gerät auf das Facebook-Konto zugreift. Man erhält dann wahlweise eine SMS oder E-Mail-Nachricht (Bild 1.7), wenn sich ein solches Gerät angemeldet hat, und kann entsprechend reagieren.

BILD 1.7 So sieht die E-Mail mit einer Anmeldebenachrichtigung aus

Unter einem Gerät versteht Facebook einen Computer, ein Mobiltelefon oder ein anderes Mobilgerät. Mit Hilfe von Cookies identifiziert Facebook die verschiedenen Geräte. Cookies sind kurze Textdateien, die der Webserver auf den Geräten ablegt und in denen er die Kennungen der Geräte speichert. Greift das Gerät auf Facebook zu, sucht der Server sein Cookie, wertet es aus und identifiziert das Gerät. Will sich nun plötzlich ein Computer, von dem aus noch nie auf Facebook zugegriffen wurde oder auf dem die entsprechenden Cookies gelöscht wurden, am Benutzerkonto anmelden, erkennt dies der Server und meldet es dem Benutzer.

Das gleiche Ziel verfolgen Anmeldebestätigungen (Bild 1.8 auf der nächsten Seite). Sind sie aktiviert, muss auf unbekannten Geräten ein Sicherheitscode eingegeben werden. Solche Maßnahmen erschweren es Hackern zwar, Zugriff auf ein fremdes Benutzer-

konto zu erlangen, ein wirklich ernstgemeinter Angriff kann damit jedoch nicht verhindert werden.

Anmeldebestätigungen bereiten unter Umständen Probleme, wenn Facebook in Verbindung mit anderen Anwendungen – wie beispielsweise Skype, ICQ, Jabber oder Empathy – unter Linux, Windows oder MacOS X genutzt wird. Diese Programme kommen nämlich zum Teil nicht mit Anmeldebestätigungen zurecht. Für solche Anwendungen müssen deshalb eigene Passwörter generiert werden, damit weiterhin ein Zugriff über sie möglich ist. Diese werden unter dem Punkt PASSWÖRTER FÜR ANWENDUNGEN eingerichtet.

BILD 1.8 Einrichten der Anmeldebestätigung

Neben den genannten Einstelloptionen besteht auch die Möglichkeit, bekannte Geräte zu verwalten und aktive Sitzungen einzusehen (Bild 1.9). „Bekannte Geräte“ sind solche, denen der Anwender bereits einen Name zugewiesen hat. Entdeckt der Anwender hier ein Gerät, das er selbst nicht registriert hat, kann er dieses Gerät löschen und weitere Schritte zum Schutz seines Kontos vornehmen.

Ähnlich verhält es sich mit den aktiven Sitzungen (Bild 1.10), nur dass diese unabhängig von registrierten Geräten sind. Hier wird angezeigt, aus welchen Regionen und mit welchem Betriebssystem und Browser – hier in der Benutzeroberfläche ebenfalls Gerät genannt – sich der Nutzer zuletzt an- und nicht wieder abgemeldet hat (hier beispielsweise mit dem Firefox-Browser unter Linux). Auch bemerkt man die Anwesenheit von Dritten. Sind Sitzungen aktiv, die nicht mehr geöffnet sind, werden sie hier beendet. So kann verhindert werden, dass ein Angreifer über die offene Sitzung in das Konto eindringt und sich Zugang zu den persönlichen Daten des Benutzers verschafft.

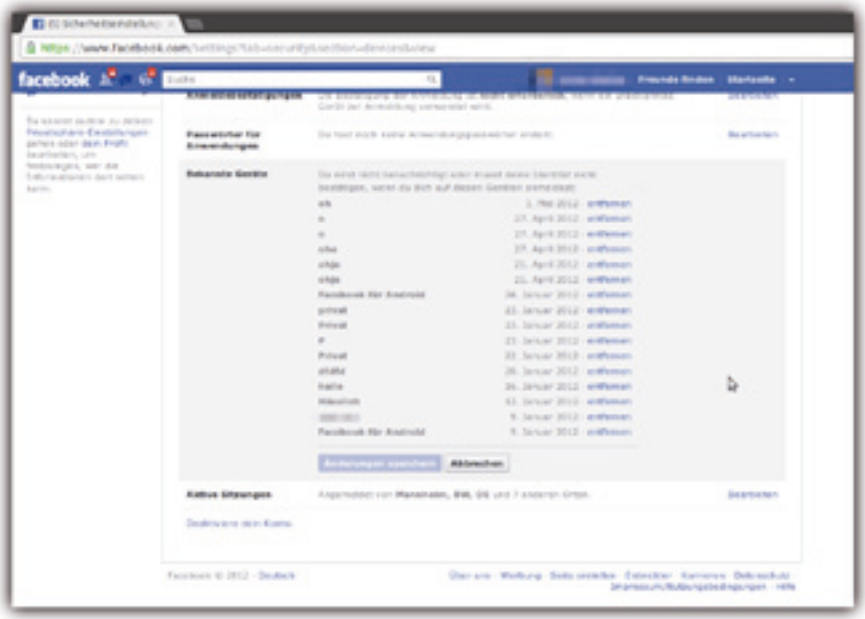

BILD 1.9 Benannte Geräte

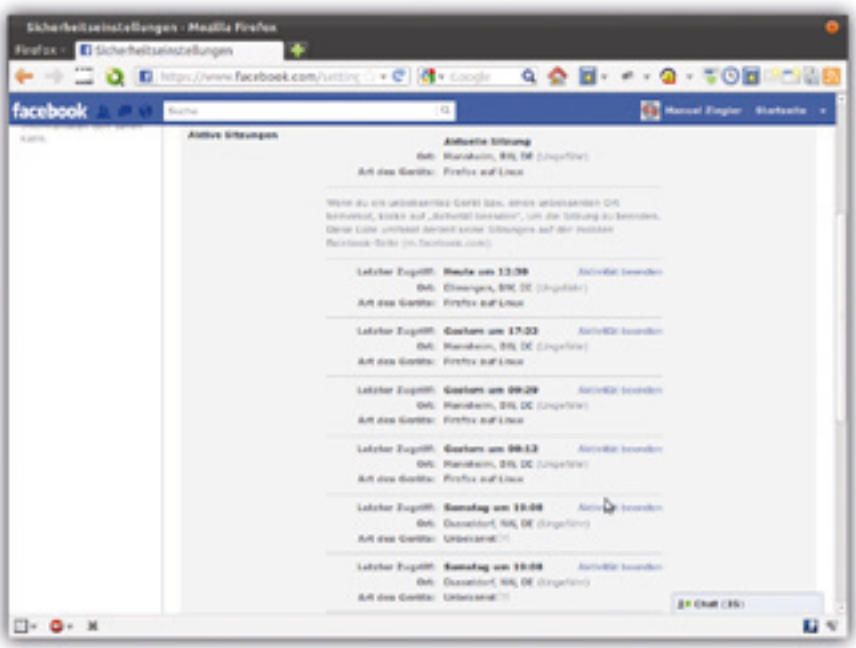

BILD 1.10 Aktive Sitzung mit Firefox-Daten

Der letzte wichtige Punkt in den Sicherheitseinstellungen ist DEAKTIVIERE DEIN KONTO. Hier kann man das eigene Konto abschalten, wenn man beispielsweise keine Lust mehr auf Facebook hat. Dieser Menüpunkt muss wörtlich genommen werden: Facebook bietet nämlich ausschließlich an, ein Konto zu deaktivieren. Will man es löschen, sucht man vergeblich nach der entsprechenden Möglichkeit – es gibt sie nicht!

Facebook-Mitglieder ärgern sich schnell über eine geballte Ladung E-Mails. Abgestellt wird das unter dem Punkt BENACHRICHTIGUNGEN in den Kontoeinstellungen. Hier sind die Anwendungen aufgelistet, die E-Mails an den Benutzer senden. Mit einem Klick auf die entsprechende Anwendung – das kann auch Facebook selbst sein – werden die Einstellungen für den E-Mailempfang dieser Anwendung angepasst.

Innerhalb von Facebook und für den Zugriff auf Facebook kann mit verschiedenen Anwendungen gearbeitet werden, denen jedoch einmalig Zugriff gewährt werden muss. Um die Einstellungen für eine dieser Anwendungen zu verwalten, muss erst unter dem Punkt ANWENDUNGEN in den Konteneinstellungen die entsprechende Anwendung ausgewählt werden (Bild 1.11).

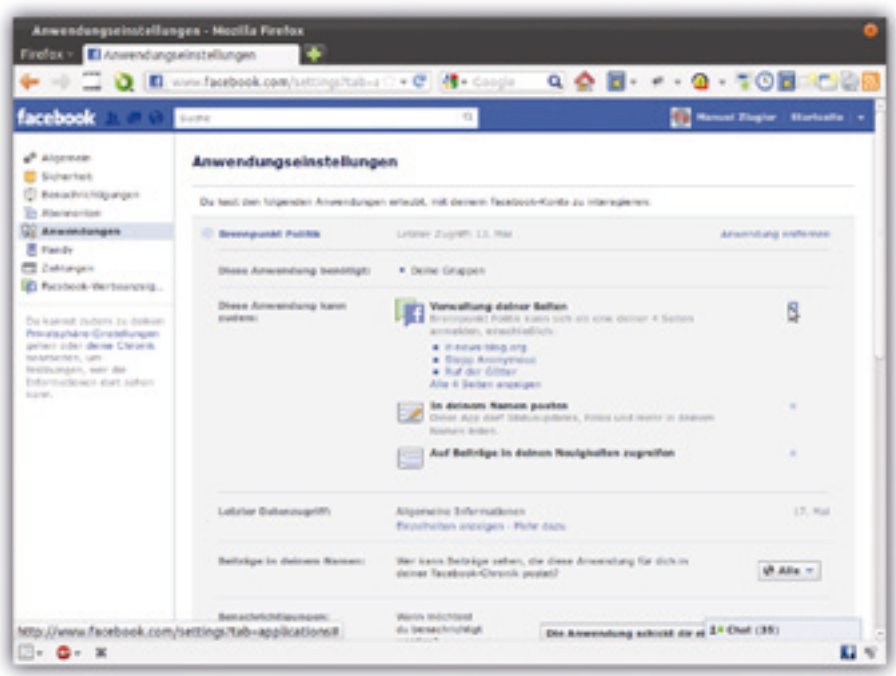

BILD 1.11 Die Berechtigungen von Anwendungen

Anschließend wird eine Liste mit den Berechtigungen angezeigt, die dieser Anwendung eingeräumt werden. Manche dieser Berechtigungen sind für die Anwendung unbedingt notwendig und können nicht entfernt werden. Andere Berechtigungen müssen nicht notwendigerweise vergeben sein und können daher entfernt werden. In der Regel sollte

man Anwendungen nicht mehr Berechtigungen einräumen als sie unbedingt benötigen, da sonst Dritte unnötigerweise an die Daten gelangen können (mehr dazu in Kapitel 4).

Um einer Anwendung alle Berechtigungen zu entziehen, klickt man auf das kleine blaue Kreuz auf der rechten Seite in der Anwendungsübersicht.

Unter dem Punkt Handy nimmt man die das Mobiltelefon betreffenden Einstellungen vor. Neben der Angabe der eigenen Mobiltelefonnummer kann der Benutzer hier die Benachrichtigungen per SMS aktivieren und deaktivieren.

Sollte man sich dazu entschließen, Nachrichten auf dem Mobiltelefon zu empfangen, sollte man vor allem den letzten beiden Punkten Nachrichten und Tägliches SMS Limit besondere Beachtung schenken. Mit ersterem wird festgelegt, unter welchen Umständen Facebook eine SMS an das Mitglied schickt. Mögliche Einstellungen sind hier Wenn jemand eine Nachricht an mein Handy schickt und Wenn mir jemand eine Nachricht schickt. Möchte der Anwender nie Nachrichten per SMS erhalten, kann diese Option ganz abgeschaltet werden.

Mit Tägliches SMS-Limit wird die Obergrenze für die täglich an das Handy versandten SMS angegeben. Hier ist eine relativ niedrige Angabe sinnvoll, sonst kann es zu bösen Überraschungen kommen.

Die Punkte Zahlungen und Facebook-Werbeanzeigen der Kontoeinstellungen setzen meist eine kommerzielle Nutzung voraus und sollen in diesem Buch nicht weiter behandelt werden.

Privatsphäre-Einstellungen

Besonders wichtig für Facebook-Benutzer sind die Einstellungen zur Privatsphäre (Bild 1.12 auf der nächsten Seite). Wie auch die Kontoeinstellungen findet man diesen Menüpunkt über das Kontextmenü auf der rechten Maustaste in der rechten oberen Ecke.

Öffnet man die Privatsphäre-Einstellungen, sieht man zunächst einen sehr kurzen Auswahldialog für die Standardeinstellung. Hier ist die Auswahl von Öffentlich, Freunde oder Benutzerdefiniert möglich. Bei der Wahl von Öffentlich kann standardmäßig jeder bei Facebook registrierte Benutzer das eigene Profil und vor allem die Statusmeldungen und Pinnwandeinträge einsehen.

Ähnliches gilt für die Wahl des Punkts Freunde. Hier können anstelle der Öffentlichkeit lediglich Freunde die entsprechenden Informationen einsehen. Bei Benutzerdefiniert dagegen öffnet sich ein Fenster, in dem ausgewählt werden kann, wer Informationen über die eigene Person betrachten darf. Hier stehen die gleichen Punkte zur Auswahl, die auch bei der sogenannten *Inline-Auswahl* bei der Veröffentlichung eines Status angeboten werden. Außerdem können hier einzelne Personen oder Angehörige einer Liste ausgeschlossen werden, wonach Statusmeldungen und Pinnwandeinträge standardmäßig vor ihnen verborgen werden.

Die Privatsphäre-Einstellungen lassen sich nach der ersten groben Auswahl noch feiner konfigurieren. Dazu findet man weiter unten auf der Seite mehrere Punkte für speziellere Einstellungen.

BILD 1.12 Privatsphäre-Einstellungen

Unter FUNKTIONSWEISE VON VERBINDUNGEN wird die grundlegende Privatsphäre bezüglich der Kontaktmöglichkeiten zwischen den Benutzern eingestellt. Speziell kann hier festgelegt werden, welche Nutzer das eigene Profil finden können, von wem Freundschaftsanfragen entgegengenommen werden sollen, wer mit einem über Nachrichten in Verbindung treten und an die eigene Pinnwand schreiben sowie Einträge an der eigenen Pinnwand lesen darf.

FUNKTIONSWEISE VON MARKIERUNGEN (Bild 1.13) geht unter den Privatsphäre-Einstellungen einen Schritt weiter und ermöglicht es, die sogenannten Markierungen in Beiträgen näher zu definieren. Wird man in einem Beitrag markiert, ist das nichts anderes als das Setzen eines Querverweises auf das eigene Profil. Das kann beispielsweise so aussehen:

Person A ist mit Person B hier: Kino

In diesem Fall wurden durch die Markierung von Person B in diesem Beitrag Informationen zum Aufenthaltsort von B preisgegeben – was aber unter Umständen von B nicht gewünscht ist. Um vor solchen Überraschungen gefeit zu sein, lohnt es sich, die Einstellungen unter FUNKTIONSWEISE VON VERBINDUNGEN mit großer Sorgfalt zu studieren:

Durch das Aktivieren der sogenannten PROFIL-ÜBERPRÜFUNG (Bild 1.14) wird eingestellt, dass man Beiträge von Freunden, in denen man selbst markiert wurde, zuerst bestätigen muss, bevor sie auf der eigenen Pinnwand veröffentlicht werden.

BILD 1.13 Einstellungen zu Markierungen

BILD 1.14 Profil-Überprüfung aktivieren

In eine ähnliche Richtung geht der Punkt MARKIERUNGEN ÜBERPRÜFEN. Hier wird definiert, dass man eine Markierung, die ein Freund im von einem selbst geschriebenen Beitrag gesetzt hat, erst bestätigen muss, bevor diese für die entsprechende Personengruppe sichtbar wird. Wird eine Markierung von einem Fremden vorgenommen, wird man unabhängig von dieser Einstellung aufgefordert, die Markierung zu bestätigen oder abzulehnen. Allerdings können nach dem Deaktivieren dieser Funktion andere Benutzer die Markierung sehen, bevor sie bestätigt wurde.

Die sogenannte MAXIMALE PROFILSICHTBARKEIT (Bild 1.15) legt fest, für welchen Personenkreis ein Beitrag, in dem man selbst markiert wurde, höchstens sichtbar ist, nachdem er auf der eigenen Pinnwand veröffentlicht wurde. Hat der entsprechende Beitrag eine niedrigere Sichtbarkeit, wird die maximale Sichtbarkeit dieses Punktes durch die niedrigere Sichtbarkeit des Beitrags überschrieben. Das bedeutet, dass ein Beitrag, der nur für bestimmte Personen sichtbar ist, nach seinem Erscheinen auf der Pinnwand weiterhin nur für diese sichtbar ist, selbst wenn die maximale Profilsichtbarkeit auf FREUNDE festgelegt wurde. Ein öffentlich sichtbarer Beitrag auf der Pinnwand des markierten Benutzers bei gleichen Einstellungen der maximalen Profilsichtbarkeit ist jedoch nur für Freunde des Benutzers sichtbar.

BILD 1.15 Maximale Profilsichtbarkeit

Unter dem Punkt MARKIERUNGSVORSCHLÄGE werden Einstellungen zur von Facebook Anfang Juni 2011 in Deutschland eingeführten Gesichtserkennung getroffen. Die Facebook-Gesichtserkennung ermöglicht es, Freunden automatisch Markierungen auf Fotos vorzuschlagen. Das läuft nach folgendem Schema ab:

Lädt ein Freund ein Foto hoch, auf dem man sich selbst befindet, kann Facebook – auch wenn der Freund selbst keine Markierung setzt – das Gesicht erkennen und gleicht es mit einer Datenbank ab, in der die bisherigen Markierungen gespeichert sind. Stimmt das Gesicht zu einem bestimmten Prozentsatz mit dem in der Datenbank gespeicherten biometrischen Muster des eigenen Gesichts überein, schlägt Facebook dem Freund vor, die auf dem Bild erkannte Person zu markieren. Der Freund kann die automatische Bestätigung anschließend bestätigen oder ablehnen.

Will man nicht, dass Facebook auf diese Weise ein biometrisches Profil erhält, müssen die Markierungsvorschläge unbedingt gesperrt werden. Trotzdem ist es aber nicht vollständig möglich, Facebook hier einen Strich durch die Rechnung zu machen, wenn man sich nicht der in Kapitel 3.2 ab Seite 88 besprochenen Techniken bedient.

Man sollte hier also auf jeden Fall die Option Niemand im Punkt Wer kann Markierungsvorschläge sehen, wenn Fotos hochgeladen werden, die dir ähneln? auswählen.

Der nächste Punkt Anwendungen und Webseiten wird im Abschnitt „Anwendungen“ noch näher betrachtet.

Mit der Option Beschränke das Publikum für ältere Beiträge kann die Sichtbarkeit aller früheren Beiträge so herabgesetzt werden, dass diese höchstens für Freunde sichtbar sind, jedoch nicht für die Öffentlichkeit oder für Freunde von Freunden. Zwar kann man das auch im Nachhinein für jeden Beitrag einzeln einstellen, allerdings ist die Möglichkeit des Kollektivs einfacher und wird wesentlich häufiger in Anspruch genommen.

Mit dem letzten Punkt Blockierte Personen und Anwendungen kann der Benutzer in der Vergangenheit gesetzte Blockierungen aufheben oder bearbeiten sowie neue Blockierungen hinzufügen. Sie sind immer dann sinnvoll, wenn einem bestimmte Personen oder Anwendungen wiederholt auf die Nerven gehen und deshalb eingeschritten werden muss.

Anwendungen

Anwendungen sind ein wichtiger Bestandteil von Facebook. Sie erweitern die grundlegenden Funktionen um zahlreiche Zusätze. Neben Spielen gibt es wirklich nützliche Anwendungen. Doch ist bei ihnen ebenso Sorgfalt wie Vorsicht geboten, denn allzu schnell erteilt man ihnen mehr Berechtigungen als sie eigentlich benötigen, wodurch Dritte an die eigenen Daten gelangen können. Daher ist es wichtig, die Berechtigungen von Anwendungen sorgfältig zu verwalten (Bild 1.16 auf der nächsten Seite).

In den bereits angesprochenen Privatsphäre-Einstellungen lassen sich die wichtigsten Aspekte zum Thema Anwendungen schnell und einfach konfigurieren, die Kategorie heißt Anwendungen und Webseiten.

Unter dem Punkt Anwendungen, die du verwendest lassen sich die benötigten Anwendungen schnell einsehen und verwalten. Fällt dort eine Anwendung auf, die nicht auf persönliche Daten zugreifen soll, lässt sie sich schnell entfernen. Außerdem können

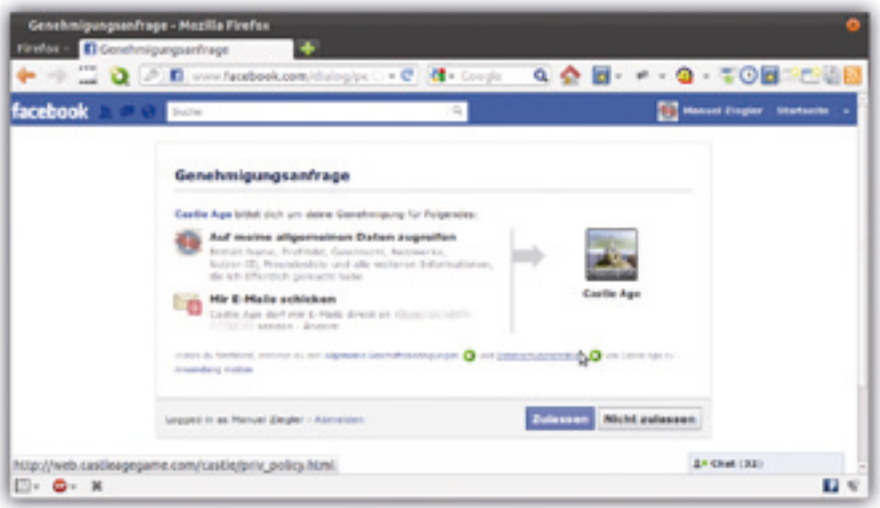

BILD 1.16 Viele Anwendungen verlangen den Zugriff auf persönliche Daten. Die Berechtigungen, die einer Anwendung verliehen werden, müssen genau geprüft werden, bevor man ihnen zustimmt

BILD 1.17 Auswahlfelder von „Wie Freunde deine Informationen an Anwendungen weitergeben, die sie nutzen“

mit einem Klick auf den Anwendungsnamen die Informationen, die dieser Anwendung bereitgestellt werden, gefiltert werden: Informationen, auf die eine Anwendung keinen Zugriff haben soll, lassen sich mit einem Klick auf ENTFERNEN vor ihr verbergen. Informationen, die eine Anwendung unbedingt benötigt, können nicht entfernt werden. Der einzige Weg, eine Information vor einer Anwendung zu verbergen, ist, die Anwendung vollständig zu löschen.

Ein besonders kritischer Aspekt von Anwendungen ist, dass sie nicht nur auf die Daten ihres eigentlichen Nutzers zugreifen, sondern auch Informationen von seinen Freunden abrufen können. Um den Zugriff von Anwendungen, mit denen die Freunde arbeiten, zu verhindern, müssen die Auswahlfelder unter dem Punkt WIE NUTZER DEINE INFORMATIONEN AN ANWENDUNGEN WEITERGEBEN, DIE SIE NUTZEN deaktiviert werden (Bild 1.17). Natürlich können den Anwendungen von Freunden auch ausgewählte Informationen überlassen werden, ratsam ist das jedoch nicht.

Beim Arbeiten mit Facebook-Anwendungen ist also stets große Sorgfalt angebracht, da sich vor allem durch sie viele Sicherheitslöcher auftun. Ganz ohne Anwendungen kommt man normalerweise in Facebook aber nicht aus. Das liegt daran, dass Funktionen wie das sogenannte Anstupsen und die über Facebook durchführbaren Umfragen in Anwendungen ausgelagert wurden und man als Nutzer nur selten vollständig auf diese Optionen verzichten möchte.

1.2.2 Google+

Lange Zeit war Facebook absoluter Marktführer auf dem Gebiet der sozialen Netzwerke. Doch als Google am 28. Juni 2011 ein eigenes soziales Netzwerk mit dem Namen Google+[12] veröffentlichte, war schon bald klar: Google+ steht in direkter Konkurrenz zu Facebook und hat die Chance, ebenso bedeutend zu werden. Obwohl der Beitritt zu Google+ zunächst nur nach Einladung durch bereits registrierte Benutzer möglich war, konnte Google+ in den ersten 88 Tagen laut eigener Angaben rund vierzig Millionen Nutzer verzeichnen. Ein derartiges Wachstum schaffte nicht einmal Facebook.

Das Konzept von Google+ ist dem von Facebook nicht unähnlich, auch wenn seine Oberfläche wesentlich intuitiver ist, und keine verschachtelten Menüs für Benutzerverwirrung sorgen. Dennoch fallen sofort einige Facebook-typische Elemente ins Auge. So erinnert der Stream von Google+ stark an die Startseite von Facebook. Ähnlich verhält es sich mit den Benutzerprofilen. Auch hier kann man klar erkennen, dass sie den Profilen von Facebook nachempfunden sind. Doch seit der Einführung von Google+ hat es auch Änderungen in Facebook gegeben, die an Google+ erinnern. Beispielsweise hat Facebook als Antwort auf die Kreise von Google+ Listen eingeführt. Auch die Möglichkeit des Videochats hat Facebook wohl von Google+ übernommen.

[12] Google+ wird unter der Adresse https://plus.google.com/ angeboten.

BILD 1.18 Die Startseite von Google+

Registrierung

Wie in jedem sozialen Netzwerk ist bei Google+ eine Registrierung erforderlich, bevor die Funktionalitäten genutzt werden können. Mittlerweile kann sich jedermann registrieren, auch wenn er zuvor nicht von einem Mitglied eingeladen wurde. Seit dem 12. Januar 2012 wurde auch das Mindestalter der Mitglieder von 18 auf 13 Jahre herabgesetzt (wohl um mit Facebook gleichzuziehen), so dass nun eine der Hauptnutzergruppen sozialer Netzwerke teilnahmeberechtigt ist.

Voraussetzung für eine Registrierung bei Google+ ist ein Konto bei Google, das für die Registrierung bei Google+ bei Bedarf neu angelegt werden kann, ohne dass man dazu gezwungen ist, andere Google-Dienste wie Google-Mail, Google-Kalender oder Youtube in Anspruch zu nehmen.

Um sich mit einem bestehenden Google-Konto für Google+ zu registrieren, muss man sich auf die Seite von Google+ begeben (Bild 1.18) und dort auf ANMELDEN klicken. Anschließend werden die mit dem Google-Konto verknüpfte Mailadresse und das für das Konto gewählte Passwort eingegeben. Google bietet im Anschluss daran eine kleine Einführung und erklärt dem neuen Mitglied die unterschiedlichen Funktionen beziehungsweise bietet die Möglichkeit, alle grundlegenden Einstellungen über einen Assistenten (Bild 1.19) vorzunehmen.

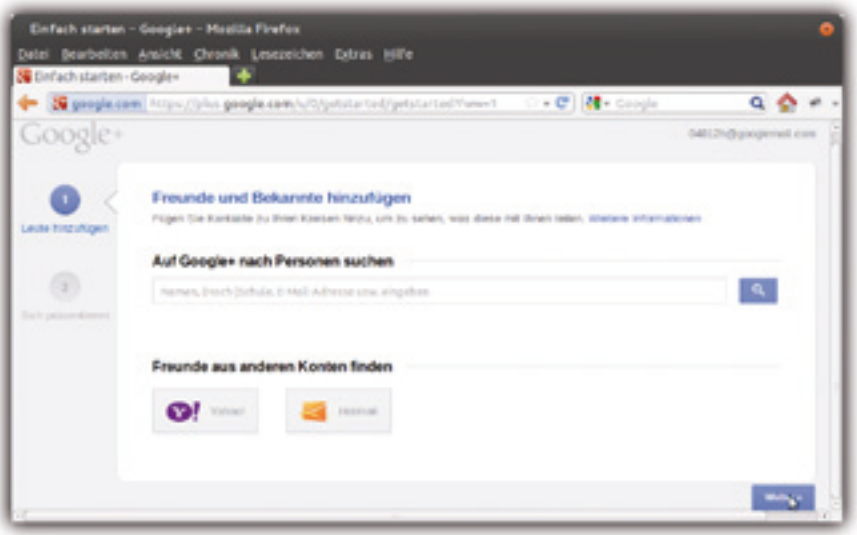

BILD 1.19 Der Assistent für die Anmeldung

Etwas aufwendiger ist die Registrierung ohne bestehendes Google-Konto, das zuerst angelegt werden muss, bevor auf die Dienste von Google+ zugegriffen werden kann. Durch einen Klick auf KONTO ERSTELLEN in der rechten oberen Ecke der Google+-Anmeldeseite (Bild 1.18) gelangt man zum entsprechenden Registrierungsformular. Hier sind neben Name, Vorname und Geburtsdatum auch der Nutzername und ein Passwort zu notieren. Optional kann auch eine alternative Mailadresse sowie eine Mobilfunknummer angegeben werden.

Nachdem man sich mit den Nutzungsbedingungen einverstanden erklärt und sein Herkunftsland angegeben hat, gelangt man mit einem Klick auf WEITER zum nächsten Schritt. Hier kann man ein Profilfoto hochladen oder per Webcam aufnehmen. Man kann diesen Schritt aber auch überspringen und sofort auf NÄCHSTER SCHRITT klicken. Nun ist das Konto fertig eingerichtet und mit einem Klick auf WEITER ZU GOOGLE+ gelangt man auf die eigene Google+ Startseite.

Die Benutzeroberfläche

Ähnlich wie die Benutzeroberfläche von Facebook besteht auch die von Google+ aus einem dreispaltigen Layout, das am oberen Rand durch eine Kopfzeile ergänzt wird (Bild 1.20 auf der nächsten Seite). Diese Kopfzeile dürfte zwar von anderen Google-Diensten bereits bekannt sein, dennoch soll sie hier kurz erklärt werden:

Im linken Teil der Leiste bieten sich die verschiedenen Dienste an, die mit einem Google-Konto zugänglich sind. Für Google+ ist eigentlich nur der eigene Vorname, dem ein + vorangestellt ist, interessant. Dieser Eintrag verweist auf die Google+-Startseite, den sogenannten Stream. Die anderen in der Leiste angeführten Dienste können zwar eben-

falls genutzt werden, sind jedoch nicht Bestandteil von Google+ und damit auch nicht Bestandteil dieses Buchs.

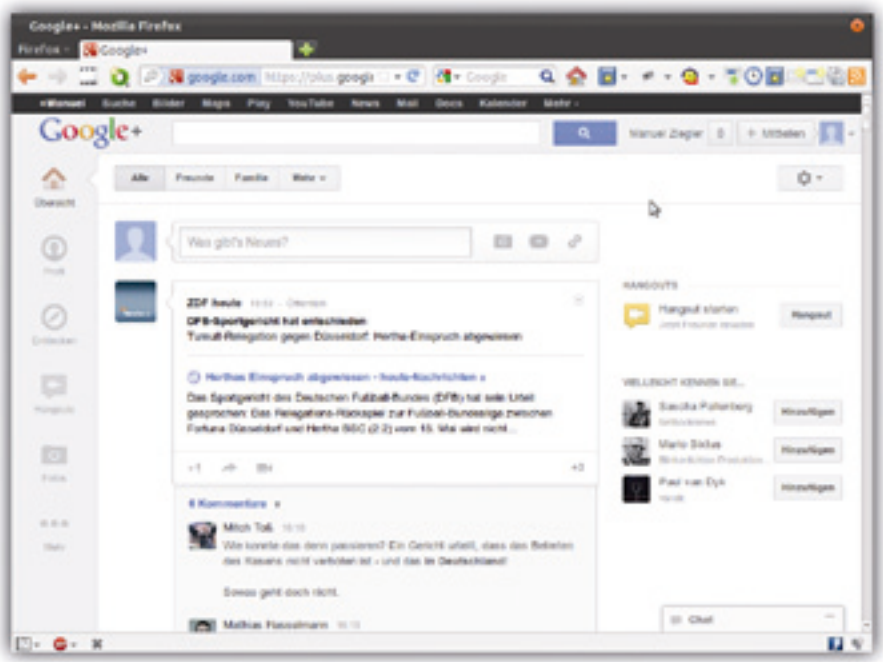

BILD 1.20 Die Benutzeroberfläche von Google+

Wesentlich interessanter ist die rechte Seite der Kopfzeile. Dort können neue Benachrichtigungen eingesehen, neue Beiträge veröffentlicht und Einstellungen geändert werden oder durch einen Klick auf den eigenen Namen oder das eigene Profilbild schnell wichtige Seiten wie der Stream oder das eigene Profil aufgerufen werden.

Unter dieser Kopfzeile, die auch beim Scrollen am oberen Bildrand haften bleibt, befindet sich eine weitere, vertikale Navigationsleiste, mit der die wichtigsten Bereiche von Google+ angesteuert werden können. Von oben nach unten gelangt man hier zum eigenen Stream, zum eigenen Profil, kann populäre Inhalte entdecken, erreicht Hangouts (also Videochats mit mehreren Personen), Fotos und mehr.

Ähnlich der Benutzeroberfläche von Facebook ist der Stream der wichtigste Bereich von Google+. Hier werden neue Beiträge anderer Benutzer angezeigt und können auch entsprechend gefiltert werden. So lassen sich mit einem Mausklick einzelne Kreise anzeigen. Auch die Benachrichtigungen werden auf dieser Seite angezeigt, sie werden – wie die einzelnen Beiträge aus den Kreisen – auf der linken Seitenspalte erreicht. Außerdem befindet sich auf dieser Seite der Chat, über den neue Unterhaltungen begonnen werden. Aktive Unterhaltungen erscheinen wie bei Facebook als Tabs am unteren Rand der Seite, können jedoch auch in einem eigenen Fenster angezeigt werden. Auf der rechten

Seitenleiste des Streams werden dem neuen Mitglied Hinweise zur effizienten Anwendung von Google+ geboten und Anzeigen abgebildet. Nicht zuletzt können von hier Hangouts begonnen werden.

Das Benutzerprofil

Möchte man sich das eigene Benutzerprofil (Bild 1.21) ansehen, klickt man in der oberen Leiste auf den eigenen Namen und wählt im sich öffnenden Drop-down-Menü den Punkt PROFIL aus. Das eigene Profil wird hier so genauso dargestellt wie jedem Besucher, der berechtigt ist, die entsprechenden Informationen zu betrachten. Durch die Eingabe eines Namens im Feld PROFIL ANSEHEN ALS auf der rechten Seite oder die Auswahl der öffentlichen Darstellung kann das Profil auch aus der Sicht eines einzelnen Nutzers beziehungsweise aus Sicht der Öffentlichkeit angezeigt werden. Auf diese Weise lässt sich schnell überprüfen, welcher Nutzer welche Informationen zu Gesicht bekommt und welche Daten ihm verborgen bleiben.

BILD 1.21 Das Benutzerprofil in Google+

Neben den Beiträgen des Benutzers, die auf dem ersten Reiter des Profils angezeigt werden, lassen sich auch Informationen über ihn wie beispielsweise seine Arbeitsstelle, Ausbildung, Geschlecht, Webseiten und ähnliches abrufen. Unter den Punkten FOTOS und VIDEOS sind seine geteilten – also die vom Benutzer veröffentlichten – Bilder und Videos zu sehen, außerdem die Bilder, auf denen er getagt (markiert) wurde. Der Punkt *+1* enthält Seiten und Inhalte aus dem Internet, die ihm gefallen oder an denen er seinen Gefallen ausdrücken möchte.

Um die im Profil abgebildeten Informationen unter dem Punkt INFO zu ändern, navigiert man einfach zum eigenen Profil und klickt dann auf die Schaltfläche PROFIL BEARBEITEN in der rechten oberen Ecke. Anschließend werden die verschiedenen bearbeit-

baren Punkte sichtbar. So kann hier beispielsweise ein Intro verfasst werden, in das man typischerweise einen kleinen, charakteristischen Text über die eigene Person schreibt. Dieser Text ist von Google dazu gedacht, die eigene Person für Freunde identifizierbar zu machen. So kann bei der Suche nach diesem Namen überprüft werden, ob auch tatsächlich die richtige Person gefunden wurde.

Der Punkt Dies und Das hat eine ähnliche Funktion wie das Intro, hier sind aber häufig nur Stichpunkte zu finden und kein zusammenhängender Text.

Weitere Punkte beziehen sich auf spezielle Merkmale des Benutzers. So ist es beispielsweise möglich, Beruf, Beschäftigung, Ausbildung, den eigenen Wohnort, seinen Beziehungsstatus oder die Kontaktmöglichkeiten für den Privat- und Geschäftsverkehr anzugeben. Für jeden dieser Punkte kann die Sichtbarkeit festgelegt werden, um bestimmte Informationen vor der Öffentlichkeit zu verbergen oder sie nur einem definierten Personenkreis zugänglich zu machen.

Am rechten Rand der Seite befinden sich zusätzliche Einstellmöglichkeiten, die sich auf Inhalte im Internet beziehen. Hier können andere Profile wie beispielsweise auch ein Facebook-Konto mit dem Google+-Konto verknüpft werden. Die Daten werden später über einen Link auf seinem Profil mit dem Benutzer in Verbindung gebracht. Außerdem kann man Seiten angeben, bei denen man selbst mitwirkt, beispielsweise Foren oder auch eigene Websites. Nicht zuletzt können aber auch andere Webseiten empfohlen werden; auf sie wird anschließend mit einem Link verwiesen.

Die Verwaltung von Freunden

Bei Google+ rücken – im Gegensatz zu Facebook – die Verwaltung der Freunde und damit die Privatsphäre des einzelnen Mitglieds in den Fokus. Google hat sich hier das Konzept der Kreise (Bild 1.22) einfallen lassen, bei dem die Freunde in unterschiedlichen Kreisen (vergleichbar mit Listen auf Facebook) organisiert werden. Außerdem lassen sich durch das Teilen von Kreisen Gruppierungen ähnlich der Gruppen in Facebook anlegen. Doch zunächst zur Funktion von Kreisen:

Soll ein anderes Mitglied als Freund hinzugefügt werden, nimmt man es in einen Kreis auf, wobei es über die Aufnahme informiert wird. So lange es den entsprechenden Benutzer jedoch nicht selbst auch in einen seiner Kreise aufnimmt, kann dieser lediglich öffentliche Informationen von ihm sehen. Der Benutzer wird allerdings nicht darüber informiert, in welchen Kreis er aufgenommen wurde. So kann er beispielsweise in einen Kreis namens *Idioten* aufgenommen werden, ohne darüber informiert zu werden.

Verwaltet werden die eigenen Kreise über den Punkt Kreise auf der Menüleiste im oberen Teil der Seite. Hier werden alle Personen, die in den eigenen Kreisen enthalten sind, sowie die einzelnen Kreise angezeigt. Die vier standardmäßig enthaltenen Kreise Freunde, Familie, Bekannte sowie nur folgen können durch eigene, individuell benannte Kreise ergänzt werden, so dass eine präzise Unterteilung der eigenen Freunde in Gruppen möglich ist; dabei kann eine Person auch mehreren Kreisen zugeordnet werden. Einzelne oder mehrere Personen können bequem per Drag&Drop in beliebige Kreise gezogen werden, die einzelnen Kreise lassen sich durch Ziehen in beliebiger Rei-

BILD 1.22 Die Verwaltung von Freunden in Kreisen

henfolge anordnen. Zieht man eine Person aus einem Kreis heraus und lässt sie los, wird sie automatisch gelöscht.

Möchte man eine neue Gruppe zusammenstellen, muss ein Kreis mit allen gewünschten Mitgliedern angelegt und anschließend geteilt werden. Dazu wird nach den Vorarbeiten dieser Kreis angeklickt und anschließend über die Option TEILEN für einen bestimmten Kreis oder für die Öffentlichkeit verfügbar gemacht. Dabei sollte man das Ankreuzfeld MICH SELBST IN GETEILTEM KREIS AUFNEHMEN aktivieren. Die Personen, mit denen dieser Kreis geteilt wurde, können anschließend mit einem Klick auf KREIS HINZUFÜGEN diesen Kreis unter einem eigenen Namen übernehmen, so dass geteilte Beiträge innerhalb dieses Kreises die gleichen Benutzer erreichen, egal wer sie veröffentlicht.

Einstellungen

Die Einstellungen von Google+ gehen teilweise fließend in die Einstellungen für das Google-Konto selbst über. Hier werden nur die für Google+ relevanten Einstellungsmöglichkeiten angesprochen.

Kontoeinstellungen

Um zu den Kontoeinstellungen zu gelangen, klickt man auf der oberen Leiste auf seinen Namen und wählt anschließend den Punkt KONTOEINSTELLUNGEN aus; es erscheint eine Anzeige wie in Bild 1.23 auf der nächsten Seite.

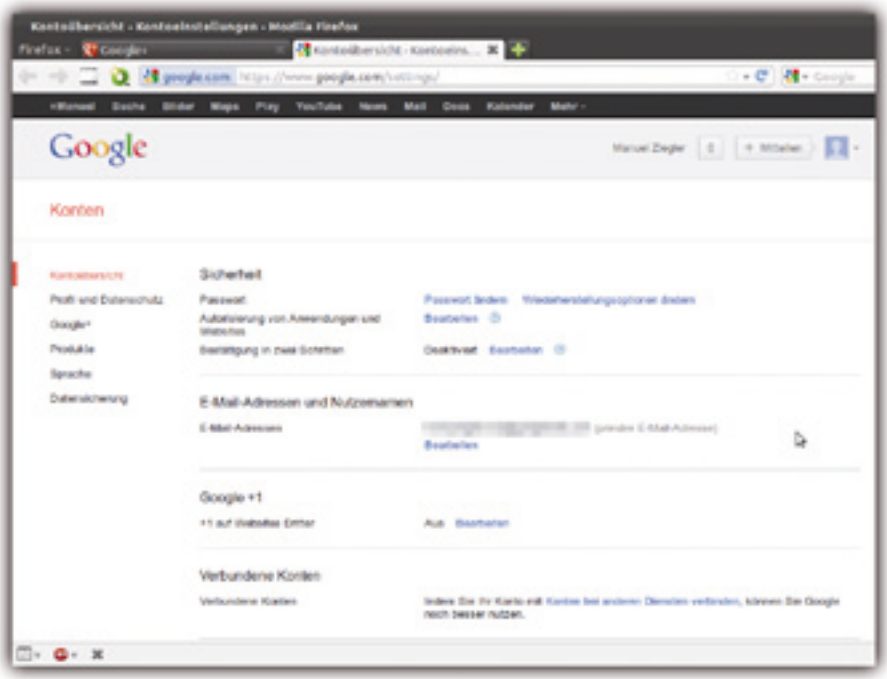

BILD 1.23 Kontoeinstellungen

Der erste Punkt auf dieser Seite ist ein Verweis auf das eigene Profil, über den die einzelnen Punkte des Profils, die ab Seite 31 bereits angesprochen wurden, verändert werden können.

Es folgen mehrere unter der Überschrift SICHERHEIT zusammengefasste Einstellungsmöglichkeiten, die vor allem die Sicherheit des Google+-Kontos gewährleisten sollen. So kann man hier beispielsweise das Passwort ändern, die Wiederherstellungsoptionen anpassen, die sogenannte Bestätigung in zwei Schritten aktivieren oder Passwörter für Anwendungen und Websites vergeben.

Interessant ist vor allem die Bestätigung in zwei Schritten. Sie sorgt dafür, dass eine Anmeldung über das Google+-Konto nur möglich ist, wenn entweder der auf den Dienst zugreifende Computer Google bekannt ist oder wenn zusätzlich zum Passwort ein Bestätigungscode, der per SMS auf ein registriertes Mobiltelefon gesendet wird, eingegeben wurde. Bei dieser Einstellung muss für eventuelle Anwendungen, die ebenfalls Gebrauch vom Google-Konto machen wie beispielsweise Mail- oder Chat-Clients, ein eigenes Passwort generiert werden. Solche Anwendungen können nämlich unter Umständen keinen Bestätigungscode anfordern, wodurch sie auf das Google-Konto nicht mehr zugreifen können. Die Passwörter werden unter dem Punkt AUTORISIERUNG VON ANWENDUNGEN UND WEBSITES erzeugt und aufgehoben.

Weitere Punkte zu den Kontoeinstellungen sind unter der Überschrift DIENSTE zusammengefasst. Hier lassen sich alle Google+-Daten oder auch das gesamte Google-Konto löschen (Bild 1.24). Es kann aber nicht geprüft werden, ob die Benutzerdaten tatsächlich gelöscht sind oder ob Google sie in Facebook-typischer Manier auch nach dem Löschvorgang in den eigenen Datenbanken behält. Allerdings sind bei Google – ganz im Gegensatz zu Facebook – noch keine Lecks, die eine solche Vermutung nahelegen würden, aufgetreten. Man darf allerdings nicht vergessen, dass Google in Bezug auf Datenschutz auch keine reine Weste hat: Immerhin werden die E-Mails von Google-Mail-Nutzern immer noch standardmäßig automatisch von einem der Googlebots mitgelesen.

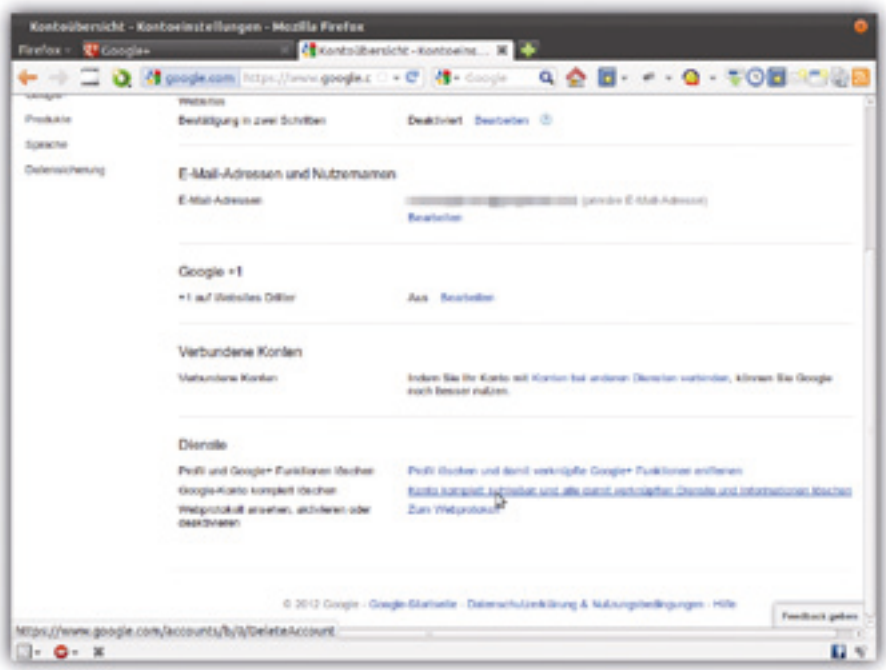

BILD 1.24 Alle persönlichen Daten löschen

Einstellungen

Neben den für das gesamte Google-Konto geltenden Einstellungen können auch ausschließlich Google+ betreffende Einstellungen vorgenommen werden, indem man auf das kleine Zahnrad-Symbol auf der rechten Seite der Google-Leiste klickt und im sich öffnenden Drop-down-Menü GOOGLE+-EINSTELLUNGEN auswählt. Unter WER KANN SICH MIT MIR UND MEINEN BEITRÄGEN AUSTAUSCHEN lässt sich festlegen, von wem Benachrichtigungen empfangen werden sollen und wer öffentliche Beiträge kommentieren darf.

Die folgenden Punkte regeln, wohin Benachrichtigungen zu versenden sind und welche Benachrichtigungen überhaupt verschickt werden dürfen. Man kann sie entweder per E-Mail oder per SMS oder auf beiden Wegen erhalten. Zusätzlich zur Gmail-Adresse kann man eine Mobiltelefonnummer hinzufügen, an die Benachrichtigungen versandt werden. Außerdem lässt sich sehr differenziert einstellen, welche Benachrichtigungen überhaupt per E-Mail empfangen werden sollen.

Besonders wichtig ist das Aktivieren beziehungsweise Deaktivieren der +1-Funktion von Google. Sie entspricht in etwa dem GEFÄLLT MIR von Facebook, allerdings kann man hier einstellen, ob mit dieser Funktion Inhalte von fremden Webseiten personalisiert werden sollen. Aktiviert man die Funktion, kann man auf Websites von Dritten sehen, ob sie einem Freund gefallen, und auch Freunde können sehen, dass einem diese Seite gefällt (Bild 1.25). Deaktiviert man diese Funktion, werden keine personalisierten Daten über die Websites Dritter angezeigt. Die Problematik der in Kapitel 3.2.1 angesprochenen Möglichkeiten zur Ermittlung der Browserhistorie lässt sich durch die Deaktivierung dieser Funktion jedoch nicht beheben.

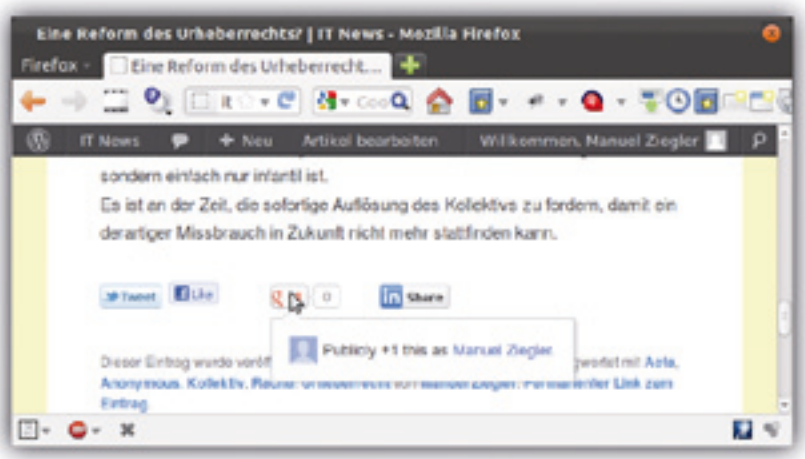

BILD 1.25 Die +1-Funktion auf anderen Seiten

Ebenso interessant sind die Möglichkeiten für das Einstellen der Funktion MEINE KREISE, die beim Veröffentlichen von Beiträgen zum Tragen kommt. Die Reichweite eines Beitrags wird generell festgelegt, indem man ihn für einzelne Personen, einzelne Kreise, mehrere Kreise oder generell für die Öffentlichkeit verfügbar macht. Damit man für Beiträge, die alle Freunde betrachten sollen, nicht umständlich alle Kreise hinzufügen muss, ist die Funktion MEINE KREISE vorgesehen, mit der ein Beitrag standardmäßig für alle Kreise des Benutzers – mit Ausnahme des Kreises NUR FOLGEN – veröffentlicht wird. Diese Funktion lässt sich hier anpassen, so dass beispielsweise Kreise wie *Idioten* ebenfalls ausgenommen werden können.

Ein letzter, wichtiger Punkt betrifft die veröffentlichten Fotos: Hier wird eingestellt, ob automatisch Standortinformationen zu hochgeladenen Fotos hinzugefügt werden sollen, ob andere Benutzer Fotos herunterladen können oder ob die automatische Gesichtserkennung erlaubt ist.

Zu beachten ist vor allem, dass ein Herunterladen von Bildern nicht vollständig verhindert werden kann. Aus vielen Browsern dürfte die Funktion BILD SPEICHERN UNTER bekannt sein. Sie wird hier von Google durch JavaScript unterdrückt. Betrachtet aber jemand die Bilder und hat in seinem Browser JavaScript deaktiviert (Bild 1.26) beziehungsweise die Funktion, die das Speichern der Bilder verhindern soll, ausgeschaltet, kann er die Bilder dennoch herunterladen und auf seinem PC abspeichern. Daher sollte man sich stets gut überlegen, ob man ein bestimmtes Foto auch wirklich veröffentlichen will. Denn man kann nie ausschließen, dass nicht jemand, für den das Bild sichtbar ist, das System überlistet und das Bild weiterverbreitet.

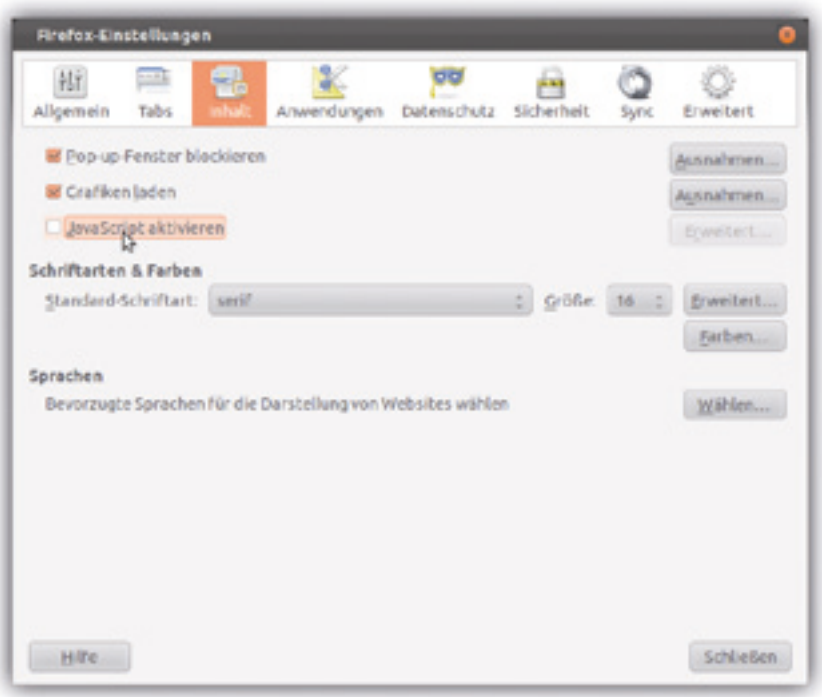

BILD 1.26 Browsereinstellungen für deaktiviertes JavaScript in Firefox

1.2.3 XING

XING unterscheidet sich etwas von den bisher vorgestellten sozialen Netzwerken. Im Gegensatz zu Facebook und Google+ erhebt es den Anspruch, professionell zu sein und das Berufsleben der Mitglieder zu bereichern. Natürlich erwartet XING dafür auch eine Gegenleistung. Deshalb werden nur einige Funktionen kostenlos angeboten und für Premium-Accounts geworben, die nur entgeltlich genutzt werden können.

Schon auf der Startseite wirbt XING mit dem Slogan *Für privates gibt's Facebook, für berufliches gibt's XING!*. Damit wird demonstriert, dass XING nicht in direkte Konkurrenz zum Platzhirsch Facebook treten will, sondern versucht, Nischen zu besetzen, die Facebook gar nicht oder nicht ausreichend abdeckt.

BILD 1.27 Die Startseite von XING

XING zählt mit ungefähr 11,4 Millionen Mitgliedern[13] zu den eher kleineren sozialen Netzwerken, konnte jedoch in gewissen Kreisen durchaus eine hohe Beteiligungsrate erreichen.

Registrierung

Das Registrieren bei XING[14] ist im Grunde ebenso einfach wie bei Facebook oder Google+. Allerdings muss der Vorsichtige bei der Anmeldung teilweise aufpassen. Mit

[13] Eigene Angabe unter http://corporate.xing.com/no_cache/deutsch/unternehmen/xing-ag/ (Stand: September 2011)

[14] http://www.xing.com

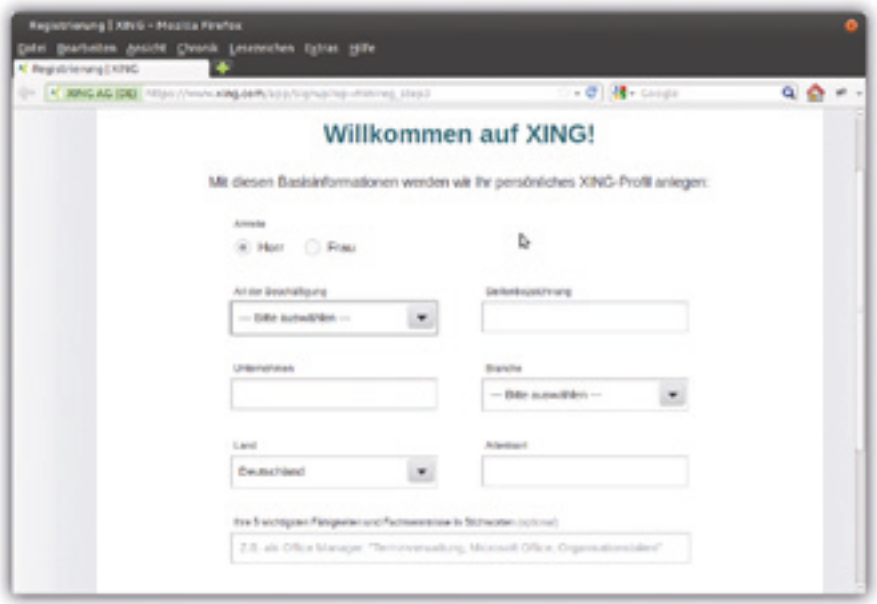

BILD 1.28 Die Registrierung bei XING

einem Klick auf die Schaltfläche JETZT KOSTENLOS REGISTRIEREN auf der Startseite gelangt man zu einem Eingabeformular (Bild 1.28), in das Familienname, Vorname, eine E-Mailadresse und ein Passwort einzutragen sind. Außerdem sind die AGB und Datenschutzbedingungen von XING zu akzeptieren, um Mitglied werden zu können.

Direkt im Anschluss erhält man an die genannte Kontaktadresse eine E-Mail mit einem Aktivierungslink. Nachdem er angeklickt wurde, wird man aufgefordert, das eigene Profil um einige Details zu erweitern. Unbedingt verlangt werden Aussagen über das eigene Geschlecht, die Art der eigenen Beschäftigung, eine nähere Bezeichnung der Arbeitsstelle und Angaben zum derzeitigen Beschäftigungsort. Zuletzt muss unter dem Punkt KARRIERE-PLÄNE angegeben werden, ob derzeit ein Interesse an Stellenangeboten besteht und wem dieses Interesse angezeigt werden soll.

Im nächsten Schritt der Registrierung muss entschieden werden, ob eine gebührenfreie Basismitgliedschaft für die eigenen Zwecke ausreicht oder ob eine kostenpflichtige Premium-Mitgliedschaft angestrebt wird.

Mit den erweiterten Funktionalitäten einer Premium-Mitgliedschaft sollen bessere Voraussetzungen für den professionellen Einsatz von XING zur Arbeitssuche oder ähnliches geschaffen werden. Üblicherweise lohnt sich die gebührenpflichtige Nutzung von XING jedoch nicht. Da eine Premium-Mitgliedschaft auch im Nachhinein erworben werden kann, sollte der neue Nutzer lieber zunächst bei der Basis-Mitgliedschaft bleiben.

Im nächsten Schritt der Registrierung, den sogenannten ERSTEN SCHRITTEN BEI XING, werden dem Benutzer grundlegende Konfigurationsmöglichkeiten angeboten. Zunächst

BILD 1.29 Konfigurationsmöglichkeiten

werden ihm aufgrund der von ihm ermittelten Daten Kontakte vorgeschlagen (Bild 1.29). Gleichzeitig bietet XING die Möglichkeit, über die Adressbücher der E-Mail-Konten bekannter Webmail-Anbieter automatisch Kontakte zu finden. Dies ist jedoch nicht empfehlenswert, Kapitel 3.2.3 gibt über die Gründe, dies abzulehnen, genauer Auskunft.

Zusätzlich zu diesen Kontaktmöglichkeiten wird dem Benutzer angeboten, sein Profil zu vervollständigen. Dazu wird in einer Statusanzeige dargestellt, zu welchem Prozentsatz sein Profil bereits vollständig ist (zu Beginn sind es meist 36 Prozent). XING versäumt es nicht, ein weiteres Mal eine Premium-Mitgliedschaft anzubieten, doch auch hier sollte auf dieses Angebot noch nicht eingegangen werden, wenn man neu in XING ist.

Die Benutzeroberfläche

Im Gegensatz zu den bereits vorgestellten Oberflächen von Facebook und Google+ folgt die Benutzeroberfläche von XING (Bild 1.30) nicht vollständig dem bei sozialen Netzwerken üblichen Dreispalten-Layout mit fixierter Kopfzeile. Vielmehr ist bei XING die linke Spalte fixiert. Über sie wird auf alle Bereiche von XING zugegriffen. Einen erweiterten Zugriff auf die einzelnen Bereiche erlaubt auch das Navigationsmenü im Kopf der Seite. Hier lassen sich die einzelnen Bereiche und ihre untergeordneten Kategorien einfach mit Hilfe eines Drop-down-Menüs aufrufen.

Neben diesen Navigationsleisten besteht die Oberfläche von XING aus zwei weiteren Spalten: Die mittlere enthält den Inhalt des momentan fokussierten Bereichs, während in der rechten ergänzender Inhalt, hauptsächlich aber Werbung eingeblendet wird.

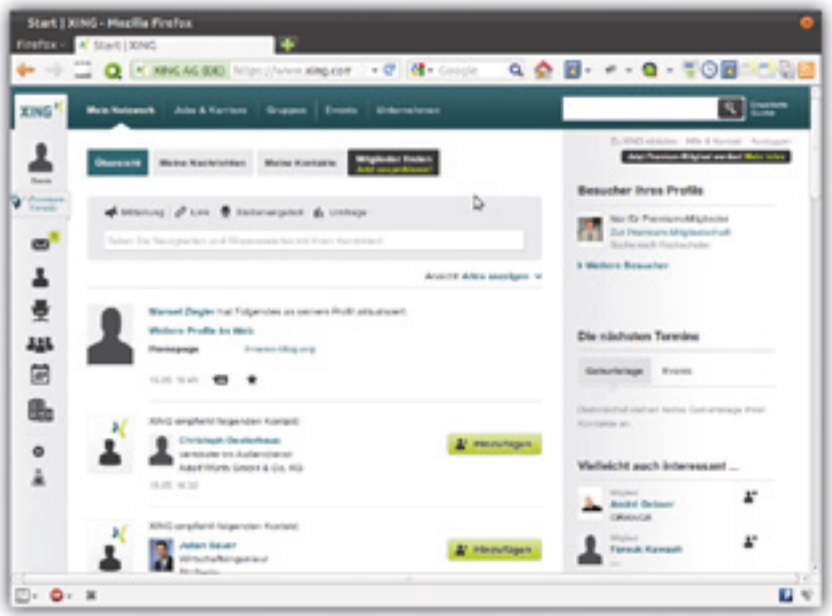

BILD 1.30 Die Benutzeroberfläche von XING

Das XING-Netzwerk selbst ist, wie Facebook oder Google+, in mehrere Bereiche aufgeteilt, die dem Benutzer über die linke Navigationsleiste zugänglich sind. Selbstverständlich gibt es auch in XING ein Profil jedes Benutzers. Klickt man auf das eigene Profilbild oder das voreingestellte Bild für Personen ohne Profilbild an zweiter Stelle von oben in der linken Navigationsleiste, gelangt man direkt zu den Einstellungen des eigenen Profils. Diese werden im nächsten Abschnitt ab Seite 42 ausführlich erläutert.

Auch die Möglichkeit der persönlichen Benachrichtigung bleibt bei XING nicht außen vor. Die persönlichen Nachrichten werden mit dem Briefsymbol in der linken Seitenleiste aufgerufen. Liegen ungelesene Nachrichten vor, steht am rechten oberen Rand eine kleine Zahl auf grünem Untergrund, dies ist die Anzahl der ungelesenen Nachrichten.

Mit einem Klick auf die angezeigte Nachrichten-Kopfzeile kann eine Nachricht vollständig betrachtet werden. Die drei Symbole rechts neben dem Nachrichtenbetreff erlauben es, mit einem Klick zu antworten, die Nachricht weiterzuleiten oder sie zu löschen. Um eine neue Nachricht zu verfassen, muss lediglich NACHRICHT SCHREIBEN im oberen rechten Bereich des Pop-up-Fensters angeklickt werden.

Direkt unter den Nachrichten sind die Kontaktanfragen untergebracht. Wie der Name schon sagt, ist es hier möglich, Kontaktanfragen zu beantworten, also anzunehmen oder abzulehnen.

Darunter wiederum befindet sich eine Schaltfläche JOBS UND KARRIERE. Hier werden dem Nutzer möglichst individuell abgestimmte Stellenangebote vorgeschlagen, sofern

er an den Vorschlägen interessiert ist. Außerdem kann man hier eigene Stellenausschreibungen durchführen, um vakante Stellen zu besetzen.

Unter dem Punkt GRUPPEN ist es möglich, Neuigkeiten aus Gruppen, in denen man aktiv ist, einzusehen. Gruppen in XING sind wesentlich besser strukturiert als solche unter Facebook. Man kann sich eine XING-Gruppe eher wie ein Forum vorstellen. Mitglieder können Beiträge in unterschiedlichen Kategorien einer Gruppe veröffentlichen. Die Gruppe bleibt dadurch übersichtlich und auch innerhalb der Gruppe kann besser zusammengearbeitet werden.

Neben den bisher genannten Punkten lassen sich Veranstaltungen (hier als EVENTS bezeichnet), an denen man teilnehmen wird, anzeigen, sowie Neuigkeiten von Unternehmen, die man abonniert hat, betrachten. Auf diese Punkte soll hier nicht weiter eingegangen werden.

Ganz unten lassen sich die Einstellungen aufrufen. Dort werden sowohl die Privatsphäre- als auch die Konteneinstellungen bearbeitet.

Das Benutzerprofil

Unter XING ist ein Benutzerprofil (Bild 1.31) deutlich kommerzieller ausgerichtet als in den anderen sozialen Netzwerken, schließlich erhebt XING auch den professionellen Anspruch. Ruft man die Profileinstellungen auf, sticht einem zunächst das eigene Profil-

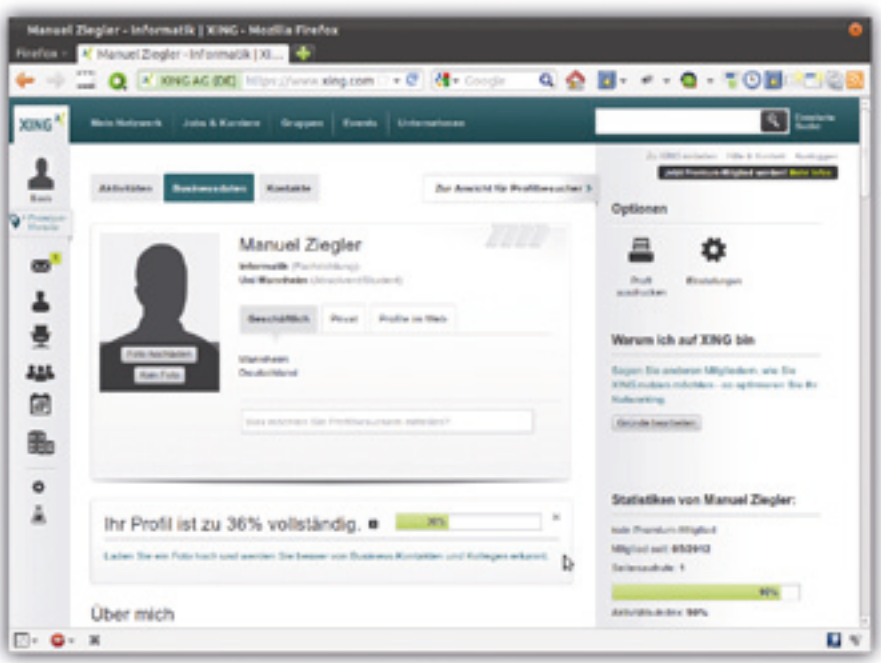

BILD 1.31 Das Benutzerprofil in XING

bild oder das Default-Profilbild in der linken oberen Ecke ins Auge. Die im Bild befindliche Schaltfläche FOTO HOCHLADEN dient dazu, das Bild durch eines von der eigenen Festplatte zu ersetzen. Ein Klick öffnet den bekannten Dialog für den Datei-Upload. Der Button KEIN FOTO löscht das persönliche Bild und ersetzt es durch das Default-Symbol.

Rechts versetzt unter dem Foto befindet sich ein Eingabefeld mit der Beschriftung WAS MÖCHTEN SIE PROFILBESUCHERN MITTEILEN?. Hier kann ein beliebiger Text eingetragen werden, der anschließend im Kopf des Profils erscheint.

Scrollt man weiter nach unten, findet man zunächst die Möglichkeit, eine sogenannte ÜBER-MICH-Seite anzulegen. XING sieht hier vor, dass die Benutzer eine Art Lebenslauf von sich anlegen und ihre Erfahrungen und Ziele in ihrem Fachgebiet detailliert beschreiben. Allerdings ist es ratsam, hier nicht gleich alles von sich zu erzählen. Ebenfalls um den Benutzer geht es bei den unter PERSÖNLICHES zusammengefassten Angaben. Dort kann das XING-Mitglied die Felder ICH SUCHE, ICH BIETE, INTERESSEN und ORGANISATIONEN nach Belieben ausfüllen. Ein ähnliches Vorgehen ist unter dem Punkt AUSBILDUNG gefragt. Hier kann der Benutzer die Stationen seiner Ausbildung, Sprachen und Zusatzqualifikationen sowie die Art der Beschäftigung mitteilen. Ergänzt wird dieser Punkt durch BERUFSERFAHRUNGEN, unter dem der Benutzer mit einem Klick auf EINTRAG HINZUFÜGEN seine ehemaligen Arbeitsstellen nennen kann.

Die Gruppe REFERENZEN UND AUSZEICHNUNGEN bleibt vor allem Premiumnutzern vorbehalten; Nutzer der Basisversion können hier lediglich erhaltene Auszeichnungen vermerken.

Unter dem Punkt WEB kann das XING-Mitglied andere Konten mit seinem Konto verknüpfen – was allerdings ebenso wenig empfehlenswert ist wie die Nutzung der unter KONTAKTDATEN angebotenen Möglichkeiten (Bild 1.32 auf der nächsten Seite). Man sollte bedenken, dass andere Mitglieder dadurch eine große Zahl von Daten erhalten werden, was gerade in einem Netzwerk wie XING, das nicht für den Zeitvertreib, sondern für professionelle Zwecke konzipiert wurde, normalerweise weniger erwünscht ist. Möchte man den anderen dennoch Daten über sich mitteilen, macht man das besser in einer persönlichen Nachricht und gibt so ganz gezielt die Daten weiter.

Einstellungen

Die Einstellungen sind in XING in die vier Punkte ZUGANGSDATEN, ANGABEN ZU MEINER PERSON, PRIVATSPHÄRE und BENACHRICHTIGUNGEN untergliedert.

Zugangsdaten

Unter dem Punkt ZUGANGSDATEN werden der eigene Benutzername und das mit dem Konto verknüpfte Passwort geändert. Als Benutzername ist üblicherweise eine Kombination aus

<Vorname>.<Nachname> <Zahl>

voreingestellt. Sofern ein selbst gewählter Name noch verfügbar ist und er den Vorgaben entspricht, wird dieser Benutzername beliebig geändert.

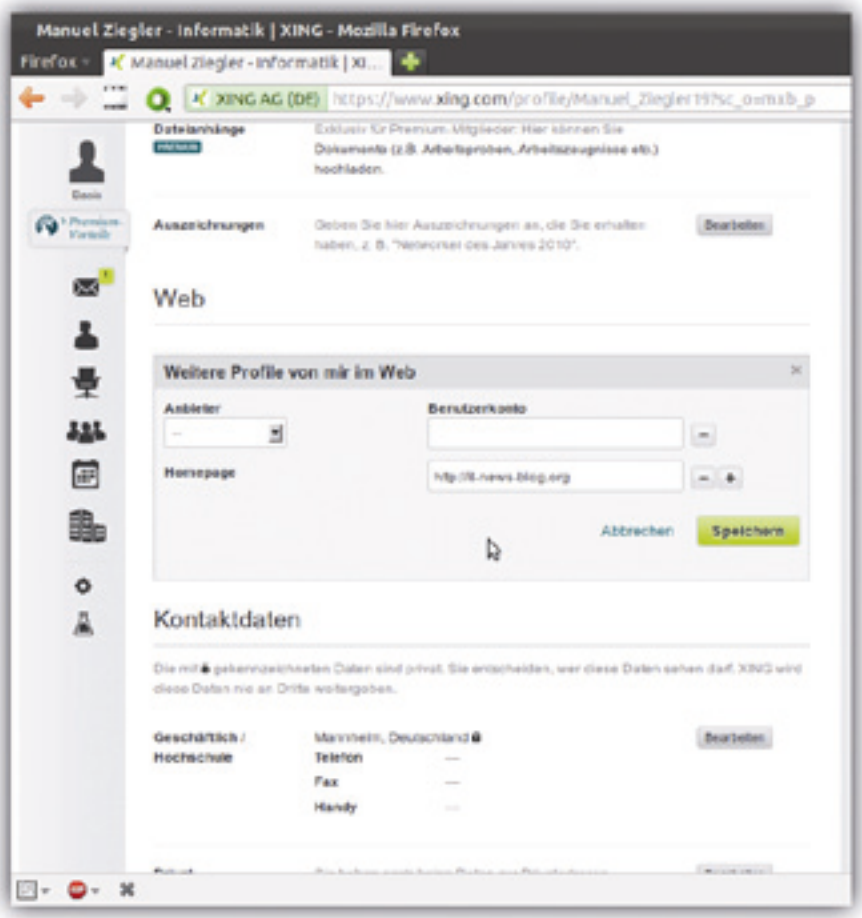

BILD 1.32 Mit anderen Konten verknüpfen

Um das Passwort zu ändern, muss zuerst das alte und anschließend zweimal das neue Passwort eingegeben werden. Der Sicherheitsgrad des neuen Passwortes wird sofort auf einer Leiste unterhalb der Eingabefelder angezeigt. Das Passwort sollte eine Sicherheit von mindestens 75 Prozent aufweisen, empfehlenswert ist nach Möglichkeit eine Sicherheit von hundert Prozent.

Angaben zu meiner Person

Unter ANGABEN ZU MEINER PERSON werden die persönlichen Daten wie Familienname, Vorname und Geburtsname, aber auch Informationen zum akademischen Abschluss sowie zum akademischen Grad festgelegt. Prinzipiell gilt auch hier: So viel angeben wie nötig (Familienname und Vorname) und so wenig wie möglich (der Geburtsname beispielsweise hat hier nichts verloren). Ob man einen akademischen Grad und Abschluss

angibt, sei jedem selbst überlassen. Zusätzlich zu diesen Einstellungen ist es hier möglich, die Spracheinstellungen zu verändern; es kann die Sprache ausgewählt werden und außerdem, ob beispielsweise bei der Suche Personen aus dem gleichen Sprachraum bevorzugt angezeigt werden sollen.

Privatsphäre

Der Punkt PRIVATSPHÄRE ist in die beiden Bereiche MEINE PRIVATSPHÄRE und NEUES AUS IHREM NETZWERK unterteilt. Die unter MEINE PRIVATSPHÄRE zusammengefassten Einstellungen betreffen vornehmlich die Reichweite persönlicher Daten. Beispielsweise kann hier eingestellt werden, ob das eigene Profil auch von Nicht-Mitgliedern, also nicht registrierten Personen aufgerufen werden darf, ob das eigene Profil und öffentliche Beiträge durch Suchmaschinen indiziert werden dürfen, für wen die eigenen Kontakte sichtbar sind, wer an die eigene Pinnwand schreiben und persönliche Nachrichten verschicken darf, ob der sogenannte Aktivitätsindex[15] (Bild 1.33) angezeigt werden darf und ob die eigene Geschäftsadresse in einer Karte angezeigt werden soll (sofern vorhanden).

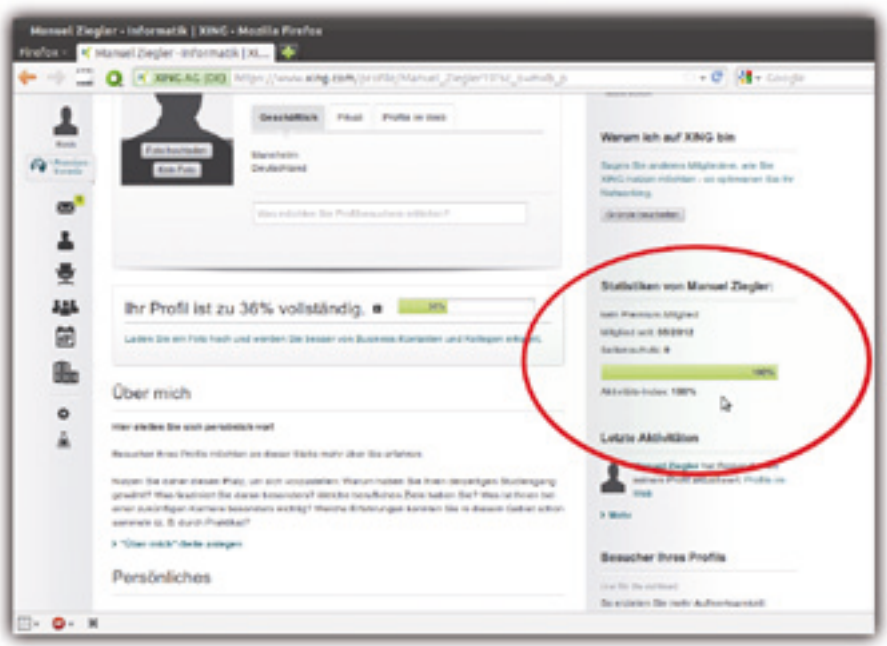

BILD 1.33 Aktivitätsindex

Unter NEUES AUS IHREM NETZWERK sind die Einstellungen für Benachrichtigungen über Änderungen an Kontakten zusammengefasst. Hier wird eingestellt, ob die Kontakte bei einer Änderung der persönlichen Daten, der Kontaktliste, der Berufserfahrung

[15] Der Aktivitätsindex gibt darüber Aufschluss, wie oft ein Benutzer sich in XING aufhält. Ruft man XING längere Zeit nicht auf, sinkt dieser Index, nutzt man XING über längere Zeit täglich, steigt der Wert an.

oder der sogenannten Stammdaten – also im wesentlichen der Kontaktdaten – benachrichtigt werden sollen. Zudem kann man einstellen, ob Kontakte über neue Events, Statusmeldungen, Stellenangebote oder Unternehmen, die mit dem eigenen Benutzerprofil verknüpft sind, informiert werden sollen.

Benachrichtigungen

Unter BENACHRICHTIGUNGEN wird eingestellt, unter welchen Umständen man Nachrichten erhalten möchte. Unter E-MAIL-EINSTELLUNGEN wird das Format der E-Mails geändert, das heißt, man entscheidet, ob man E-Mails im HTML- oder in reinem Textformat erhalten möchte.

Unter ICH WÜNSCHE EINE BENACHRICHTIGUNG PER E-MAIL stellt man ein, wann man per E-Mail über Neuigkeiten auf XING benachrichtigt werden möchte. Und unter XING NEWSLETTER UND E-MAIL-TIPPS wird festgelegt, ob man einen wöchentlichen Newsletter von XING erhalten und in unregelmäßigen Abständen über Sonderangebote informiert werden möchte, also ob das Zusenden von Werbung erwünscht ist.

1.2.4 meinVZ

Das Netzwerk meinVZ gehört zu einer Reihe von Netzwerken der Firma VZ Netzwerke Ltd. und ist mit knapp 16 Millionen[16] registrierten Benutzern eines der größten sozialen Netzwerke in Deutschland (siehe auch Tabelle 1.1 auf Seite 2). Neben dem Netzwerk meinVZ, das seit kurzem auch unter dem Namen FreundeVZ bekannt ist, gehören die Netzwerke SchülerVZ und StudiVZ zur Gruppe der VZ-Netzwerke (VZ steht hier für Verzeichnis). meinVZ ist direkt mit dem für Studenten gedachten Netzwerk StudiVZ verbunden und stellt insofern eine Besonderheit im Gebiet der sozialen Netzwerke dar. Eine Verbindung mit dem Netzwerk SchülerVZ gibt es aus rechtlichen Gründen derzeit nicht.

Zum Zeitpunkt der Drucklegung dieses Buchs standen die VZ-Netzwerke vor einer organisatorischen und inhaltlichen Umstrukturierung. Die folgenden Angaben treffen deswegen möglicherweise nicht mehr ganz zu.

Registrierung

Die Registrierung für meinVZ verläuft ähnlich wie die Anmeldung bei anderen sozialen Netzwerken und ist nicht sonderlich kompliziert. Unter der Webadresse www.meinVZ.net findet man ein Formular mit der Bezeichnung KOSTENLOS REGISTRIEREN (Bild 1.34). Dort trägt man den Vor- und Nachnamen, das Geburtsdatum und das Geschlecht ein und klickt anschließend auf WEITER.

Im nächsten Schritt werden weitere Angaben verlangt, um die Registrierung abzuschließen. Man muss die Region angeben, in der man lebt, hierbei wird sogar der Landkreis abgefragt. Außerdem wird eine Kontakt-E-Mailadresse verlangt, die gleichzeitig als Benut-

[16] Laut eigenen Angaben (Stand: Oktober 2011 http://www.meinvz.net/presse)

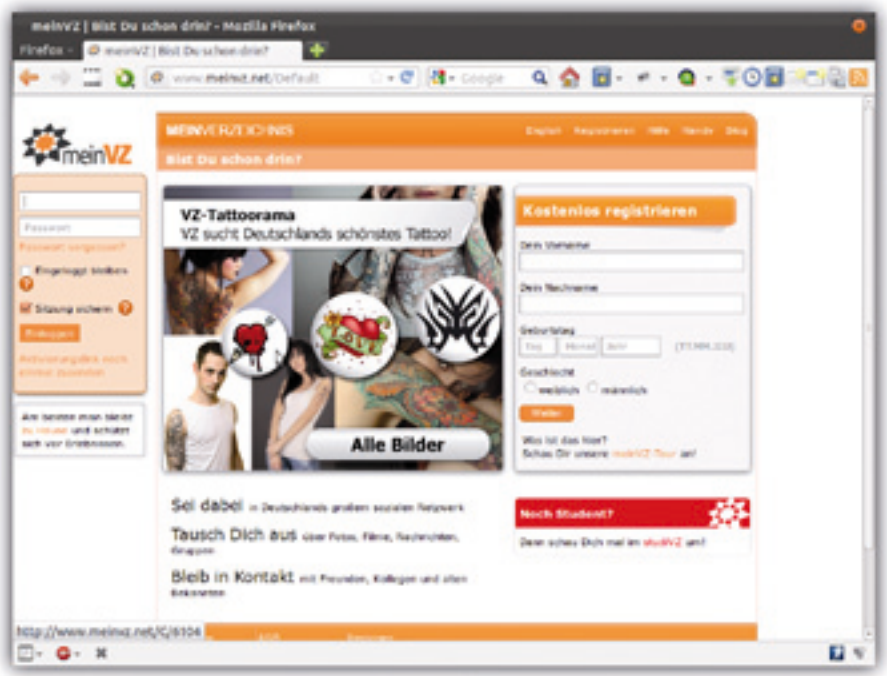

BILD 1.34 Die Startseite von meinVZ

zerkennung für das Login gilt. Zudem muss ein Passwort für die Authentifizierung definiert und einmal wiederholt werden.

Bevor die Registrierung abgeschlossen werden kann, müssen die AGB und der Verhaltenskodex sowie die Datenschutzerklärung von meinVZ akzeptiert werden (natürlich sollte man sie vorher auch lesen!). Um zu bestätigen, dass man ein Mensch ist und das Registrierungsformular nicht automatisiert von einem Computer ausgefüllt wurde, muss man eine Zeichenfolge abtippen, die in einem Captcha angezeigt ist.

Nach einem Klick auf JETZT REGISTRIEREN gelangt man zum letzten Schritt der Bestätigung der Registrierung. Dazu erhält man eine E-Mail mit einem Link, den man lediglich anzuklicken braucht. Oft wird dies allerdings beim ersten Mal mit einer Fehlermeldung quittiert. Klickt man den Link dann erneut an, führt das in der Regel zum Erfolg.

Ist die Registrierung abgeschlossen, kann man sich mit Hilfe des Loginformulars links auf der Startseite einloggen (Bild 1.34).

Direkt nach dem Login findet man sich auf der Startseite von meinVZ wieder. Eigentlich ist man auf der Startseite von FreundeVZ, da neue Benutzer automatisch die neue Oberfläche FreundeVZ vorgesetzt bekommen. Da diese Oberfläche die alte Oberfläche von meinVZ in naher Zukunft fast vollständig ablösen wird, wird im Folgenden nur die FreundeVZ-Oberfläche erläutert. Wer sich dennoch mit der alten Oberfläche von meinVZ

beschäftigen möchte, findet auf der unteren linken Seite der Benutzeroberfläche einen Kippschalter für den Wechsel zwischen den beiden Oberflächen (siehe auch Bild 1.35).

Die Benutzeroberfläche

Die FreundeVZ-Oberfläche ist ähnlich wie die Benutzeroberfläche von Facebook aufgebaut. Die linke Seitenleiste dient der Navigation in den unterschiedlichen Kategorien von FreundeVZ. Die breite mittlere Spalte zeigt den Inhalt der aktuell ausgewählten Kategorie, während auf der rechten Seite Werbe- und andere Anzeigen untergebracht sind.

Die Kopfzeile der Seite enthält wie bei Facebook eine Suchleiste, auf der nach Mitgliedern oder Benutzergruppen (Themen) gesucht werden kann, und in der Fußzeile der Seite wird eine Chatfunktion angeboten.

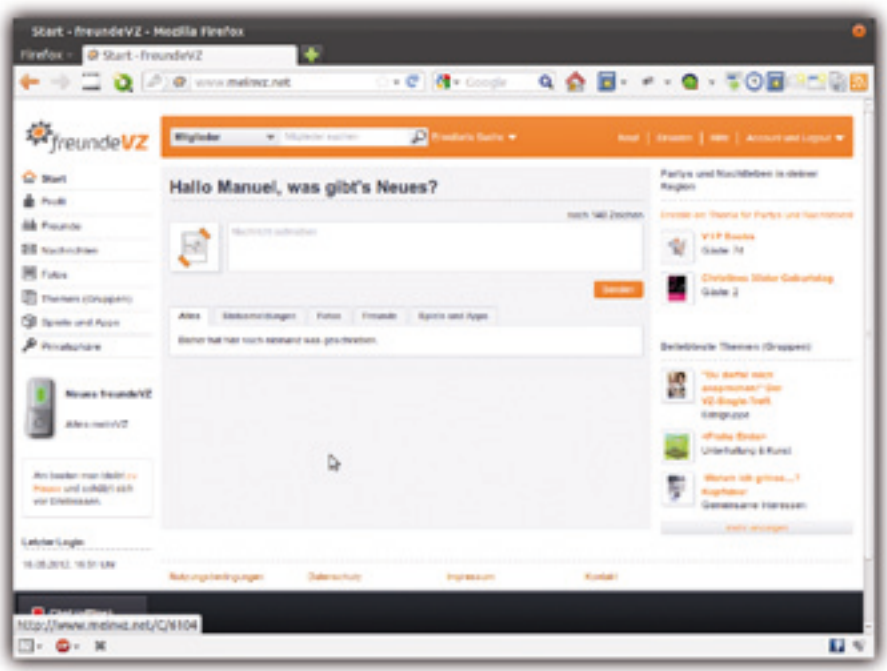

BILD 1.35 Die Oberfläche von FreundeVZ

Das Benutzerprofil

Um das eigene Profil zu betrachten, klickt man in der Navigation der linken Seitenleiste auf den Punkt PROFIL. Dort wird das eigene Profil zunächst so angezeigt, wie es auch Besucher zu sehen bekommen. Rechts neben dem Profilbild – sofern vorhanden – befindet sich die neueste vom Benutzer veröffentlichte Nachricht, darunter allgemeine Infor-

mationen über ihn. So steht dort beispielsweise, welchem Verzeichnis er angehört, also entweder meinVZ, FreundeVZ oder StudiVZ. Weiterhin sind dort das Anmeldedatum und das Datum des letzten Updates notiert. Mit „Update“ ist hier die letzte Änderung gemeint, die der Benutzer am eigenen Profil vorgenommen hat. Zudem befinden sich dort Angaben über das Geschlecht sowie die Region, aus der ein Benutzer stammt.

Unter diesem Kurzprofil, das noch um die Punkte Auf der Suche nach, Beziehungsstatus, Geburtstag und Über dich erweitert werden kann, sind weitere Informationen über das Mitglied zu finden, unterteilt in die Kategorien Interessen, Themen, Pinnwand sowie Spiele und Apps. Während Interessen ziemlich nach eigenem Ermessen ausgefüllt werden kann, hängen die anderen Punkte von den Aktivitäten des Benutzers ab. So sind unter Themen die Gruppen (in meinVZ als Themen bezeichnet) aufgelistet, denen der Benutzer angehört, der Punkt Pinnwand enthält alle Einträge auf seiner Pinnwand (ähnlich einem Gästebuch), und der Punkt Spiele und Apps listet die vom Benutzer verwendeten Spiele beziehungsweise Anwendungen auf.

Um die Angaben im eigenen Profil zu ändern (Bild 1.36), klickt man auf das Stiftsymbol in der rechten oberen Ecke der Profil-Anzeige.

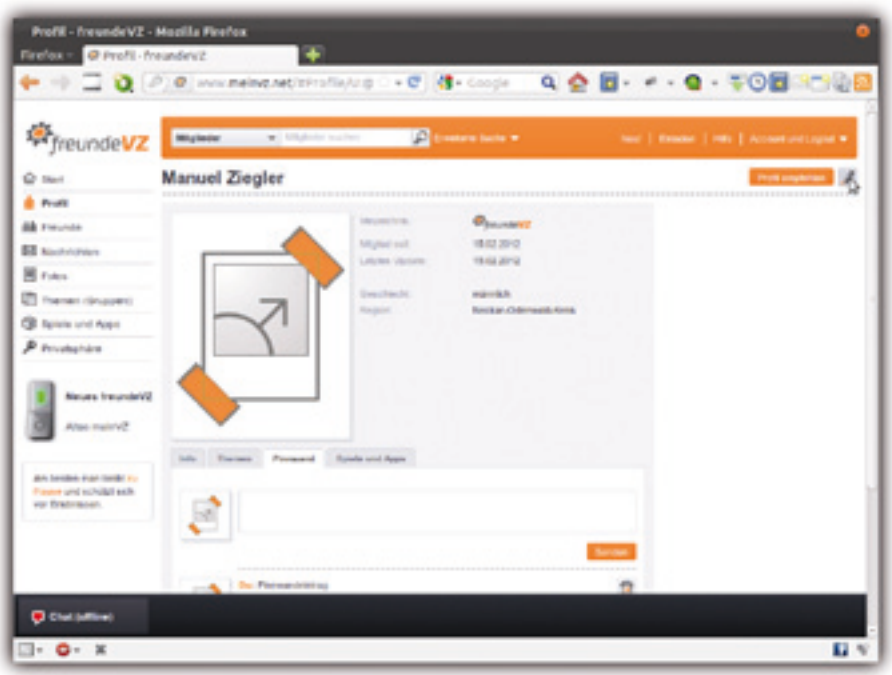

BILD 1.36 Profil ändern

Einstellungen

Die Einstellungen, die man als Benutzer vornehmen kann, sind in FreundeVZ in drei Hauptkategorien unterteilt:

- In den Account-Einstellungen lässt sich einsehen, unter welcher IP man sich in seinem Benutzerkonto angemeldet hat (oder von welcher IP aus sich ein Fremder eingeloggt hat). Außerdem kann man von dieser Seite ausgehend das eigene Benutzerpasswort ändern. Die Account-Einstellungen erreicht man, indem man in der rechten oberen Ecke auf ACCOUNT UND LOGOUT klickt und anschließend auf den Link ACCOUNT-EINSTELLUNGEN.
- Die Benachrichtigungseinstellungen werden ebenfalls über das Drop-down-Menü unter dem Punkt ACCOUNT UND LOGOUT erreicht. Anschließend muss hier auf den Punkt BENACHRICHTIGUNGEN geklickt werden. Dort lässt sich einstellen, bei welchen Ereignissen man per E-Mail benachrichtigt werden möchte.
- Die Privatsphäre-Einstellungen (Bild 1.37) werden unter dem Punkt PRIVATSPHÄRE in der linken Navigationsleiste aufgerufen. Aktuell (Stand März 2012) musste man dazu zur alten Benutzeroberfläche meinVZ wechseln, da das Ändern der Privatsphäre-Einstellungen über die FreundeVZ-Oberfläche noch nicht möglich war. Es wird jedoch automatisch angeboten, die Oberfläche zu wechseln.

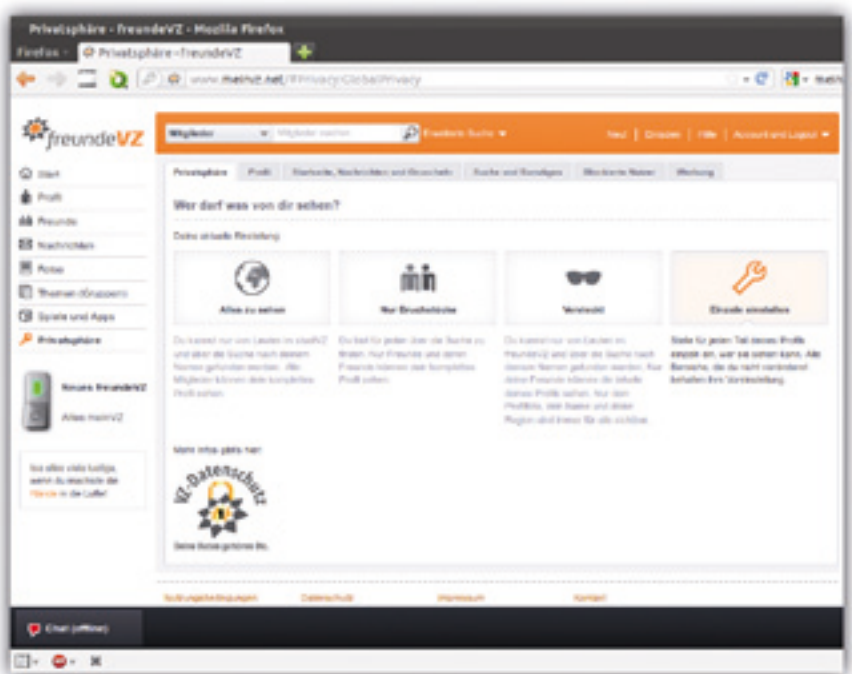

BILD 1.37 Privatsphäre-Einstellungen

Die Privatsphäre-Einstellungen sind im Grunde selbsterklärend und ähnlich wie die Privatsphäreeinstellungen der übrigen sozialen Netzwerke umgesetzt, so dass weitere Erklärungen an dieser Stelle eigentlich nicht nötig sind.

1.2.5 myspace

MySpace, heute auch myspace genannt, ist ein soziales Netzwerk, das anders als die bisher vorgestellten das Hauptaugenmerk auf Multimedia (ursprünglich nur Musik) legt. Bis zum Jahre 2008, als es von Facebook als Spitzenreiter abgelöst wurde, galt myspace sogar als das größte soziale Netzwerk. Seitdem ist ein Rückgang der Benutzerzahlen zu beobachten und mittlerweile ist es sogar möglich, sich direkt über Facebook, dem einstigen Konkurrenten, einzuloggen.

BILD 1.38 Die Startseite von myspace

Registrierung

Soll myspace nicht nur in Verbindung mit dem eigenen Facebook-Account genutzt werden, kann man sich dort als Mitglied registrieren. Dazu klickt man auf der Startseite von myspace[17] in der Kopfzeile der Seite die gelbe Schaltfläche REGISTRIEREN (Bild 1.38).

[17] Unter http://www.myspace.com/

Daraufhin wird das Registrierungsformular aufgerufen, das zur Registrierung bei myspace ausgefüllt werden muss. Hier ist zunächst der Account-Typ zu wählen, wobei die Optionen BAND und STANDARD zur Auswahl stehen (Bild 1.39). Als normaler Anwender wählt man hier gewöhnlich den Typ STANDARD aus; möchte man jedoch ein Konto für eine Band anlegen, wählt man BAND. Anschließend füllt man im Formular die Felder für den Nachnamen beziehungsweise Vornamen, die Mailadresse, das Geburtsdatum, das Geschlecht sowie für das Benutzerpasswort aus. Außerdem muss man – wie bei zahlreichen anderen sozialen Netzwerken – bestätigen, dass man keine Maschine ist und dazu eine angezeigte Zeichenfolge abtippen.

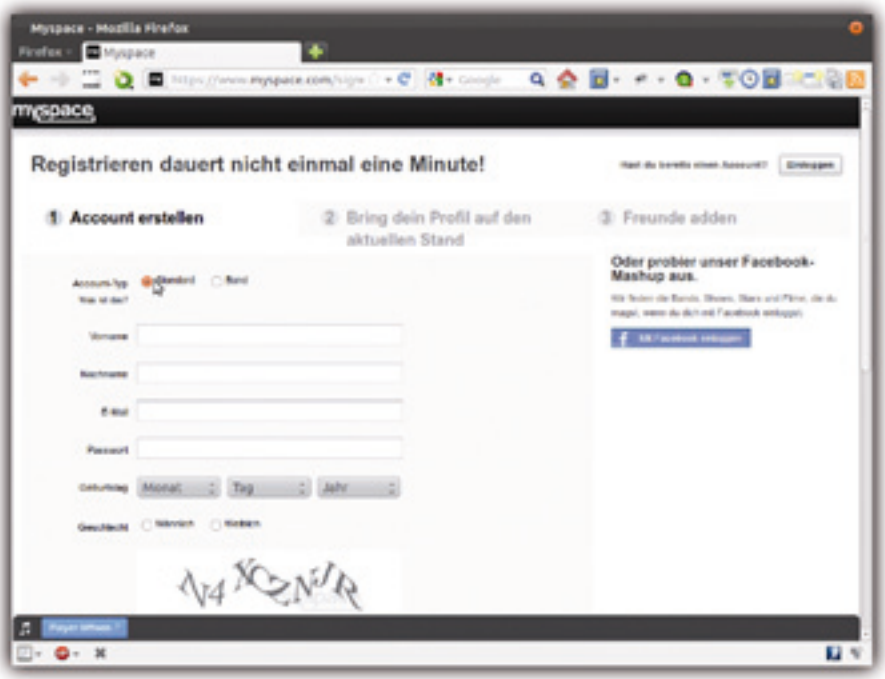

BILD 1.39 Account-Typ während dem Anmeldung auswählen

Mit einem Klick auf KOSTENLOS REGISTRIEREN gelangt man zum zweiten Schritt des Registriervorgangs. Jetzt wird man dazu aufgefordert, sein Profil auf den aktuellen Stand zu bringen und Informationen wie Herkunftsland, Bundesland sowie Wohnort preiszugeben. Üblicherweise sind diese Felder bereits vorausgefüllt, meist muss jedoch nachgebessert werden. Es ist zudem möglich, die Angaben zum Wohnort auszulassen, auch wenn dies nicht ausdrücklich erwähnt wird.

Mit einem Klick auf WEITER gelangt man zum dritten und letzten Schritt der Registrierung. Hier kann man angezeigte Bands und Interpreten zu seinen Freunden hinzufügen sowie die eigene Mailadresse nach in myspace registrierten Freunden durchsuchen lassen. Von dieser Funktion wird jedoch dringend abgeraten, weitere Informationen dazu

in Kapitel 3.2.3. Um die Registrierung abzuschließen, muss man noch auf den Aktivierungslink in der an die angegebene Mailadresse gesendeten E-Mail klicken.

Die Benutzeroberfläche

Die Benutzeroberfläche von myspace (Bild 1.40) ist wie die Benutzeroberflächen anderer sozialer Netzwerke in drei Spalten aufgeteilt. Auch die Oberfläche von myspace hat eine Kopfzeile, die beim Scrollen auf der Seite mit nach unten wandert und über die alle wichtigsten Punkte des Benutzerkontos erreicht werden.

Die linke der drei Spalten enthält die einzelnen Navigationselemente, mit denen sich die unterschiedlichen Dienste und Seiten von myspace aufrufen lassen. Diese werden in der mittleren Spalte angezeigt, während die rechte Spalte für Anzeigen reserviert ist.

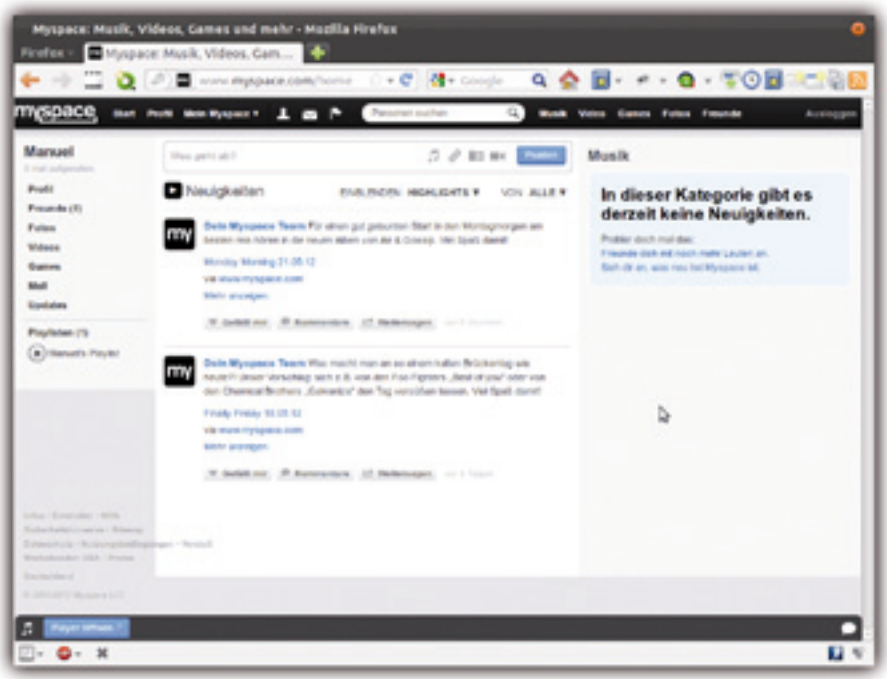

BILD 1.40 Die Benutzeroberfläche von myspace

Das Benutzerprofil

Das Benutzerprofil (Bild 1.41) erreicht man entweder über die Kopfzeile oder über die linke Seitenleiste. In beiden Fällen klickt man auf PROFIL, um zu seinem eigenen Profil zu gelangen.

In myspace hat man beim Benutzerprofil wesentlich mehr Freiheiten als in anderen sozialen Netzwerken. Um dem Profil etwas Individualität zu verleihen, kann man zwischen unterschiedlichen Designs wählen. Wer sich noch mehr Unverwechselbarkeit

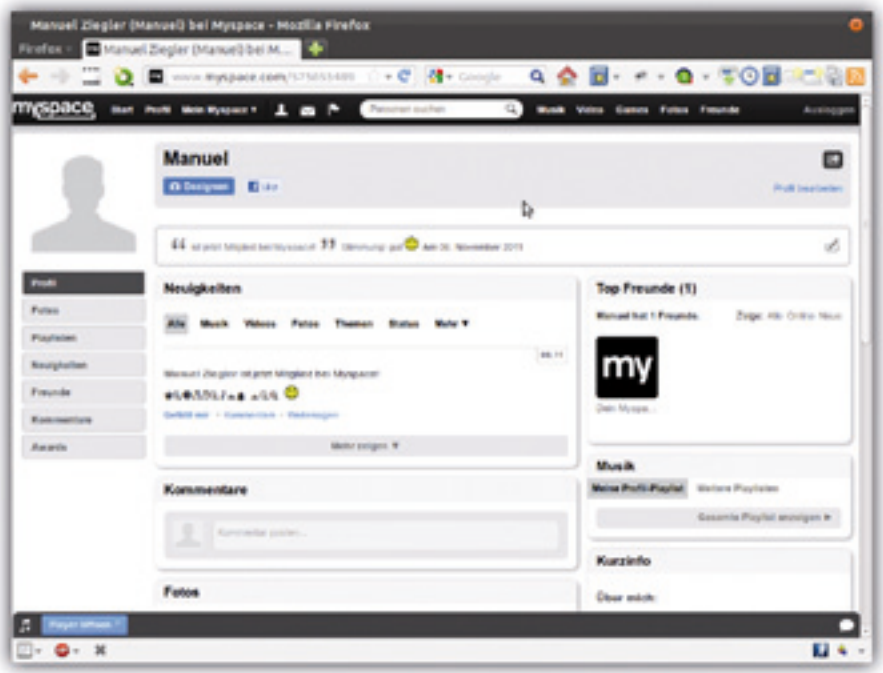

BILD 1.41 Das Benutzerprofil von myspace

wünscht, kann sogar ein eigenes Design zusammenstellen. Ansonsten ist auch bei myspace das Benutzerprofil in mehrere Kategorien unterteilt. Zu finden sind die Punkte PROFIL, FOTOS, PLAYLISTEN, NEUIGKEITEN, FREUNDE, KOMMENTARE und AWARDS. Anhand dieser Aufteilung wird bereits deutlich, dass das Hauptaugenmerk dieses Netzes auf Multimedia liegt.

Möchte man sein Profil bearbeiten, findet man in der rechten oberen Ecke einen Link PROFIL BEARBEITEN. Eine Änderung des Designs wird über die Schaltfläche DESIGNEN direkt unter dem eigenen Namen vorgenommen.

Einstellungen

Ein Kritikpunkt an myspace ist, dass die Einstellungen nicht so einfach zu finden sind wie in den anderen sozialen Netzwerken. Um zu ihnen zu gelangen, muss man in der Kopfzeile der Seite auf den Punkt MEIN MYSPACE klicken und im aufklappenden Dropdown-Menü unter der Überschrift ACCOUNT entweder MEIN ACCOUNT oder MEIN DATENSCHUTZ auswählen.

Unter MEIN ACCOUNT lassen sich Informationen wie die Kontakt-E-Mailadresse, der Vor- und Nachname sowie der angezeigte Name im Profil ändern. Unter DATENSCHUTZ werden die Einstellungen zur Privatsphäre des Nutzerkontos vorgenommen.

Natürlich hat man auch die Möglichkeit für weitere Einstellungen, dafür stehen unter den Einstellungen die Kategorien Keine Captchas mehr, E-Mail und IM-Adressen, Passwort, Handy, Verbundene Services, Ignorierte Nutzer und Account löschen zur Verfügung. Man findet sie, wenn man die Account- oder Datenschutz-Einstellungen aufruft und dann in der linken Seitenleiste die entsprechende Kategorie anklickt. Anschließend lassen sich dort die entsprechenden Einstellungen vornehmen.

1.2.6 Twitter

Twitter ist ein soziales Netzwerk mit dem primären Ziel, Kurznachrichten zu versenden. Der Hauptaugenmerk liegt bei Twitter also darauf, Informationen zu teilen und nicht, Nutzerprofile zu bauen. Anders als bei Netzwerken wie Facebook und Co. steht bei Twitter die Kommunikation im Vordergrund. Dabei ist es nicht einmal unbedingt nötig, dass man Twitter tatsächlich aktiv nutzt, sondern man kann sich bequem von anderen mit Informationen – den sogenannten Tweets – versorgen lassen und ganz darauf verzichten, selbst Tweets zu schreiben.

Im Gegensatz zu zahlreichen anderen sozialen Netzwerken scheinen die Betreiber von Twitter keinen unstillbaren Hunger nach Benutzerdaten zu haben und so hat es Twitter geschafft, auch in Fachkreisen, insbesondere bei Hackern, anerkannt zu sein.

Allerdings gibt es auch Ausnahmen und so ist bekannt, dass Twitter Daten von Smartphone-Benutzern ausspioniert. Die Twitter-App ermöglicht es den Betreibern, den Standort des Benutzers über den im Smartphone integrierten GPS-Empfänger zu ermitteln sowie seine Kontaktdaten auszulesen.

Registrierung

Wer ein Benutzerkonto im Twitter-Netzwerk anlegen möchte, findet auf der Startseite von Twitter (Bild 1.42) ein Anmeldeformular, in das der eigene Name, die E-Mailadresse sowie ein Passwort eingetragen werden müssen. Danach gelangt man mit einem Klick auf die Schaltfläche Melde dich bei Twitter an zum nächsten Schritt der Registrierung. Dort kann man sich einen Benutzernamen aussuchen und die Nutzungsbedingungen lesen. Sollten Probleme mit der Mailadresse oder dem Passwort auftreten, werden diese dort ebenfalls gemeldet und können behoben werden. Mit einem Klick auf den Button Mein Benutzerkonto erstellen gelangt man zu einer gut gemachten Einführung in Twitter (Bild 1.43). Dort erfährt man auch, was ein sogenannter Tweet ist: eine Kurznachricht bestehend aus maximal 140 Zeichen.

Mit einem Klick auf Weiter gelangt man zum nächsten Schritt der Einführung. Hier kann man verschiedenen Personen und Organisationen des öffentlichen Lebens, die in Twitter besonders populär sind, folgen. Twitter empfiehlt hier, mindestens fünf Personen/Organisationen zu folgen, jedoch hat man auch die Möglichkeit, mit einem Klick auf Überspringe diesen Schritt niemandem oder weniger als dem Quintett zu folgen.

BILD 1.42 Die Startseite von Twitter

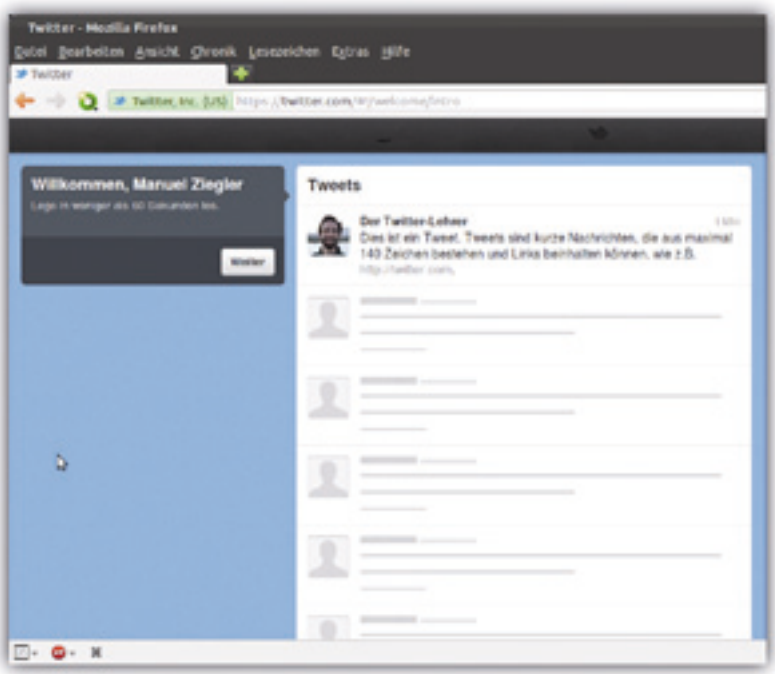

BILD 1.43 Registrierung bei Twitter

Mit einem Klick auf WEITER gelangt man zum nächsten Schritt, in dem man die unterschiedlichen Kategorien nach den Personen und Organisationen durchsuchen kann, denen man folgen möchte. Auch hier empfiehlt Twitter wieder, fünf Personen beziehungsweise Organisationen auszuwählen, aber auch dieser Schritt kann übersprungen werden. Im Anschluss daran geht es darum, Personen zu finden, die man tatsächlich kennt. Hier kommt wieder einmal ein „Freundefinder“ zur Anwendung, der aber keinesfalls empfehlenswert ist, weshalb hier auf den Link ÜBERSPRINGE DIESEN SCHRITT geklickt werden sollte. Anschließend befindet man sich auf seiner persönlichen Startseite.

Nun muss noch die E-Mailadresse bestätigt werden, um das Konto endgültig freizuschalten. Dazu klickt man in der von Twitter erhaltenen E-Mail auf den entsprechenden Bestätigungslink.

Die Benutzeroberfläche

Die Benutzeroberfläche von Twitter (Bild 1.44) ist einfach und übersichtlich. Im Kopf der Seite befindet sich eine Navigationsleiste. Darunter ist die Seite zweigeteilt: In der schmalen linken Spalte wird dem Benutzer eine kurze Profilstatistik gezeigt, die ihm die Anzahl der eigenen Tweets, die Anzahl der Personen, denen man folgt (Following) sowie die Personen, die einem selbst folgen (Follower), offenbart. Darunter werden Vorschläge angezeigt, wem man folgen könnte, sowie Trends, die weltweit große Beachtung finden.

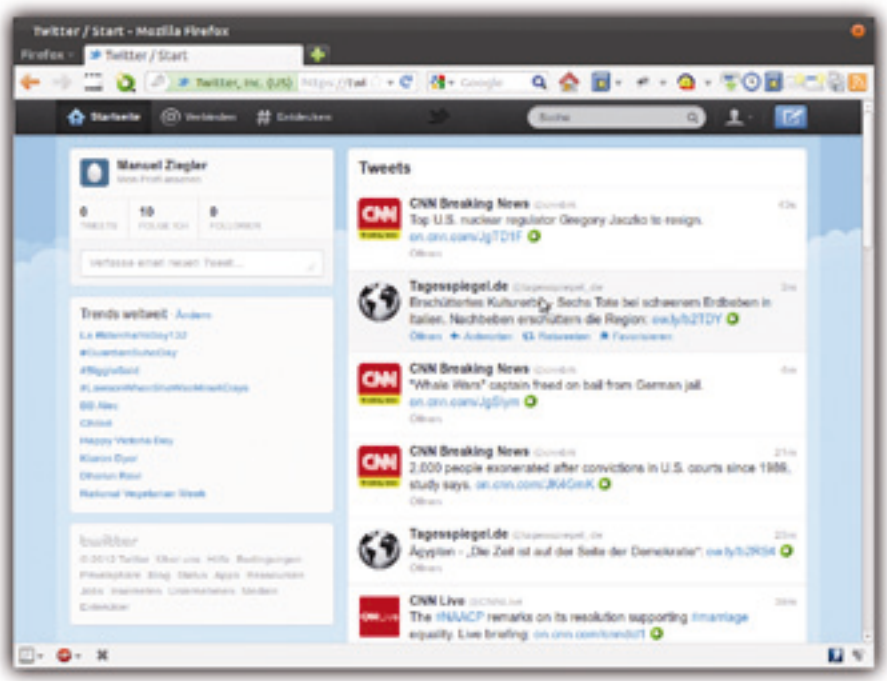

BILD 1.44 Die Benutzeroberfläche von Twitter

In der breiteren rechten Spalte werden die einzelnen Tweets, also die einzelnen Kurznachrichten chronologisch angeordnet präsentiert. Angezeigt werden die Tweets von allen Personen, denen man selbst folgt. Auch wenn das Profil in Twitter eine untergeordnete Rolle spielt, kann man es betrachten und bearbeiten. Dazu klickt man auf seinen eigenen Namen in der linken oberen Ecke der Seite.

Die Navigation im Kopfbereich der Seite bietet dem Benutzer im Grunde die folgenden sechs Elemente:

- Die Startseite wurde gerade mit der Benutzeroberfläche beschrieben.
- Unter dem Punkt @Verbinde findet man die Interaktionen der eigenen Person mit anderen Benutzern. hier wird beispielsweise angezeigt, wer einem folgt, oder in der Unterkategorie Erwähnungen auch, von wem man in einem Tweet erwähnt wurde.
- Der Punkt #Entdecke bietet dem Benutzer eine schnelle Übersicht über aktuelle Themen, die möglicherweise von Interesse für ihn sind.
- In der Suchleiste kann man nach Bekannten suchen.
- Daneben befinden sich die Profil-Einstellungen; außerdem hat man dort die Möglichkeit, sich abzumelden.
- Mit der Schaltfläche ganz rechts wird ein neuer Tweet verfasst.

Twitter hat sich in den letzten Monaten allerdings etwas gewandelt und sich in Richtung benutzerprofilbasiertes Netzwerk verändert. Zwar stehen noch immer die Tweets im Vordergrund, aber im Vergleich zu früher spielt das Benutzerprofil eine zunehmende Rolle. Auch hinsichtlich der Benutzerdaten hat Twitter sein Verhalten etwas angepasst, und so werden seit kurzem auch die Daten der Twitter-Benutzer gesammelt und ausgewertet.

2 Spionage durch andere Benutzer

Soziale Netzwerke bringen viele Vorteile, aber teilweise auch ernsthafte Gefahren mit sich. Deren Ursache sind meist unzureichender Datenschutz oder auch Datenmissbrauch. Beginnend mit der offensichtlichsten Gefahr sozialer Netzwerke – der Spionage durch andere Benutzer –, sollen die folgenden Abschnitte einen Überblick über die möglichen Risiken geben und Lösungsmöglichkeiten zeigen.

Spionage durch andere Benutzer ist in den sozialen Netzwerken das wohl bedenklichste Problem. Jeder möchte schließlich seine Privatsphäre bewahren und nicht vor jedermann seine ganzen Lebensumständen und seinen persönlichen Schwierigkeiten ausbreiten. In sozialen Netzwerken wird die Reichweite einer Information jedoch oft unterschätzt. Eine Nachricht, die eigentlich nur für wenige Personen gedacht war, kann Zigtausende von Mitgliedern erreichen, ohne dass man als Autor dieser Information einen Fehler im Versand gemacht hat. Schuld daran sind meist unübersichtliche Benutzeroberflächen sowie unzureichende Hinweise über den Datenschutz seitens der Betreiber.

Allerdings ergeben sich manche Probleme auch erst durch das Fehlverhalten von Benutzern. Diese können im Eifer des Gefechts manchmal nicht unterscheiden, welche Informationen in soziale Netzwerke gehören und welche Informationen dort besser nicht publiziert werden sollten. Manchmal wird man auch von der Illusion, man könne schließlich alles wieder löschen, dazu verleitet, brisante Informationen zu teilen. Hat man dann das Geteilte zurückgenommen, wird schnell klar, dass man seine Rechnung ohne das Internet gemacht hat. Denn hat ein Beitrag einmal einen bestimmten Bekanntheitsgrad erreicht, ist es unmöglich, ihn wieder spurlos zu entfernen. Dieser Bekanntheitsgrad ist schon erreicht, wenn eine große Suchmaschine wie Google oder Bing einen Beitrag „liest“, das heißt, den Inhalt in ihren Index aufnimmt. Dann kann der Beitrag selbst zwar beliebig oft gelöscht werden. Gibt man danach aber die richtigen Suchbegriffe in eine Suchmaschine ein, erscheinen immer wieder Auszüge beziehungsweise der gesamte Text des Beitrags als Suchergebnis.

Natürlich kann man sagen, dass man doch nichts zu verbergen hat, warum sollte man also Maßnahmen ergreifen, um die persönlichen Daten zu schützen. Das klingt generell zwar plausibel, allerdings sollte man sich die Frage stellen, ob man wirklich nichts zu verbergen hat – das wichtigste Gut ist doch die Privatsphäre, die unter allen Umständen

vor neugierigen Privatleuten und Firmen, die es nicht immer gut mit einem meinen, und dem Staat geschützt werden muss. Um die Dringlichkeit dieser Annahme zu demonstrieren, werden im Folgenden drei Fälle geschildert, bei denen der mangelnde Datenschutz sicherlich selbst von den Harmlosesten und Selbstgerechtesten als störend empfunden wird.

2.1 Kompromittierende Fotos

2.1.1 Verbreitung

Es wird zwar selten passieren, dass man auf der Straße erkannt wird, weil in einem sozialen Netz Bilder von einem selbst veröffentlicht sind. Passiert es aber trotzdem, kann das unter Umständen einen tiefen Eingriff in das Privatleben darstellen. Man stelle sich folgendes Szenario vor:

> *Tom geht an einem Freitagabend zu einem Fest im Nachbarort. Er hat zusammen mit seinen Freunden reichlich Spaß, blickt jedoch etwas zu tief ins Glas. Als Tom am nächsten Mittag erwacht, hat er das komische Gefühl, dass auf der Festivität des vorherigen Tages etwas schiefgelaufen ist. Als er dann seinen Computer hochfährt, den Webbrowser startet und sich im sozialen Netzwerk seiner Wahl einloggt, hat er die Bestätigung für sein schlechtes Gefühl: Ein Bild, auf dem er verlinkt ist, kursiert in diesem Netzwerk und erhält reichlich Resonanz bei den Benutzern. Tom überschlägt kurz und geht davon aus, dass dieses Bild bereits nahezu 1000 Mitglieder erreicht hat. Dabei zeigt ihn das Bild nackt auf der Tanzfläche stehend bei einer obszöne Geste in Richtung Kamera. Sofort löscht Tom die Verlinkung auf sich selbst, doch das Bild kann er nicht löschen.*
>
> *Es kommt wie es kommen musste: Als Tom in der folgenden Woche zu einem Vorstellungsgespräch eingeladen wird, erkennt ihn der Leiter der Personalabteilung, der das kursierende Bild von Tom einen Tag zuvor gesehen hat, wieder.*

Wie konnte es dazu kommen, schließlich hat Tom doch richtig gehandelt und die Verlinkung seiner Person auf diesem Bild umgehend entfernt? Nehmen wir an, die Verlinkung wurde rechtzeitig entfernt, der Abteilungsleiter stieß also zufällig auf das Bild und wurde nicht durch einen Hinweis in Toms Profil förmlich darauf aufmerksam gemacht. Zu diesem Zufall kam es, weil das Foto von einem von Toms Freunden veröffentlicht wurde, der ihm nur einen kleinen Streich spielen wollte, jedoch niemals auch nur im Entferntesten daran dachte, ihm zu schaden. Allerdings unterschätzte er die Reichweite einer Information in sozialen Netzwerken. Nachdem das Bild bei einigen Bekannten gut angekommen war und diese das Bild kommentiert oder wiederum mit ihren Freunden geteilt hatten, war eine Lawine losgetreten, die nicht mehr aufzuhalten war.

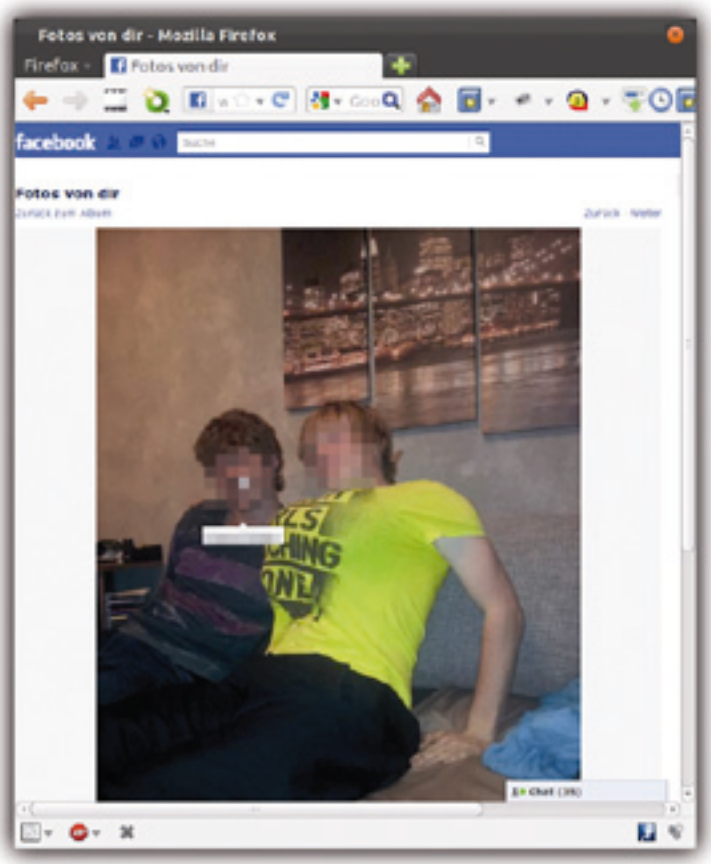

BILD 2.1 Markierungen auf Bildern: Keine Seltenheit in sozialen Netzwerken (hier: Markierung eines Benutzers in Facebook)

Nachdem die ersten zehn Freunde das Bild geteilt hatten, erreichte das Bild insgesamt bereits tausend verschiedene Personen. Würde nur ein lächerliches Zehntel von ihnen dem Bild überhaupt Beachtung schenken und von diesen nur etwa ein Fünftel das Bild weiterverbreiten, würde das Bild anschließend zirka zweitausend zusätzliche Personen erreichen. Mit dem nächsten Schritt würden grob überschlagen etwa viertausend Leute hinzukommen und beim übernächsten Schritt würde ihre Anzahl bereits um achttausend steigen. Das heißt, das Bild würde nach nur vier Schritten bereits ungefähr fünfzehntausend Empfänger erreichen – genug, um Tom bei jedem einzelnen Bewohner einer Kleinstadt bekanntzumachen und das innerhalb nur weniger Stunden bis Tage.

Zugegeben, diese Gefahr ist nur sehr schwer einzudämmen und das Bild wäre im geschilderten Fall wohl trotzdem an einige Tausend Benutzer gegangen. Aber mit geeigneten Maßnahmen kann meist Schlimmeres verhindert werden, auch wenn zuweilen nur noch Schadensbegrenzung möglich ist.

2.1.2 Wiedererkennung

In deutlich kleinerem Maßstab, aber auf ähnliche Art und Weise, bewegt sich die Wiedererkennung auf Fotos. Hier muss der Betrachter die auf dem Foto abgebildete Person bereits kennen, wenn sie beispielsweise nicht direkt in die Kamera blickt und daher eine Wiedererkennung im Grunde nicht möglich ist. Allerdings kann die Wiedererkennung auf Bildern mindestens ebenso peinlich enden wie die Wiedererkennung aufgrund von Bildern. So könnte im oben geschildertem Fall beispielsweise zwei Tage später in Toms Heimatort etwas wie „Habt ihr schon gehört? Tom war am Freitag so betrunken, dass er sich auf der Tanzfläche ausgezogen hat.“ oder Schlimmeres die Runde machen. Zwar ist es in diesem Fall notwendig, Tom bereits zu kennen, bevor man das Bild von ihm gesehen hat, allerdings ist ein Missgeschick doch viel peinlicher, wenn alle Freunde es kennen, als wenn „nur“ irgendwelche Fremde davon wissen. Die Wiedererkennung auf Bildern kann auf alle Fälle stark erschwert werden, ganz unterbinden kann man jedoch auch sie nicht. Aber schließlich kann man auch in der Realität nicht verhindern, dass man Thema des Dorftratsches ist, nachdem man etwas Aufsehenerregendes getan hat.

Was man jedoch unterbinden kann, ist die Erkennung auf Bildern, die man selbst veröffentlicht hat. Hier hat man die Veröffentlichung der Bilder selbst in der Hand und kann durchaus selbst entscheiden, ob es sinnvoll ist, ein Bild zu veröffentlichen oder ob man sich mit der Veröffentlichung schadet.

Bilder von sich selbst

Möchte man nicht wiedererkannt werden, muss man auf das Veröffentlichen von Fotos der eigenen Person verzichten. Allerdings ist das leichter gesagt als getan, eventuell ist es ja sogar gewünscht, dass man von Freunden und Bekannten identifiziert wird. Vielleicht möchte man sich mit Bildern von sich selbst auch darstellen und seine eigene Schönheit hervorheben. Unter solchen Umständen ist es denkbar schwierig, auf Bilder zu verzichten.

Hat man bereits Bilder von sich selbst veröffentlicht, wird es ein Problem, sie wieder zu löschen. Sie werden zwar recht einfach aus dem eigenen Profil entfernt, es ist allerdings unmöglich, die Bilder vollständig aus dem Internet zu entfernen, wenn sie bereits relativ populär sind. So kann es passieren, dass andere diese Bilder bereits kopiert und selbst veröffentlicht haben oder dass die Bilder in Suchmaschinen als sogenanntes Thumbnail[1] zwischengespeichert wurden und weiterhin in den Suchergebnissen erscheinen.

Dagegen kann man im Grunde nichts unternehmen außer die für die Weiterverbreitung verantwortlichen Personen zu bitten, dies zu unterlassen und im Zweifelsfall rechtlich gegen sie vorzugehen (siehe dazu weiter unten). Daher sollte man sich bereits beim Veröffentlichen eines Bilds ganz genau überlegen, ob man das wirklich will oder ob man diese Veröffentlichung später vielleicht bereuen könnte.

[1] Thumbnails sind Vorschaubilder, meist Verkleinerungen des Originals in einer niedrigeren Auflösung.

Es spricht nichts dagegen, Fotos von sich selbst zu veröffentlichen, wenn man sich nicht daran stört, dass andere dem Namen auch ein Gesicht zuordnen können. Allerdings integrieren die größeren sozialen Netzwerke wie Facebook und Google+ in letzter Zeit zunehmend Gesichtserkennungsprogramme und unterbreiten Vorschläge darüber, wer sich auf dem Bild befinden könnte. Die von Facebook und Google+ angewandte Gesichtserkennung basiert darauf, dass bestimmte Muster eines Benutzergesichts in Datenbanken gespeichert werden. Erkennen nun Facebook oder Google+ ein Gesicht, werden dessen charakteristische Muster mit den Datenbankeinträgen verglichen. Stimmen die Merkmale zu einem bestimmten Prozentsatz mit den gespeicherten Merkmalen eines Benutzers überein, kann die Gesichtserkennungssoftware die Person identifizieren, zumindest mit einer Wahrscheinlichkeit in Höhe des entsprechenden Prozentsatzes.

Die anderen Mitglieder können ein Gesicht identifizieren, wenn der Betroffene die Sicherheitseinstellungen in seinem Profil nachlässig konfiguriert hat. Möchte man nicht erkannt werden, muss man, wenn man einmal ein Bild von sich selbst als Profilbild oder als einfaches Bild veröffentlicht hat, darauf achten, seine Einstellungen zu pflegen. Auch sollte man des öfteren die Geschäfts- beziehungsweise Nutzungsbedingungen des Dienstes durchsehen und bei Änderungen (was des Öfteren vorkommt) rechtzeitig reagieren, um gegebenenfalls einem erleichterten Datensammeln vorzubeugen.

Geschäftsbedingungen

Die Geschäftsbedingungen der Dienste findet man entweder im Impressum oder oft auch unter den Begriffen „Nutzungsbedingungen“ oder „Datenschutz“, auf die ganz unten auf der Eintrittsseite der Webpräsenz verlinkt wird. Auch wenn es sich meist um recht viel Text handelt, sollte er aufmerksam gelesen werden.

Neben den Bildern, die man selbst veröffentlicht hat, gibt es natürlich auch solche, auf denen man abgebildet ist, die aber von anderen veröffentlicht wurden. Auch wenn einem das nicht gefällt: Es gibt es keine Möglichkeit, diese Bilder selbst zu löschen. Man kann nur hoffen, dass man rechtzeitig davon erfährt, dass solche Bilder hochgeladen werden sollen, um noch im Vorfeld zu versuchen, dies zu verhindern.

Man muss nämlich wissen, dass es nach deutschem Recht verboten ist, Bilder von einer Privatperson ohne deren Erlaubnis irgendwo zu veröffentlichen; man spricht hier vom sogenannten Recht am eigenen Bild.[2] Weiß man, dass jemand ein Foto veröffentlichen will, kann man dies rechtzeitig verbieten, notfalls muss das Verbot mit rechtsanwaltlicher und gerichtlicher Hilfe durchgesetzt werden. Man kann jedoch nicht jede Aufnahme und damit Publikation verhindern. Entscheidend ist, was beziehungsweise wer

[2] Für Persönlichkeiten, die im Rampenlicht stehen, gilt dieses Recht natürlich genauso, allerdings wird ihnen vor Gericht etwas weniger Privatsphäre zugestanden als Normalbürgern. Trotzdem mussten manche Verlage Prominenten bereits Schadensersatz für widerrechtlich veröffentlichte Fotos bezahlen.

fotografiert wird beziehungsweise wurde. Wird man explizit als Person allein oder in einer klar definierten Gruppe aufgenommen, muss man gefragt werden beziehungsweise kann man die Aufnahme verbieten, wenn man damit nicht einverstanden ist. Ist man Teil einer Menschenmenge, kann man die Aufnahme nicht verbieten. Ist man eine Person des öffentlichen Lebens – beispielsweise ein Musiker oder Schauspieler bei einem Auftritt auf der Bühne – kann man das Fotografieren ebenfalls nicht verbieten. Wer in solchen Fällen das Fotografieren komplett verbieten kann, ist der Veranstalter.

Was man jedoch meistens verhindern kann, ist die Markierung der eigenen Person auf Bildern.

Markierung

In vielen sozialen Netzwerken können die Benutzer ihre Freunde auf Fotos markieren. Es wird dann ein Rahmen um den Kopf der Person gezogen, zudem erscheint ihr Name, siehe Bild 2.2.

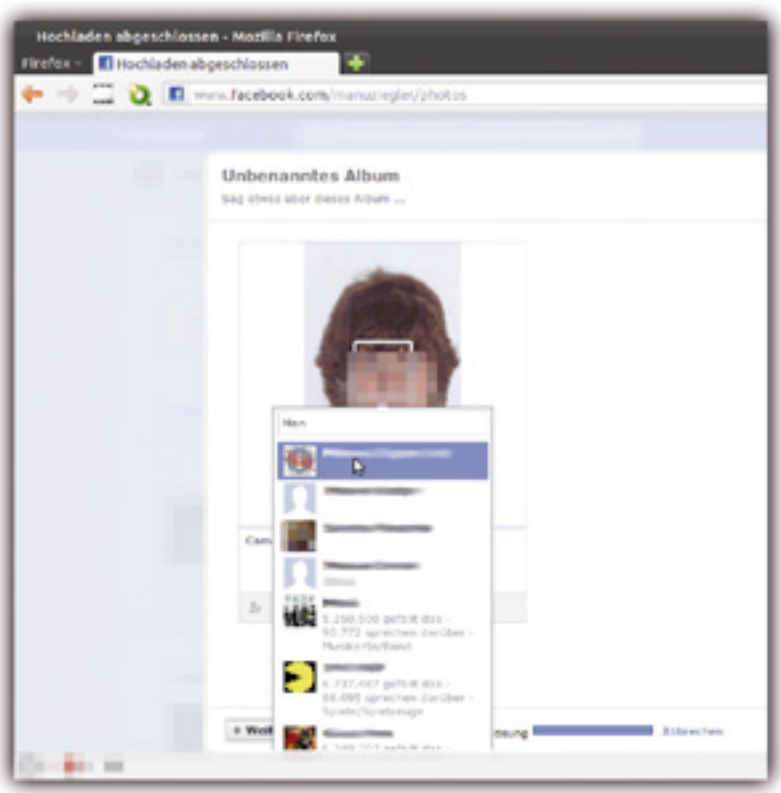

BILD 2.2 Hier schlägt Facebook vor, dass es sich bei der Person auf dem Foto um das Mitglied X handelt

Große soziale Netzwerke koppeln die Markierung mit der Gesichtserkennungsfunktion, die – das Einverständnis des Markierten vorausgesetzt – dem Urheber eines Fotos die Namen von den auf dem Bild Abgebildeten vorschlägt.

Wenn man von seinen Freunden und Bekannten nicht auf jedem beliebigen Bild markiert werden möchte, ist es notwendig und auf jeden Fall empfehlenswert, diese Funktion zu unterbinden beziehungsweise einzustellen, dass eine Verlinkung des eigenen Profils mit dem Bild vor der Anzeige bestätigt werden muss. Es sei jedoch angemerkt, dass man trotz eines Verbots markiert werden kann, man wird dann lediglich nicht mit dem Bild verlinkt.

Nachfolgend wird für die einzelnen sozialen Netzwerke dargestellt, wie in den Einstellungen eine Markierung unterbunden wird.

Facebook

Um zu verhindern, dass man von anderen auf Fotos verlinkt wird, geht man zu den Privatsphäre-Einstellungen des Benutzerkontos. Dort klickt man unter dem Punkt Profil und Markieren auf Einstellungen bearbeiten (Bild 2.3).

BILD 2.3 Diese Einstellungen sind zu empfehlen

Im sich öffnenden Fenster kann man nun vier Einstellungen für Markierungen vornehmen:

- Der Punkt Wer kann Beiträge sehen, die auf deinem Profil angezeigt werden, weil du darin markiert bist? betrifft alle Beiträge, in denen man als Benutzer

markiert wurde. Hier kann man einstellen, für welche Empfänger diese Beiträge direkt im eigenen Profil sichtbar sind. Sinnvoll ist es, hier *Freunde* oder eine noch niedrigere Stufe zu wählen.

- Der Punkt Beiträge in denen Freunde dich markieren, prüfen, bevor sie auf deiner Chronik erscheinen bietet die Option, eine Markierung erst bestätigen zu müssen, bevor sie im eigenen Benutzerprofil erscheint. Sie sollte aktiviert werden, um den Überblick zu behalten und um selbst zu entscheiden, welche Markierung auf dem eigenen Profil erscheinen soll und welche nicht.
- Mit dem Punkt Markierungen, die Freunde zu deinen eigenen Beiträgen auf Facebook hinzufügen, prüfen können vor der Veröffentlichung Markierungen, die in eigenen Beiträgen vorgenommen werden, überprüft werden. Diese Funktion ist im Grunde überflüssig, da jeder selbst mit der Prüfung der Markierung seiner eigenen Person dafür verantwortlich ist, ob eine Markierung in seinem Profil erscheint oder nicht. Nutzt man diese Funktion, spielt man Facebook gegebenenfalls die Karten zu und gibt ungewollt zusätzliche Daten über sich und seine Freunde preis.
- Der Punkt Wer kann Markierungsvorschläge sehen, wenn Fotos hochgeladen werden, die dir ähneln ist der wohl wichtigste, wenn man verhindern möchte, dass man von anderen Personen auf Fotos markiert wird. Hier sollte auf jeden Fall der Punkt Niemand ausgewählt werden.

Google+

Unter Google+ heißt das Verlinken auf Fotos Taggen. Unter den Einstellungen (Adresse: https://www.google.com/settings/plus) geht es um das Feintuning der sogenannten Tags auf Fotos. Dazu scrollt man bis zum Punkt Fotos und entfernt das Häkchen am Punkt Mein Gesicht automatisch auf Fotos finden und meinen Kontakten anbieten, mich zu taggen. Außerdem sollte man alle Personen und Kreise des Punkts Für diese Personen sollen Foto-Tags für meinen Namen automatisch als Links zu meinem Profil zugelassen werden: entfernen, um Tags, die ohne die automatische Gesichtserkennung von Google vorgenommen wurden, zumindest so weit wie möglich zu unterdrücken.

meinVZ

Unter meinVZ kann man das Verlinken der eigenen Person auf Fotos im Gegensatz zu Facebook und Google+ vollständig unterbinden. Dazu besucht man die Seite http://www.meinvz.net/Privacy/Settings und scrollt bis zum Punkt Wer darf mich auf Fotos verlinken?. Anschließend wählt man hier den Punkt Niemand aus oder alternativ Meine Freunde, wenn ich zugestimmt habe. Hier muss eine Verlinkung erst bestätigt werden, bevor sie auch tatsächlich angezeigt wird.

Anschließend kann man von niemandem mehr beziehungsweise nur nach ausdrücklicher Bestätigung auf Bildern markiert werden.

2.2 Informations-Overkill

Es ist eine Binsenweisheit, dass Mitglieder sozialer Netzwerke dazu neigen, viel zu viel über sich selbst zu erzählen, und sei es auch nur unbewusst.

Um die Problematik zu verdeutlichen, soll zunächst wieder ein Beispiel vorgestellt werden. Im Folgenden sind Freunde allerdings nicht unbedingt Freunde im üblichen Sprachgebrauch, sondern es kann sich dabei auch um Bekannte oder sogar Fremde handeln, mit denen man in sozialen Netzwerken befreundet ist beziehungsweise die sowohl das Profil als auch eine Vielzahl von Beiträgen einsehen können:

Tom ist inzwischen etwas älter geworden und über die Sache mit dem Bild ist längst Gras gewachsen. Als Tom eines Tages auf einer Party im eigenen Heimatort ist, trifft er ein schönes Mädchen. Er unterhält sich die ganze Nacht mit ihr und verabredet sich mit ihr am nächsten Tag zum gemeinsamen Abendessen. Zufrieden mit sich selbst und guter Dinge erwacht Tom am nächsten Tag, startet wie immer seinen Computer und sieht nach, was es in den sozialen Netzwerken seiner Wahl Neues gibt. Wie immer tauscht Tom dort auch mit seinen Freunden zahlreiche Informationen aus, aber seine Verabredung am Abend lässt er unerwähnt. Auf die Frage, ob er am Abend zusammen mit seinen Freunden kegeln gehe, antwortet er nur ausweichend. Außerdem findet Tom das Mädchen von gestern und schickt ihr eine Freundschaftsanfrage, die sie selbstverständlich entgegennimmt. Nachdem Tom sich noch eine Weile mit dem Mädchen unterhalten hat, begibt er sich zum vereinbarten Treffpunkt und muss dort angekommen feststellen, dass einige seiner Bekannten, unter anderem auch seine Ex-Freundin, ebenfalls in besagtem Restaurant sitzen. Tom denkt sich dabei nichts weiter, bis er feststellt, dass diese ihn beobachten und heimlich Bilder von ihm und dem Mädchen aufnehmen.

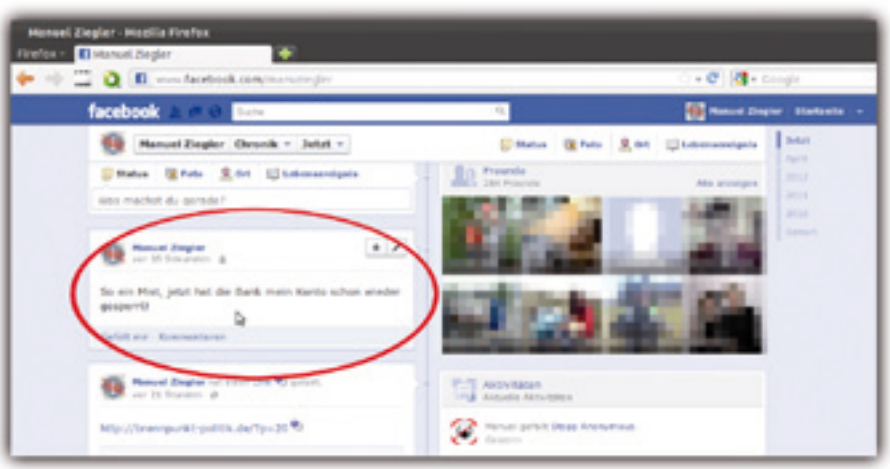

BILD 2.4 Solche Statusmeldungen gehören nicht in soziale Netzwerke

Natürlich könnte es sein, dass die Bekannten rein zufällig in dem gleichen Restaurant gesessen haben. Aber um darzustellen, welche Gefahr von sozialen Netzwerken ausgehen kann, nehmen wir einmal an, dass hier kein Zufall im Spiel war. Wir stellen uns also vor, dass die Ex-Freundin von Tom, die immer noch wütend darüber ist, dass Tom sie einst betrogen hat, sich an Tom rächen möchte. Zu diesem Zweck hat sie Tom über die von ihm genutzten sozialen Netzwerke beobachtet (neudeutsch würde man auch vom Stalken sprechen), um eine Gelegenheit zu finden, sich an ihm zu rächen.

Nun muss man wissen, dass Tom als stolzer Besitzer eines teuren Smartphones keine Gelegenheit auslässt, mobil Informationen in sozialen Netzwerken zu teilen. Auf der Party am vorherigen Abend hat er ganz selbstverständlich auch Fotos von sich und dem Mädchen geschossen, die über die sozialen Netzwerke, in denen er Mitglied ist, geteilt wurden. Als Tom dann am nächsten Tag zuhause in eben jenen sozialen Netzwerken aktiv war, konnten seine Freunde sehen, dass Tom nun mit einer gewissen Lisa, dem Mädchen, befreundet ist. Normalerweise würde man sagen, dass Tom eben jemand neues kennengelernt hat, aber wenn man bisher Toms Aktivitäten in sozialen Netzwerken beobachtet hat und Tom vielleicht sogar privat näher kennt, weiß man, dass er auf Parties recht häufig neue Freundinnen findet. Sieht man nun, dass diese Lisa und das Mädchen auf den Bildern von Tom die gleiche Person sind, kann man sich schon einiges zusammenreimen, und besonders Toms Ex-Freundin kann das, sie kennt seinen Charakter ja näher als wir.

Woher Toms Ex-Freundin wusste, wo sie Tom findet, ist in Kapitel 2.3 ab Seite 78 beschrieben. Zunächst soll betrachtet werden, aus welchen Gründen Toms Verabredung nun scheitern wird.

Weder das Teilen der Bilder, auf denen er und Lisa abgebildet sind, noch die Freundschaftsanfrage, die Tom an Lisa gesendet hat, sind schuld daran, dass Toms Ex-Freundin ihm auf die Schliche gekommen ist. Es ist vielmehr Toms grundsätzliches Verhalten in sozialen Netzwerken. Jemand, der soziale Netzwerke so regelmäßig und vielseitig nutzt wie Tom, darf im Hinblick auf die Sicherheit der eigenen Daten keine Kompromisse eingehen. Toms Fehler war, dass er im Laufe der Zeit berechenbar wurde: Er legte immer wieder das gleiche Verhalten an den Tag und verbreitete niemals widersprüchliche Informationen. Das führte dazu, dass er von jeder Person, die sich näher mit seinem Profil beziehungsweise seinen Profilen beschäftigte, leicht durchschaut werden konnte.

Dieses Verhalten ist an sich nicht negativ und bei reger Nutzung sozialer Netzwerke ist es auch nicht weiter schlimm, berechenbar zu sein, da sich gewisse Fälle dann nur selten wiederholen und ein Beobachter daraus keine eindeutigen Schlüsse ziehen kann. Doch bei der intensiven Nutzung sozialer Netzwerke muss man als Nutzer sein Verhalten anpassen, wenn man zumindest einen Teil seiner Privatsphäre wahren möchte. Natürlich ist auch der Verzicht auf eine derart intensive Nutzung, wie sie offensichtlich bei Tom der Fall ist, sinnvoll. Schließlich muss man doch nicht von jeder Party sofort Bilder veröffentlichen und vor allem muss aus den Bildern nicht sofort ersichtlich sein, wer alles mit auf der Party war beziehungsweise wen man dort kennengelernt hat. Diese Dinge haben in sozialen Netzwerken nichts zu suchen. Man spricht hier auch von Datensparsamkeit: Nur so viele Daten über sich preisgeben, wie unbedingt nötig.

2.2.1 Datensparsamkeit

Möchte man verhindern, dass andere Benutzer zu viel über die eigene Person in sozialen Netzwerken erfahren, ist eine der Lösungsmöglichkeiten der Einsatz sozialer Netzwerke in Maßen. Was auch immer soziale Netzwerke an Funktionalitäten bieten, die meisten Benutzer nutzen diese blind, ohne zu wissen, was sie damit eigentlich tun. Schon allein das Bewusstsein über die Reichweite einer Information trägt oft zu einem besonnenen Umgang mit ihnen bei. Allerdings ist dieses Bewusstsein bei den allerwenigsten Nutzern ausgeprägt.

Um einen Eindruck davon zu bekommen, welche Informationen welche Reichweite haben, soll ein kleines Beispiel betrachtet werden:

Wie weit eine Information reichen kann, wenn sie einmal öffentlich geteilt wurde, ist erschreckend. Sie kann im ganzen Netzwerk, teilweise sogar von nicht registrierten Besuchern gesehen werden und kann damit potentiell jeden Menschen auf der Erde, der einen Zugang zum Internet hat, erreichen. Wie viele Personen von öffentlichen Informationen tatsächlich erreicht werden, lässt sich schwer sagen, weil dies von der Relevanz dieser Information abhängt. Besonders populäre öffentliche Informationen erreichen insgesamt rund 10 Millionen Benutzer, je nach Netzwerk und Zielgruppe. Die meisten öffentlichen Inhalte kommen jedoch über mehrere hunderttausend bis zu wenigen Millionen Betrachter nicht hinaus.

Auch wie weit eine Information reicht, die nur für Freunde sichtbar ist, wurde bereits vorgerechnet, die Reichweite hängt hier direkt von der Anzahl der Freunde ab.

Interessant wird es bei den Zwischenformen, bei denen sowohl die eigenen Freunde als auch deren Freunde erreicht werden. Hier werden die meisten Informationen veröffentlicht, da dieser Kreis in den meisten sozialen Netzwerken die Standardeinstellung ist.

Eine Information, die für Freunde von Freunden[3] veröffentlicht wurde, kann mehrere Tausend Personen erreichen, obwohl die Bezeichnung dieser Reichweite (Freunde von Freunden) doch eigentlich ziemlich harmlos erscheint. In Kapitel 2.3 ab Seite 78 wird auf diese Option nochmals eingegangen und in Anhang A.1 befindet sich eine Faustformel für die Berechnung der Empfängerzahl.

Geht man mit sozialen Netzwerken besonnen um, zeichnet man sich dadurch aus, dass man nicht mehr Informationen preisgibt als für die sinnvolle Nutzung der sozialen Netzwerke nötig sind.

Dabei ist es wichtig zu wissen, welche Informationen in sozialen Netzwerken tabu sein sollten, welche Funktionen nicht genutzt werden sollten, um der Preisgabe bestimmter Informationen vorzubeugen, und vor allem welche Tragweite die Herausgabe einer einzigen Information haben kann. Außerdem ist darauf zu achten, dass man nicht versehentlich anderen die Möglichkeit gibt, jene Informationen zu veröffentlichen, die man selbst nicht preisgibt. Man muss jedoch immer bedenken, dass soziale Netzwerke grundsätzlich die eigene Privatsphäre angreifen und dass diese Angriffe nicht vollstän-

[3] Diese Benennung stammt aus Facebook und soll hier der Einfachheit halber für alle sozialen Netzwerke gelten.

dig abgewehrt werden können. Schließlich gilt es in sozialen Netzwerken ja Kontakte zu knüpfen, was der Privatsphäre zumindest im Internet gewissermaßen entgegensteht. Wenn man im Bezug auf soziale Netzwerke also von einer Wahrung der Privatsphäre spricht, ist das keine wirkliche Wahrung der Privatsphäre, sondern vielmehr nur Schadensbegrenzung der vorangegangenen Verletzungen der Privatsphäre.

Tabu-Informationen

Möchte man seine Privatsphäre wahren, muss man sich zunächst darüber im Klaren sein, was man eigentlich wahren möchte. Unter Privatsphäre betrachtet schließlich jeder Nutzer etwas anderes, weswegen dieser Begriff nicht endgültig definiert werden kann. Ein Finanzminister legt an seine Privatsphäre sicherlich ganz andere Maßstäbe als ein Schüler. Auch das, was Tom früher als Wahrung der Privatsphäre betrachtet hat, ist nicht der Maßstab, nach dem man sich als Nutzer sozialer Netzwerke richten sollte, Tom musste ja schließlich auch auf die harte Tour dazulernen. Außerdem kann sich die eigene Einstellung zur Privatsphäre im Lauf der Zeit wandeln; man denke beispielsweise an Filmschauspieler und andere Berühmtheiten des gesellschaftlichen Lebens, die am Anfang ihrer Laufbahn die Journalisten nur zu gerne an jedem Detail des Privatlebens teilnehmen lassen und nach einigen Jahren Fotografen verprügeln, die sich vor dem Gartenzaun herumdrücken.

Aber egal, wie man selbst seine Privatsphäre definiert, gewisse Angaben gehören auf jeden Fall dazu und daher nicht in soziale Netzwerke. Welche Informationen das sind, kann man anhand einer Faustregel ermitteln. Man muss sich bei jeder Information, um die man in sozialen Netzwerken gerade gebeten wird, immer die Frage stellen, ob man sie auch in der Realität jedem, den man nur flüchtig kennt, auf die Nase binden würde. Schließlich sind soziale Netzwerke so angelegt, dass man darin mit jedem, den man nur flüchtig kennt, befreundet ist (zumindest tendiert das Nutzerverhalten dahin).

Es gilt generell, dass auch in sozialen Netzwerken unsere gesellschaftlichen Normen und Gebräuche eingehalten werden müssen. Es kommt zwar immer wieder vor, dass manche Mitglieder darin ihr gesamtes Leben einschließlich ihres Sexualverhaltens dokumentieren – was in bestimmten Kreisen sogar positiv aufgenommen wird –, aber ein solches Verhalten ist keineswegs ratsam. Soziale Netzwerke sind keine Tagebücher, sondern müssen eher wie das eigene Äußere behandelt werden: Schließlich versucht man auch in der Öffentlichkeit möglichst gepflegt und seriös aufzutreten, anstatt seine Schwächen zu zeigen und einen schlampigen Eindruck zu hinterlassen. Genauso wenig, wie man auf der Straße zu irgendeiner Person geht, die man flüchtig kennt, und ihr erzählt, was man in seinem Leben falsch gemacht hat, sollte man das in sozialen Netzwerken machen.

In sozialen Netzwerken kommt besonders für Ausbildungsplatz- und Arbeitsplatzsuchende noch ein wichtiger Grund hinzu, sich tadellos zu benehmen: Arbeitgeber haben schon seit langem damit begonnen, ihre Bewerber mit Hilfe sozialer Netzwerke näher kennenzulernen und auch anhand des dortigen Erscheinungsbilds eine Auswahl zu treffen. Ein Bewerber, der täglich von seiner letzten Sauftour erzählt, hat auf jeden Fall

weniger Chancen für eine Einstellung als ein zurückhaltender Bewerber. Dabei kann es natürlich durchaus der Verschwiegene in Wirklichkeit ein wesentlich schlimmerer Saufbold sein als sein Konkurrent. Der Arbeitgeber wird dies aber vor dem Einstellungsgespräch nicht erfahren, denn anders als in sozialen Netzwerken ist es in der Realität wesentlich schwieriger, Informationen über andere einzuholen.

Dies haben auch längst diverse Geheimdienste und die Polizei erkannt, die soziale Netzwerke regelmäßig für ihre Recherchen nutzen. Der Bundesnachrichtendienst, der auf Verschwiegenheit angewiesen ist, hat aus gutem Grund seine internen Mitarbeiter vor einer Mitgliedschaft in Facebook und sozialen Netzwerken mit ähnlichen Konzepten gewarnt. Wer Mitglied in einem primär amerikanischen Netzwerk ist (Facebook und Google+ sind solche), muss sich außerdem dessen bewusst sein, dass seine Daten in Übersee gespeichert werden und sicherlich auch den mehr als einem Dutzend amerikanischen Geheimdiensten – der bekannteste ist die CIA – in die Hände fallen können. Finden sie keinen Gefallen an dem, was sie über jemanden lesen, kann es bei einer Einreise nach Amerika durchaus passieren, dass man auf dem Flughafen von der Einwanderungsbehörde abgewiesen wird und nicht ins Land darf.

Halten wir also fest:

Achtung!

Berichte über Dinge, Ereignisse oder Erfahrungen, die einen allgemeinen negativen Eindruck außerhalb des engen Bekanntenkreises hinterlassen könnten, haben in sozialen Netzwerken nichts verloren. Hier muss man streng mit sich selbst ins Gericht gehen und genau prüfen!

Ebenso verhält es sich mit persönlichen Daten. Noch vor wenigen Jahren gab niemand seine persönlichen Daten ohne weiteres preis. Eine in den achtziger Jahren geplante Volkszählung schlug hohe Wellen, viele Tausende Bürger demonstrierten gegen das Vorhaben, in dem – nach heutigen Maßstäben „harmlose" – Daten über beispielsweise die eigene Wohnung und Bildung abgefragt wurden.[4] Noch vor wenigen Jahren galten Firmen, die persönliche Daten sammelten, als kriminell oder wurden zumindest als unseriöse Organisationen betrachtet. In dieser Zeit verdienten Hacker ein Vermögen damit, Kontaktdaten wie E-Mailadressen und Anschriften ausfindig zu machen und einer bestimmten Person zuzuordnen. Sie konnten diese Daten dann an Werbefirmen verkaufen, die damit ihre Werbebotschaften personalisieren beziehungsweise erst einen Empfänger für sie finden konnten. Als eines Tages bekannt wurde, dass Google Nutzerdaten speichert und auswertet, um gezielt Werbung einblenden zu können, war dies ein handfester Skandal, natürlich auch, weil Google überhaupt im Besitz dieser Daten war. Man machte sich auch große Sorgen darum, dass die Daten durch ein Leck unbefugten Dritten in die Hände fallen könnten. Heute scheint es niemanden mehr zu interessieren, wer alles ohne Hürden an die eigenen Daten gelangen kann. Man muss nur einmal ein

[4] Die Volkszählung im Jahre 2011 ging da schon viel protestärmer und ungehinderter über die Bühne.

soziales Netzwerk aufrufen und sich durch die Profile einiger Benutzer klicken, um festzustellen, dass jemand, der an persönlichen Daten interessiert ist, dort alles findet, was er finden möchte.

Anfang Juni 2012 schlug der Forschungsauftrag der Schufa an das vom SAP-Gründer gestiftete Hasso-Plattner-Institut in Potsdam, wie eine „technische Verarbeitung öffentlicher Web-Daten" durchzuführen sei, hohe Wellen der Empörung. Das Institut kündigte schließlich den Auftrag mit der Begründung, dass „angesichts mancher Missverständnisse in der Öffentlichkeit über den vereinbarten Forschungsansatz und darauf aufbauender Reaktionen ein solches wissenschaftliches Projekt nicht unbelastet und mit der nötigen Ruhe durchgeführt werden könne"[5]. Hier muss genau gelesen werden: „Technische Verarbeitung" bedeutet, dass man die Benutzerdaten aus den sozialen Netzwerken nicht mehr manuell erfasst, sondern gleich automatisch auswertet.

Achtung!

Daten wie der Wohnort, die E-Mailadresse, die Anschrift oder gar die Telefonnummer dürfen in sozialen Netzwerken niemals öffentlich oder für Freunde sichtbar angegeben werden. Das gilt auch für alles Finanzielle – oder wer würde schon seine Kontoauszüge an seine Haustür heften?

Absolut tabu sind Informationen über den Arbeitgeber, das gilt sowohl für direkte als auch für indirekte. Ein schnell mal in einer Unterhaltung ausgeplaudertes „Mein Chef, der alte Geizkragen, hat mal wieder die Bilanz frisiert" taugt als Grund für eine fristlose Kündigung, wenn der alte Geizkragen Wind davon bekommt.

Vermeidbare Informationen

Neben den Daten, die man unter keinen Umständen preisgeben darf, gibt es solche, die zwar nicht weitergegeben werden sollten, deren Weitergabe aus Versehen oder anderen Gründen jedoch keine allzu unangenehmen Folgen nach sich zieht. Dazu gehört alles, was man nicht unaufgefordert in der Öffentlichkeit erzählen würde, was man jedoch auf Nachfrage durchaus auch weniger gut Bekannten oder sogar Fremden preisgibt.

Zu diesen Informationen gehört beispielsweise das Geburtsdatum. Es ist zwar gängig und im Grunde auch keine schlechte Idee, sein Geburtsdatum in sozialen Netzwerken zu veröffentlichen und damit an den eigenen Geburtstag erinnert zu werden. Allerdings ist in der Praxis die Reichweite des Geburtsdatums, auch wenn es nur für die Freunde sichtbar ist, meist zu hoch. Natürlich ist es praktisch, an den Geburtstag eines Freunds erinnert zu werden, ohne ihn in einen Kalender eintragen oder sich merken zu müssen, und selbstverständlich gratuliert man auch jemandem, von dem man weiß, dass er Geburtstag hat, aber man sollte sich doch fragen, ob die vielen Glückwünsche überhaupt von Herzen kommen. Lässt man seinen Freunden den Geburtstag anzeigen, findet man

[5] Siehe http://www.hpi.uni-potsdam.de/presse/mitteilung/beitrag/schufa-forschungsprojekt-gekuendigt.html

an diesem Tag unter Umständen mehrere hundert Glückwünsche auf seiner Pinnwand, von denen nur selten einer mehr Text als „Alles Gute“ gefolgt von einem Smiley enthält. Begegnet man den Gratulanten später am Tag in der Realität, denken diese oft gar nicht daran, dass ihr Gegenüber ja Geburtstag hat. Was hat es also für einen Sinn, das Geburtsdatum zu veröffentlichen? Das ist nur eine Information mehr, die Fremde beziehungsweise flüchtige Bekannte über die eigene Person haben.

Ähnlich verhält es sich mit der Veröffentlichung von Interessen und Hobbys. Natürlich findet man auf diese Weise einfacher Kontakte, die zu einem passen, aber im Grunde ist es ohnehin schwierig, in sozialen Netzwerken herzliche Kontakte zu anderen aufzubauen, bei denen man sich sicher sein kann, dass man nicht absichtlich getäuscht wird. Wer wirklich virtuelle Kontakte pflegen will, kann natürlich Interessen und Hobbys angeben, sollte sich jedoch im Klaren darüber sein, dass es sich bei diesen Kontakten in den meisten Fällen nur um virtuelle Bekanntschaften handeln wird. Wer auf der Suche nach echten Bekanntschaften ist, sollte einfach hinausgehen in die Welt und auf andere Menschen zugehen. Er wird dort eher fündig werden als in sozialen Netzwerken, in denen es nur allzu leicht ist, sich zu verstellen oder andere absichtlich zu täuschen.

Ebenso verhält es sich mit Informationen über Ausbildung und Schule. Wer noch zur Schule geht, hat eigentlich keinen Grund dazu, dies ungefragt weiterzugeben. Wer die Schule bereits absolviert hat und stolz auf seinen Abschluss ist, sollte sich vielleicht trotzdem überlegen, ob er dies wirklich erzählen muss. Und wer auf der Suche nach alten Schulfreunden ist, täte vielleicht besser daran, einige alte Unterlagen herauszusuchen und die Schulfreunde direkt zu kontaktieren, ohne zahlreichen Unbeteiligten Informationen über seinen Abschluss und damit indirekt auch über sein Alter zu geben.

Prinzipiell sollte jede persönliche Information genau überdacht und nur dann veröffentlicht werden, wenn man nach reiflicher Überlegung immer noch der Meinung ist, dass dies unbedingt sein muss. Außerdem ist es sinnvoll, das eigene Profil von Zeit zu Zeit als Außenstehender zu betrachten und immer wieder von neuem zu prüfen, ob diese oder jene Information dort wirklich bleiben muss oder ob sie nicht besser aus dem Profil gestrichen werden sollte.

Pseudonyme

Manchmal ist es sinnvoll, vollständig anonym zu bleiben und nur Wenigen unter dem echten Namen bekannt zu sein – zum Beispiel dann, wenn man eine regional, national oder sogar international recht bekannte Persönlichkeit ist. Dann möchte man einerseits natürlich seine Fans nicht enttäuschen, aber auch nicht mit jedem von ihnen befreundet sein und ständig von Fragen oder persönlichen Nachrichten genervt werden. In diesem Fall ist es sinnvoll, das Benutzerprofil unter einem Pseudonym anzulegen. Aber nicht nur Personen im Rampenlicht der Öffentlichkeit ist die Wahl eines Pseudonyms zu empfehlen: Auch wer aufgrund seiner Tätigkeiten in sozialen Netzwerken verfolgt wird, sollte er sich ein Pseudonym zulegen.

Mitglieder der Internet-Aktivistengruppe Anonymous beispielsweise engagieren sich unter anderem für die Aufklärung der Bevölkerung über eine als Sekte geltende Organi-

sation. Weil diese dafür bekannt ist, gegen Kritiker sowohl auf legalem als auch auf illegalem Weg aggressiv vorzugehen, treten die Aktivisten von Anonymous in der Öffentlichkeit wie auch in sozialen Netzwerken unter Pseudonymen auf.

Aber nicht nur in solchen Extremfällen sind Pseudonyme sinnvoll. Wenn die Mitglieder eines sozialen Netzwerks auf irgendeine Weise aufgelistet werden, erscheinen sie meistens unter dem eigenen Namen. Das scheint auf den ersten Blick nicht weiter schlimm zu sein, aber bereits wenn jemand den Namen einer realen Person kennt, kann er mehr über sie herausfinden – bis hin zur Ermittlung von Passwortdaten (siehe Kapitel 4).

Bei der Wahl des Pseudonyms, unter dem man im Internet auftritt, ist jedoch einiges zu beachten. Soll das gleiche Pseudonym in unterschiedlichen sozialen Netzwerken und auf unterschiedlichen Webseiten gelten, müssen einige Regeln für wirkliche Anonymität berücksichtigt werden: Hinter dem Pseudonym dürfen niemals Angaben stehen, mit denen die versteckte Person charakterisiert werden kann. Vor allem darf das Pseudonym nirgends in Verbindung mit dem realen Namen auftreten. Selbst seine Verbindung mit Angaben wie beispielsweise dem Geburtsdatum ist fragwürdig. Vor allem aber muss man sich darüber klar sein, dass eine scheinbare Streuung der Daten – also die Veröffentlichung verschiedener Daten an verschiedenen Orten – keine wirkliche Streuung ist. Steht zum Beispiel auf einer Seite das gewählte Pseudonym in Verbindung mit dem Geburtsdatum und auf einer anderen Seite in Verbindung mit Interessen und Hobbys, können diese Informationen einfach zusammengeführt werden. Der Eindruck, Fremde könnten ohnehin nicht genug über die hinter dem Pseudonym stehende Person herausfinden, ist deshalb schlichtweg falsch. Wenn Informationen so gestreut werden, ziehen findige und erfahrene Datensammler daraus sogar den Schluss, dass diese Informationen der Wahrheit entsprechen und einer konkreten Person zugeordnet werden können. Sind alle Informationen an einer Stelle veröffentlicht, sieht dies dagegen erfundener aus.

Öffentliche Konversationen

Informationen über sich selbst gibt man vor allem in Gesprächen preis. Es ist also vergebliche Liebesmüh, beim eigenen Profil darauf zu achten, keine brisanten und möglichst wenige sonstige Daten bekanntzugeben, wenn man anschließend über soziale Netzwerke öffentliche Unterhaltungen führt, aus denen mühelos Informationen über die eigene Person herauszulesen sind.

Betrachten wir beispielhaft eine typische Unterhaltung zwischen zwei Gesprächspartnern, aus der eine Menge Informationen gewonnen werden kann:

Tom: „Wo ist mein Schlüssel“ – so lustig!

Lisa: Das kann doch jedem mal passieren, außerdem war ich gar nicht betrunken.

Tom: Nein ... du hast nur den Schlüssel in deiner Tasche nicht gefunden!

Lisa: Ja und? Meine Oma findet Ihre Brille auch öfter nicht, das liegt bei uns in der Familie.

Tom: Jaja, heute Abend wiederholen wir das ... Das wird der Hammer! ;-)

Aus dieser Unterhaltung kann man einiges herauslesen: So wird zum Beispiel klar, dass Tom und Lisa in naher Vergangenheit, wahrscheinlich am Vortag, zusammen getrunken haben und Lisa dann ihren Schlüssel, wahrscheinlich den zu ihrer Wohnung, nicht fand, als Tom sie nach Hause brachte, obwohl er in ihrer Tasche war. Außerdem erfährt man, dass Lisa und Tom an diesem Abend wohl wieder gemeinsam etwas trinken gehen werden.

Sicherlich ist es Tom und Lisa nicht recht, dass man derart viel aus ihrer Unterhaltung herauslesen kann, aber sie führen sie trotzdem. Dabei müssten sie doch wissen, dass selbst jemand, der die beiden nicht näher kennt, die wesentlichen Punkte dieser Unterhaltung zu einem relativ vollständigen Gesamtbild zusammensetzen kann. Aber vermutlich ist das beiden nicht klar, sonst würden sie das Gespräch so nicht führen.

Problematisch bei solchen Unterhaltungen ist schon die Motivation, warum sie überhaupt begonnen werden. Da man davon ausgehen kann, dass Tom Lisa nicht lächerlich machen möchte, ist anzunehmen, dass der Grund der Unterhaltung einfach nur das Verlangen nach der Aufmerksamkeit Dritter ist. Tom möchte dem Leser dieser Unterhaltung sagen: „Sieh her, ich hatte gestern einen schönen Abend zusammen mit Lisa“. Würde Tom sich selbst seine Beweggründe klarmachen, würde er vermutlich diese Unterhaltung gar nicht beginnen – zumindest nicht öffentlich. Aber da Tom von dem Bedürfnis erfüllt ist, der Welt mitzuteilen, dass er und Lisa eine Beziehung miteinander haben, und vielleicht auch, dass Lisa ihm „gehört“, ist es ihm in dieser Situation praktisch unmöglich, objektiv zu urteilen. Das ist gewissermaßen verständlich, schließlich hat jeder ab und zu eine Phase, in der er die Welt nur durch seine Augen sieht. Dennoch ist ein derartiges Mitteilungsbedürfnis schädlich. Man muss sich bereits im Vorfeld überlegen, was sinnvolle Themen für öffentliche Unterhaltungen sind und welche Themen zu Szenarien wie dem oben geschilderten führen.

Prinzipiell gilt, dass Themen, die der Darstellung eines vergangenen Ereignisses dienen, meist aus einem spontanen Mitteilungsbedürfnis heraus entstehen und oft zu einer später vielleicht ungewollten Preisgabe von Informationen führen. Der beste Rat für eine öffentliche Konversation ist die Bedachtsamkeit: Stets überlegt handeln, sich den Grund für die Unterhaltung genau überlegen (dabei auch das Unterbewusstsein erforschen), in die Zukunft und an die möglichen Auswirkungen denken und aus Geltungsbewusstsein nicht voreilig Unterhaltungen beginnen, die man später bereut. Auch wenn es schwierig sein kann, sich an diese Vorsätze zu halten, ist es in letzter Konsequenz einfacher, als sich im Ernstfall damit herumzuschlagen, bestimmte Informationen wieder aus den Köpfen seiner Freunde zu entfernen.

2.2.2 Privatsphäre-Einstellungen

Möchte man keine so einschneidenden Abstriche wie in Abschnitt 2.2 bisher beschrieben machen, aber dennoch nicht jedermann Zugang zu seinen persönlichen Informationen gewähren, sollte man sich mit den sogenannten Privatsphäre-Einstellungen in sozialen Netzwerken vertraut machen. Diese Einstellungen sollte man sorgfältig vorneh-

men, unabhängig davon, ob man sich an die in Kapitel 2.2 erwähnten Hinweise hält oder nicht, da in sozialen Netzwerken die Veröffentlichung bestimmter Daten nicht vermieden werden kann. Im Grunde kann man in den Privatsphäre-Einstellungen der großen Netzwerke ganz genau festlegen, wer einen Beitrag oder eine Information lesen darf und wer nicht. Die präzise Einstellung der Reichweite eines Beitrags erfordert allerdings enorm viel Zeit und liefert zudem dem Betreiber zahlreiche Informationen über die eigenen Kontakte (siehe dazu auch Kapitel 3). Aus diesem Grund ist meist ein Mittelweg zwischen Aufwand und Kontrolle über die Reichweite am besten und es gilt stets, dass ein Beitrag besser in einem sehr kleinen als in einem zu großen Rahmen veröffentlicht werden sollte.

Privatsphäre-Einstellungen geben dem Benutzer die grundsätzliche Möglichkeit, zu entscheiden, welche Schichten[6], die sich um den Benutzer herum bilden, von einem Beitrag erreicht werden sollen. Grundsätzlich wird dabei die Möglichkeit geboten, zu entscheiden, ob eine Information nur von einem selbst, nur von den Freunden, von den Freunden und deren Freunden oder von der Öffentlichkeit gesehen werden darf. Zusätzlich kann eine Information auch vor bestimmten Benutzern verborgen sowie nur für bestimmte sichtbar gemacht werden. Weil die genaue Umsetzung dieser Datenkapselung vom jeweiligen sozialen Netzwerk abhängt, soll hier vor allem ein allgemeines Modell zur Datenkapselung erarbeitet werden.

Was Fremde wissen dürfen

Die Entscheidung, was Fremde über die eigene Person wissen dürfen, muss zwar individuell beantwortet werden, generell gilt allerdings, dass Fremde so wenige Informationen wie nur möglich erlangen können sollten. Natürlich gibt es auch Ausnahmen von dieser Regel, indem Themen, auf die man einen möglichst großen Benutzerkreis aufmerksam machen möchte, durchaus öffentlich (oder im Bereich Sichtbar für Freunde von Freunden) geteilt werden dürfen. Ansonsten sollte gelten, dass Fremde im Grunde keine Informationen über die Person hinter dem Benutzerkonto erlangen können sollten.

Das beliebte Argument, dass man von möglichen Freunden gar nicht gefunden werden kann, wenn diese keine Informationen sehen können, solange sie nicht mit einem befreundet sind, ist nicht von der Hand zu weisen. Es gibt allerdings auch andere Möglichkeiten, mit einer Person in Kontakt zu treten. Wenn ein Freund tatsächlich mit mir (in sozialen Netzwerken) befreundet sein möchte, kann er mich jederzeit kontaktieren und nach meinem Benutzernamen und so weiter fragen.

Möchte man dennoch von anderen Personen gefunden werden, empfiehlt es sich, ein geeignetes Profilfoto zu wählen, auf dem Fremde unter Umständen nicht unbedingt sofort das Aussehen der dahinterstehenden Person ablesen können, bei dem Freunde jedoch wissen, um wen es sich handelt. Denkbar wäre in diesem Zusammenhang beispielsweise ein Foto, auf dem mehrere Personen abgebildet sind. Freunde können dann

[6] Siehe Anhang A.2: Schichten um einen Benutzer

anhand des Namens die gesuchte Person identifizieren, während Fremde keine Anhaltspunkte haben, wer auf dem Foto wer ist.

Was Freunde wissen dürfen

Üblicherweise würde man sagen, dass Freunde doch eigentlich alles über die eigene Person wissen dürfen. Allerdings muss man stets bedenken, dass der Freundeskreis in sozialen Netzwerken meist wesentlich weiter gefasst ist als im realen Leben des durchschnittlichen Bürgers. Während man als Durchschnittsmensch normalerweise kaum mehr als zehn bis zwanzig Freunde hat, denen man alles erzählen würde (in der Realität hat man eigentlich nur einen oder zwei solche engen Freunde), ist man in sozialen Netzwerken im Durchschnitt mit hundert bis zweihundert Personen befreundet. Das entspricht eher einem Bekannten- als dem Freundeskreis, und mit diesem möchte man wahrscheinlich auch nicht alle seine Sorgen und Probleme teilen.

Aus diesem Grund muss man genau überlegen, was man mit seinen Freunden teilen möchte und was nicht. Prinzipiell gilt, dass Freunde zwar einiges über die eigene Person erfahren dürfen, bestimmte Informationen jedoch nicht mit ihnen geteilt werden sollten. Es ist in Ordnung, wenn die Freunde über Hobbys und Interessen des Benutzers Bescheid wissen. Wenn sie jedoch auch über seine Sorgen und Probleme informiert sind, ist dieser wohl einen entscheidenden Schritt zu weit gegangen und hat zu viele Informationen ausgebreitet.

Was niemanden etwas angeht

Was in sozialen Netzwerken niemanden etwas angeht, sind vor allem die eigenen Schwierigkeiten, Nöte und Sorgen. Wenn man diese veröffentlicht oder auch an seine Freunde weitergibt, gibt man zu viele persönliche Informationen preis. Neben den persönlichen Problemen gibt es jedoch auch andere Dinge, die in sozialen Netzwerken nichts zu suchen haben: An erster Stelle steht dabei der Beziehungsstatus. Es geht nicht jeden etwas an (auch nicht alle Bekannten), ob man nun Single ist oder ob man sich in einer Beziehung befindet.

Genauso irrelevant ist das Geburtsdatum für alle Freunde in sozialen Netzwerken. Es hat sich zwar die Unsitte verbreitet, das Geburtsdatum zu veröffentlichen und dadurch andere am betreffenden Tag durch das soziale Netzwerk auf den eigenen Geburtstag aufmerksam zu machen, allerdings stellt sich die Frage, was das eigentlich soll. Der Effekt besteht meist in einem Berg von Glückwünschen, die alle den gleichen Text enthalten und von denen neunzig Prozent aus Pflichtgefühl ausgesprochen werden. Auf solche Glückwünsche kann man durchaus verzichten, wenn man bedenkt, dass man durch diesen Verzicht auch darauf verzichten kann, intime Daten wie das eigene Geburtsdatum zu veröffentlichen.

Letztendlich muss jeder selbst entscheiden, welche Informationen niemanden etwas angehen. Man sollte jedoch grundsätzlich bedenken, dass die meisten Informationen über die eigene Person niemanden etwas angehen und in sozialen Netzwerken grundsätzlich nichts zu suchen haben.

2.3 Verratener Aufenthaltsort

Bei der Erläuterung, warum Tom von seiner Ex-Freundin gefunden wurde, wurde im vorangehenden Kapitel der eigentlich wichtigste Punkt vernachlässigt: Woher wusste Toms Ex-Freundin, wo und wann sich Tom mit dem Mädchen treffen würde? Natürlich kann man jetzt Toms Angewohnheit, mit Mädchen, die ihm gefallen, immer zur gleichen Uhrzeit in das gleiche Restaurant zu gehen, nennen. Aber wenn Tom diese Angewohnheit hätte und seine Ex-Freundin das wüsste, bräuchten wir hier nicht über die Gefahren sozialer Netzwerke sprechen, sondern vielmehr darüber, wie man sich in unserer Gesellschaft verhält und was Wertschätzung bedeutet. Obwohl das sicherlich auch ein schönes Thema wäre, wollen wir davon ausgehen, dass Tom keine derartige Angewohnheit hat und seine Ex-Freundin auch keine Gedanken lesen kann.

Wann also hat Tom die schicksalshaften Informationen preisgegeben? Tom hat beschlossen, das Restaurant mit dem Zug aufzusuchen und auf der Fahrt dorthin war er selbstverständlich mobil in den sozialen Netzwerken seiner Wahl unterwegs. Toms Smartphone hat auch eine hübsche Funktion, mit der Tom via GPS Lokalitäten in seiner Umgebung auswählen kann. Seinen Freunden wird dann angezeigt, dass sich Tom gerade dort befindet. Das kann beispielsweise so aussehen: *Tom ist gerade hier: Restaurant Troja*.

Tom ist es gewohnt, diese Funktion seines Mobiltelefons zu nutzen und macht sich deshalb auch keine Gedanken darüber, was er eigentlich anstellt. Seine Ex-Freundin ist nun aber in der Lage zu bestimmen, wo Tom ist. Und da ein üblicher Zusatz – nämlich die Personen, mit denen er im Restaurant Troja beisammen ist – fehlt, kann Toms Ex-Freundin Eins und Eins zusammenzählen und weiß, dass er nun in diesem Restaurant eine Verabredung mit einem Mädchen hat, höchstwahrscheinlich mit dieser Lisa. Sie weiß es zwar nicht genau, aber sie ist sich doch ziemlich sicher.

Diesmal kann man Toms Fehler an einer einzigen Situation festmachen: Er hätte die Information über seinen Aufenthaltsort nicht teilen dürfen.

In manchen Fällen kann die Kenntnis anderer über den eigenen Aufenthaltsort durchaus nützlich sein, beispielsweise wenn man unterwegs in eine Notsituation gerät. Trotzdem ist davon abzuraten, diese Informationen über soziale Netzwerke zu teilen, da andere Benutzer und vor allem auch der Betreiber mit ausreichenden Informationsmaterialien ein Bewegungsprofil anlegen kann und damit die Gewohnheiten des Nutzers erfahren.

2.3.1 Ortsangaben und Positionsdaten

Ortsangaben und Positionsdaten stellen die wohl brisantesten Informationen in sozialen Netzwerken dar. Schließlich möchte man für gewöhnlich keinen ungebetenen Besuch bekommen, wenn man gerade im Kino ist, gemütlich einen Kaffee trinkt oder zusam-

men mit Freunden unterwegs ist. Außerdem will man vielleicht nicht, dass andere erfahren, wo man gerade ist oder am Abend zuvor war. Um das zu verhindern reicht es nicht, jene Funktionen der sozialen Netzwerke abzuschalten beziehungsweise einfach nicht zu nutzen, die es ermöglichen, Informationen über den aktuellen Aufenthaltsort zu teilen. Vielmehr muss zusätzlich darauf geachtet werden, dass diese Informationen nicht von fremden Personen geteilt werden können und dass Geräte wie Smartphones nicht automatisch Positionsdaten weitergeben.

Explizite Ortsangaben

Soziale Netzwerke auf Mobilgeräten bergen wie zahlreiche sogenannte Apps für Smartphones eine große Gefahr, was den Datendiebstahl durch die Betreiber betrifft. Diese Gefahr reicht von dem Ermitteln von Kontaktdaten aus dem Adressbuch des Mobiltelefons bis hin zum Ermitteln der Positionsdaten des Besitzers über GPS. Wie das technisch funktioniert, ist in Kapitel 3.3.2 näher beschrieben, in Bild 2.5 sind die aktuellen Positionsdaten des Smartphones zu sehen.

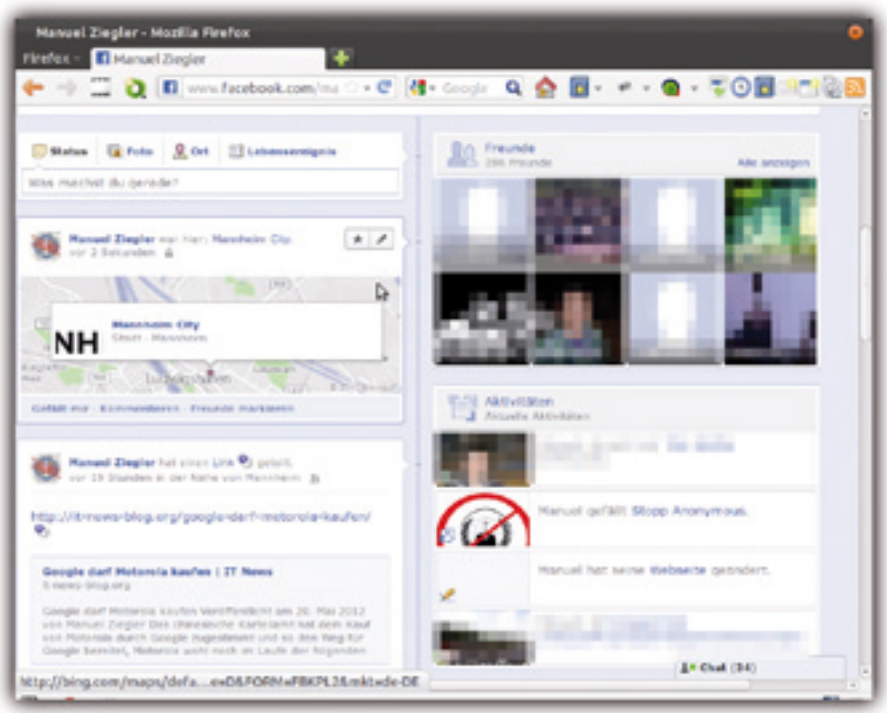

BILD 2.5 Für viele Smartphone-Besitzer ist es üblich, ihren aktuellen Standort über soziale Netzwerke mitzuteilen. Oft verraten sie auch die Personen, die sie gerade begleiten. Für den Schutz persönlicher Daten ist das negativ

Daher sollte man, bevor man eine Anwendung eines sozialen Netzwerkes installiert – und generell auch bei allen Apps, die man auf seinem Smartphone oder auch Tablet installiert –, darauf achten, welche Berechtigungen man dieser Anwendung einräumt und vor allem, ob man bereit ist, diese Berechtigungen zu vergeben. Generell kann davon ausgegangen werden, dass eine Anwendung, die beispielsweise die Berechtigung hat, Standortinformationen über den Benutzer abzurufen, dies auch tut. Und zwar unabhängig davon, mit welcher Begründung die Anwendung versucht, dies zu rechtfertigen.

Es gilt also besondere Vorsicht für die Nutzung sozialer Netzwerke auf Mobilgeräten und meist ist es sinnvoller, sich mit etwas mehr Umstand auf der mobilen Version der Webseite des sozialen Netzwerkes einzuloggen, als auf eine nicht unbedingt viel bequemere App zurückzugreifen, die gleichzeitig zahlreiche Daten ihres Benutzern ermittelt.

Implizite Ortsangaben

Neben den direkt als Positionsdaten erkennbaren Daten gibt es solche, die nicht sofort als Positionsdaten erkennbar sind, jedoch relativ einfach zu derartigen Daten ausgewertet werden können. Bei diesen Informationen handelt es sich um implizite Verweise des Benutzers selbst auf den eigenen Aufenthaltsort. Zwar kann daraus nicht unbedingt jeder ablesen, wo man sich gerade befindet, allerdings wird es Freunden üblicherweise nicht schwerfallen, dies anhand der Benutzerkommentare herauszufinden.

Ein Beitrag wie dieser gibt recht exakte Informationen darüber, wo sich der Benutzer gerade aufhält:

> *Aufgrund einer verspäteten S-Bahn ist der vor uns liegende Streckenabschnitt noch belegt. Wir werden daher mit einer Verspätung von ca. 5 Minuten in Heidelberg eintreffen – Deutsche Bahn.*

Hier ist ziemlich klar, dass der Verfasser dieser Meldung gerade in einem Zug sitzt, nach Art der Durchsage wahrscheinlich in einem Regionalexpress, der durch Heidelberg fährt oder Heidelberg als Ziel hat.[7] Und mit ein wenig Aufwand würde sich sogar bestimmen lassen, in welchem Zug genau. So viele Informationen herauszugeben war aber vielleicht gar nicht die Absicht des Urhebers, er wollte sich eigentlich nur über die Deutsche Bahn beschweren. Dass er dabei in einem Zug sitzt, durften die Leser durchaus erfahren, aber in welchem Zug, wollte er sicherlich nicht ohne weiteres veröffentlichen. Auch hier gilt also wieder, sich vor dem Veröffentlichen eines Beitrags darüber klar zu werden, welche Informationen er enthält und was man wirklich preisgeben möchte. Ein Einbrecher wird sich jedenfalls darüber freuen, dass er fünf Minuten mehr Zeit für das Durchsuchen der Wohnung des Smartphone-Besitzers hat.

Aber nicht nur Beiträge dieser Art tragen Positionsinformationssssen in sich, sondern auch solche, bei denen ein Außenstehender keine Information über den Aufenthaltsort erraten würde. Betrachten wir dazu ein Beispiel:

---

[7] Und dem aufmerksamen Leser ist damit auch klar, aus welcher Region der Autor dieses Buchs stammt. Dieser „Fehler“ fiel erst beim Redigieren des Manuskripts auf, was zeigt, wie leicht einem in dieser Hinsicht Patzer unterlaufen können, und dass derartige Fehler selbst denen passieren, die sich intensiv mit dem Thema beschäftigen.

Toms jüngerer Bruder Tim ist, anders als Tom, kein großer Party-Fan. Er trifft sich am Wochenende lieber mehr oder weniger regelmäßig mit seinen Freunden im örtlichen Jugendraum, wo diese gemeinsam große Mengen an Alkohol konsumieren. Tim ist noch ziemlich unreif und stolz darauf, dass er mehr Alkohol konsumieren kann als die meisten anderen, und zwar ohne sich zu übergeben.

Außerdem hat Tim die dumme Angewohnheit, immer dann, wenn er in den Jugendraum geht, um sich zu betrinken, einen Beitrag mit dem Inhalt „Saufen" zu veröffentlichen.

In letzter Zeit hat Tim Probleme mit einem Jungen aus dem Nachbarort. Diesem schuldet er eine kleine Summe Geld und wird daher immer wieder von ihm belästigt. Als Tim an diesem Abend in den Jugendraum kommt, wird er dort bereits von diesem Jungen und dessen Clique erwartet und um den geschuldeten Betrag einschließlich angemessener Zinsen erleichtert.

Der Junge musste sich gar nicht auf seinen Verdacht verlassen, dass Tim jedes Wochenende im Jugendraum aufkreuzen würde, er musste nur warten, bis Tim einen Beitrag „Saufen" veröffentlichte. Man muss nämlich nur in der Historie von Tims Beiträgen so weit zurückgehen, bis dieser Beitrag einmal kommentiert wurde, woraus hervorgeht, dass es in den Jugendraum geht. Dann kann man sich sicher sein, dass das immer so ist, wenn der Beitrag relativ regelmäßig auftritt.

Hier kommt wieder das Problem der Berechenbarkeit ins Spiel, das auch schon Tims Bruder Tom in seinen jungen Jahren hatte: Wer sich in sozialen Netzwerken berechenbar zeigt, gibt automatisch zahlreiche Informationen über sich preis, die er vielleicht gar nicht in Händen Fremder wissen möchte.

Auch Beiträge, die mobil veröffentlicht wurden, können Zündstoff enthalten. Selbst wenn sie gar nicht absichtlich mit Standortinformationen versehen wurden, ist es unter Umständen durchaus möglich, dass aus den Beiträgen geschlossen werden kann, dass sie mobil geschrieben wurden. So kann unter einem mit einem Android-Smartphone veröffentlichten Beitrag beispielsweise stehen „... via Android". Dies liefert zwar keine direkte Information über die aktuelle Position und zeigt nur, dass man gerade unterwegs ist. Allerdings kann ein Fremder, der jemanden über einen längeren Zeitraum beobachtet, feststellen, wann jemand zuhause oder unterwegs ist, und so Einblicke in dessen Tagesablauf gewinnen – und/oder dessen Abwesenheit sogar für einen Einbruch ausnutzen.

3 Datenmissbrauch durch Netzbetreiber

In Kapitel 2 wurde der Datenmissbrauch durch einfache Spionage anderer Benutzer dargestellt. Diese bekommen über soziale Netzwerke sehr einfach eine große Zahl von Informationen über die Mitglieder. Aber die größte Gefahr für die persönlichen Daten geht eigentlich von den Betreibern selbst aus. Sie bieten ihren Nutzern den Dienst nicht an, weil sie sich besonders gemeinnützig zeigen möchten, sondern, weil sie mit deren Daten Geld verdienen möchten, zum Beispiel indem sie ihnen individuell abgestimmte Werbeinhalte einblenden. Die Werbeanzeigen sind in Wirklichkeit Links, die auf die Internetpräsenz des Werbenden führen. Klickt jemand auf eine solche Werbeanzeige, bedeutet dieser Klick in dem meisten Fällen bares Geld für den Netzwerkbetreiber. Kauft das Mitglied auch noch auf der angepriesenen Seite ein, wird der Netzbetreiber je nach Werbevertrag zusätzlich noch am Gewinn beteiligt[1].

Wenn man sich überlegt, dass Mark Zuckerberg, der Gründer von Facebook, innerhalb weniger Jahre zum Multimilliardär wurde, stellt sich die Frage, ob Werbung wirklich seine einzige Verdienstquelle ist – oder ob im Hintergrund noch ganz andere Geschäfte mit den ihm von den Mitgliedern überlassenen Daten laufen. Die mangelnde Transparenz des Unternehmens kann diese Zweifel nicht aus dem Weg räumen. Wie dem auch sei, fest steht jedenfalls, dass die Betreiber sozialer Netzwerke ganz und gar nicht sozial sind, sondern aus den Daten ihrer Benutzer Profit schlagen und sie zu diesem Zweck auch rücksichtslos nutzen. Facebook behält sich beispielsweise vor, personenbezogene Daten an Dritte weiterzugeben, nachdem der Benutzer in den Datenschutzrichtlinien darüber informiert wurde[2]:

> *„Darum machen wir Informationen, die wir über dich erhalten, anderen nicht zugänglich, es sei denn:*
>
> 1. *wir haben deine Genehmigung dazu erhalten;*
> 2. *wir haben dich beispielsweise in diesen Richtlinien darüber informiert; oder wir haben deinen Namen sowie alle anderen personenbezogenen Informationen von diesen Daten entfernt.“*

[1] Nachvollziehbar durch die Werbeangebote der einzelnen sozialen Netzwerke, beispielsweise bei Facebook unter http://www.facebook.com/advertising.

[2] Siehe http://www.facebook.com/about/privacy/your-info#howweuse

Dieser Passus ist ein Freibrief: Indem Facebook dem Mitglied die Richtlinien zugänglich macht, wird das Mitglied darüber informiert, dass seine Daten weitergegeben werden – der Beweis sind die individuell auf das Mitglied abgestimmten Werbeanzeigen. Das größte Problem dabei ist, dass sie sich nicht nur der freiwillig von den Nutzern angegebenen Daten bedienen, zu denen bereits Beiträge zählen, sondern dass sie auch auf eigene Faust Daten ermitteln und einfach jede Information speichern, die sie bekommen können – ungeachtet dessen, ob sie relevant ist oder nicht. In den Datenverwendungsrichtlinien von Facebook kann man beispielsweise nachlesen, welche Daten Facebook über einen Nutzer erhält[3]. Auch bei Google kann man in den Datenschutzrichtlinien nachlesen, woher Google seine Daten über die Mitglieder erhält. Dabei stellt man fest, dass wie bei Facebook zahlreiche Daten ermittelt werden, wenn man auf Seiten surft, die eigentlich gar nicht zu Google gehören[4]. Mehr zu diesen Vorgehensweisen ist in Kapitel 3.3 ab Seite 99 nachzulesen.

3.1 Der finanzielle Wert von Mitgliedsdaten

Vor allem den jungen Mitgliedern scheint es egal zu sein, ob die Betreiber sozialer Netzwerke ihre persönlichen Daten ermitteln und auswerten könnten, sonst würden sie ihre Daten nicht so freigiebig herausrücken. Allerdings muss man ihnen zugute halten, dass sie gar nicht wissen, welche Auswirkungen das haben kann. Hier liegen eklatante Informationslücken vor. Und das dürfte wohl auch der Grund dafür sein, weshalb die Betreiber bislang von ihren Nutzern nicht in ihre Schranken gewiesen wurden.

Was die Betreiber tatsächlich aus den angegebenen Daten ermitteln können, hängt natürlich von der Art und Anzahl der Informationen ab und ist daher vom Benutzer durchaus zu kontrollieren, wenn auch nur äußerst schwer. Im Folgenden soll betrachtet werden, welche Daten der Betreiber gewinnen und was er mit ihnen anfangen kann.

Als Beispiel soll abermals Tom dienen. Weil er täglich soziale Netzwerke nutzt, kann der Betreiber von ihm nicht nur zahlreiche Daten ermitteln, sondern sogar deren Richtigkeit überprüfen.

Das funktioniert folgendermaßen: Durch Toms Aktivitäten in den sozialen Netzwerken fallen Daten an, die in Datenbanken gespeichert werden. Es handelt sich um Informationen darüber, mit wem sich Tom unterhält, auf welche Weise er das tut (öffentlich oder privat) und über was er mit dieser Person spricht. Diese Daten werten die Betreiber automatisch aus. Dabei wird beispielsweise ermittelt, mit wem Tom zuletzt kommuniziert hat oder mit wem er sich am häufigsten unterhält. Verfolgt man die Werbeeinblen-

[3] Siehe http://www.facebook.com/about/privacy/your-info#inforeceived

[4] Siehe http://www.google.de/intl/de/policies/privacy/

dungen in bestimmten sozialen Netzwerken[5] aufmerksam, kann man auch vermuten, dass die Betreiber persönliche Nachrichten sowie für eine größere Gruppe sichtbare Beiträge nach Schlagwörtern durchsuchen und diese ebenfalls speichern. Mit dieser Technik und der vom Benutzer in seinem Profil gespeicherten Daten lässt sich langfristig ein relativ vollständiges Bild des Benutzers generieren, ohne dass auch nur ein menschlicher Mitarbeiter für das Auswerten der Angaben benötigt würde. Wird ein Nutzer über längere Zeit beobachtet, können die Daten anhand der Häufigkeit, nach der sie anfallen, auf Plausibilität beziehungsweise Gültigkeit geprüft werden.

Wenn Tom einmal einen Beitrag veröffentlicht, in dem beispielsweise das Wort Elektronik vorkommt, kann noch kein Schluss auf das berufliche oder private Umfeld gezogen werden. Wenn Tom, von Beruf Elektriker, jedoch häufiger Wörter wie Sicherung, Schaltung, Spannung oder Stromstärke in seine Beiträge und persönlichen Nachrichten schreibt, könnte ein Mensch assoziativ feststellen, dass Tom irgendeinen Bezug zur Elektrotechnik hat. Ähnlich verhält es sich bei der maschinellen Auswertung. Der Auswertungsmechanismus kann erkennen, ob mehrere Wörter aus einer bestimmten Kategorie stammen und Tom so mit der Elektrotechnik in Verbindung bringen, anstatt ihn mit Spannung oder dergleichen zu korrelieren, was Unsinn wäre.

Doch was tun die Betreiber mit diesen Daten, nachdem sie sie sorgfältig gespeichert und analysiert haben? Die Antwort ist einfach: Sie verdienen Geld damit. Trotz der meist mangelhaften bis ungenügenden Transparenz der Unternehmen, die hinter den sozialen Netzwerken stehen, kann man durchaus davon ausgehen, dass die Haupteinnahmequelle die auf den Benutzer abgestimmte Werbung ist. Schließlich ist die Mitgliedschaft in den sozialen Netzwerken meistens kostenlos.

Es ist also interessant zu erfahren, wie die Betreiber es mit Hilfe dieser Daten schaffen, dem Benutzer zielgerichtetere Werbung anzuzeigen, als wenn sie diese Auswertung nicht betreiben würden – ein profitorientiertes Unternehmen würde die Daten schließlich wohl kaum ermitteln, wenn es sich finanziell nicht lohnen würde.

Um zu verstehen, wie in einem sozialen Netzwerk mit Werbung Geld verdient wird, muss man zunächst wissen, was eigentlich hinter Werbung steckt. Jede Firma, die ein Produkt herstellt, möchte dieses Produkt den potenziellen Käufern bekannt machen. Dies geht entweder über Mundpropaganda durch zufriedene Käufer, die ihren Bekannten oder Kollegen von den Vorteilen dieses Produkts erzählen oder über Produktbesprechungen in Medien wie Zeitschriften, dem Fernsehen oder Radio. Diese beiden Methoden kosten den Hersteller nichts.[6] Allerdings kann diese Art der Werbung auch nicht gesteuert werden; findet sich niemand, der das Produkt aus freien Stücken anpreist, erfährt auch niemand von ihm. Um das Produkt wirklich allen Konsumenten nahezubringen, die sich dafür interessieren könnten, muss der Hersteller selbst aktiv werden

[5] Gibt man in Facebook in den Profilinformationen keinen Hinweis auf ein bestimmtes Thema, spricht dieses Thema jedoch öfter in persönlichen Nachrichten oder geteilten Beiträgen an, kann man nach einiger Zeit Werbeanzeigen zu genau diesem Thema beobachten.

[6] ...auch wenn mittlerweile gut ein Drittel der positiven Produktbesprechungen in Zeitschriften und Onlineshops vom Hersteller in Auftrag gegeben und bezahlt wird (laut einer Meldung des Bayrischen Rundfunks vom Mai 2012).

und Werbung machen. Dies macht er in Form von Anzeigen. In gedruckten Medien und auch im Internet handelt sich dabei meist um fotografische Darstellungen von Produkten, versehen mit einem Text, der deren Einzigartigkeit hervorhebt und die positiven Auswirkungen seines Erwerbs auf den Kunden schildert. Damit der Hersteller seine Anzeigen im jeweiligen Medium abdrucken oder herzeigen darf, muss er vom Verlag beziehungsweise dem Betreiber des Mediums einen Platz in einer Zeitschrift oder auf einer Webseite mieten.

Wie viel Geld der Werbende dem Betreiber als Miete zahlen muss, hängt davon ab, wie viele Personen die Anzeige sehen werden – also wie hoch bei einer Zeitschrift die Druckauflage ist und wie viele Besucher eine Webseite hat – und wie gut er die gewünschte Zielgruppe für sein Produkt erreicht beziehungsweise wie hoch der Prozentsatz derjenigen ist, die gar nicht als Kunde in Betracht kommen. Der Werbefachmann spricht hier vom Streuverlust. Der ideale Anzeigenplatz ist ein Medium mit sehr vielen Lesern beziehungsweise Besuchern, deren Merkmale genau bekannt sind: ihre Vorlieben, ihr Alter, ihr Beruf, die Hobbys und das Einkommen.

Ein Anzeigenplatz in einem Medium, das diese Kombination erfüllt, ist sehr teuer. Die Mitgliedszeitschrift des größten deutschen Automobilverbands, die die beiden genannten Kriterien bezüglich Auflage und Zielgruppenansprache erfüllt, verlangt beispielsweise 113.920,– Euro zuzüglich Mehrwertsteuer für eine Anzeige im Format A4 in einer einzigen Ausgabe[7]. Dieser Preis ist fest (eventuell noch in gewissen Grenzen verhandelbar), der Verlag kann ihn verlangen und bekommt ihn auch bezahlt, weil er die Höhe der Auflage und die Zusammensetzung der Leserschaft nachweisen kann. Je kleiner die Anzeige ist, desto weniger kostet sie – allerdings wird sie dann von den Lesern auch öfter übersehen. Man denke hier nur an die vielen optisch gleichen privaten Kleinanzeigen in den Tageszeitungen und Wochenblättern.

Das Mieten von Anzeigenplatz in einem sozialen Netzwerk unterscheidet sich von der Belegung von Zeitschriftenseiten. Natürlich gilt auch hier, dass die Miete für Anzeigenfläche proportional zur Anzahl der Besucher und genauen Ansprache der gewünschten Zielgruppe steigt. Allerdings ist die Art der Werbung und die Bezahlung eine andere: In Facebook[8] beispielsweise besteht eine Werbeanzeige aus einem Titel mit 25 Zeichen, einem Text mit 135 Zeichen und wahlweise einem Minibild mit einer Höchstgröße von 110 x 80 Bildpunkten (eine Briefmarke wäre im Vergleich dazu riesig); eine andere Größe geht nicht. Bei der Preisgestaltung kann der Werbetreibende zwischen Klicks und Impressionen wählen. Wenn jemand einmal auf seine Anzeige klickt, zahlt er an Facebook zwischen 40 und 60 Eurocent pro Klick. Impression bedeutet, dass seine Anzeige immer wieder eingeblendet wird. Wird eine Anzeige tausendmal eingeblendet, kostet dies 20 bis 30 Eurocent. Die Preise sind nicht fest, sondern werden gemäß der Nachfrage berechnet. Wenn mehrere Werbetreibende den selben Anzeigenplatz belegen möchten, kommt in einer Art Auktion derjenige zum Zug, der am meisten zahlt. Facebook kann dann locker ein bis zwei Drittel mehr vom Werbekunden kassieren. Dieser Preis wird

[7] Siehe http://media.adac.de/mediaservice/mediadaten/.

[8] Diese Daten wurden übernommen von http://www.Facebook-Werbung.com.

wohl auch gern bezahlt, denn die Zielgruppe ist genau bekannt und durchanalysiert – schließlich teilen viele Mitglieder dem Unternehmen hinter dem sozialen Netzwerk ohne Zögern mit, aus welchem Land sie kommen, nennen ihr Alter (Geburtstag), ihr Geschlecht, ihre Ausbildung und Arbeit, sogar den Beziehungsstatus und ihre persönlichen Interessen. Und wenn schon nicht freiwillig, dann anhand ihrer Beiträge, die maschinell auf Schlüsselwörter durchsucht und ausgewertet werden.

Der Preis pro Besucherklick und pro tausend Einblendungen hört sich erst einmal nicht hoch an, aber um eine Million Mitglieder zu erreichen wie in einer hochauflagigen Zeitschrift – und dies wiederholt –, kann das auf die Dauer schon ganz schön ins Geld gehen. Rein statistisch gesehen klicken nämlich weit weniger als ein halbes Prozent der Nutzer eine Anzeige an. Um genügend Interessierte auf die eigene Webpräsenz zu locken, müssen viele Anzeigen geschaltet oder sehr oft eingeblendet werden. Außerdem sind es viele Hersteller, die ihre Produkte in sozialen Netzen bewerben, da kommen schon erkleckliche Werbeeinnahmen zustande.

In XING Werbung zu schalten, kostet sogar bis zum Zehnfachen der Gebühren von Facebook[9]. Der Grund ist wohl, dass XING behauptet, das Netzwerk eines beruflich aktiven und erfolgreichen Personenkreises zu sein.

Der Kunde eines sozialen Netzes ist also in erster Linie nicht das Mitglied – dieses ist ja in den meisten Netzwerken kostenfrei dabei – sondern der Werbetreibende. Mit ihm wird das Geld verdient. Aber auch diese Strategie scheint Erfolg zu haben und rund um die Werbung in den sozialen Netzen hat sich bereits eine florierende Industrie aus spezialisierten Werbeagenturen entwickelt. Agenturen wie google-plus-marketing.ch bieten den Bau kompletter Firmenportale inklusive 1000 Freunden beziehungsweise Followern für Preise um die 2000 Euro an.

In sozialen Netzen scheint Werbung also besonders effizient zu sein. Um herauszufinden, warum das so ist, muss man sich überlegen, unter welchen Umständen sich jemand dazu entscheidet, ein Produkt zu erwerben. Sicherlich lässt man sich stark davon beeinflussen, ob Freunde möglicherweise das Produkt bereits besitzen oder ob Leute, die man mag oder sogar bewundert, ein solches Produkt bereits gekauft haben. Das Produkt sollte zudem seriös wirken und preiswert sein (oder entsprechend wirken).

Ein weiterer Grund könnte sein, dass in sozialen Netzwerken Werbeanzeigen besser beachtet werden als in Printmedien. Im Internet kann eine Anzeige nämlich personalisiert werden. Kennt man den Namen des Mitglieds eines Netzes, kann es direkt angesprochen werden. Dies fällt ihm wesentlich besser ins Auge als eine anonyme Zeitschriftenanzeige, die zu ignorieren er gelernt hat.

Mit Hilfe der Daten, die über das Mitglied eines sozialen Netzes ermittelt wurden, ist es sehr einfach, ihn glauben zu machen, ein bestimmtes Produkt sei bei den Freunden sehr beliebt. Der Betreiber muss der Anzeige nur einfach ein paar Behauptungen wie *Freund A, Freund B und 20 weiteren Freunden gefällt das* hinzufügen, um das Interesse des Benutzers zu wecken.

[9] Nachzulesen unter http://www.adconion.com/files/de-DE/download/exklusiv/ XING_Mediadaten_DE_Januar%202011.pdf

Mit diesen Tricks manipuliert der Betreiber direkt die einzelnen Benutzer. Man wendet sozusagen seine eigenen Daten gegen ihn an, um ihn dazu zu bewegen, ein bestimmtes Produkt zu erwerben.

Natürlich muss man nicht unbedingt jede Werbung hinnehmen. Mit sogenannten Werbeblockern – das sind Erweiterungen für einen Browser, die Werbung auf Webseiten automatisch herausschneiden – kann die in Facebook geschaltete Werbung blockiert werden.

Adblock Plus[10] ist eine solche Erweiterung für Firefox, Chrome und andere Browser, mit dem Werbeanzeigen auch unter Facebook ausgeblendet werden können. Auch die an späterer Stelle vorgestellten Erweiterung *DoNotTrack Plus* blendet die Anzeigen aus.

3.2 Missbrauch freiwillig veröffentlichter Daten

Freiwillig veröffentlichte Daten werden von den Betreibern der sozialen Netzwerke ausgiebig ausgewertet und genutzt. Unter diesen Daten ist alles zu verstehen, was der Benutzer jemals in sozialen Netzwerken mit anderen Benutzern geteilt hat oder dort auch nur für sich selbst sichtbar gespeichert hat. Das bedeutet, dass die Betreiber von sozialen Netzwerken auch Inhalte persönlicher Nachrichten auswerten könnten. Beweisbar ist das derzeit nicht, aber es gibt einige Indizien, die diese These untermauern. Erwähnt man in persönlichen Nachrichten beispielsweise häufiger Begriffe eines bestimmten Themengebietes, kann man nach einiger Zeit Werbeanzeigen zu diesem Thema auf seiner Seite beobachten.

Zumindest bei Facebook kann der Verdacht, dass der Betreiber speichert und auswertet, wer mit wem wie oft kommuniziert, auf diese Weise gestützt und von jedem nachvollzogen werden. Man kann das recht einfach feststellen: Gibt man oben in das Suchfeld einen Buchstaben ein, wird bereits nach Ausdrücken gesucht, die mit diesem Buchstaben beginnen, und diese in der Vorschau angezeigt. „Seltsamerweise“ werden nach der Eingabe eines beliebigen Buchstabens im Suchfeld die engsten Freunde an oberster Stelle angezeigt beziehungsweise die Personen, mit denen man in Facebook am häufigsten kommuniziert.

Auch die Chat-Funktion auf der rechten Seite enthält an oberster Stelle die Personen, mit denen man sich am häufigsten digital unterhält. Damit ist zwar noch nicht bewiesen, dass Facebook auch den Inhalt der persönlichen Nachrichten ermittelt. Allerdings kann man davon ausgehen, dass die Entwickler von Facebook nicht dumm sind und deshalb eindeutige Rückschlüsse auf Datenspionage verhindern. Nur weil der Dienst dadurch wesentlich benutzerfreundlicher wird, erfährt man, dass Daten über die Kommunikation zwischen den Benutzern gespeichert werden. Der Betreiber riskiert damit zwar,

[10] Für Firefox zu beziehen von https://addons.mozilla.org/de/firefox/addon/adblock-plus/, Homepage auf http://adblockplus.org/de/, die Chrome-Version ist auf http://adblockplus.org/de/chrome erhältlich.

dass misstrauische und technisch versierte Mitglieder sehen können, welche Daten ausgewertet werden. Weil solche Mitglieder aber in der Minderheit sind, werden sie hingenommen. Im Gegenzug wird der Dienst für die große Masse benutzerfreundlicher, und von dieser erfährt der Betreiber größere Zustimmung als vom Rest Ablehnung. Allerdings ändert dies nichts an der Tatsache, dass Facebook riesige Datenmengen gewinnt, die beispielsweise durchaus für eine Psychoanalyse brauchbar wären. Mit diesen Daten und der Flut weiterer Daten, die zusätzlich ermittelt werden, ist es möglich, dass der Betreiber den Benutzer beinahe besser kennt als dieser sich selbst.

BILD 3.1 Es ist zwar komfortabel, Freunde vorgeschlagen zu bekommen (siehe rechts), vor allem dann, wenn man mit diesen auch tatsächlich befreundet ist, allerdings sollte jedem klar sein, dass die sozialen Netzwerke eine Vielzahl von Daten über den Benutzer benötigen, um solche Vorschläge unterbreiten zu können

Welche Informationen die Betreiber sozialer Netzwerke tatsächlich aus den freiwillig gelieferten Benutzerdaten gewinnen können und worauf generell zu achten ist, ist in den folgenden Kapiteln erläutert.

3.2.1 Datenspeicherung verhindern

Um Spionage durch andere Benutzer zu verhindern, wurden in Kapitel 2 die Privatsphäre-Einstellungen empfohlen. Mit dieser Differenzierung der Reichweite können Daten in unterschiedlichen Freundeskreisen veröffentlicht und bestimmte Informationen vor Fremden und entfernten Bekannten verborgen werden. Wenn man die Empfänger sorgfältig filtert, können Informationen, die nicht alle kennen sollen, also getrost publiziert werden.

Allerdings helfen selbst die durchdachtesten Privatsphäre-Einstellungen nicht dabei, Informationen vor dem Betreiber des sozialen Netzes zu verheimlichen – sein langer Arm reicht überall hin. Um ihn kurzzuhalten, hilft nur, vertrauliche Informationen in einem sozialen Netzwerk überhaupt nicht zu verteilen. Schließlich hat der Betreiber die Möglichkeit, sämtliche Angaben zu ermitteln. Egal, ob sie öffentlich oder nur für Freunde sichtbar sind, in persönlichen Nachrichten erwähnt werden oder ausschließlich für den Nutzer selbst sichtbar sind – er kann sie bei Bedarf jederzeit aus seinen Datenbanken abrufen und auswerten.

Das bedeutet für die Nutzer sozialer Netzwerke, dass sie sich bereits mit der Entscheidung zur Registrierung damit abfinden müssen, dass von nun an Daten über sie gesammelt werden, egal wie sehr sie sich bei der Wahrung der Privatsphäre anstrengen. Sobald man Mitglied eines sozialen Netzwerks ist, trägt man automatisch dazu bei, die Datenbank des Betreibers mit persönlichen Daten zu bereichern. Auch Daten nur für den Autor selbst sichtbar zu machen, ist unter diesem Aspekt reine Augenwischerei und zugleich eine freiwillige Fütterung der Datenbank der Netzwerke – sozusagen die Absegnung des Datenmissbrauchs durch den Betreiber.

Besonders bemerkenswert ist es, dass oft Beiträge, die vom Benutzer bereits gelöscht wurden, dennoch in den Datenbanken gespeichert bleiben. Als es vor einiger Zeit einem Studenten der Rechtswissenschaften gelang, die Herausgabe aller ihn betreffenden bei Facebook gespeicherten Daten zu erwirken, stellte er außer der Tatsache, dass seine Daten intern unter insgesamt 57 Kategorien abgelegt waren und 1200 Seiten umfassten, auch fest, dass darunter zahlreiche von ihm in der Vergangenheit gelöschte Beiträge enthalten waren. In einem Interview mit 1Live berichtet der Student Max Schrems von seinen Erkenntnissen[11]. Am 7.2.2012 berichtete die Computerwoche[12] abermals von Daten, die nach der Löschung wieder aufgetaucht waren. Facebook berief sich auf einen Fehler im System – aber für die meisten Datenschützer war damit klar, dass Facebook Daten auch nach der Löschung aufbewahrt, um immer umfassendere Informationen über den Nutzer gewinnen zu können.

Dass es sich keineswegs um einen Fehler handelt, sondern um Absicht – das Einräumen eines Fehlers sollte wohl nur die Mitglieder besänftigen –, verrät das Impressum bzw. die Nutzungsbedingungen von Facebook. Hätten die Datenschützer oder der Student vor

[11] Siehe auch http://www.einslive.de/magazin/extras/2011/09/28/110928_iv_max_ schrems.jsp

[12] http://www.computerwoche.de/netzwerke/web/2504579/

der Mitgliedschaft auf http://www.Facebook.com/legal/terms?ref=pf in Punkt 2.2 nachgelesen, hätten sie folgenden Text gefunden:

> *„Wenn du IP-Inhalte löschst, werden sie auf eine Weise entfernt, die dem Leeren des Recyclingbehälters auf einem Computer gleichkommt. Allerdings sollte dir bewusst sein, dass entfernte Inhalte für eine angemessene Zeitspanne in Sicherheitskopien fortbestehen (für andere jedoch nicht zugänglich sind).“*

Der Recyclingbehälter auf einem Computer entspricht unter Windows dem Mülleimer. Wenn auf einem PC Dateien gelöscht werden, werden sie zuerst automatisch in den Mülleimer verschoben. Wenn danach der Inhalt des Mülleimers gelöscht wird, wird dabei lediglich der zugehörige Verzeichniseintrag gelöscht. Das bedeutet: Die Daten sind weiterhin auf der Festplatte vorhanden und können – solange sie nicht durch neuere Daten überschrieben werden – restauriert werden. Was eine angemessene Zeitspanne ist, wird nicht näher definiert. Dem einen erscheinen zwei Tage wie eine Ewigkeit, der andere, der mit den Daten Geld verdient, hält vielleicht ein Jahr für angemessen. Über diesen Begriff können sich die Betreiber und Mitglieder trefflich streiten.

Allerdings steht in Punkt 2.1 im Impressum/Nutzungsbedingungen von Facebook:

> *„Für Inhalte wie Fotos und Videos („IP-Inhalte“), die unter die Rechte an geistigem Eigentum fallen, erteilst du uns durch deine Privatsphäre- und Anwendungseinstellungen die folgende Erlaubnis: Du gibst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz für die Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammenhang mit Facebook postest („IP-Lizenz“). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst, außer deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht.“*

Was genau unter IP-Inhalten verstanden wird, konnte im Impressum nicht eruiert werden. Man sollte vorsichtshalber davon ausgehen, dass davon nicht nur Fotos und Videos betroffen sind, sondern auch die Inhalte aller Beiträge. Schließlich hat der Verfasser/dasMitglied das geistige Eigentum an ihnen, weil er sie geschrieben (und quasi erfunden) hat. Dies bedeutet, dass Facebook die Fotos, Inhalte und privaten Daten, die seine Anwender posten, jederzeit – ohne weitere Genehmigung – an beliebige Firmen oder Privatpersonen weiterverkaufen darf. Und dies ist unter normalen Umständen auch nach ihrer Löschung durch den eigentlichen Urheber möglich, denn dass auch alle seine Freunde die Inhalte löschen, wenn ein Mitglied sein Konto und seine Daten löscht, ist unwahrscheinlich. Punkt 2.1 ist also Facebooks Freifahrschein für das Bunkern und Verkaufen von Daten.

Allerdings wird auf der Impressumsseite https://www.Facebook.com /terms/provisions/german/index.php für deutsche Mitglieder eine Einschränkung getroffen:

> *„Ziffer 2 gilt mit der Maßgabe, dass unsere Nutzung dieser Inhalte auf die Verwendung auf oder in Verbindung mit Facebook beschränkt ist.“*

Deutsche Mitglieder haben also Glück, ihre Inhalte dürfen „nur“ an in Facebook Werbetreibende oder Firmen weiterverkauft werden, die in irgendeiner Form mit Facebook zu tun haben. Und das sind eine ganze Menge.

Die Gruppe http://europe-v-facebook.org warnt jedoch vor allem im Hinblick auf die kürzlich neu eingeführten AGB davor, dass in Zukunft jede Information, die man als Benutzer auf Facebook angibt, der Plattform gehören könnte.

Durch Täuschung des Netzwerkbetreibers

Da man als Mitglied eines sozialen Netzwerks dem Betreiber nicht verbieten kann, bestimmte Informationen über einen zu gewinnen und vorzuhalten, muss man nach anderen Lösungen suchen. Einer der effizientesten, aber auch einer der aufwendigsten Wege ist die systematische Täuschung des Netzwerkbetreibers durch das Veröffentlichen diffuser Daten. Unabdingbar dabei ist, dass man selbst den Überblick über seine publizierten Informationen behält und sie entweder durch entsprechend gegenläufige Informationen egalisiert oder durch eine Vielzahl ähnlicher Informationen dramatisiert und auf diesem Weg das Bild über sich selbst verzerrt. Solche verzerrten Informationen sind für den Netzwerkbetreiber nichts wert.

Der Vorteil dieses Verfahrens ist gleichzeitig sein Nachteil: Je nach Inhalt der Informationen entsteht ein völlig falsches Bild über den Verbreiter der Daten. Weil man aber nur den Betreiber des sozialen Netzwerks und nicht auch noch zusätzlich seine eigenen Freunde täuschen möchte, gilt es einen Weg zu finden, der den eigenen Ruf nicht ruiniert. Die allgemeinen Techniken dafür werden nachfolgend vorgestellt.

Generell sei aber angemerkt, dass das Täuschen laut den Nutzungsbedingungen des jeweiligen Diensts verboten sein kann. Im Impressum von Facebook ist beispielsweise unter Punkt 4.1 zu lesen:

> *„Du wirst keine falschen persönlichen Informationen auf Facebook bereitstellen [....]“*

Wenn ein Mitglied sich nicht an diesen Passus hält, kann es aus dem Netz geworfen werden. Der Grund ist klar: Falsche Informationen sind finanziell wertlos, weil sie nicht verkauft werden können – beziehungsweise dürfen, wenn der Betreiber weiß, dass sie falsch sind. Würde er sie dennoch verkaufen, würde er den Kunden betrügen.

Prinzipiell können Informationen, die Netzbetreiber aus Nachrichten und Beiträgen gewinnen, auf zweierlei Arten verborgen werden:

- Der einfachere Weg ist es, das soziale Netzwerk mit beliebigen Daten zu fluten, die in alle möglichen Richtungen gehen. Dabei werden die tatsächlich relevanten Daten so verborgen, dass ihre Bedeutung mit der Menge der Datenflut abnimmt und schließlich zu vernachlässigen ist.
- Der bessere Weg ist es, gezielt durch selbst veröffentlichte Informationen den vorhandenen Informationen entgegenzuwirken oder solche Informationen zu verfassen, die in die gleiche Richtung wie die ursprüngliche Information gehen und diese weiter dramatisieren. Dadurch entsteht ein verzerrtes Bild der eigenen Identität, das aller-

dings deutlich realistischer wirkt als das mit dem ersten Verfahren erzeugte. Diese Arbeitsweise erfordert allerdings einen erheblich höheren Aufwand als die zuerst geschilderte Variante.

Nachdem ein Beitrag, der eine gewisse Information trägt, im sozialen Netzwerk veröffentlicht wurde, wird sein Inhalt automatisch vom Betreiber ausgewertet. Damit der Betreiber die aus dem Beitrag gewonnenen Erkenntnisse nicht weiter beziehungsweise nicht in entsprechendem Maße weiterverwenden kann, muss der Nutzer Maßnahmen treffen, um die Information dieses Beitrags zu verschleiern. Dazu ein einfaches Beispiel:

Tom schreibt eines Tages in sozialen Netzwerken den Beitrag *Ich bin Vegetarier*. Als er merkt, dass er seit der Veröffentlichung dieses Beitrags immer wieder Werbung für vegetarische Kochbücher und dergleichen bekommt, ärgert er sich und würde seinen Beitrag am liebsten rückgängig machen. Da dies bekanntlich nicht möglich ist, hat Tom zwei Möglichkeiten, um die Werbung für vegetarische Kochbücher zu unterbinden:

- Erstens kann er den Dienst mit uneinheitlichen Informationen fluten. Wenn die Angaben automatisch ausgewertet werden, entsteht ein diffuses Bild über das Mitglied. Der Betreiber kann daraus nicht mehr entnehmen, welche Art von Produktwerbung er Tom anzeigen soll, so dass ihm keine andere Wahl bleibt, als die Anzeigen thematisch zu streuen. Das heißt, dass mehr oder weniger der Zufall entscheidet, zu welchem Thema Tom Werbung angezeigt bekommen wird.
- Oder Tom arbeitet seiner ursprünglichen Aussage inhaltlich entgegen – verbreitet also das Gegenteil – oder spitzt sie zu. Entgegenarbeiten könnte er beispielsweise durch die Aussage *Ich liebe Fleisch*, während er seine Aussage weiter verschärfen könnte mit *Ich bin Veganer*.

Im Folgenden sollen die beiden Möglichkeiten anhand dieses Beispiels genauer betrachtet werden.

Ungerichtete Informationsüberflutung

Bei der ungerichteten Informationsüberflutung des sozialen Netzwerks werden regelmäßig nicht aufeinander aufbauende Beiträge veröffentlicht, die insgesamt den Dienst derart mit Informationen überfluten, dass die inhaltliche Bedeutung eines einzelnen Beitrags in den Hintergrund rückt. Man kennt dies im echten Leben von Briefen oder E-Mails: Je mehr man bekommt und je länger ein Schreiben ist, desto weniger wird sein Inhalt zur Kenntnis genommen.

Die einzige Schwierigkeit bei diesem Verfahren besteht darin, ausreichend Themen für Beiträge zu finden. Wie man solche Themen findet, bleibt jedem selbst überlassen, es empfiehlt sich allerdings ein kurzes Brainstorming, bevor man mit dem Veröffentlichen beginnt. Man sollte sich die Themen notieren und sich auch daran halten, denn andernfalls wird die Mehrzahl der Beiträge sich automatisch mit den Themen befassen, die einen tatsächlich interessieren. Nur wenn man sich an den eigenen Plan hält und etwas Disziplin walten lässt, sind die Beiträge auch tatsächlich ungerichtet.

Welchen Inhalt die Beiträge tatsächlich haben, ist dabei eigentlich gar nicht so sehr von Bedeutung, man kann sie auch lustig schreiben. Auf diese Weise macht man diese Bei-

träge auch für die eigenen Freunde lesbar. Diese Beiträge nur für sich selbst zu veröffentlichen, ist nicht empfehlenswert. Es ist nämlich durchaus möglich, dass einem der Betreiber auf die Schliche kommt und das Täuschungsmanöver erkennt. Er wird dann die Beiträge ignorieren (oder schlimmstenfalls den Urheber sogar aus dem Dienst ausschließen). Ob die Inhalte tatsächlich ignoriert werden, kann man allerdings nicht überprüfen – es ist nur möglich, der Eventualität vorzubeugen. Der Inhalt der Beiträge muss mindestens ein Schlagwort zu einem bestimmten Thema enthalten, so dass das System auf diesen Reiz reagiert und das Thema auch registriert.

Tom hat, nachdem er von dieser Möglichkeit erfahren hat, einige weitere Beiträge veröffentlicht:

Mein neues Auto ist transparent.

Windows ist fehlerfrei!

Der DAX klettert – Na dann wird das Wetter morgen ja schön.

Solche Sprüche reichen durchaus aus, um dem sozialen Netzwerk Anreize für Werbung zu geben, und können ohne weiteres veröffentlicht werden. Sie gelten einfach als Witze oder werden von den meisten Nutzern ignoriert. Toms ursprüngliche Aussage, dass er Vegetarier ist, hat damit für den Auswertungsmechanismus der sozialen Netzwerke nur noch ein Viertel des ursprünglichen Werts, da die anderen Aussagen ebenfalls ausgewertet werden. Als Ergebnis muss Tom jetzt nur noch in jeder vierten Werbeanzeige etwas über Kochbücher für Vegetarier lesen.

Aufbau einer virtuellen Identität

Die zweite Möglichkeit der Egalisierung eines Beitrags besteht darin, sich eine virtuelle Identität aufzubauen. Der Gedanke hinter dem Verfahren ist, dass es belanglos ist, ob die Betreiber persönliche Daten ermitteln können, wenn diese ohnehin nicht stimmen beziehungsweise wenn sie mit dem Ziel, den Betreiber zu täuschen, angelegt wurden.

Dafür ist es allerdings erforderlich, sich genau zu überlegen, wie sich die eigenen Interessen – die man ja schließlich auch noch verfolgen möchte, wenn man mit seinen Freunden kommuniziert – mit einer virtuellen Identität vereinbaren lassen, die mit der eigenen Person möglichst wenige Gemeinsamkeiten hat.

In Toms Beispiel war das die Verzerrung der Information, dass er Vegetarier ist. Er würde demnach entweder angeben, er sei Veganer, oder er würde so tun, als sei er kein Vegetarier. Dieses Verhalten müsste Tom auf alle seine Eigenschaften anwenden: Entweder er verstärkt/dramatisiert eine Eigenschaft oder er stellt sie abgeschwächt dar beziehungsweise egalisiert sie.

Das wichtigste bei beiden Varianten ist es, nie auf eine Werbebotschaft, die tatsächlich interessant ist, zu klicken. Wurde das Interesse wirklich geweckt, kann man das Produkt immer noch in einer Suchmaschine suchen, aber ein Klick auf die Werbeanzeige bestätigt dem Dienstbetreiber das Interesse. Auf diese Weise werden zukünftig verstärkt derartige Werbeanzeigen auch mit Manipulationscharakter angezeigt werden.

Beachten muss man allerdings, dass man die Produkte, die in den in Google-Diensten geschalteten Werbeanzeigen angepriesen werden, natürlich nicht über die Google-Suchmaschine suchen darf, da die Daten aller Google-Dienste zentral zusammengefasst werden. Dies geht indirekt aus den Datenschutzerklärungen Googles hervor[13]. Dort ist nachzulesen, dass Informationen über eine Person von allen Google-Diensten gesammelt und gespeichert werden. Da man in der Regel nur ein Google-Konto besitzt, werden diese Informationen also zusammengeführt.

Möchte man sich ein Produkt, auf das man in einer Werbeanzeige aufmerksam wurde, näher ansehen, sollte man es in einer anderen Suchmaschine suchen. Es bietet sich ohnehin an, regelmäßig die Suchmaschinen zu wechseln, damit die Betreiber nicht allzu viele Daten über ihre Nutzer erhalten. Es gibt eine ganze Reihe von Suchmaschinen, darunter auch sogenannteMeta-Suchmaschinen wie Search.com (leider wurde das hervorragende Scroogle vor einiger Zeit eingestellt).

Stellt man an eine solche Maschine eine Frage, leitet sie die Meta-Suchmaschine an verschiedene Suchmaschinen weiter und zeigt die Ergebnisse dann auf einer Seite an. Auf diese Weise bleibt der Anwender also anonym, selbst wenn die Daten des Anfragenden gespeichert würden. Eine echte anonyme Suchmaschine ist DuckDuckGo.com, sie speichert die Daten der Anfragenden nicht und kann sogar direkt aus dem anonymen TOR-Netzwerk[14] unter der Adresse 3g2upl4pq6kufc4m.onion ohne den Umweg über einen Internet-Gateway angesteuert werden. Normale, aber beliebte Suchmaschinen sind Microsofts Bing, Yahoo, Ask.com, und MSN Live Search. Die Dienste Web.de, GMX und T-Online suchen über Google, sind also als Maßnahme gegen das Datensammeln weniger zu empfehlen. Weitere Suchmaschinen bieten unter anderem Altavista, Fastbot, Freenet-Suche, Hotbot und Wikipedia.

Nutzer von Firefox oder SeaMonkey stellen eine neue Suchmaschine im Eingabefeld rechts oben im Browser ein, sie müssen nur das Pulldown-Feld aufklappen und die Auswahl aus den angebotenen Maschinen treffen.

Es können aber auch Suchmaschinen, die an dieser Stelle nicht voreingestellt verfügbar sind, in den Browser integriert werden, wenn es für sie eine Mozilla-Erweiterung gibt, wie zum Beispiel für DuckDuckGo. Im Dialog Liste der Suchmaschinen verwalten, (Bild 3.2 auf der nächsten Seite) der über das nach unten weisende Dreieck im Suchen-Fenster und dort unter Suchmaschinen verwalten... angezeigt wird, wird die Zeile Weitere Suchmaschinen hinzufügen... angeklickt. Im Hauptfenster öffnet sich die Seite für die Suchmaschinen auf *https://addons.mozilla.org*. Ist die gewünschte Suchmaschine angezeigt, klickt man ihren Button Zu Firefox hinzufügen (oder Zu Seamonkey hinzufügen). Ruft man den Dialog erneut auf, ist die Liste ergänzt (Bild 3.2). DuckDuckGo findet man nicht auf Anhieb, deshalb gibt man in das in Bild 3.2 hinter dem Suchmaschinendialog halb verdeckte Suchfenster mit dem grünen Button den Namen der Suchmaschine ein, die dann in einer Liste passender Addons angeboten wird.

[13] Siehe http://www.google.de/policies/privacy/

[14] Weitere Informationen zu diesem kostenlosen Anonymisierungs-Netzwerk findet man auf seiner Webpräsenz unter https://www.torproject.org/

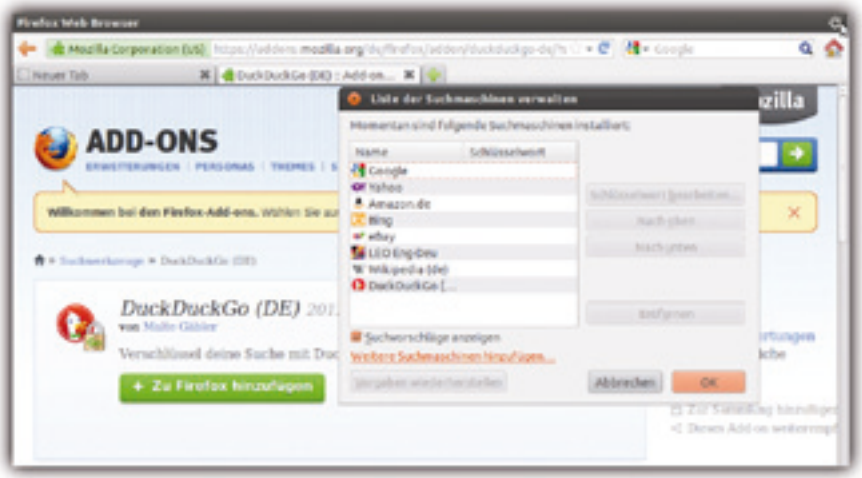

BILD 3.2 So wird im Firefox eine andere Suchmaschine eingestellt

In Browsern, wo es nicht so einfach ist, die Suchmaschine zu wechseln, sollte man die alternative Suche entweder direkt durch die Angabe der URL beginnen oder die Übernahme der Suchmaschinenadresse beispielsweise in die Favoriten überlegen.

Irregeführte Gesichtserkennung

Vor allem in den großen sozialen Netzwerken ist die Gesichtserkennungsfunktion direkt integriert. Der Betreiber kann auf dieser Grundlage mit einer gewissen Sicherheit eine Person namentlich identifizieren, sobald sie einmal markiert wurde[15]. Diese Gesichtserkennungsfunktion kann jedoch ganz einfach getäuscht werden und sogar ohne größeren Aufwand. Dazu benötigt man lediglich ein computergeneriertes Durchschnittsgesicht, das Merkmale möglichst vieler menschlicher Gesichter enthält. Solche Bilder werden durch sogenanntes Morphing erzeugt. Diese spezielle Technik erzeugt Übergänge in Bild (und Farbe). Beim Morphing wird ein Quellbild mit geeigneten Transformationen so verändert, dass daraus ein Zielbild entsteht. Beim Erzeugen eines Durchschnittsgesichtes wird versucht, ein möglichst realistisches Gesicht darzustellen, das so genau wie möglich zwischen zwei Gesichtern liegt. Wird dieses Verfahren auf möglichst viele Gesichter angewandt, erhält man die gemeinsamen Merkmale möglichst vieler Gesichter. Die Ergebnisse dieses Morphing-Schritts werden anschließend auf die gleiche Weise wieder miteinander kombiniert, bis schließlich ein Bild entsteht, nämlich das gesuchte Durchschnittsgesicht. Man kann sich diesen Vorgang wie das Durchlaufen eines Binärbaums in umgekehrter Reihenfolge, also von den Blättern zur Wurzel, vorstellen (Bild 3.3).

[15] Die Biometrie erreicht allgemein eine Trefferquote bis zu 90 Prozent.

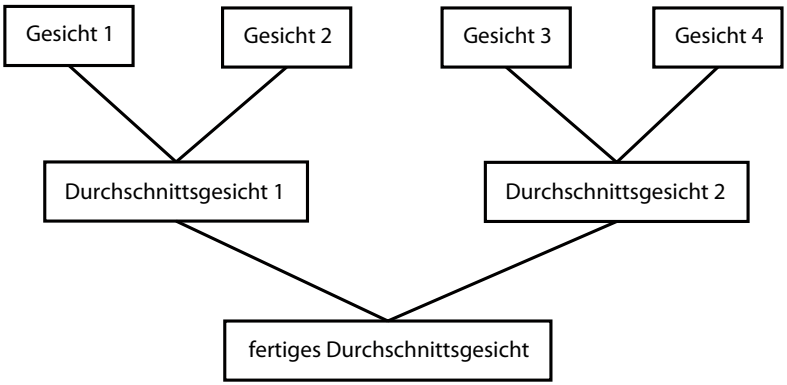

BILD 3.3 Ablauf beim Morphing eines Durchschnittsgesichts

Auf einem solchen Durchschnittsgesicht[16] (Bild 3.4) kann man sich dann als Benutzer verlinken. Die Gesichtserkennung des sozialen Netzwerkes schlägt dann auf nahezu jedes reale Gesicht an und spielt verrückt. Damit die Verlinkung nicht als Täuschung erkannt und verworfen wird, sollte man das entsprechende Gesicht in unterschiedliche Bilder einbetten und sich entweder auf allen verlinken oder sich auf unterschiedliche Durchschnittsgesichter verlinken.

BILD 3.4 Gemorphte Durchschnittsgesichter von http://beautycheck.de/cmsms/index.php/durchschnittsgesichter

[16] Man findet solche Gesichter beispielsweise auf http://beautycheck.de/cmsms/index.php/durchschnittsgesichter

Anschließend ist es für die Gesichtserkennung des sozialen Netzwerkes praktisch unmöglich, sinnvolle Vorhersagen zu machen, ob sich die Person auf einem Bild befindet oder nicht, da nahezu jedes Gesicht Merkmale aufweist, die auch in dem als Nutzer identifizierten Durchschnittsgesicht enthalten sind. Der Benutzer kann nun nicht mehr automatisch identifiziert werden. Es müsste manuell gefiltert werden, was aber viel zu aufwendig ist, weshalb das Morphing für eine gewisse Anonymität sorgt.

Durch Wechsel des Accounts

Nicht jeder möchte regelmäßig Zeit dafür aufwenden, den Betreiber zu täuschen oder möchte es seinen Freunden zumuten, zwischen relevanten und nicht relevanten Inhalten zu unterscheiden. Hier bietet sich das regelmäßige Wechseln des eigenen Benutzerkontos als weitere Möglichkeit an, dem Datenmissbrauch durch die Betreiber vorzubeugen.

Die Idee dahinter ist, dass der Betreiber immer nur über einen relativ geringen Zeitraum Daten sammeln kann, so dass zum Zeitpunkt, an dem das Benutzerkonto wieder gewechselt wird, noch nicht genug Daten vorliegen, um tatsächlich etwas mit ihnen anfangen zu können. Beim neuen Benutzerkonto fängt der Betreiber wieder bei Null an und das Spiel beginnt von vorne.

Soweit zumindest die Theorie. In der Praxis müssen einige Hürden überwunden werden, damit diese Technik auch wirklich zum Erfolg führt.

Besonders wichtig sind unterschiedliche Namen für das alte und das neue Benutzerkonto. Legt man es auf den gleichen Namen an, kann es passieren, dass der Dienst automatisch die Übereinstimmung der realen Personen hinter den beiden Benutzerkonten erkennt und dann die Daten der beiden Konten zusammenführt. Dieses Risiko besteht zwar auch bei der Wahl unterschiedlicher Namen, kann jedoch durch weitere Maßnahmen minimiert werden.

So sollte der Wohnort – wenn man ihn überhaupt angeben möchte – nicht in den beiden Konten identisch sein, ebenso müssen sich die Interessen und das Profilbild auf jeden Fall unterscheiden.

Der größte Schwachpunkt dürfte die nahezu identische Freundesliste beider Konten sein, die sich aufgrund der gleichbleibenden Freunde natürlich nicht verhindern lässt. Daher ist es sinnvoll, auch das alte Konto in die Freundesliste aufzunehmen, so dass es sich beim neuen Konto auch um einen nahen Freund des alten Kontos handeln könnte. Zudem sollten sich die Freundeslisten nie hundertprozentig gleichen. Es ist nicht schwer, einige zusätzliche Freunde zu finden und oft auch keine schwere Entscheidung, einen Freund, mit dem man ohnehin noch nie kommuniziert hat, aus der Freundesliste zu streichen.

Vor allem in Zeiträumen, in denen beide Konten gleichzeitig genutzt werden, sollte man darauf achten, dass vor dem Login in das jeweils andere Konto stets die Chronik sowie die Cookies gelöscht werden oder dass mit unterschiedlichen Browsern gearbeitet wird. Andernfalls können die sozialen Netzwerke gegebenenfalls feststellen, dass vom glei-

chen PC in beide Konten eingeloggt wurde. Dies verhält sich im Grunde ganz ähnlich zu der ab Seite 102 in Kapitel 3.3.1 beschriebenen Technik.

Möchte man sich von einem Account ab- und direkt in einem anderen anmelden, ist zusätzlich darauf zu achten, dass der Betreiber nicht an der IP-Adresse feststellen kann, dass es sich um die gleiche natürliche Person handelt. Daher sollte die Verbindung zum Internet über den Router kurzzeitig getrennt und anschließend wieder neu aufgebaut werden, so dass man vom Internetprovider eine neue IP-Adresse zugewiesen bekommt.

Wie im Browser die Chronik und Cookies gelöscht werden, ist dem Anhang zu entnehmen. Dort ist auf Seite 169 auch beschrieben, wie man eine neue IP-Adresse abruft.

3.3 Missbrauch zusätzlicher Daten

Würden die Betreiber lediglich die vom Benutzer freiwillig angegebenen Daten erfassen, könnte man sich entspannt zurücklehnen und in dem Wissen, dass der Betreiber lediglich die Daten erfährt, die man selbst preisgibt, gemütlich einen Kaffee trinken und sich dabei überlegen, was man denn überhaupt weitergeben möchte. Allerdings haben die Betreiber der sozialen Netzwerke die lästige Angewohnheit, auf eigene Faust Daten zu ermitteln, um zusätzliche Informationen über ihre Mitglieder zu erhalten. Das beginnt bereits in den sozialen Netzwerken selbst. Hier speichern die Betreiber die Zugriffe auf die Profile anderer Personen, obwohl diese zumeist für den Benutzer gar nicht angezeigt werden können. Dadurch erfahren sie, welche anderen Mitglieder einen Benutzer besonders interessieren und können so ihr Bild von ihm, das anhand der Analyse seiner Kommunikation gewonnen werden konnte, weiter präzisieren.

Natürlich ermitteln die Betreiber auch Daten über das Computersystem des Benutzers, so wie es heutzutage von nahezu jeder Website getan wird.

Recht leicht herauszufinden ist, mit welchem Browser der Benutzer den Dienst aufruft. Weil der Browser beim Webserver anklopft und um Übermittlung der Webseite bittet, kann diese Anfrage (genauer: ihr Header) daraufhin untersucht werden, welcher Browser darin vermerkt ist, welches Betriebssystem auf dem PC des Benutzers installiert ist und welche Spracheinstellungen gewählt sind. Wie einfach das ist, kann jeder selbst auf Webseiten wie beispielsweise http://www.ip-secrets.info/ erfahren.

Der IP-Header kann bei einigen Browsern auch unterdrückt beziehungsweise ein alternativer Header kann angegeben werden (Bild 3.5), unter dem dann die Anfragen gesendet werden. Allerdings ist das nicht unbedingt ratsam, da viele Webseitenbetreiber speziell auf bestimmte Browser angepasste Versionen der Seite ausliefern, die dann unter Umständen im tatsächlichen Browser nicht richtig dargestellt werden.

Aber viel bedenklicher als die Browserkennung ist, dass der Betreiber anhand einer IP-Adresse herausfinden kann, wo sich der Benutzer gerade befindet (die sogenannte Lokalisierung beziehungsweise Geo-IP). Diese Abfrage ist keine spezifische Eigenheit

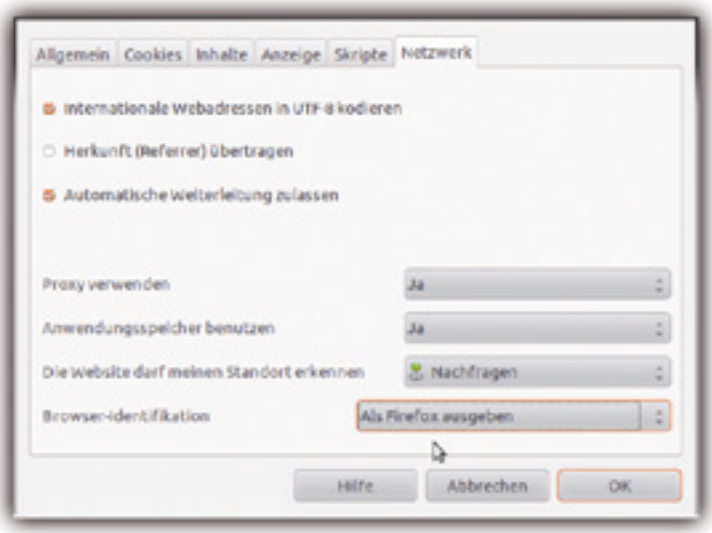

BILD 3.5 Alternativen Header einstellen (hier unter Opera)

sozialer Netze und kann prinzipiell von jedem Webseitenbetreiber durchgeführt werden. Allerdings ist das in sozialen Netzwerken besonders bedenklich, da sich hier die IP-Adresse direkt einer natürlichen Person zuordnen lässt. Damit kann zwar nicht ganz exakt festgestellt werden, wo sich das Mitglied genau befindet, jedoch ist eine gewisse Tendenz erkennbar. So ist meist problemlos feststellbar, in welchem Bundesland, immer jedoch ist exakt zu erkennen, in welchem Land sich jemand befindet. Grund hierfür sind die IP-Nummernkreise der jeweiligen Internetprovider und wie diese sie ihren Kunden regional zuteilen.

Anhand dieser Daten kann auch festgestellt werden, ob jemand gerade unterwegs ist oder sich zuhause befindet. Mit Sicherheit lässt sich sagen, dass eine Person zuhause ist, wenn sie sich von der Region aus einloggt, von der sie sich fast immer einloggt. Im Umkehrschluss kann man davon ausgehen, dass sie unterwegs ist, wenn sie sich von einem Standort einloggt, der außerhalb dieser Region liegt.

Daten wie diese kann mit mehr oder weniger großem Aufwand jeder Netzwerkbetreiber ermitteln. Ihre Ermittlung lässt sich aber durch eine spezielle Internetverbindung umgehen, die als Tunnel durch das Internet gelegt ist und auf der die Daten verschlüsselt übertragen werden. Bei einem solchen VPN (Virtual Private Network) loggt sich der Benutzer auf einem Server des VPN-Providers ein und sendet deshalb automatisch alle Anfragen, die er normalerweise direkt an die besuchte Webseiten senden würde, an den VPN-Server. Dieser leitet sie dann an ihr Ziel weiter. Die Zielseiten können lediglich die IP-Adresse und den Header des VPN-Servers sehen und senden ihre Antwort an diesen Server, der die Antwort dann an den Benutzer weiterleitet. Die Funktionsweise einer VPN-Verbindung ist in Bild 3.6 dargestellt.

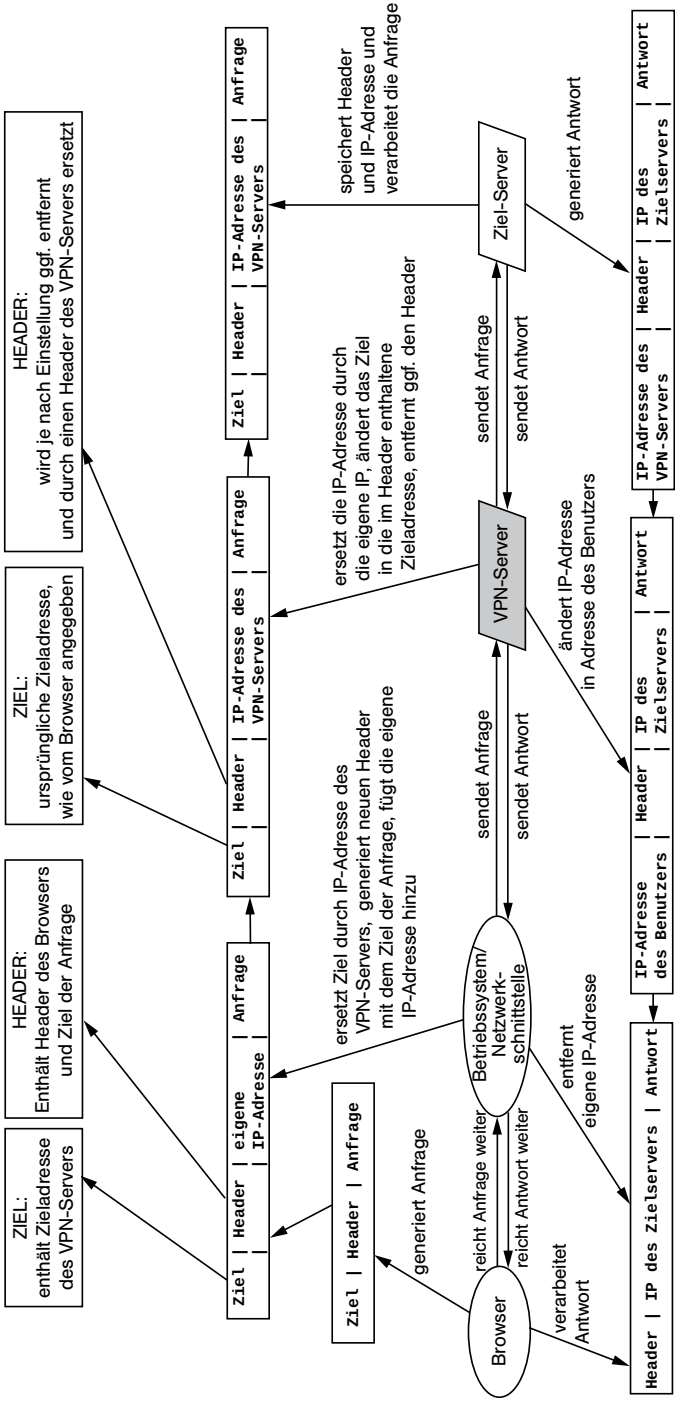

BILD 3.6 Funktionsweise einer VPN-Verbindung

Es gibt eine Reihe meist kostenpflichtiger VPN-Anbieter, deren Namen mit einer Suchmaschine gefunden werden können. Allerdings ist der Aufwand zum Einrichten der VPN-Software auf dem PC recht hoch und man kann sich zu Recht fragen, ob jemand mit einem derart hohen Sicherheitsbedürfnis überhaupt Mitglied in einem sozialen Netz werden sollte. Aus diesem Grund soll dieses Thema hier auch nicht weiter vertieft werden.

Die Betreiber der großen sozialen Netzwerke haben aber auch zahlreiche andere Methoden in petto, die im Internet zwar nicht unüblich sind, jedoch nur selten so massiv zum Einsatz kommen wie in den sozialen Netzwerken. Mit diesen Methoden ist es möglich, eine immense Flut an Informationen zu erhalten, die nur äußerst schwer zu bewältigen und auszuwerten ist. Mit Hilfe der großen Serverfarmen gelingt das den Betreiber offensichtlich dennoch, so dass gerade diese Methoden die Datensammelwut der Betreiber so bedenklich machen. Mittlerweile erscheinen viele Betreiber so dreist, dass eigentlich nur noch die Technik in ihrem Verlangen nach zusätzlichen Informationen Grenzen setzt. Das Erste Deutsche Fernsehen veröffentlichte im Mai 2012 einen Bericht zum diesjährigen Grundrechtereport, in dem soziale Netzwerke wie Facebook als Datenkraken gehandelt werden[17].

3.3.1 Browser-Historie (Gefällt-mir-Button)

Der einst von Facebook eingeführte *Gefällt mir*-Button zeigt den Freunden, dass einem der Inhalt einer Website oder die Seite selbst gefällt. An sich ist das ja eigentlich nicht schlimm, doch die Art und Weise, wie Facebook und mittlerweile auch andere Betreiber dieses Konzept ausnutzen, ist beängstigend. Das gleiche gilt für den *+1*-Button von Google+, dem bisher noch nicht so viel Beachtung beigemessen wurde.

Aber warum eigentlich soll es gefährlich sein, wenn man angeben kann, dass einem eine Seite gefällt? Wenn das wirklich so schlimm ist, braucht man diesen Button doch einfach nicht zu benutzen und schon hat sich die Gefahr in Luft aufgelöst – könnte man meinen. Das ist leider nicht richtig, ganz im Gegenteil: Sogar Webseitenbesucher, die nicht in sozialen Netzwerken wie Facebook oder Google+[18] registriert sind, müssen sich Gedanken machen.

Mit dem Gefällt-mir-Button[19] ist es den Betreibern möglich, mehr oder weniger lückenhaft die Browserhistorie (oft auch als Verlauf beziehungsweise Chronik bezeichnet) zu ermitteln. Sie erfahren also, welche Internetseiten man mit dem Browser besucht hat. Kennt der Dienst die besuchten Webseiten, weiß er genau, für was sich sein Mitglied interessiert und kann Werbung ganz individuell auf ihn abstimmen. Aber wer weiß, was der Netzbetreiber sonst noch alles mit den Daten über die Benutzeraktivitäten macht?

[17] Siehe http://www.tagesschau.de/grundrechtereport102.html

[18] Bislang ist es nur diesen beiden Betreibern gelungen, ein solches Konzept flächendeckend umzusetzen.

[19] Im folgenden soll die Bezeichnung Gefällt-mir-Button sowohl für den gleichnamigen Button von Facebook als auch für den +1-Button von Google stehen.

BILD 3.7 Facebooks Gefällt-mir-Button ist auf zahlreichen Seiten zu finden

Nicht umsonst macht sich beispielsweise Facebook die Arbeit, Benutzerdaten in 57 Kategorien abzulegen, die rund 1200 Seiten umfassen. Es ist zwar möglich, dass diese Daten tatsächlich „nur" für den Verkauf individualisierter Anzeigenplätze genutzt werden, allerdings ist nicht von der Hand zu weisen, dass mit den Daten noch weitere Geschäfte gemacht werden könnten.

Technik

Es fragt sich natürlich, wie es möglich ist, dass Firmen wie Facebook oder Google in der Lage sind, den Browserverlauf eines Benutzers festzustellen. Wären beide Firmen Hersteller von Webbrowsern, wäre die Antwort ziemlich einfach: Die Benutzerdaten werden im Hintergrund an die Betreiber übertragen. Google war als Produzent des Webbrowsers Google Chrome für derartige Spionage bekannt, hat dieses Ärgernis aber angeblich abgestellt.[20] Allerdings werden E-Mails von Nutzern des Maildienstes Gmail auch heute noch automatisch erfasst und ihr Inhalt nach Schlagworten gefiltert und ausgewertet[21].

Aber dennoch haben die beiden Unternehmen Facebook und Google anscheinend eine solch besondere Stellung im Internet, die es ihnen erlaubt, die Browserhistorie der Internetbesucher zu erfassen. Beide bieten Dienste an, die von mehreren hundert Millionen Menschen täglich genutzt werden. Der Begriff Google hat sich schon vor mehreren Jahren zu einem Synonym von Suchmaschine entwickelt. Ebenso ist Facebook der Inbegriff eines sozialen Netzwerkes für Millionen von Mitgliedern.

Aber dieser Umstand alleine ermöglicht es den Unternehmen nicht, die Browser-Historie der Benutzer auszulesen. Es ist vielmehr das Konzept des Gefällt-mir-Buttons, der es ermöglicht, die besuchten Seiten zu speichern. Dabei wird nicht der Verlauf oder die

[20] Wer einen Chrome sucht, der nichts zu Google meldet, sollte SRWare Iron von http://www.srware.net/software_srware_iron_download.php installieren.

[21] Siehe auch http://support.google.com/mail/bin/answer.py?hl=en&answer= 1304609

Chronik ausgelesen, das kann technisch gesehen ein Websitebetreiber gar nicht. Die Seitenaufrufe werden über ein anderes System erfasst: Facebook beziehungsweise Google+ versprechen den Betreibern von Websites, von den Vorteilen des sozialen Netzwerkes kostenlos profitieren zu können. Sie müssen dazu lediglich einen kleinen Codeschnipsel, der zur Darstellung des Gefällt-mir-Buttons verantwortlich ist, in ihre Webseite einbinden. Zuvor können sie Facebook beziehungsweise Google optional noch etwas über die Webseite mitteilen, beispielsweise über den Inhalt und dergleichen.

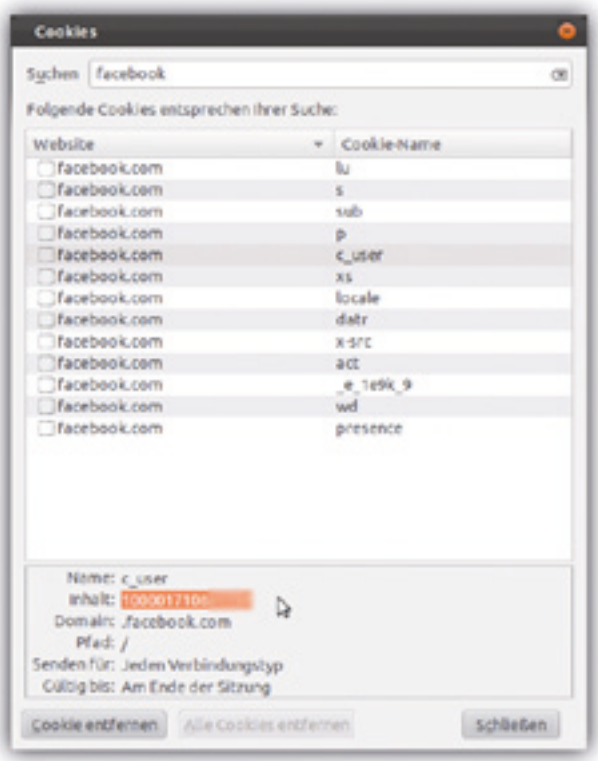

BILD 3.8 Das c_user-Cookie von Facebook und sein Inhalt: die eindeutige Benutzerkennung des entsprechenden Facebook-Nutzers

Die Betreiber von Webseiten profitieren auch tatsächlich von sozialen Netzwerken, wenn sie den Button in ihre Seiten einbinden, denn über ihn machen die Besucher, denen die Seite gefällt und die ihn anklicken, automatisch Werbung bei ihren Freunden für diese Seite. Und zwar ohne dass die Freunde das direkt als Werbung empfinden, sondern vielmehr der Empfehlung eines Freundes folgen, wenn sie die Seite ebenfalls besuchen.

Der Codeschnipsel zur Darstellung des Buttons enthält aber auch eine Falle: Hinter dem Button steckt ein ganzes Programm, das auf dem PC des Anwenders ausgeführt wird.

Mit JavaScript[22] und AJAX[23] wird vom PC aus eine Verbindung zu einem Server von Facebook oder Google aufgebaut. Über diese Verbindung wird dem Betreiber des sozialen Netzwerkes mitgeteilt, dass jemand gerade die Seite besucht, unabhängig davon, ob der Gefällt-mir-Button betätigt wurde oder nicht. Nun können die Betreiber des sozialen Netzwerkes den Benutzer identifizieren, und zwar über sogenannte Cookies (Bild 3.8).

Cookies sind kleine Textdateien, die auf der Festplatte des Benutzers abgelegt werden und die meist eine Kennung enthalten, die den Benutzer identifizierbar macht. Diese Cookies können vom Betreiber des sozialen Netzwerks ausgelesen werden, wobei die Benutzerkennung an den Server übertragen wird. So erfährt er, dass der Benutzer, dem die entsprechende Kennung zugeordnet ist, gerade diese Seite betrachtet. Das funktioniert auch noch, nachdem sich der Benutzer abgemeldet hat. Früher wurde einfach ein Cookie mit der Benutzerkennung beim Ausloggen nicht gelöscht. Als man Facebook deshalb jedoch an den Pranger stellte, behauptete man dort, es handle sich dabei um einen Fehler und änderte das Verfahren innerhalb weniger Stunden. Nun wird die Benutzerkennung mit dem Logout vernichtet.

Es gibt es noch eine andere Möglichkeit, mit der auch nicht-registrierte Benutzer auf diese Weise ausspioniert werden können: Beim Besuch der Seite wird geprüft, ob der Besucher bereits über ein Cookie mit einer Kennung verfügt. Hat er sich nun ausgeloggt, ist keines vorhanden. In diesem Fall wird ihm eine neue, nicht vergebene Kennung zugewiesen, unter der seine Daten gespeichert werden. Auch von nicht registrierten Anwendern, also von Nutzern, die überhaupt kein Facebook-Konto besitzen, werden auf diese Weise Daten erfasst. Meldet sich ein Benutzer nun wieder an, wird seine vorübergehende Kennung ausgelesen; womöglich werden die unter dieser Kennung ermittelten Daten sogar auf seine reale Kennung überschrieben, so dass den Daten eine natürliche Person zugeordnet werden kann.

In der Frankfurter Allgemeinen Zeitung wurde bereits 2010 über derartige Paradigmen berichtet, die sich bis heute nicht grundlegend geändert haben.[24] Besitzt der Internetnutzer kein Benutzerkonto, werden die Daten dauerhaft unter der vorübergehenden Kennung gespeichert. Damit können diesem Benutzer dennoch auf ihn abgestimmte Werbebotschaften eingeblendet werden, wenn er Seiten besucht, über die Werbung aus den sozialen Netzwerken abgerufen wird. Sollte sich ein solcher Internetnutzer jemals in einem entsprechenden sozialen Netzwerk registrieren, hat der Betreiber bereits zahlreiche Daten über ihn und kennt ihn genau – ohne dass der Benutzer das vermuten würde.

Wie bereits erwähnt sind Facebook und Google+ die einzigen sozialen Netzwerke, denen eine flächendeckende Umsetzung des Gefällt-mir-Buttons gelungen ist. Das liegt vor allem daran, dass Facebook der absolute Platzhirsch bei sozialen Netzwerken ist.

[22] Eine Skriptsprache, mit der Webseiten dynamisch gestaltet werden. Die JavaScript-Programme werden dabei auf dem PC des Besuchers ausgeführt.

[23] Mit ***A****synchronous* ***J****avaScript* ***a****nd* ***X****ML* werden nach Aufbau einer Webseite im Browser zwischen dem Anwender-PC und dem Server Daten ausgetauscht.

[24] Siehe auch http://www.faz.net/aktuell/feuilleton/medien/soziale-netzwerke-facebook-weiss-alles-ueber-uns-1936297.html

Google+ dagegen ist ein Unternehmensbereich des Konzernriesen Google und hat dadurch ganz andere Mittel als die meisten anderen Netzwerke. Google kontrolliert gewissermaßen das Internet, denn alleine die gleichnamige Suchmaschine hat mit einer Verbreitung von über 81 Prozent bei den Internetsurfern[25] eine solche Vormachtstellung, dass bei ihrem Zusammenbruch beinahe eine Katastrophe für die Betreiber von Websites und ihre Besucher ausgelöst würde.

Man kann also sagen, dass nur die bedeutendsten Unternehmen der Sparte soziale Netzwerke in der Lage dazu sind, eine Infrastruktur wie diese umzusetzen. Allerdings ist das nicht weniger bedenklich, schließlich besitzen gerade diese Unternehmen ohnehin die meisten Daten von ihren Benutzern und auch von Fremden und können somit am effizientesten Profile über uns Internetsurfer anlegen.

Gegenmaßnahmen

Natürlich gibt es auch Möglichkeiten, sich gegen die von den Betreibern großangelegten Spionageattacken erfolgreich zur Wehr zu setzen. Sie beruhen darauf, jene Skripte zu blockieren, die mit den Gefällt-mir-Buttons eingebunden werden.

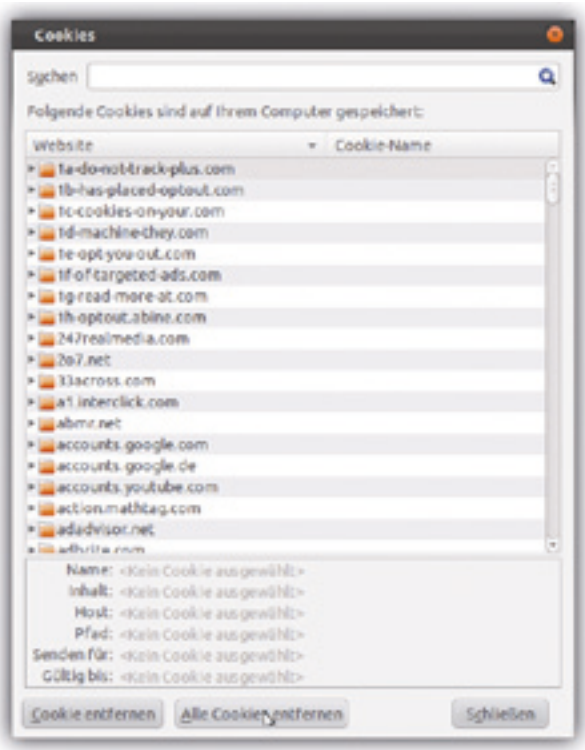

BILD 3.9 Browsereinstellung zum Löschen von Cookies

[25] Siehe http://www.seo-united.de/suchmaschinen.html

Die einfachste, aber auch am wenigsten effiziente Möglichkeit ist sicherlich, von Zeit zu Zeit die Cookies zu löschen (Bild 3.9). Dabei versucht man, die Verbindung zwischen sich und den mit seinem Namen verknüpften Daten zu trennen. Ist man jedoch beispielsweise bei Facebook oder Google+ registriert, ist dieser Weg ziemlich schwierig. Man muss stets darauf achten, dass man vor dem Login alle Cookies des Betreibers löscht. Weiter darf man, während man eingeloggt ist, keine Websites mit einem Gefällt-mir- oder +1-Button besuchen (dies sind mittlerweile recht wenige) und nach dem Logout muss man wiederum alle Cookies löschen. Zudem muss man von Zeit zu Zeit zwischen den Logins relevanten Cookies löschen.

In vielen Browsern kann man einstellen, dass die Cookies beim Schließen des Browsers automatisch gelöscht werden. Diese Einstellung ist sinnvoll und sollte möglichst generell gewählt werden, um der Spionage vorzubeugen. Ist diese Einstellung nicht möglich oder möchte man die entsprechenden Cookies löschen, während der Browser geöffnet ist, muss man mit der Suchfunktion quasi die Stecknadel im Heuhaufen finden. Am besten löscht man alle Cookies des jeweiligen Anbieters, also beispielsweise alle Cookies der Seiten google.de und google.com. Auch bei Facebook sollte man, falls möglich, alle Cookies löschen. Auf jeden Fall muss das mit *c_user* bezeichnete Cookie gelöscht werden: Es enthält die User-ID des Facebook-Accounts und kann so direkt dem eigenen Benutzerkonto zugeordnet werden.

Mittlerweile ist es jedoch nicht mehr nötig, die Cookies jedes Mal händisch zu löschen. Mit Hilfe von Erweiterungen für den Webbrowser kann man das sogenannte Tracking (Verfolgen von Besuchern) durch bestimmte Webseiten automatisch blockieren. Dabei wird verhindert, dass Programm-/Skriptcode, der von bestimmten Domains aus eingebunden wird, überhaupt geladen (beziehungsweise ausgeführt) wird. So wird es für die Betreiber der entsprechenden Netzwerke unmöglich, durch die Gefällt-mir- und die +1-Buttons zu ermitteln, welche Seite ein Benutzer besucht hat.

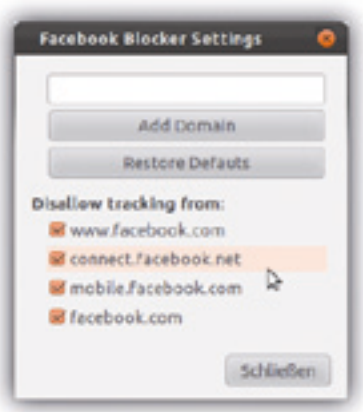

BILD 3.10 Die Einstellungen des Facebook Blocker 1.4

Ein Addon, das den Gefällt-mir-Button von Facebook erfolgreich blockt und für zahlreiche Browser verfügbar ist, ist der sogenannte *Facebook Blocker*. Er ist für Safari 5, Google Chrome, Firefox 3 sowie Opera 11 erhältlich und kann für diese Plattformen heruntergeladen werden.[26]

Für den aktuellen Firefox (leider nicht für SeaMonkey) gibt es ebenfalls ein Plugin[27], Vorgängerversionen sind abwärts bis Firefox 3.5 erhältlich. Durch einen Klick auf +ZU FIREFOX HINZUFÜGEN wird ein automatischer Installationsvorgang gestartet, der das Addon auf einfachem Wege in den Browser einbindet.

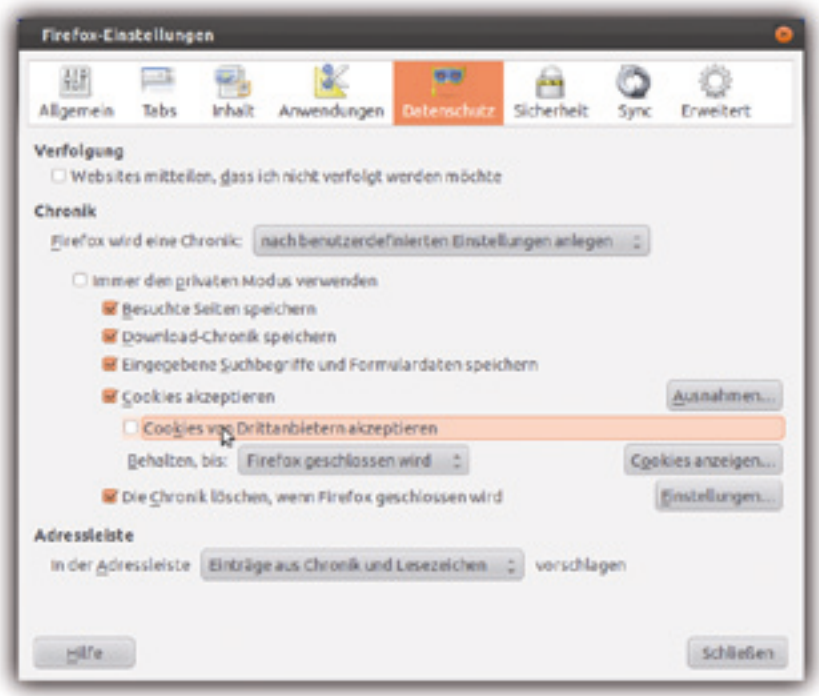

BILD 3.11 „Cookies von Drittanbietern akzeptieren“ im Firefox ausschalten

Das sogenannte Tracking im Firefox generell zu stoppen, ist leicht: Im EINSTELLUNGEN-Menü (unter Windows im Menü EXTRAS, bei Linux in BEARBEITEN und bei MacOS X im Menü FIREFOX zu finden) klickt man dafür auf den Reiter DATENSCHUTZ und entfernt das Häkchen bei COOKIES VON DRITTANBIETERN AKZEPTIEREN (Bild 3.11). Das verhindert, dass Cookies, die beispielsweise beim Besuch der Facebook-Seite angelegt wurden, ausgelesen werden können, wenn der Besucher auf einer Seite ist, die nicht zu Facebook gehört, aber einen Gefällt-mir-Button oder ähnliches von Facebook enthält. Der Besu-

[26] Die Bezugsquelle ist http://webgraph.com/resources/facebookblocker/

[27] Es kann von der Mozilla-Adresse https://addons.mozilla.org/de/firefox/addon/ Facebook-blocker/ installiert werden.

cher kann nicht mehr identifiziert werden und die Betreiber weder ihn noch seine Aktivitäten verfolgen.

Chrome und sein Open-Source-Bruder Chromium bieten eine ähnliche Möglichkeit. In den EINSTELLUNGEN werden unter dem Punkt DETAILS die CONTENT-EINSTELLUNGEN ausgewählt. Dort wird unter dem Punkt COOKIES das Häkchen an der Stelle DRITTANBIETER-COOKIES UND WEBSITEDATEN BLOCKIEREN (Chromium) beziehungsweise AUSNAHMEN IGNORIEREN UND DRITTANBIETER-COOKIES BLOCKIEREN bei Google Chrome gesetzt, um die Cookies von Drittanbietern zu sperren.

Den Besitzern des Internet Explorers von Microsoft stehen die vielfältigen Browser-Erweiterungen nicht zur Verfügung. Das Tracking lässt sich deshalb nur durch das Verbieten der Drittanbieter-Cookies blockieren. Dafür muss in den INTERNETOPTIONEN auf dem Reiter DATENSCHUTZ der Button ERWEITERT angeklickt und in der Spalte COOKIES VON DRITTANBIETERN auf BLOCKEN geklickt werden (Bild 3.12). Anschließend müssen alle geöffneten Fenster mit einem Klick auf OK wieder geschlossen werden, um die Änderung zu bestätigen.

BILD 3.12 Das Blockieren von Drittanbieter-Cookies in den Internet-Optionen von Windows (hier bei der Consumer Preview von Windows 8)

Um einen Blocker für das Tracking seitens Google zu finden, muss man deutlich länger suchen. Letztlich ist nur ein allgemeiner Blocker sinnvoll, der das Tracking durch bestimmte Seiten stoppt. Die einfachste Möglichkeit besteht darin, die Cookies von Drittanbietern nicht zu akzeptieren, aber es gibt auch Browser-Addons, die das nur für bestimmte Seiten tun. *DoNotTrackPlus* ist ein solches Addon für den Firefox[28]. Die Erweiterung ist auch für Google-Chrome beziehungsweise Chromium erhältlich. Allerdings ist vor allem bei Google Chrome der Sinn dieses Plugins unklar, sofern es gegen Google angewandt werden soll, da bekannt ist, dass Google Chrome im Hintergrund selbst Benutzerdaten an Google überträgt. Und das kann auch durch das Plugin nicht verhindert werden.

In den Datenschutzhinweisen von Chrome listet Google eine ganze Reihe von Fällen auf, in denen Chrome Daten an Google Server überträgt[29].

Das Plugin gibt es auch für Safari und selbst der Internet Explorer wird unterstützt, so dass er Facebook ebenfalls blockieren kann, da auch diese Funktion von DoNotTrackPlus unterstützt wird. Auf der Herstellerseite http://www.abine.com/dntdetail.php kann die jeweilige Version heruntergeladen werden. Sie blockiert bereits in der Standardkonfiguration nahezu alle Firmen, sozialen Netzwerke und Suchmaschinen, die versuchen, Daten über den Nutzer zu sammeln, gewährt dem Nutzer dabei jedoch trotzdem die entsprechenden Funktionen. So ist beispielsweise der Gefällt-mir-Button zwar sichtbar; solange er nicht gedrückt wird, werden aber keine Benutzerdaten an Facebook übertragen.

Eine Radikalkur gegen Facebook und Co. stellt das Eintragen der entsprechenden Server direkt in die hosts-Datei des PCs dar. Damit wird die Namensauflösung für diese Server im Internet abgeschaltet. Damit Facebook, Google und Twitter nicht mehr angesteuert werden können (und das ist wörtlich zu nehmen!), trägt man deren Server in diese Datei ein. Man findet sie unter Windows im Verzeichnis C:\Windows\ system32\ drivers \etc\[30], unter Linux und anderen unixartigen Betriebssystemen in /etc. In der Datei steht bei Einzelplatz-PCs meist nur die einzelne gültige Zeile

```
127.0.0.1 localhost
```

(alles hinter einem # Zeichen wird übergangen). In dieser Datei ergänzt man beispielsweise die folgenden Zeilen

```
127.0.0.1 facebook.com www.facebook.com twitter.com www.twitter.com
127.0.0.1 plus.google.com google-analytics.com www.google-analytics.com
127.0.0.1 accounts.google.com
127.0.0.1 www.addthis.com www.mister-wong.de delicious.com del.icio.us
```

[28] Es kann von der Adresse https://addons.mozilla.org/de/firefox/addon /donottrackplus/ einfach installiert werden, indem auf der Webseite auf die Schaltfläche Zu Firefox hinzufügen geklickt wird.

[29] Nachzulesen unter http://www.google.com/chrome/intl/de/privacy.html.

[30] Das C:\Windows gilt dann, wenn Windows auf Laufwerk C: in \Windows installiert ist (das sogenannte „WINDIR“) das man in einem CMD-Fenster mit dem Befehl echo %WINDIR% abfragen kann.

und verhindert damit, dass von diesem PC aus die entsprechenden Internetserver über ihre Namen angesteuert werden können. 127.0.01 ist nämlich die interne Adresse des lokalen PCs, auf die jetzt alle Anfragen auf die angegebenen Server umgeleitet werden. Indem man 127.0.0.1 durch die IP-Adresse oder die URL einer Webseite ersetzt, kann man die Anfragen auch an diese umleiten. Dies machen sich manchmal Hacker zunutze, die so beispielsweise die Benutzer eines Online-Banking-Systems auf eine gleich aussehende, aber gefälschte Seite umleiten, um an deren Bankdaten zu kommen.

Hinter www.addthis.com verbergen sich übrigens die Folgen-Buttons. Die hier gezeigten Server können beliebig ergänzt werden. Dabei muss man beachten, dass facebook.com und www.facebook.com unterschiedliche Servernamen sind und deshalb auch immer einzeln aufgeführt werden. (Das kann man sehen, indem man die zugehörigen IP-Adressen mit einem ping-Befehl ermittelt. Man gibt dazu einfach in ein Terminal oder in die Eingabeaufforderung von Windows folgenden Befehl ein:

`ping facebook.com` bzw. `ping www.facebook.com`

Anschließend erscheint in Klammern die jeweilige IP-Adresse der Server).

An dieser Stelle sei noch eine Warnung angebracht: Wer die hosts-Datei auf seinem Rechner verändert, greift in die Namensauflösung des eigenen Rechners ein. Macht man hier einen Fehler, kann es passieren, dass bestimmte Webseiten nicht mehr erreichbar sind. Man sollte diese Datei also nur bearbeiten, wenn man genau weiß, was man tut.

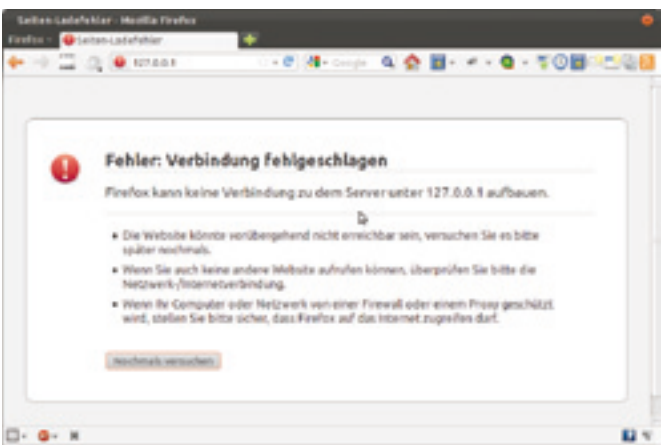

BILD 3.13 Durch das Verknüpfen mit dem Localhost unter 127.0.0.1 in der hosts-Datei werden Webserverzugriffe gewaltsam unterbunden

3.3.2 Positionsdaten

Seit dem Siegeszug von Smartphones werden sogenannte Apps auch für soziale Netzwerke entwickelt. Eine Facebook-App (Bild 3.14) ist bereits auf vielen Smartphones vorinstalliert, aber auch Apps für Twitter, XING oder myspace sind in Gebrauch. Vor allem

auf Android-Smartphones werden die einzelnen Google-Dienste (und damit auch Google+) teilweise oder vollständig in das Android-Betriebssystem eingebunden. Allerdings gibt es seit neuestem zusätzlich Apps für Google+.

So schön solche Apps auch sein mögen – häufig bergen sie im Hinblick auf Spionage durch die Betreiber der sozialen Netzwerke große Gefahren. Man braucht sich nur einmal die Liste an Berechtigungen, die man diesen Anwendungen erteilt, genauer ansehen, um deren Risikopotential zu erkennen.

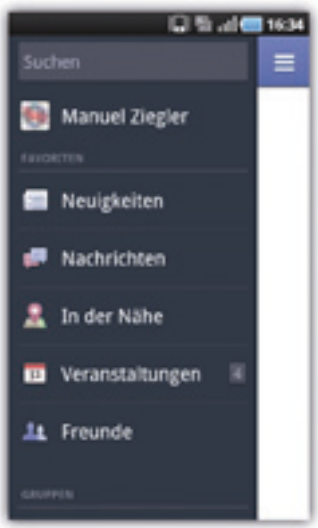

BILD 3.14 Die Facebook-App unter Android

Nicht selten werden Standortinformationen abgerufen und die auf dem Mobilgerät gespeicherten Daten durchsucht. Deshalb ist es empfehlenswert, schon bei der Installation solcher Apps aus dem jeweiligen App-Store zu ermitteln, welche Berechtigungen man der App durch die Installation verleiht und welche Berechtigungen auch wirklich notwendig sind. Beispielsweise räumt man diesen Prograämmchen häufig die Berechtigung ein, auf das Telefonbuch zuzugreifen, ohne dass diese Funktion für die entsprechende App wirklich notwendig wäre. Noch viel unnötiger ist es, ihr zu erlauben, Standortinformationen abzurufen. Dies gilt auch bei sozialen Netzwerken. Natürlich bringen manche Netzwerke Funktionen mit sich, die den Standort kennen müssen, beispielsweise dann, wenn man seine aktuelle Position in sozialen Netzwerken teilen möchte. Allerdings sind diese Funktionen meist ziemlich überflüssig und im Hinblick auf den Datenschutz sowieso nicht empfehlenswert.

Es ist davon auszugehen, dass zahlreiche Betreiber über diese Funktionen hinaus zusätzliche Standortinformationen anfordern und im Hintergrund an ihre Server übertragen.

Technik

Im Grunde ist der Abruf von Standortinformationen für die Betreiber der sozialen Netzwerke überhaupt kein Problem. Wurde bei der Installation die Berechtigung zum Abruf von Standortinformationen erteilt, kann der Betreiber jederzeit Standortinformationen anfordern. Dies geht auf zweierlei Weise:

- Die meisten modernen Smartphones verfügen über einen GPS-Empfänger, der den Standort des Smartphones und damit den des Benutzers auf bis zu zehn Meter exakt bestimmen kann.
- Ist kein GPS-Empfänger verbaut beziehungsweise wurde dieser ausgeschaltet, kann das Telefon einen allgemeinen netzbasierten Standort ermitteln. Diese Standortbestimmung wird durch die Beschaffenheit des Mobilfunknetzes ermöglicht. Prinzipiell handelt es sich um die gleiche Methode, mit der auch die Polizei ein Mobiltelefon ortet. Befindet sich ein Mobiltelefon in der Nähe eines Sendemasts und empfängt ein Signal von ihm, loggt es sich bei ihm ein. Jeder Sendemast ist durch eine eigene Kennung identifizierbar. Diese wird beim Login an das Mobiltelefon übertragen, so dass der Standort des Sendemasts ermittelt werden kann. Somit ist es möglich, den Umkreis, in dem sich der Besitzer dieses Mobilfunkgeräts befindet, anhand der Reichweite des Signals vom Sendemast festzulegen und seine ungefähre Position zu ermitteln.

Die Betreiber der sozialen Netzwerke müssen zwischen diesen beiden Fällen jedoch in der Regel gar nicht unterscheiden, da das Betriebssystem des Smartphones die Bestimmung des Standorts übernimmt und lediglich die Ergebnisse an die anfragende Anwendung, also an die App des entsprechenden sozialen Netzwerks, weitergibt. Diese App kann anschließend mit der erhaltenen Information machen, was sie will. Da eigentlich alle Apps von sozialen Netzwerken auch einen unbeschränkten Internetzugang haben, ist es durchaus möglich, die Standortinformationen in regelmäßigen Abständen abzurufen und im Hintergrund an die eigenen Server zu übertragen.

Es ist ziemlich ernüchternd zu betrachten, wer alles diese Technik anwendet. Nahezu sämtliche Betreiber von sozialen Netzwerken, die eine App für Mobilgeräte anbieten, rufen auch Informationen zum Standort des Benutzers ab beziehungsweise lassen sich die Berechtigung dazu einräumen. Man kann das ganz einfach selbst feststellen, indem man die Berechtigungen von entsprechenden Apps betrachtet.

Wie man aus den Berechtigungslisten der Anwendungen erfährt, benötigen die populärsten Apps von Facebook, Twitter, XING, Google und Co. – und nicht nur diese – bei der Installation die Berechtigung, den Benutzerstandort abzurufen.

Google hätte das eigentlich nicht einmal nötig. Da die meisten Smartphones unter dem System Android laufen, das von Google selbst entwickelt und lizenziert wird, ist es für Google prinzipiell nicht weiter schwer, den Standort eines beliebigen Benutzers jederzeit abzurufen. Natürlich kann man mit so einem Verhalten leicht seinen Ruf ruinieren, insbesondere in der Open-Source-Gemeinde, für die der Datenschutz eigentlich heilig ist (zumindest in der Theorie). Aber Apple hat das schließlich auch nicht davon abgehalten, auf iPhone und Co. aufzuzeichnen, wo sich der Benutzer zu welchem Zeitpunkt befand.

Nachdem Apple im April 2011 damit für große Aufregung gesorgt hatte, berichtete die Zeitschrift Focus darüber[31].

Nahezu jeder Betreiber spioniert also die Positionsdaten seiner Nutzer aus und die Entwickler von Smartphone-Anwendungen unterstützen dies nach Kräften. Und nahezu jede App, die einen bestimmten Beliebtheitsgrad bei Smartphone-Besitzern hat, ermittelt heute standardmäßig Positionsdaten und überträgt sie im Hintergrund an die Server des Betreibers. Das ist ein Trend, den es in Zukunft anzuhalten gilt, sofern man nicht rund um die Uhr von Unternehmen observiert werden möchte.

Gegenmaßnahmen

Ist eine Anwendung, die eine Berechtigung für das Ermitteln von Positionsdaten hat, erst einmal installiert, ist es nicht mehr möglich, ihr diese Berechtigung wieder zu entziehen – zumindest nicht in aktuellen Systemen wie Android oder IOS.

Der einzige Weg, um zu verhindern, dass die Betreiber der sozialen Netzwerke an Positionsdaten gelangen, ist, die Anwendungen nicht zu nutzen oder sie wieder zu deinstallieren. Möchte man von unterwegs auf die sozialen Netzwerke zugreifen, kann man die Webseiten jederzeit im Browser eines Smartphones aufrufen und das ganz ohne die Übertragung von Positionsdaten. Die meisten Betreiber stellen sogar eine mobile Version ihrer Seite zur Verfügung, die genauso komfortabel ist wie eine App.

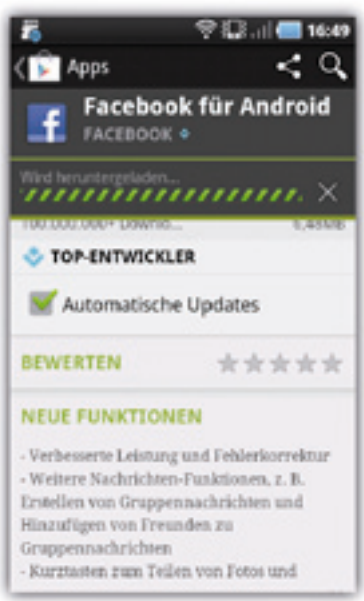

BILD 3.15 Die mobile Version des Facebook-Diensts wird installiert

[31] Siehe auch http://www.focus.de/digital/handy/iphone/iphone-bewegungsprofile-apple-gesteht-fehler-ein_aid_621902.html

3.3.3 Freundefinder

Die letzte hier vorgestellte Technik zur Ermittlung von Zusatzinformationen über den Benutzer ist im Grunde ein einfaches Täuschungsmanöver. Man versucht dem Benutzer vorzugaukeln, man biete ihm irgendwelche Vorteile, verfolgt dabei aber das Ziel, an weitere Daten über ihn zu gelangen.

Dabei können sich die Methoden der einzelnen Betreiber stark unterscheiden und sie sind auch stets mehr oder weniger erfolgreich. So bietet Facebook, Google+, XING und Co. dem Benutzer in etwa an:

> *„Wir finden deine Freunde für dich, wenn du uns das Passwort zu deinem E-Mail-Account gibst. Natürlich werden wir dieses Passwort niemals speichern, wir haben ja auch gar kein Interesse daran, deine E-Mails zu lesen!"*

Andere soziale Netzwerke wie etwa myspace und Amen versuchen, über Facebook an weitere Benutzerdaten zu kommen, etwa auf folgendem Weg:

> *„Melde dich mit deinem Facebook Benutzerkonto an, damit du von Anfang an sofort gut vernetzt bist."*

Oder

> *„Verknüpfe dein Facebook-Konto mit deinem Benutzerkonto, so dass du noch mehr Aufmerksamkeit auf dich ziehen kannst."*

Als aufgeklärter Nutzer sollte man davor zurückschrecken, sich mit seinem Facebook-Konto bei anderen Diensten einzuloggen. Nach Erfahrung des Autors halten sich inzwischen glücklicherweise zahlreiche Nutzer an diese „Verhaltensgrundregel". Diejenigen aber, die davon Gebrauch machen, öffnen den sozialen Netzwerken Tür und Tor zu ihren persönlichen Daten.

Technik

Da sich die verschiedenen Betreiber unterschiedliche Täuschungsmanöver einfallen lassen, funktionieren diese Techniken auch auf unterschiedliche Art und Weise. Sie werden im Folgenden erläutert.

Den Beginn macht die doch etwas plumpe Idee von Facebook, den Benutzern anzubieten, man würde seine Freunde finden, wenn er dem Dienst seine E-Mailadresse sowie sein Kennwort nennt. Zwar wurde diese Idee von vielen anderen Betreibern, darunter auch Google+ und XING übernommen, so richtig erfolgreich war damit bisher jedoch niemand.

Das Versprechen bei dieser Technik ist, dass anhand der Kontaktdaten in den E-Mailkonten des Benutzers die Personen ausfindig gemacht werden, die bei Facebook registriert sind, und dem Benutzer dann als Freunde vorgeschlagen werden. Die Voraussetzung ist natürlich, dass der Benutzer das Passwort zu seinem Mailkonto herausrückt, damit der Netzwerkbetreiber einmaligen Zugang zum Konto erhält. Natürlich soll das

Passwort angeblich nirgendwo gespeichert und selbstverständlich niemals wieder verwendet werden. Ob dieses Versprechen vertrauenswürdig ist oder nicht, muss der Nutzer selbst entscheiden. Ich persönlich glaube es nicht.

Eine ähnliche Idee hatten auch die Betreiber kleinerer sozialer Netzwerke wie myspace oder Amen. Sie stellen sich jedoch etwas geschickter an und bieten dem Benutzer scheinbar große Vorteile, nämlich die Möglichkeit, sich ohne Registrierung direkt mit dem eigenen Facebook-Account anzumelden. Damit spart er sich die Zeit zum Ausfüllen des Registrierungsformulars, weshalb seine Registrierung wahrscheinlicher ist als ohne diese Funktion. Als – für den Betreiber – angenehmen Nebeneffekt lässt er gleichzeitig noch wesentlich mehr Daten beim entsprechenden sozialen Netzwerk zurück. Bei der Anmeldung via Facebook wird dem sozialen Netzwerk nämlich implizit Zugang auf zahlreiche persönliche, von Facebook gespeicherte Daten gewährt. Eine derartige Fülle an Informationen würden die Betreiber dieser sozialen Netzwerke vermutlich vom Nutzer niemals erhalten. Er bekommt davon jedoch nicht viel mit und hat unter Umständen sogar den Eindruck, er hätte im sozialen Netzwerk gar keine Daten hinterlassen.

Ähnlich wie diese Technik funktioniert auch die Verknüpfung des Facebook-Kontos (oder anderer Konten) mit einem Konto bei einem anderen sozialen Netzwerk. Hier wird dem sozialen Netzwerk – also beispielsweise myspace, XING, Google+ und Co. – ebenfalls Zugang zu den Daten der verknüpften Konten gewährt; allerdings erst, nachdem der Benutzer registriert ist. Die Gründe sind hier sehr vielseitig: So spricht man bei XING

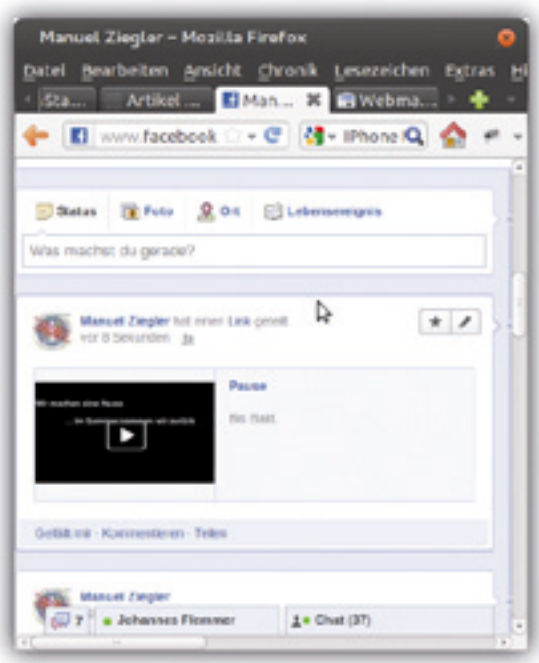

BILD 3.16 Die Meldung zu einem Youtube-Video in Facebook

davon, dass man sich durch eine Verknüpfung mit dem Facebook-Konto noch besser präsentieren könnte – was eigentlich ein offensichtlicher Widerspruch ist zu dem von XING propagierten Leitspruch *Für privates gibt es Facebook, für berufliches gibt es XING*.

Bei Google+ sollen andere Benutzer ein umfassenderes Bild von der eigenen Person erhalten. Nach der Lektüre dieses Buches mag das zwar eher abschreckend erscheinen, allerdings scheint dieser Umstand für manche Leute durchaus einen Anreiz darzustellen.

Plattformen wie Youtube geben der Verknüpfung mit dem Facebook-Konto sogar einen durchaus nützlichen Anstrich. So ist es möglich, das Facebook-Konto mit Youtube dahingehend zu verknüpfen, dass in Facebook automatisch eine neue Meldung generiert wird, sobald in Youtube ein neues Video veröffentlicht wird (Bild 3.16).

Für Videoproduzenten sowie für kleine und mittelständische Firmen, die Youtube als Werbeplattform nutzen, ist dies durchaus gewinnbringend.

Gegenmaßnahmen

Um zu verhindern, dass die Betreiber sozialer Netzwerke Zusatzinformationen zur eigenen Person erhalten, ist es wohl am einfachsten, darauf zu achten, dass derartige Fallen rechtzeitig durchschaut und entsprechende Angebote nicht genutzt werden. Wenn das Kennwort eines anderen Benutzerkontos verlangt wird, muss man sich sehr gut überlegen, ob die Angabe dieses Passworts tatsächlich notwendig ist oder ob es auch ohne geht. Ist man sich nicht sicher, gibt man das Passwort nicht an.

Besonders die Mitarbeiter von Firmen, die beruflich in den sozialen Netzen zu tun haben, dürfen unter keinen Umständen Passwörter zu E-Mailadressen der Firma oder zu anderen Benutzerkonten im Besitz der Firma herausgeben. Aber auch Privatpersonen sollten die gebotene Vorsicht walten lassen.

Hinterfragt man ab und zu gewisse Dinge und gehorcht nicht nur blind den freundlichen Anweisungen von amerikanischen Großkonzernen, lassen sich hinter so einfachen Vorgängen wie der Anmeldung mit einem Facebook-Konto schnell die eigentlichen Beweggründe erkennen und dem Datenmissbrauch kann rechtzeitig vorgebeugt werden.

4 Datendiebstahl

Während die Spionage durch andere Benutzer durchaus legitim sein kann, weil ihnen Daten aus freien Stücken überlassen werden, ist Datendiebstahl immer kriminell. Dabei ist die Spionage eine der Grundlagen für Datendiebstahl, denn ohne sie gewinnen Kriminelle keine Ansatzpunkte für das Stehlen von Daten und erkennen in den meisten Fällen auch keinen Grund, sich für die Daten von anderen zu interessieren.

Während die Spionage durch andere Benutzer lediglich im Rahmen sozialer Netzwerke selbst stattfindet, sind die sozialen Netzwerke nur einer von vielen Schauplätzen für Datendiebstahl. Datendiebstahl[1] liegt dann vor, wenn sich jemand Daten verschafft, die nicht für ihn bestimmt sind, und dabei eine Sicherung wie beispielsweise einen Passwortschutz überwindet, und diese Daten für seine Zwecke nutzt. Dabei kann es sich durchaus um Straftaten handeln, wobei die sicherlich schmerzhafteste zu finanziellen Verlusten führt, wie beim Diebstahl und dem Missbrauch von Kreditkartendaten oder dem Abräumen von Konten bei Geldinstituten. Datendiebstahl kann auch zum Zwecke der Geldwäsche begangen werden oder die Verbrecher sind einfach auf den Verkauf persönlicher Daten aus. Die Ursachen von Datendiebstahl können aber auch persönliche Beweggründe wie Rache sein. Aber aus welchem Grund auch immer Datendiebstahl begangen wird, in den meisten Fällen ist er äußerst ärgerlich und kann durch richtiges, präventives Verhalten vermieden werden.

Wichtig zu wissen ist, dass die Gefahr des Datendiebstahls nicht nur in sozialen Netzwerken besteht, sondern im gesamten Internet. Da ein Internetnutzer gewöhnlich mehrere Benutzerkonten auf den unterschiedlichsten Webseiten besitzt, ist es für einen Kriminellen relativ einfach, zahlreiche Informationen über ihn zusammenzutragen, wenn er alle Benutzerkonten kennt. Gelingt es dem (im Sprachgebrauch oft als „Hacker“[2] bezeichneten) Kriminellen dann, in den Konten des Benutzers nur eine einzige Schwachstelle zu finden, ist es sehr wahrscheinlich, dass ab diesem Zeitpunkt eine Barrieren nach der anderen, von denen die übrigen Konten geschützt werden, fällt. Das liegt daran, dass die Konten meist eng miteinander verwoben sind und von Konto A oft ein Zugriff auf Konto B und umgekehrt möglich ist.

---

[1] Rechtsanwalt Dr. Volker Hermann auf http://www.datenschutz-praxis.de/ fachwissen/fachartikel/201ewer-ohne-erlaubnis-des-betroffenen-daten-ausspaht-macht-sich-strafbar201c

[2] Der richtige Begriff ist aber „Cracker“.

Damit dies nicht geschieht, sind einige grundlegende Sicherheitsaspekte beim Verhalten im Internet zu beachten. Sie sind speziell in den sozialen Netzwerken sehr wichtig, da über diese die benötigten Daten ermittelt werden können, um andere Konten oder gar die Konten der sozialen Netzwerke zu knacken.

Den Daten in sozialen Netzwerken widmen Datendiebe besondere Aufmerksamkeit, da die Benutzerkonten leider oft wie ein offenes Buch geführt werden. Das Landesamt für Verfassungsschutz in Baden-Württemberg weist darauf hin, dass die „nach wie vor unzureichenden Sicherheitsstandards dieser Netzwerke keinen ausreichenden Schutz vor professionellen Angriffen auf die passwortgeschützten Bereiche bieten“[3]. Aufgrund mangelnder Privatsphäre-Einstellungen können Angreifer eine Vielzahl Daten über Mitglieder gewinnen, die später dazu genutzt werden, um an die gewünschten Informationen zu gelangen. Um Datendiebstahl in sozialen Netzwerken wirksam vorbeugen zu können, ist ein umfassender Schutz der Privatsphäre notwendig – genau so wie er auch notwendig ist, um sich vor Spionage durch andere Benutzer zu schützen.

Kriminelle können über die Daten eines Benutzers in sozialen Netzwerken auch an umfangreiche Datensätze gelangen, die sie später an dubiose Firmen verkaufen und Angehörige fremder Nachrichtendienste, Konkurrenten oder Nachrichtenhändler sammeln solche Informationen über Firmenmitarbeiter[4].

Um dem Datendiebstahl so gut wie möglich vorzubeugen, helfen umfangreiche Privatsphäre-Einstellungen.

Natürlich gibt es auch außerhalb sozialer Netzwerke Datenbanken mit zahlreichen Informationen über eine Vielzahl von Menschen. Man denke nur an Telefonbücher, in denen beispielsweise sehr schnell Bewohner einer bestimmten Region gefunden werden, was in sozialen Netzwerken meist so einfach nicht möglich ist. Aber trotzdem sind die sozialen Netzwerke der bevorzugte Schauplatz für Datendiebstahl. Grund sind vor allem ihr Aufbau und ihr Zweck. Schließlich dienen sie dazu, mit anderen Menschen in Verbindung zu treten, und so ist es nicht weiter verwunderlich, dass diejenigen, die auf der Suche nach Daten sind, gerade dort fündig werden. Außerdem haben soziale Netzwerke den Vorteil, dass ihre Mitglieder nicht allein aufgrund der Region, aus der sie stammen, und aufgrund ihres Namens gruppiert werden (wie das beispielsweise in Telefonbüchern der Fall ist). Vielmehr ergeben sich aus der Struktur der Dienste komplexe Netze, in denen Benutzer aktiv sind und die es einem geübten Beobachter erlauben, Gemeinsamkeiten zwischen Benutzern herauszulesen und diese Information für eigene Zwecke zu missbrauchen.

Zudem ist es in sozialen Netzwerken sehr einfach, Zugang zu Informationen zu erlangen, die für die Öffentlichkeit nicht sichtbar sind. Oft genügt es schon, einem Freund des Beobachteten einen Freundesantrag zu stellen, um umfangreiche Informationen über einen Benutzer in die Hand zu bekommen. Damit ist es für Datendiebe unglaublich einfach, an Fremde heranzukommen, ohne Verdacht zu erregen. Wie eigene Erfahrungen,

[3] Unterhttp://www.verfassungsschutz-bw.de/index.php?option=com_content&view=article&id=615&Itemid=176

[4] Siehe auch hier wieder http://www.verfassungsschutz-bw.de/index.php?option =com_content&view=article&id=615&Itemid=176

aber auch Berichte aus Hackerkreisen zeigen, suchen sie sich irgendeine Person aus dem Freundeskreis des Beobachteten heraus, um weitere Informationen über ihr Ziel zu erlangen.

Ein letzter Grund, warum Daten in sozialen Netzwerken so gefährdet sind, ist ihre potentielle Anfälligkeit. Natürlich würde jeder fachkundige Sicherheitsexperte sagen, einen Dienst wie Facebook zu „hacken“ stelle ein Ding der Unmöglichkeit dar, aber auszuschließen ist dieser Fall dennoch nicht. Ein Grundgesetz in der Programmierung ist nämlich, dass es so gut wie kein Programm gibt, das fehlerfrei und gegen alle Eventualitäten abgesichert ist. Und egal wie viel Zeit und Kosten in die Entwicklung einer Anwendung gesteckt werden, man kann ihr Verhalten nicht auf alle Fehler- und Missbrauchsfälle testen. Darum ist es im Grunde nur eine Frage der Zeit, bis ein kreativer Hacker eine Lücke im System findet und sie für seine Zwecke ausnutzt. Derartiges kam bereits vor. So gab es in der Vergangenheit vor allem in den VZ-Netzwerken häufiger Datenlecks. Gerade im Jahr 2009 kam es dort zu mehreren Datenpannen, wie die Zeitschrift Focus berichtete[5], aber auch Facebook musste schon Fehler eingestehen, die es Werbetreibenden erlaubten, personenbezogene Daten von Nutzern abzurufen[6].

Das Interesse der Datensammler an den in sozialen Netzwerken gespeicherten Daten ist also schon allein wegen der Fülle an Informationen äußerst groß. Schützen kann man sich selbst nur in begrenztem Umfang, ein Teil des Datenschutzes verbleibt stets beim Netzbetreiber.

4.1 Datensammler

Es muss nicht betont werden, dass es in Deutschland verboten ist, Daten von Benutzern zu stehlen, das heißt: sie ohne deren Erlaubnis zu erheben. Allerdings werden manche Verfahren zum Erlangen von Daten vor Gericht sogar als durchaus legal bewertet oder sie bewegen sich nur an der Grenze zur Illegalität, überschreiten sie aber nicht. Dennoch haftet ihnen ein starker Hautgout an.

Datensammler sind stets darauf aus, Informationen über andere Personen zu ermitteln. Hier gibt es die unterschiedlichsten Typen, die auch die unterschiedlichsten Zielgruppen ins Visier nehmen. So kann ein Datensammler darauf aus sein, Daten von Benutzern zusammenzutragen, um sie später auf dem Schwarzmarkt an dubiose Werbefirmen und Trickbetrüger zu verkaufen. Ein anderer Datensammler ist beispielsweise selbst ein Trickbetrüger und auf der Suche nach Daten möglicher Opfer aus einer bestimmten Zielgruppe, beispielsweise Jugendliche und junge Erwachsene.

[5] Nachzulesen unter http://www.focus.de/digital/digital-news/schueler-vz-datenpanne-offenbar-erneut-100000-sensible-daten-aufgetaucht_aid_448831.html

[6] Siehe http://www.golem.de/1105/83390.html

Wieder andere Datensammler sind im Auftrag eines staatlichen Geheimdienstes aktiv und möchten ihre Datenbank füttern. Es ist durchaus nicht unüblich, dass die Geheimdienste Bürger fremder Staaten beobachten. In diesem Zusammenhang sollte man bedenken, dass hinter den großen sozialen Netzwerken amerikanische Firmen stecken und einiges darauf hindeutet, dass die USA (und nicht nur diese) in Europa Firmen ausspionieren, um an deren Know-how zu gelangen und auch im Terrorismus-Bekämpfungswahn Ausländer zu überwachen.

Der größte staatliche Datensammler entsteht derzeit in Utah, Amerika. Dort soll das Utah Data Center, das von der amerikanischen Agentur für Sicherheit (NSA) betrieben wird, ab dem Jahr 2013 alle Verbindungsdaten samt Inhalt der amerikanischen Bürger sammeln. Darunter sollen sich Handy-Gespräche, Google-Suchanfragen und E-Mails befinden. Laut Deutsche Mittelstands-Nachrichten[7] sollen auch die Daten von Bürgern anderer Staaten nicht unangetastet bleiben – wer sich in amerikanischen Netzen aufhält, ist hier nach Einschätzung des Autors sicherlich besonders gefährdet.

Eine weitere Gruppe von Datensammlern wird umgangssprachlich als Hacker bezeichnet. Sie gehören beispielweise einer Vereinigung an, die sich zum Ziel gesetzt hat, bestimmten Personen eine Lehre zu erteilen. So wurden Anfang Januar mehrere hundert politisch Andersdenkende von der Internet-Aktivistengruppe Anonymous entlarvt, anschließend wurden zahlreiche Benutzerkonten geknackt und die Daten auf einer Internetplattform veröffentlicht[8].

Teilweise sind es auch Einzeltäter, die auf Daten aus sind, mit deren Hilfe sie sich persönlich bereichern können; sie haben Daten von Kreditkarten und anderen Bankkonten im Visier. Und manchmal kommt es auch vor, dass diese Einzeltäter im jugendlichen Übermut darauf aus sind, sich einen Namen in der Internetwelt zu machen oder dass sie einfach nur experimentierfreudig sind.

Egal wie die Motive sind – solche Datensammler stellen eine ernsthafte Gefahr für die Internetnutzer dar und speziell die Nutzer von Massenmedien wie die sozialen Netzwerke sind in hohem Maße betroffen.

Immer wieder gelingt es den Datensammlern auch, über Anwendungen in sozialen Netzwerken Würmer und Viren zu verbreiten. Würmer sollen das Zielsystem und dessen Daten zerstören. Viren sind noch gefährlicher, weil sie sich auf dem Computer des Anwenders einnisten – meist ohne dass dieser etwas davon erfährt. Von dort lesen sie Daten aus und senden sie an den Urheber des Virus. Er kann damit beispielsweise Zugangsdaten für das Online-Banking ausspionieren und einen finanziellen Schaden anrichten.

Teilweise sind Datensammler auch darauf aus, Informationen über Unternehmen zu erhalten, wobei sie den Umweg über die Mitarbeiter nehmen müssen. Sie geben sich ihnen gegenüber als frühere Beschäftigte, alte Schulfreunde, Urlaubsbekanntschaften oder dergleichen aus und gewinnen damit nach und nach das Vertrauen. Dabei fragen sie ihr Opfer nebenbei nach Informationen über den Arbeitgeber aus und erhalten so

[7] Siehe http://www.deutsche-mittelstands-nachrichten.de/2012/03/40120/

[8] Bericht beispielsweise auf Golem: http://www.golem.de/1201/88742.html

oft detaillierte Bilder über die Struktur des Unternehmens. Diese Art des Ausforschens heißt auf Neudeutsch „Social Engineering“. Manchmal gelingt es den Angreifern schließlich, an brisante Daten wie Zugangsdaten in das Firmennetzwerk oder ähnliches zu gelangen – schon haben sie ihr Ziel erreicht und sich einen Zugang ins Unternehmen erschlichen[9].

Egal, welche Beweggründe die Datensammler haben, für die Nutzer sozialer Netzwerke ist vor allem eines wichtig: Sie stellen eine Gefahr für sie und ihre Freunde dar, und soziale Netzwerke schaffen oft erst die Rahmenbedingungen dafür, dass diese Datensammler erfolgreich sein können.

4.1.1 Eigene Gegenmaßnahmen

Um Datensammler generell abzuwehren, ist eine Reihe von Verhaltensmaßnahmen zu treffen. Die wohl wichtigste Vorkehrung sind die in Kapitel 2 vorgestellten Privatsphäre-Einstellungen sowie die besonnene Nutzung der sozialen Netzwerke. Zudem sollte man stets wachsam bleiben und verdächtige Signale keinesfalls ignorieren. Im Folgenden werden einige Regeln vorgestellt, die zu beachten sind, um wenigstens die allernötigsten Vorkehrungen gegen Datendiebstahl zu treffen.

Vor allem jene Datendiebe, die persönlichen Kontakt zu den Benutzern aufnehmen, sind leicht auszuschalten. Erhält man Freundesanfragen von jemandem, den man nicht kennt beziehungsweise nicht identifizieren kann, sollte man sie grundsätzlich nicht annehmen. Erst wenn geklärt ist, um wen es sich bei dem Unbekannten handelt und man sich sicher sein kann, dass das Gegenüber vertrauenswürdig ist, sollte man eine Freundschaftsanfrage annehmen. Damit lässt es sich verhindern, dass Fremde beziehungsweise Datensammler als vermeintliche Freunde zahlreiche Informationen über einen selbst ermitteln können.

Ebenso sollten bestimmte Daten für niemanden, vor allem aber nicht für die Öffentlichkeit sichtbar gemacht werden. Dazu gehören Anschrift, Handynummer, Telefonnummer und E-Mailadresse. Diese Daten ermöglichen die eindeutige Identifikation der natürlichen Person. Zwar kann man durch die eigene E-Mailadresse am wenigsten als natürliche Person identifiziert werden, sie sollte jedoch auf jeden Fall geheim gehalten werden, da mit ihr eine Identifikation im Internet möglich ist. So kann man mit Kenntnis der E-Mailadresse die anderen Benutzerkonten ausfindig machen, die unter dieser Adresse angelegt wurden, und auf diese Weise tiefgreifende Erkenntnisse über einen Benutzer gewinnen.

Aus dem gleichen Grund ist auch darauf zu achten, dass Leuten, denen die E-Mailadresse eines Benutzers bekannt ist, keinesfalls dessen Benutzerkonto angezeigt wird. Eine Option wie Mein Profil für Personen anzeigen, denen meine Mailadresse bekannt ist (Bild 4.1) darf niemals aktiviert werden! Andernfalls könnten Fremde, die eine E-Mailadresse von einer beliebigen Seite im Internet ermittelt haben, diese nur in

[9] Marc Ruef (2007): Die Kunst des Penetration Testing, C&L Verlag ISBN 978-3-393-6546-49-1.

BILD 4.1 Die Option „Wer kann dich anhand der angegebenen E-Mail-Adresse oder Handynummer finden?" darf nicht auf „Öffentlich" und nach Möglichkeit auch nicht auf „Freunde von Freunden" gestellt werden

sozialen Netzwerken wie Facebook einzugeben, um weitere Daten über den Besitzer zu erhalten.

Das Problem der Verbreitung von Viren und Würmern nimmt mit dem Wachstum der sozialen Netzwerke stetig zu. Es ist für Mitglieder sozialer Netzwerke wie Facebook nicht unüblich, Nachrichten von Freunden zu bekommen, in denen – meist auf Englisch – behauptet wird, man wäre auf einem bestimmten Bild zu sehen. Und zu diesem Bild gibt es natürlich auch einen Link. Betrachtet man den Namen der verlinkten Datei genauer, wird man feststellen, dass sie eine doppelte Dateinamensendung besitzt, beispielsweise *virus.jpg.exe*. Nicht der Name, sondern die Endung *.jpg.exe* ist ein klares Indiz dafür, dass es sich um Schadsoftware handelt, die da verlinkt wurde. Klickt man den Link an, wird browserabhängig teilweise ein automatischer Download begonnen, der die Schadsoftware – getarnt als Bild – auf den Rechner herunterlädt. Öffnet man das vermeintliche Bild dann mit einem Doppelklick, wird die Software automatisch auf dem Rechner installiert und der eigene PC von einem Virus befallen.

Je nach Virus ist es möglich, dass anschließend gleiche Nachrichten über Facebook an andere Anwender versandt werden, die ebenfalls einen Link zu einem Virus enthalten. Obwohl man sich als langjähriger Nutzer an solche Viren-Einschleusversuche gewöhnt haben sollte und sie mit der gebotenen Vorsicht handhaben müsste, lassen sich leider immer wieder zahlreiche Mitglieder von derartigen Nachrichten täuschen. Sie fördern dadurch die Verbreitung derartiger Viren und fügen sich selbst Schaden zu[10].

Hier sei auf Abschnitt 4.2.1 ab Seite 130 hingewiesen, in dem das Anlegen sicherer Passwörtern erläutert wird. Auch sie beugen Datendiebstahl vor.

[10] Am 21.5.12 erschien in der Computerwoche ein Bericht zu derartigen Facebook-Würmern und ihrer Verbreitung, siehe http://www.computerwoche.de/ security/2513157/

4.1.2 Gegenmaßnahmen der Betreiber

Egal, welche Vorsichtsmaßnahmen der Benutzer trifft beziehungsweise überhaupt treffen kann, verbleibt doch stets eine gewisse Restverantwortung beim Betreiber des sozialen Netzwerks, die ihm nicht abgenommen werden kann und über deren Umsetzung alleine er entscheidet. Dabei handelt es sich vor allem darum, wie er die Daten der Benutzer speichert, wie er mit ihnen gegenüber Dritten umgeht und auf welche Art und Weise er die Daten im Netzwerk transportiert.

Wenn man die Maßnahmen, die der Betreiber zum Schutz der persönlichen Daten ergreift, gut kennt, erfährt man, welche Sicherheitsprobleme ein soziales Netzwerk tatsächlich mit sich bringt, und kann sich als Anwender auf die Risiken einstellen.

Die größte Verantwortung trägt der Betreiber sicherlich beim Speichern der Benutzerdaten und ihrem Schutz vor dem Zugriff Dritter. So wäre es beispielsweise unverantwortlich, wenn die Daten der Benutzer vollständig unverschlüsselt in den Datenbanken abgelegt würden. Zumindest brisante Daten wie das Passwort sowie Antworten auf Sicherheitsfragen sollten unter allen Umständen verschlüsselt gespeichert werden. Aus Sicht des Benutzers wäre es sogar am besten, dass Daten wie Passwörter so verschlüsselt würden, dass sie nicht einmal mehr durch den Betreiber selbst rekonstruiert werden können. Dies ist mit sogenannten Einweg-Verschlüsselungsverfahren[11] möglich.

Leider lassen sich jedoch meist keine Informationen darüber gewinnen, wie der Betreiber Passwörter tatsächlich speichert. Man muss daher vom schlechtesten Fall ausgehen, nämlich dass sie so gespeichert werden, dass sie rekonstruierbar sind oder im schlimmsten Fall sogar im Klartext in den Datenbanken stehen.

Noch schlimmer steht es um die restlichen Daten. Sie zu verschlüsseln und regelmäßig wieder zu entschlüsseln wäre zwar ein gewisser technischer Aufwand, der jedoch durchaus vertretbar ist, um sie vor Dritten zu schützen. Man kann jedoch annehmen, dass keines der sozialen Netzwerke die Daten seiner Benutzer verschlüsselt speichert, zumindest gibt es keine Anhaltspunkte für das Gegenteil.

Würde nicht die Gefahr bestehen, dass durch Angriffe auf die Server der Betreiber Daten in die Hände von Dritten gelangen könnten, wäre das unverschlüsselte Speichern der Daten unproblematisch; der Betreiber würde ohnehin dafür sorgen, dass er selbst die Daten wieder entschlüsseln kann. Da aber die Gefahr von Angriffen durch Dritte nicht auszuschließen ist und sogar mit jedem Nutzer, der sich neu registriert, zunimmt, stellt die unverschlüsselte Speicherung der Benutzerdaten ein großes Risiko für das Mitglied des sozialen Netzwerks dar.

[11] Angewendet werden häufig symmetrische Verschlüsselungsverfahren wie Blowfish, das neuere Twofisch oder AES. Diese sind allerdings bei Kenntnis des Schlüssels umkehrbar. Wirkliche Einwegverfahren wie der Message-Digest Algorithm 5 (MD5) sind heute nur noch sehr selten anzutreffen, da die meisten als unsicher gelten. Der Grund für die mangelnde Sicherheit solcher kryptographischer Hashfunktionen ist, dass unterschiedliche Klartexte den gleichen Geheimtext ergeben könnten (bei MD5 die gleiche Prüfsumme) und somit keine hundertprozentige Sicherheit gegeben ist.

Nahezu ebenso groß ist die Verantwortung, die der Betreiber für den Schutz der Benutzerkonten trägt. Hier kommt es darauf an, wie schnell (und ob überhaupt) der Betreiber erkennt, dass ein Fremder versucht, Zugang zu einem ihm nicht gehörenden Benutzerkonto zu erlangen. Der Schutz der Passworte ist bei eigentlich allen in diesem Buch behandelten sozialen Netzwerken mangelhaft. Auch wenn mehrmals hintereinander ein falsches Passwort eingegeben wird, verhindert keiner der behandelten Dienste weitere Login-Versuche, obwohl es eigentlich ihre Aufgabe wäre, das Benutzerkonto vor Fremdzugriffen zu schützen.

BILD 4.2 Das Einrichten einer Sicherheitsfrage ist nur einmalig und unwiderruflich möglich. Es empfiehlt sich nicht, die Sicherheitsfrage einzurichten, da der Zugriff auf das Benutzerkonto über die Sicherheitsfrage möglich wird. Die Antwort auf eine Sicherheitsfrage zu erraten ist wesentlich einfacher, als ein Passwort zu erraten, da die Frage vorgegeben ist und der Benutzer so einen Anhaltspunkt hat. Wenn beispielsweise nach dem Mädchenname der Mutter gefragt ist, kann ein Hacker diesen oft anhand der im Profil der sozialen Netzwerke angegebenen Verwandtschaftsverhältnisse ermitteln und hat anschließend Zugriff auf das Konto

Hier wäre ein ähnliches Vorgehen wie beim Online-Banking zwingend erforderlich, nämlich dass nach einer bestimmten Anzahl an Versuchen Schluss ist, keine weiteren Versuche mehr angenommen werden und das Benutzerkonto schon nach einer geringen

Zahl von – beispielsweise zehn – Fehlversuchen (beim Online-Banking wird bereits nach drei Versuchen gesperrt) erst wieder durch einen autorisierten Benutzer oder durch ein Master-Passwort freigeschaltet werden muss.

Noch schlimmer ist es in den sozialen Netzwerken, die die Reaktivierung des Benutzerkontos erlauben, indem eine Sicherheitsfrage beantwortet werden muss (Bild 4.2). Facebook beispielsweise bietet seinen Benutzern die Möglichkeit, eine solche Sicherheitsfrage einzurichten. Dabei wird die Sicherheitsfrage direkt vorgegeben, und die mögliche Antwort darauf zu erraten ist oft einfacher, als das Passwort eines Benutzers herauszufinden.

Ein letzter Verantwortungsbereich der Betreiber liegt darin, die Kommunikation zwischen Anwender und sozialem Netzwerk über abhörsichere Verbindungen abzuwickeln. So senden fast alle Betreiber sozialer Netzwerke die Kommunikation über ungesicherte Verbindungen, wobei alle Daten im Klartext übertragen werden und damit von potentiellen Angreifern mit den geeigneten Werkzeugen abgefangen und gelesen werden können, ohne dass irgendeine Art von Barriere überwunden werden muss.

Einige Betreiber, zum Beispiel Facebook und Google+, bieten allerdings auch über das verschlüsselnde Datenübertragungsprotokoll SSL gesicherte Verbindungen an. Vertraulichen Daten wie Passwörter oder auch die Session-ID, die Hacker benötigen, um die aktuelle Sitzung des Benutzers mit dem sozialen Netzwerk abzuhören beziehungsweise um selbst eine Verbindung im Namen des Benutzers mit dem sozialen Netzwerk herzustellen, werden darüber verschlüsselt und damit so übertragen, dass sie nicht abgefangen werden können.

Sofern die einzelnen Betreiber Maßnahmen ergreifen, um die Daten des Benutzers in den genannten Fällen abzusichern, nehmen sie ihre Verantwortung im Hinblick auf die Gefahr des Datendiebstahls wahr. Mit Ausnahme von Google leistet aber eigentlich kein Betreiber ausreichenden Schutz vor Datendiebstahl. In nahezu jedem sozialen Netzwerk können die Benutzerkonten durch Brute-Force – also durch das Ausprobieren aller möglichen Kennwörter – geknackt werden, ohne dass die Betreiber einschreiten würden.

Nicht unerwähnt bleiben darf, dass zahlreiche Dienste die IP-Adresse eines Benutzers speichern. Facebook zum Beispiel gibt in den Datenschutzrichtlinien[12] zu, dass es Daten wie die IP-Adresse von Nutzern ermittelt (und damit unter Umständen auch speichert).

Auch Google räumt in seinen Datenschutzbestimmungen[13] ein, dass IP-Adressen protokolliert werden. Mit dieser Adresse kann der Anwender im Internet mehr oder weniger eindeutig identifiziert werden. Die IP-Adresse wechselt zwar bei jeder Einwahl per DSL (und auch bei den meisten anderen Verbindungsverfahren), durch die Kombination von Benutzername und Auswertung der Geo-Location kann der Anwender aber im Zweifelsfall bis zu dem Internetanschluss beziehungsweise Router, über den er sich im sozialen Netzwerk eingeloggt hat, zurückverfolgt werden. Loggt sich der Anwender immer von

[12] Siehe auch http://www.facebook.com/about/privacy/your-info#inforeceived

[13] Nachzulesen unter http://www.google.com/intl/de/policies/privacy/

der selben geographischen Position in das soziale Netz ein, kann der ungefähre Standort des Internetanschlusses ermittelt werden.

Das Speichern der IP-Adressen ist bei den Datenschützern umstritten, da der Netzwerkbetreiber so ähnlich wie der Internetprovider einen Einblick gewinnen kann, wer zu welchem Zeitpunkt welche IP-Adresse hatte.

Ganz einfach hat es Google, wenn sich der Anwender zusätzlich zu Google+ gleichzeitig über Google Maps Routen berechnen lässt. Hier weiß der Provider nach kurzer Zeit den genauen Wohnort bis hin zu Straße und Hausnummer.

In der Europäischen Union sind die Internetprovider gesetzlich dazu verpflichtet, die Verbindungsdaten über mehrere Monate hinweg zu speichern (Vorratsdatenspeicherung), damit die Polizei im Zweifelsfall illegale Aktivitäten zurückverfolgen kann. Diese Pflicht ist ungeliebt, weil sie Speicherplatz, Arbeit und Ärger kostet. Durch das zusätzliche Speichern solcher Daten in sozialen Netzwerken geht ein weiteres Stück Privatsphäre verloren.

Ein letzter kritischer Punkt, der bereits weiter oben in anderem Zusammenhang aufgegriffen wurde, ist der häufig im Ausland befindliche Firmensitz sozialer Netzwerke. Liegt er beispielsweise in den USA, ist es den dortigen Behörden erlaubt, jederzeit Zugriff auf die Server des Betreibers zu erlangen. Und Unternehmen sind aufgrund des Antiterrorgesetzes „Patriot Act“ dazu verpflichtet, die von ihnen gespeicherten Daten an die Behörden weiterzugeben – darunter natürlich auch die der deutschen Mitglieder. Google soll die Daten seiner internationalen Nutzer bereits weitergemeldet haben[14].

Nach deutschem Recht ist das nicht erlaubt, zumindest nicht so einfach. Es muss schon ein konkreter Verdacht gegen denjenigen vorliegen, dessen Daten abgerufen werden sollen. Folgerichtig berufen sich Betreiber wie Facebook darauf, dass sie nicht dem deutschen Datenschutz unterlägen, da ihr Firmensitz schließlich in Irland beziehungsweise den USA sei. Dies ist im Impressum von Facebook unter Punkt 18.1 nachzulesen:

> *„Wenn du in den USA oder Kanada ortsansässig bist oder dort deinen Hauptgeschäftssitz hast, stellt diese Erklärung eine Vereinbarung zwischen dir und Facebook, Inc. dar. Anderenfalls stellt diese Erklärung eine Vereinbarung zwischen dir und Facebook Ireland Limited dar. Die Begriffe „uns“, „wir“ und „unser“ verweisen jeweils entweder auf Facebook, Inc. oder Facebook Ireland Limited.“*

[14] Gemäß Wirtschaftswoche vom 6. August 2011: http://www.wiwo.de/politik/ ausland/datenspeicherung-google-server-in-europa-vor-us-regierung-nicht-sicher/5156042.html

4.2 Identitätsdiebstahl

Eine besonders drastische Form des Datendiebstahls ist der sogenannte Identitätsdiebstahl. Bei ihm ermitteln Angreifer so viele Daten über jemanden, dass sie in der Lage sind, dessen Identität im Internet anzunehmen. Häufig knacken bei einem solchen Identitätsdiebstahl auch Fremde die Onlinekonten des Opfers und bringen sie unter ihre Kontrolle, um vollständig seine Identität anzunehmen (Bild 4.3).

BILD 4.3 Das Zurücksetzen des Facebook-Kennworts

Die Gründe für einen derartigen Identitätsdiebstahl sind vielseitig; oft werden im Namen des Opfers Straftaten verübt, die sich anschließend nur schwer den eigentlichen Tätern nachweisen lassen[15].

Das Opfer hat dabei nicht nur mit dem Verlust seiner Onlinekonten zu kämpfen, sondern muss auch noch versuchen zu beweisen, dass er die Taten, die in seinem Namen verübt wurden, nicht begangen hat. Oder Kriminelle bedienen sich einer gestohlenen

[15] Hierzu vor allem die 415 Seiten umfassende, vom Bundesministerium des Inneren finanzierte und im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) verfasste Studie „Identitätsdiebstahl und Identitätsmissbrauch im Internet", die als Datei „Studie_Identitaetsdiebstahl_090610.pdf" ergoogelt werden kann.

Identität, um möglichst effizient und anonym Viren zu verbreiten. Zudem erhoffen sich manche Täter, durch Identitätsdiebstahl an die finanziellen Mittel des Opfers zu gelangen.

Identitätsdiebstahl betrifft nicht nur soziale Netzwerke, sondern geht meistens von einer E-Mailadresse aus und zieht sich dann durch alle mit dieser E-Mailadresse verknüpften Konten. Allerdings werden oft die in sozialen Netzwerken verfügbaren Daten herangezogen, um Zugang zu einer E-Mailadresse zu erlangen, zumindest wird das in Hacker-Kreisen berichtet. Hat ein Angreifer erst einmal Zugang zur E-Mailadresse eines Benutzers, kann er sich gewiss sein, dass ihm alle mit dieser Adresse verknüpften Konten in die Hände fallen werden. Seine erste Tat wird wahrscheinlich nämlich sein, das Kontokennwort auf ein eigenes zurückzusetzen, um sich dann ungeniert bedienen zu können. Schließlich erlauben die meisten Konten das Neudefinieren des Passworts, wenn man die mit ihnen verknüpfte E-Mailadresse in Händen hält.

4.2.1 Eigene Gegenmaßnahmen

Einem Identitätsdiebstahl kann grundsätzlich jeder zum Opfer fallen. Allerdings kann man es Angreifern derart erschweren, Zugriff auf das eigene Benutzerkonto zu erlangen, dass sie aufgeben und sich ein anderes Opfer suchen. Die größten Erfolge erzielt man hier mit sicheren Passwörtern. Es reicht jedoch nicht, nur die Konten in sozialen Netzwerken mit sicheren Passwörtern zu versehen, sondern auch für jedes einzelne Benutzerkonto, das auf irgendeiner Webseite angelegt wurde. Hierbei ist vor allem dem E-Mailkonto besondere Aufmerksamkeit zu widmen – schließlich ist es der Schlüssel zu beinahe sämtlichen Benutzerkonten, über die man in den Weiten des Internets verfügt. Hat ein Hacker Zugriff auf das E-Mailkonto eines Benutzers, hat er in den meisten Fällen die Kontrolle über nahezu alle seine Benutzerkonten, da die meisten mit der Möglichkeit ausgestattet sind, das Passwort per E-Mail zurückzusetzen.

Daneben spielt es oft auch eine sicherheitsrelevante Rolle, an wie viele persönliche Daten ein Hacker gelangt. Kann er ausreichend viele in seinen Besitz bringen, um die Antworten auf Sicherheitsfragen zu erraten, muss er nicht unbedingt ein Passwort eingeben, um Zugriff auf einzelne Benutzerkonten zu erlangen, sondern kann sich sogar über die Sicherheitsabfrage für vergessene Passwörter einschleichen.

Viele Passwörter werden jedoch durch das Abhören ungesicherter Verbindungen geknackt[16]. Daten werden häufig unverschlüsselt versandt und auch Passwörter werden vor dem Versand nicht verschlüsselt. Ein Hacker kann diese Daten auf ihrem Weg vom Anwender zum Empfänger aus dem Datenstrom auslesen und aus ihnen die gewünschten Passwörter herauslösen. Als Nutzer sollte man also nach Möglichkeit auf sichere https-Verbindungen zurückgreifen, um sich zu schützen.

[16] Siehe auch: Thomas Werth (2012): Penetrations-Tests. C&L-Verlag, ISBN 978-3-936546-70-5

Sicheres Passwort

Die wichtigste Vorkehrung gegen Identitätsdiebstahl ist die Wahl eines sicheren – das heißt, durch Fremde nicht erratbaren – Passworts. Die Wahl eines sicheren Passworts ausschließlich für Benutzerkonten sozialer Netzwerke reicht jedoch keineswegs aus: Wie bereits erwähnt müssen für sämtliche Benutzerkonten im Internet sichere Passwörter gewählt werden. Dabei ist es am besten, wenn sich die Passwörter der verschiedenen Konten deutlich unterscheiden. Das sicherste Passwort sollte stets das des E-Mail-Accounts sein, da dieses Konto, abgesehen von Onlinekonten bei Geldinstituten, das absolut wichtigste Benutzerkonto eines Internetnutzers darstellt.

Bei der Wahl unterschiedlicher Passwörter für verschiedene Benutzerkonten sollte man stets beachten, dass die Summe aller Benutzerkonten eine Art Kette darstellt, die die Tür zu den persönlichen Daten verschließt. Gelingt es einem Angreifer, ein Glied dieser Kette zu brechen, erhält er dadurch höchstwahrscheinlich so viele Informationen, dass mit diesem Glied auch der Rest der Kette gebrochen werden kann. Das liegt wie schon mehrfach erwähnt daran, dass die Benutzerkonten eines Internetnutzers heute meist eng miteinander verknüpft sind. Oft kann man von einem Benutzerkonto auch auf andere Benutzerkonten zugreifen, was es einem Angreifer natürlich leicht macht, alle Benutzerkonten unter seine Kontrolle zu bringen. Das schwächste Passwort ist also der Maßstab, nach dem beurteilt werden muss, ob die Daten eines Benutzers sicher sind oder nicht.

Richtlinien

Die wohl wichtigste Regel bei der Wahl eines Passworts ist es, keines zu wählen, das von Fremden oder auch von Freunden mit der eigenen Person in Verbindung gebracht werden kann. So ist es beispielsweise so ziemlich der schlechteste Einfall, den Namen seines Lieblingsfußballvereins als Passwort anzugeben. Noch eine Spur ignoranter ist es, wenn man diesen Verein nahezu vergöttert und alle Profile in sozialen Netzwerken Bilder von diesem Verein enthalten. Leider kommen derartige Passwörter nicht selten vor. Eine mindestens ebenso schlechte Idee ist es, den eigenen Vornamen als Passwort zu wählen oder den Begriff *Passwort* selbst.

Die genannten Beispiele sind keinesfalls aus der Luft gegriffen. Hacker probieren als erstes, mit solchen Passwörtern einen Benutzeraccount zu knacken – und das aus gutem Grund, denn sie haben damit in vielen Fällen Erfolg. Das Cracker-Programm John the Ripper enthält eine Liste der meistgenutzten Passwörter[17]. Mit dabei sind an dieser Stelle die Wörter „password“, „1234356“, „fuckyou“, „iloveyou“ sowie unzählige Vornamen. Laut der Berichte des Sicherheitsunternehmens Imperva soll es eine Liste mit nur 5000 Passwörtern geben, die von insgesamt zwanzig Prozent der Internetnutzer verwendet werden[18]. Eine erschreckende Quote!

Fast genauso einfach zu knacken sind Passwörter, die genau so oder in leicht veränderter Groß-/Kleinschreibung in Wörterbüchern stehen oder bei denen es sich um Namen von Firmen, Bands, Organisationen oder ähnliches handelt.

[17] Siehe dazu auch http://it-news-blog.org/die-haufigsten-passworter/

[18] Siehe dazu auch http://www.imperva.com/docs/WP_Consumer_Password_ Worst_Practices.pdf

Mit Hilfe von speziellen Programmen wie beispielsweise John the Ripper können derartige Passwörter schon im ersten Schritt, der sogenannten Wörterbuchattacke, geknackt werden[19]. Dabei werden die nach einer Statistik häufigsten Passwörter ausprobiert und mit ihnen auch die gängigsten Begriffe der Sprache des Benutzers.

Erst wenn mit diesen Programmen das Passwort nicht gefunden werden konnte, gehen die Angreifer daran, mit Hilfe weiterer Brute-Force[20]-Methoden systematisch alle möglichen Wörter auszuprobieren, bis das richtige gefunden ist. Aufgrund der großen Anzahl an Zeichen und der meist unbestimmten Zahl der Stellen eines Kennworts brauchen Brute-Force-Verfahren bei einem Kennwort von geringer bis mittlerer Stärke im Durchschnitt mehrere Wochen bis Monate, um es zu knacken. Brute Force anzuwenden, lohnt sich für einen Kriminellen, der Zugang zum Konto eines normalen Nutzers bekommen möchte, nicht wirklich. Professionelle Forensiker dagegen, die Beweise für eine Straftat suchen, lassen ein Brute-Force-Programm auch schon mal mehrere Monate gegen ein Passwort laufen, um ans Ziel zu gelangen.

Benutzer erwarten von einem Passwort, dass sie keine Ewigkeit brauchen, um es einzugeben, vor allem aber, dass sie es sich einfach merken können. Es ist schließlich lästig, ständig den Tresor zu öffnen (sei es einen echten oder einen Softwaretresor) und die dort notierten Kennwörter herauszusuchen, wenn man nur kurz seine E-Mails abrufen möchte. Es muss deshalb ein Mittelweg aus Sicherheit und Bequemlichkeit gefunden werden – allerdings darf die Bequemlichkeit nicht zu sehr überwiegen, sonst kann es später sehr unbequem werden.

Ein Passwort sollte aus nicht weniger als acht Zeichen bestehen, man muss sich jedoch bewusst sein, dass die Sicherheit eines Passworts exponentiell in Abhängigkeit von der Anzahl der Zeichen wächst, und sollte sich daher gut überlegen, ob es sich nicht lohnt, ein oder zwei Stellen mehr einzubauen.

Bei einem achtstelligen Kennwort belaufen sich die erlaubten Zeichen auf zirka 128 (dies entspricht der Hälfte der Zeichen des ASCII-Zeichensatzes). Davon werden nur etwa hundert üblicherweise verwendet, so dass ein Hacker pro Stelle nur zirka hundert Zeichen austesten muss.

Für ein achtstelliges Kennwort gibt es also 100^8 Möglichkeiten (das sind 10 Billiarden). Mit nur einer Stelle mehr, also 100^9 Möglichkeiten (1 Trillion), muss ein Angreifer das Hundertfache an Varianten durchprobieren, wenn er die Anzahl der Stellen kennt. Da ein Angreifer die Anzahl der Stellen meist nicht kennen kann (weil sie bei den aller-

[19] Wie das genau geht, ist in Thomas Werths Buch „Penetrations-Tests“ nachzulesen (C & L Computer- und Literaturverlag, Böblingen, 2012).

[20] *Brute Force* ist eine Sammlung von Methoden zum Knacken von Passwörtern. Sie funktionieren auf eine ähnliche Weise, nach der man meistens auch beim Knacken eines Zahlenschlosses vorgeht. Brute Force basiert darauf, dass alle möglichen Kombinationen von Buchstaben, Zahlen und Sonderzeichen so lange ausprobiert werden, bis ein Passwort gefunden wird. Im einfachsten Fall geht man dabei der Reihe nach vor, komplexere Fälle ordnen die einzelnen Möglichkeiten nicht der Reihe nach, sondern erzeugen eine Art Gitter, das den gesamten Bereich der Möglichkeiten abdeckt und vor allem in den Bereichen mit der größten Wahrscheinlichkeit, also beispielsweise im Bereich von sechs- bis zehnstelligen Passwörtern, die engsten Maschen ausbildet.

meisten Passwortvergaben variabel ist), muss er theoretisch für ein n-stelliges Kennwort maximal $100^1 + 100^2 + 100^3 + 100^4 \ldots + 100^n$ Möglichkeiten probieren.

Nochmal: Es lohnt sich auf jeden Fall darüber nachzudenken, ob man nicht ein oder zwei zusätzliche Stellen in sein Passwort einbauen sollte.

Passwörter aus Sätzen

Eine beliebte Möglichkeit, sich Passwörter zu merken, ist das Bilden von Passwörtern aus ganzen Sätzen. Dabei werden jeweils die Anfangsbuchstaben der einzelnen Wörter unter Beachtung der Groß-/Kleinschreibung mit den enthaltenen Satzzeichen aneinandergereiht. Die Kunst ist es, sich möglichst lange, aber dennoch einfache Sätze auszudenken. So kann ein Passwort einfach zu merken und dennoch extrem sicher sein.

Der Satz

> *Peter legt zehntausend Euro bei einer Schweizer Bank in US-Dollar an und spart dabei Steuern, erhält aber andererseits auch einen besonders guten Zinssatz von 4,7 Prozent pro Jahr*

würde das Passwort *PlzEbeSBiUS-DausdS,eaaaebgZv4,7PpJ* ergeben. Ein solch langer Satz ist zwar nicht ganz so einfach zu merken wie ein relativ kurzer, das resultierende Passwort ist dafür aber extrem sicher. Ganz ehrlich, wer kann ein solches Passwort erraten?

Es gibt jedoch auch noch eine empfehlenswerte Erweiterung der Satzmethode: Für Zahlenwerte wie Zehntausend wird die tatsächliche Zahl eingesetzt und Begriffe wie „Euro“, „Dollar“, „und“ und „Prozent“ werden mit den dafür gängigen Zeichen abgekürzt. Unter Anwendung dieser Regel würde aus dem obigen Satz das folgende Kennwort entstehen:

> *Pl10000€beSBiUS-$a&sdS,eaaaebgZv4,7%pJ*

Es ist in einer sinnvollen Zeitspanne nicht zu knacken und stellt damit ein sehr sicheres Kennwort dar, das durchaus für ein E-Mailkonto gewählt werden kann.

Automatische Passwörter

Mit Hilfe von Skripten wie dem folgenden kurzen Java-Programm lassen sich sichere Kennwörter auch automatisch generieren:

```
import java.io.BufferedReader;
import java.io.InputStreamReader;

public class passwordGenerator {
  /**
   * @param args
   */

  public static void main(String[] args) {
    char randomChar = 0;
    int  MAX = 125;
    int  MIN = 33;
```

```
    System.out.println("Bitte Anzahl der Zeichen angeben");
    BufferedReader br = new BufferedReader(
                        new InputStreamReader(System.in));
    String s = null;
    int n = 8;

    try {
      s = br.readLine();
      n = Integer.parseInt(s);
    } catch (Exception e) {        // Eingabefehler
      System.out.println("Eingabefehler, 8-stelliges Kennwort wird " +
                         "erzeugt!");
    }

    String password = "";          // nicht null!
    for (int i = 0; i < n; i++) {
      randomChar = (char) (MIN + (Math.random() * (MAX - MIN)));
      password += randomChar;
    }
    System.out.println(password);
  }
}
```

Dabei werden meist zufällige Zeichen aneinandergereiht, um ein Kennwort von vorgegebener Länge zu erhalten. Auf diese Weise generierte Kennwörter haben den Vorteil, dass sie eine beliebig bestimmbare Länge haben können und man sich keine kleine Geschichte ausdenken muss, um ein derartiges Kennwort zu erzeugen. Der Nachteil solcher Kennwörter ist jedoch, dass sie notiert werden müssen und es für einen Durchschnittsmenschen beinahe unmöglich ist, sich ein generiertes Kennwort ab einer Länge von zwanzig Zeichen zu merken.

Dennoch können auf diese Weise generierte Kennwörter unter Umständen für E-Mailkonten genutzt werden. Da man E-Mails in der Regel mit einem Client abruft, der ein solches Kennwort speichern kann, ist es nicht unbedingt erforderlich, sich das Kennwort zu merken (notieren sollte man es sich jedoch in jedem Fall!). Der eigene E-Mail-Account wird dadurch bedeutend besser abgesichert als auf herkömmliche Art – dies gilt aber nur so lange, wie dem Angreifer nicht der Computer in die Hände fällt.

Zum automatischen Generieren von Passwörtern gibt es zahlreiche Werkzeuge. Unter der Webadresse www.passwort-generator.com findet sich ein solches Werkzeug, das einfach zu bedienen ist und durchaus sichere Passwörter liefert. Dort kann neben der Passwortlänge und der Art der darin enthaltenen Zeichen auch ausgewählt werden, wie viele Passwörter generiert werden sollen und ob diese einfach zu merken sein sollen oder nicht. Wählt man allerdings die Option **Einfach zu merken**, muss man sich darüber im Klaren sein, dass die Passwörter kein ausreichend hohes Maß an Sicherheit für kritische Einsatzzwecke bieten.

Durch einen Klick auf **Generieren** wird die ausgewählte Anzahl an Passwörtern erzeugt. Anschließend kann man sich für eines davon entscheiden.

Ein ähnlicher Generator für Passwörter wird auch unter der Adresse www.sicherespasswort.com angeboten. Dort hat der Benutzer zwar keine Möglichkeit, über die Zusammensetzung des Passwortes zu entscheiden, allerdings werden die unterschiedlichen Passwörter in die Kategorien *Gut*, *Besser*, *Stark* und *Sehr stark* eingeordnet, und so kann der Benutzer auf diese Weise die Zusammensetzung und Länge bestimmen.

Bei den Passwortgeneratoren muss darauf geachtet werden, dass zur Erzeugung der Passwörter keine persönlichen Daten vom Generator verlangt werden dürfen! Wird beispielsweise die E-Mailadresse des Benutzers abgefragt, ist sofort von der Nutzung des Programms Abstand zu nehmen! So kam es Anfang Januar 2012 im Rahmen der Vergeltungsaktion #OpBlitzkrieg, die von der Internet-Aktivistengruppe Anonymous gegen eine bestimmte politische Gruppierung geführt wurde, zu folgender Situation:

Nachdem es einigen Aktivisten von Anonymous gelungen war, persönliche Daten von Parteispendern oder Kunden eines bestimmten Versandhauses zu stehlen, veröffentlichten sie die Daten auf einer eigens dafür gegründeten Prangerplattform (die mittlerweile aus dem Internet genommen wurde). Weitere Aktivisten des Kollektivs Anonymous beschäftigten sich daraufhin damit, die E-Mailkonten der Kunden des Versandhauses unter ihre Kontrolle zu bringen. Laut Anonymous verlief diese Aktion zunächst nur sehr schleppend und man konnte keine Erfolge verzeichnen, da man einfach zu schlecht organisiert war, um die Passwörter der Mailkonten ohne weitere Anhaltspunkte zu knacken. Allerdings währte diese Situation nicht lange. Nach etwa zwei Stunden gelang es einem der Aktivisten, das Passwort zu einem E-Mailkonto zu erraten (angeblich handelte es sich bei diesem Passwort um den Vornamen des Eigentümers) und so die Kontrolle über dieses Mailkonto zu übernehmen. Ausgehend vom Mailkonto fielen den Aktivisten anschließend alle Benutzerkonten, die der Besitzer dieses Mailkontos angelegt hatte, in die Hände.

BILD 4.4 Gefährliche Falle! Trug ein Besucher seine Mailadresse ein und klickte auf „Passwort anfordern“, wurde seine Mailadresse in der Datei data.txt gespeichert und die Aktivisten von Anonymous konnten Zugriff auf die Konten des Besuchers erlangen. Es handelt sich hier um den „Original“-Passwortgenerator, der im Rahmen von #OpBlitzkrieg zum Einsatz kam

Der eigentliche Geniestreich der beteiligten Hacker sah folgendermaßen aus:

Man schrieb einen Passwortgenerator (siehe Bild 4.4), bei dem man seine E-Mailadresse angeben musste, um ein vermeintlich sicheres Passwort zu erhalten. Der Clou dabei war, dass der Passwortgenerator zwar ein sicheres Passwort lieferte, dabei aber die Mailadresse aufzeichnete[21]. Allerdings war der Passwortgenerator in so großer Eile programmiert worden (schließlich durfte vor dessen Verbreitung nicht bekannt werden, dass der Benutzer, der ihn verbreitet, gehackt wurde), dass stets das gleiche Passwort ausgegeben wurde.

Über den Benutzer, dessen Konten geknackt wurden – darunter sein E-Mail- und Facebook-Konto, zahlreiche Accounts in diversen Partnerbörsen, ein Konto bei einem Onlinebuchhändler und zahlreiche weitere Konten – wurde dann an seine Freunde in etwa folgende Nachricht verbreitet (aber nur an die Freunde, bei denen man davon ausging, dass sie Anhänger einer bestimmten politischen Richtung waren):

> *Anonymous versucht, uns alle zu hacken, wir müssen Vorkehrungen treffen, um uns dagegen zu wappnen. Ich habe von einem guten Freund, der Berater bei einem Sicherheitsunternehmen ist, das folgende Skript [Webadresse] empfohlen bekommen, um ein sicheres Passwort für alle meine Konten im Internet zu generieren. Ihr solltet das auch tun, sonst könnte Anonymous Zugang zu allen euren Konten im Internet bekommen.*

Eingebettet in eine dem Benutzer angemessene Sprache und verschärft durch zahlreiche Beleidigungen gegenüber Anonymous wurde diese Nachricht an die Freunde des Benutzers gesendet.

In den folgenden achtundvierzig Stunden riefen laut Angaben einzelner Anonymous-Aktivisten über fünfhundert Empfänger des E-Mails den Passwortgenerator auf. Von diesen trugen zirka dreihundert ihre Mailadresse ein, um das angeblich sichere Passwort zu erhalten. Lediglich ein einziger wurde misstrauisch und trug seine Mailadresse zweimal ein, um zu prüfen, ob das zu unterschiedlichen Passworten führte. Von den dreihundert Personen, die ihre Mailadresse angegeben hatten, wurden laut der Aktivisten von Anonymous insgesamt fünfzig gehackt, da sie das neue Passwort auch tatsächlich in Gebrauch nahmen. Man geht allerdings davon aus, dass die anderen das Passwort nicht aus Vorsicht nicht anwandten, sondern weil es mit zwanzig Zeichen wohl zu lang war.

Unter denen, deren Onlinekonten geknackt wurden, befanden sich nach den Erkenntnissen der Aktivisten sogar insgesamt drei Personen, die eine Ausbildung zum Fachinformatiker absolviert hatten oder gerade absolvierten. Das beweist, wie wenig Wert heute auf Sicherheit gelegt wird und welche Aufklärungsarbeit noch geleistet werden muss.

---

[21] Paradoxerweise wurden alle E-Mailadressen, die von den Besuchern eingegeben wurden, in einer Datei gespeichert (bezeichnet mit data.txt), die in einem Unterverzeichnis des Passwortgenerators lag und in höchstem Maße ungeschützt war. Hätte ein aufmerksamer, fachkundiger Benutzer also auch nur ein wenig Zeit investiert, um die Sicherheit des Passwortgenerators zu prüfen, wäre er unweigerlich auf diese Datei gestoßen und hätte die Gefahr umgehend erkennen müssen.

Dieses Beispiel zeigt, wie leicht man auf Tricks wie diesen hereinfallen kann, und dass es enorm wichtig ist, keine persönlichen Daten anzugeben, um sich von einem Skript ein Passwort generieren zu lassen. Skripte im Internet sind außerdem grundsätzlich kritisch zu betrachten, weil man nicht weiß, wer hinter der Seite steht. Die IP-Adresse des Besuchers erfährt der Webseitenbetreiber automatisch. Es ist aber auch ein Paradebeispiel dafür, wie leicht es für Hacker ist, sich Zugang zu den Konten einer ganzen Benutzergruppe zu verschaffen. Durch ein schwaches Passwort eines einzigen Benutzers gewinnen sie das Vertrauen mehrerer Dutzend anderer Benutzer, indem sie anschließend in die Rolle des gehackten Benutzers schlüpfen. Das ist viel zu leicht, wenn man bedenkt, dass es bei derartigen Angriffen auch um Geld gehen kann. Über einige Konten im Internet ist es nämlich beispielsweise auch möglich, Kreditkartendaten zu erlangen.

Sichere Verbindungen

Ist man im Internet unterwegs, laufen die Daten zwischen den Servern und den Clients die meiste Zeit über Verbindungen, bei denen die Daten unverschlüsselt werden. Das heißt im Klartext, dass sie für jedermann lesbar sind. Das wohl am weitesten verbreitete Protokoll zur Übertragung von Daten im Internet ist http (Hypertext Transfer Protocol)[22]. Es ist das reguläre Protokoll des WWW. Mit ihm werden alle Datenpakete unverschlüsselt transportiert. In diesen Paketen befinden sich natürlich auch vertrauliche Daten wie Passwörter, die unverschlüsselt ohne weiteres von einem Dritten, der sich zwischen den Benutzer und den Server hängt und die ausgetauschten Pakete mitprotokolliert, ausgelesen werden können.

Um Daten verschlüsselt zu übertragen, müssen serverseitig sichere Übertragungsprotokolle wie beispielsweise https (Hypertext Transfer Protocol Secure) eingeschaltet werden. Ein Dritter, der die Leitung abhört, kann aus diesem Datenstrom unmöglich die Passwörter herausfinden und lesbar machen. Zwar könnte er die übertragenen, verschlüsselten Daten mitschneiden, aber diese Informationen haben für ihn keinen Nutzwert, weil er nur eine Folge kryptischer Zeichen vor sich hat. Er müsste vor der Auswertung erst die Verschlüsselung brechen. Die Verschlüsselung ist aber meist so sicher, dass ihr Entschlüsseln nach mathematischer Wahrscheinlichkeit so lange dauern würde, dass die Daten nicht mehr relevant sind. Man geht derzeit von zirka fünf bis zehn Jahren aus, die benötigt würden, die zugrundeliegende Verschlüsselungstechnik zu brechen, selbst wenn mehrere Personal Computer täglich rund um die Uhr mit dieser Aufgabe betraut wären. Es ist also – zumindest bisher – praktisch unmöglich, die Verschlüsselung einer derartigen Verbindung zu knacken.

Allerdings gab es in der Vergangenheit immer wieder Lücken in ähnlichen Verschlüsselungsverfahren, die es Hackern ermöglichten, sie zu knacken. Ausschließen kann man solche Lücken auch heute nicht, eine Verschlüsselung gilt nämlich immer nur so lange

[22] Über dieses Protokoll werden die Inhalte von Websites übertragen. Schon sein Name deutet darauf hin, dass es sich bei den mit ihm übertragenen Daten um HTML-Seiten (Hypertext Markup Language) handelt. Abgekürzt wird der Name des Protokolls mit http; dieser Begriff dürfte jedem Internetnutzer schon einmal in Verbindung mit einer URL, also mit einer Webadresse, begegnet sein.

als sicher, bis jemand sie gebrochen hat. Es ist also durchaus möglich, dass ein mathematisches Genie die gewählte Verschlüsselung knackt und die Verbindung anschließend wieder unsicher ist.

4.2.2 Gegenmaßnahmen der Betreiber

Trotz der vielfältigen Möglichkeiten, die ein Nutzer zur Sicherung seiner Daten ergreifen kann, verbleibt eine gewisse Verantwortung beim Betreiber der sozialen Netzwerke für die Sicherheit ihrer Systeme. Er muss alles daransetzen, eventuelle Lücken in den Systemen zu finden, die es Angreifern ermöglichen könnten, durch absichtlich gesetzte oder unabsichtlich vorhandene Hintertüren (sogenannte Backdoors) in das System einzubrechen und Daten zu stehlen. In der Vergangenheit kamen solche Angriffe mehrfach vor, und auch wenn die Betreiber stets versuchen, derartige Pannen so gut wie möglich zu vertuschen, wurden schon mehrere solcher Pannen in der Öffentlichkeit bekannt – wie zum Beispiel im Dezember 2011 eine Sicherheitslücke, die es ermöglichte, Fotos fremder Facebook-Nutzer zu betrachten[23].

Zugegebenermaßen ist es nicht leicht, wirklich sichere Systeme zu entwerfen, und Sicherheitslücken können nie vollständig vermieden werden. Allerdings sollten die Betreiber sozialer Netzwerke größtmöglichen Wert darauf legen, ihre Systeme sauber zu programmieren und eventuelle Sicherheitslücken umgehend zu schließen. Daneben sollten die Daten der Benutzer auf den Servern der Betreiber durch mehrfache Barrieren abgesichert werden, so dass Eindringlinge ins System nicht sofort Zugang zu den riesigen Datenmengen bekommen, die dort gespeichert sind. Es muss unbedingt darauf geachtet werden, dass die Datenbanken mit den Benutzerdaten nicht mit allseits bekannten Methoden[24] so manipuliert werden können, dass sie ihre Daten freiwillig herausgeben beziehungsweise dass sich Angreifer einen Zugang zu ihnen verschaffen können. Auch sollte darauf geachtet werden, dass die vom Betreiber vergebenen Session-IDs (Sitzungskennungen) so sicher sind, dass sie nicht gefälscht oder zufällig erraten werden können.

Session-IDs sind Sitzungskennungen. Loggt sich ein Benutzer bei einem Online-Dienst ein, erhält er vom Server eine Session-ID, die auf seinem Rechner gespeichert wird und mit der er sich für die Dauer seines Besuchs ausweist. Das Verfahren dient dazu, einen erneuten Loginvorgang bei jeder neuen Anfrage an den Server zu vermeiden und persönliche Daten trotzdem vor fremden Zugriffen zu schützen. Errät ein Angreifer allerdings eine Session-ID, kann er ohne Benutzerpasswort auf dessen Konto zugreifen.

Nachfolgend werden die Maßnahmen der jeweiligen Betreiber vorgestellt, mit denen sie dem Identitätsdiebstahl vorbeugen, und wie man als Benutzer auf Identitätsdiebstahl reagiert und auch die Betreiber in die Pflicht nimmt.

---

[23] Siehe http://www.golem.de/1112/88231.html

[24] Wie beispielsweise dem SQLInject. Dies ist eine Hacking-Methode, bei der Anfragen an eine Datenbank von einem Angreifer so präpariert werden können, dass die Datenbank freiwillig die in ihr gespeicherten Daten an ihn zurücksendet.

Facebook

Facebook hat ein großes Interesse daran, die Benutzer vor Identitätsdiebstahl zu bewahren, schließlich ist es gewissermaßen das Geschäftsmodell, möglichst aussagekräftige Informationen über die einzelnen Mitglieder zu erhalten. Wenn ein Hacker Identitätsdiebstahl betreibt, kann das Facebook also nicht recht sein.

Facebook trifft daher wohl auch die größten Vorsichtsmaßnahmen, um Identitätsdiebstahl zu verhindern. Nach Einschätzung des Autors ist der Dienst technisch durchaus in der Lage, Identitätsdiebstahl in über siebzig Prozent der Fälle festzustellen. Das liegt daran, dass wohl einfach jede Information über einen Benutzer gespeichert ist und daher seine Gewohnheiten ebenso wie sein Standort bekannt sind. Zudem legt Facebook auf den Rechnern der Benutzer zahlreiche Cookies ab (vgl. Bild 4.5), um sie zu identifizieren.

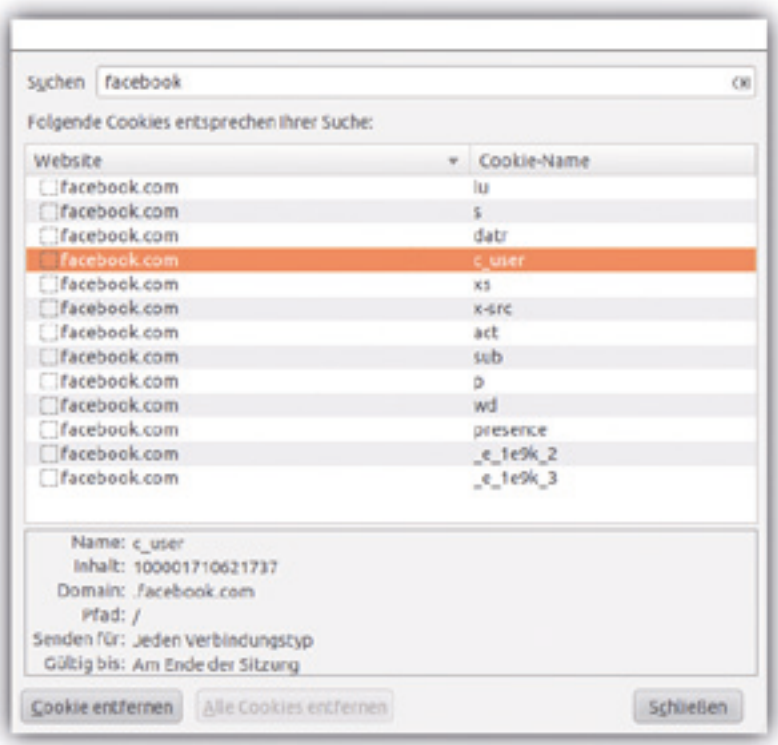

BILD 4.5 Die Cookies von Facebook: eine viel zu lange Liste!

Betrachtet man die Möglichkeiten von Facebook, einen Identitätsdiebstahl zu bemerken, offenbart sich eine ausgefeilte Benutzerüberwachung.

Üblicherweise interessiert sich ein Hacker nicht für Personen aus seinem Umfeld, sondern konzentriert sich auf bestimmte Kreise, gegen die er eine Abneigung hegt, die er

blamieren oder um Geld erleichtern möchte. Aus diesem Grund wird sich ein Hacker meist aus einer völlig anderen Region in das Benutzerkonto des Benutzers einloggen, als der Besitzer dieses Kontos es für gewöhnlich tut.

Es kann auch passieren, dass sich ein Hacker mit einem anderen Browser einloggt als üblicherweise der Besitzer des Benutzerkontos. Den Namen des Browsers sowie die Region, aus der sich der Hacker beziehungsweise der Benutzer eingewählt hat, kann Facebook jederzeit aus dem vom Browser gesendeten Header, der die Browserkennung sowie die IP-Adresse des Benutzers enthält, ermitteln. Hinzu kommt, dass ein normaler Benutzer üblicherweise sämtliche Facebook-Cookies auf seinem PC lässt und daher schon vor dem Login identifiziert werden kann. Ein Hacker wird Facebook aber stets ohne Facebook-Cookies besuchen, um dem Dienst nicht die Möglichkeit zu geben, zu ermitteln, von welchem Account er sich zuvor angemeldet hat.

Es ist zudem unwahrscheinlich, dass der Hacker das Passwort des Benutzers kennt. Daher wird er es in den meisten Fällen per E-Mail zurücksetzen, was Facebook natürlich nicht entgehen wird.

Mit den hier aufgeführten Daten kann Facebook automatisch ermitteln und abwägen, ob es sich um einen Angriff auf das Benutzerkonto handelt oder ob der Benutzer lediglich sein Verhalten geändert hat.

Für einen Benutzer, dessen Identität gestohlen wurde, bietet Facebook die folgenden Möglichkeiten an, darauf zu reagieren: Hat man keinen Zugriff mehr auf sein Konto, kann man sich per E-Mail ein neues Passwort zusenden lassen. Wenn man ein Mobiltelefon bei Facebook registriert hat, kann man auch per SMS ein neues Kennwort anfordern. Hat man keinen Zugriff auf seinen E-Mailaccount und kein Handy registriert, bietet Facebook einem nach wiederholten Schwierigkeiten beim Loginvorgang an – und nur, nachdem das Konto gesperrt wurde –, die Identität durch einen Personalausweis oder irgendein anderes amtliches Papier nachzuweisen (Bild 4.6).

Dadurch gelangt Facebook jedoch in den Besitz wirklich vertraulicher persönlichen Daten und hat zudem eine Bestätigung für die Identität des Benutzers. Deshalb sollte man sich diesen Schritt gut überlegen. Man kann sein Konto jedoch auch sperren lassen, um sich vor dem Zugriff durch Dritte zu schützen. Unter der Adresse http://www.facebook.com/ help/hacked ist beschrieben, wie man vorgeht, wenn man ein kompromittiertes Facebook-Konto melden möchte.

Nachdem man unter der Adresse http://www.facebook.com/hacked auf die Schaltfläche Mein Konto wurde kompromittiert geklickt hat, muss man ein bestehendes oder ein altes Kennwort anzugeben. Anschließend wird man aufgefordert, dem Konto sowie seiner Mailadresse ein neues Kennwort zuzuweisen, sofern man den Verdacht hat, dass auch diese kompromittiert wurden. Im nächsten Schritt muss man eine Sicherheitsfrage einrichten. Auch wenn dies nach Meinung des Autors ein sicherheitstechnischer Fehler ist, lässt sich dieser Schritt leider nicht vermeiden. Zuletzt erscheint ein Fenster, in dem die aktualisierten Daten des Benutzerkontos dargestellt sind und das darauf hinweist, dass die Kontosperre nun aufgehoben ist. Mit einem Klick auf Anmelden hat man dann wieder die Kontrolle über sein Konto.

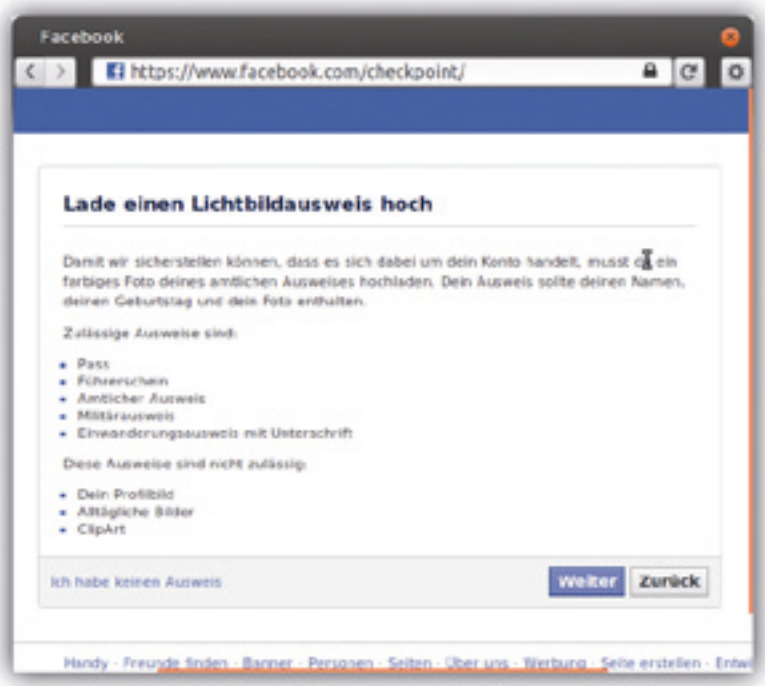

BILD 4.6 Die endgültige Identifikation eines Benutzers bei Facebook

Twitter

Twitter bietet dem Benutzer lediglich die Möglichkeit, das Passwort per E-Mail zurückzusetzen. Dazu klickt man auf den Link PASSWORT VERGESSEN (direkt bei der Anmeldung) und gibt dann die mit dem Konto verknüpfte E-Mailadresse an. Anschließend muss man bestätigen, dass man ein Mensch ist. Hat man bei Twitter keinen Zugang mehr zu seiner E-Mailadresse, muss man sich per E-Mail an das Unternehmen wenden und um eine Löschung des Benutzerkontos bitten. Dies kann nach Erfahrung des Autors recht lange dauern und ist nicht immer erfolgreich. Unter der Adresse https://support.twitter.com/groups/33-report-a-violation/topics/122-reporting-violations/articles/90565-mein-konto-wurde-kompromittiert ist beschrieben, wie man einen gehackten Benutzeraccount meldet.

Kritisch ist, dass es standardmäßig nur von einer der hinterlegten Mailadressen möglich ist, ein Konto zu sperren. Wurden auch diese Adressen kompromittiert, muss sich der Benutzer selbst durchschlagen und Twitter auf einem selbstgewählten Weg kontaktieren.

XING

Auch XING bietet standardmäßig nur die Möglichkeit, das Konto durch den Versand eines neuen Kennworts zurückzusetzen. Auch dazu muss man auf den Link PASSWORT VERGESSEN klicken und seine E-Mailadresse angeben. Möchte man sein Konto löschen lassen, muss man sich ebenfalls an den Betreiber wenden und ihn darum bitten, den Account zu löschen oder zu sperren. Dafür muss man sich an den Support unter http://www.xing.com/app/help?op=start;tab=contact wenden.

Google+

Google+ bietet dem Nutzer die Möglichkeit, das Kennwort per E-Mail zurückzusetzen. Dazu kann die Mailadresse des Google-Accounts oder eine mit dem eigenen Konto verknüpfte E-Mailadresse angegeben werden, an die das Passwort anschließend versandt wird.

Falls man andere Probleme mit der Anmeldung hat – beispielsweise weil man den Verdacht hegt, dass ein Fremder das eigene Konto gekapert hat –, kann man weitere Maßnahmen ergreifen, um das Konto zu schützen. Google kann anhand von zahlreichen Fragen über die eigene Person unter Umständen den Zugang zum eigenen Konto wiederherstellen oder es vor dem Zugriff durch Dritte sperren. Unter der Adresse http://support.google.com/accounts/bin/static.py?hl=de&page=ts.cs&ts=2402620 beschreibt Google das weitere Vorgehen, nachdem man eine Kompromittierung des Kontos festgestellt hat.

Auf der Seite zur Passwortwiederherstellung[25] kann man die gewünschte Option (also beispielsweise PASSWORT VERGESSEN) auswählen und anschließend seinen Benutzernamen eingeben. Nun erscheinen die unterschiedlichen Möglichkeiten der Zurücksetzung des Kennworts. Wer keinen Zugriff mehr auf seine Mailadresse hat, kann sich das Passwort per SMS an eine hinterlegte Handynummer senden lassen. Ist keine Handynummer hinterlegt und hat der Benutzer keinen Zugriff mehr auf seine Mailadresse, kann der Zugang zum entsprechenden Google-Konto nicht wiederhergestellt werden.

meinVZ

meinVZ bietet lediglich die Möglichkeit, den Zugang über die E-Mail-Adresse wiederherzustellen. Hat man auf sie keinen Zugriff mehr oder wurde das E-Mail-Konto durch Dritte entwendet, gibt es keine Standardmethode, um sein meinVZ-Konto vor unbefugtem Zugriff zu schützen. Hier muss der langwierige und mühsame Weg über die Kontaktaufnahme mit dem Betreiber genommen werden. Das Formular http://www.meinvz.net/Contact/2 ermöglicht es dem Nutzer, Kontakt mit dem Betreiber aufzunehmen und ihn um eine Sperrung des Kontos zu bitten.

[25] Sie lautet http://accounts.google.com/RecoverAccount

myspace

Wie die meisten anderen Anbieter bietet myspace nur eine Möglichkeit für das Wiederherstellen des eigenen Benutzerkontos, nämlich den Weg über die E-Mailadresse. Auch hier ist Eigeninitiative gefragt, wenn man eine Sperrung seines Kontos erwirken will, und auch hier ist man vom Wohlwollen des Betreibers abhängig. Man muss daher meist ziemlich lange auf eine Sperrung warten – wenn es einem überhaupt gelingt, diese zu erwirken. Als einzige Anlaufstelle bietet myspace die Seite http://www. myspace.com/help. Das ist ziemlich mager, wenn man bedenkt, welche Probleme Identitätsdiebstahl mit sich bringen kann.

5 Rufmord

Versucht jemand, den Ruf einer anderen Person zu ruinieren (zu „ermorden“), spricht man von Rufmord. Rufmord ist keineswegs nur ein Problem sozialer Netzwerke, sondern vielmehr die Folge sozialer Spannungen. In ausgeprägten Fällen kann Rufmord strafbar sein, nämlich dann, wenn jemand einen anderen bezichtigt, eine bestimmte Tat begangen zu haben, jedoch weiß, dass das nicht stimmt.

5.1 Arten von Rufmord

Auch wenn der Rufmord nicht mit den sozialen Netzwerken erfunden wurde, sondern seit Anbeginn der Menschheit ein probates Mittel zum psychischen und finanziellen Ruin eines Gegners ist, erleichtert das Internet den Rufmord doch wesentlich. Es ist in Foren und Netzwerken relativ einfach, vor einem breiten Publikum erfundene Geschichten über jemanden zu verbreiten, ohne dass dieser es verhindern kann. Stellt man sich geschickt an, bemerkt das Opfer gar nichts von den Machenschaften, insbesondere dann nicht, wenn es nicht selbst Mitglied in dem Forum oder sozialen Netzwerk ist, in dem es verleumdet wird.

In Verbindung mit einer einfachen Form von Identitätsdiebstahl können sich Kriminelle sogar als die Zielperson selbst ausgeben und sich unter deren Namen schlecht benehmen. Möglich ist das, weil man in sozialen Netzwerken nie eindeutig identifiziert werden kann. Schließlich muss bei der Registrierung nicht anhand eines Ausweises nachgewiesen werden, dass man genau die Person ist, die man unter dem angegebenen Namen behauptet zu sein. Jedermann kann einfach ein Benutzerkonto unter dem Namen von jemand anderem anlegen, in Kapitel 2.2.1 auf Seite 69 wurde dies ja sogar als Sicherheitsmaßnahme empfohlen. Ist das Konto dann eingerichtet, ist es anschließend nicht schwierig, das Opfer in ein schlechtes Licht zu rücken und sich in seinem Namen so richtig unanständig zu benehmen.

Insbesondere wenn das Opfer nicht in sozialen Netzwerken registriert ist, fällt das Anlegen eines gefälschten Benutzerkontos unter seinem Namen leicht. Wenn der Betrüger dann fleißig am seinem Ruf sägt, werden seine entfernten Freunde und Bekannte – oder

auch Kunden, die mit dem Charakter und den Gewohnheiten des Opfers nicht so vertraut sind – sich wahrscheinlich eher von ihm zurückziehen und zukünftigen Kontakt meiden, als mit ihm zu sprechen und nach den Gründen für sein seltsames Benehmen zu fragen.

Ist jemand in sozialen Netzwerken registriert, ist es schwerer, im Namen dieser Person zu handeln. Sinnvoll ist eine Verleumdung ja nur im Bekannten- beziehungsweise Freundeskreis, also bei den Personen, die einen schlechten Eindruck vom Opfer gewinnen sollen. Enge Freunde würden aber eine Fälschung der Identität schnell bemerken, weil ihnen ein ungewöhnliches Verhalten auffallen würde und sie nachfragen würden, was denn passiert sei.

Natürlich ist Rufmord auch hier ärgerlich, denn einen bestimmten Kreis von Empfängern erreicht der Verantwortliche in jedem Fall und irgendetwas bleibt immer hängen, wenn mit Schmutz geworfen wird.

Je nach Ausmaß ist Rufmord im deutschem Recht strafbar. Unterschieden werden dabei drei Arten von Rufmord (StGB §§186, 187):

- Der am schwächsten ausgeprägte Fall, die *Diskreditierung*, besteht darin, das Vertrauen oder die Glaubwürdigkeit, die einer bestimmten Person entgegengebracht wird, zu untergraben. Diskreditierung selbst ist noch nicht strafbar, sofern diese nicht in einem Ausmaß, das den folgenden beiden Fällen entspricht, ausgeübt wird.
- Die sogenannte *üble Nachrede* besteht darin, Tatsachen, die nicht erwiesen sind, aber dazu dienen, eine andere Person herabzuwürdigen oder verächtlich zu machen, zu behaupten oder zu verbreiten. Dieser Fall von Rufmord ist strafbar und findet seinen Bestand in §186 des Strafgesetzbuches (StGB). Als Strafmaß ist dafür eine Geldstrafe und in besonders schweren Fällen sogar Gefängnis von bis zu zwei Jahren vorgesehen.
- Die sogenannte *Verleumdung* unterscheidet sich von der üblen Nachrede darin, dass dabei wissentlich Lügen über das Opfer verbreitet werden, während im Fall der üblen Nachrede lediglich Tatsachen, die als nicht erwiesen gelten, behauptet werden. Bei der Verleumdung behauptet der Täter also absichtlich Dinge, die frei erfunden sind, um das Opfer in Verruf zu bringen oder ihm auf andere Weise zu schaden. Auch Verleumdung wird gewöhnlich mit Geldstrafen geahndet, in besonders schweren Fällen sind Haftstrafen von bis zu fünf Jahren vorgesehen.

5.2 Gegenmaßnahmen

Bei einer besonders schweren Form des Rufmords kann das Opfer eine Anzeige gegen den Urheber erstatten. Üblicherweise landet man jedoch selten tatsächlich vor Gericht, in den meisten Fällen genügt es, den Verursacher abzumahnen und ihm die rechtlichen Konsequenzen seines Handelns aufzuzeigen – sofern man den Urheber kennt und Zugriff auf ihn hat.

Kennt man den Urheber der Kampagne nicht beziehungsweise kennt nicht seinen echten Namen oder führt er trotz einer Abmahnung seine Rufmordkampagne fort, ist man darauf angewiesen, dass der Betreiber des sozialen Netzes einschreitet und die Machenschaften unterbindet, das heißt, den fraglichen Inhalt löscht.

Auch die Polizei wird sich an den Netzbetreiber wenden und ihn auffordern, den strittigen Inhalt zu löschen. Sollten dadurch Kosten entstehen, werden sie natürlich an den Täter weitergereicht. Dies steht so auch in Punkt 15.2 des Impressums von Facebook:

> *„Wenn jemand einen Anspruch bezüglich deiner Handlungen, deiner Inhalte oder deiner Informationen auf Facebook gegen uns erhebt, wirst du uns von sämtlichen Schäden, Verlusten und Ausgaben (einschließlich angemessener Anwaltshonorare und Rechtskosten) schadlos halten.“*

Auf den Benutzeroberflächen aller Dienste werden Funktionen angeboten, mit denen ein Opfer dem Betreiber Verstöße gegen die Ordnung und über den Missbrauch von Daten in jeglicher Form melden kann. Leider reagieren diese in den seltensten Fällen darauf, und falls doch, dann meist nur, wenn vermehrt Beschwerden und Meldungen eingehen.

So ist es beispielsweise in Facebook möglich, es dem Betreiber anzuzeigen, wenn jemand eine Identität gestohlen hat und unter falschem Namen auftritt. Aber auch hier werden Einzelmeldungen nicht unbedingt überprüft und verfolgt. Facebook sagt selbst im Impressum[1]:

> *„Wenn dir auf Facebook etwas auffällt, von dem du denkst, dass es gegen unsere Bestimmungen verstößt, solltest du uns das melden. Bitte denke daran, dass durch das Melden eines Inhalts nicht garantiert wird, dass er von Facebook entfernt wird.*
>
> *Aufgrund der Vielfalt unter unseren Mitgliedern ist es möglich, dass du Inhalte als beunruhigend empfindest, diese aber gleichzeitig nicht unter unsere Kriterien für Inhalte, die entfernt oder blockiert werden, fallen.* [...]“

Um einen Missetäter zu melden, muss man seine Chronik (oder sein Profil) besuchen und mit einem Klick auf das Einstellungssymbol die Option MELDEN/BLOCKIEREN auswählen. Anschließend kann der Grund angeklick werden, weshalb die Person gemeldet werden soll (Bild 5.1). Ähnlich verhält es sich bei den anderen Netzwerken: Die Funk-

[1] Siehe unter http://www.facebook.com/communitystandards

tionen sind zwar vorhanden, eine Reaktion auf Beschwerden ist jedoch in den seltensten Fällen zu erwarten.

BILD 5.7 So wird in Facebook ein Betrüger gemeldet

Hat die Meldung keinen Erfolg, muss man versuchen, den Betreiber per E-Mail oder Kontaktformular zu erreichen. Bei Facebook ist dies ohne weiteres gar nicht möglich. Die meisten anderen Anbieter stellen immerhin ein Kontaktformular bereit oder geben im Impressum eine Kontakt-Mailadresse an. Leider ist auch dieses Vorgehen in den meisten Fällen wirkungslos und der Benutzer muss sich auf eine lange Wartezeit gefasst machen und außerdem nachweisen, dass es sich tatsächlich um einen Fall von Rufmord handelt. Dieses Verhalten der Betreiber ist zwar nicht sonderlich rühmlich, jedoch nachvollziehbar. Wäre es so einfach, ein Benutzerkonto zu deaktivieren oder einen Beitrag zu löschen, könnten übermütige Nutzer aus Jux und Tollerei andere Nutzer ärgern, und Probleme wie Cybermobbing würden zur Tagesordnung in sozialen Netzwerken gehören.

Es ist also letztlich sehr schwierig, gegen Rufmord vorzugehen. Man muss sich vor einer Meldung gut überlegen, ob sich der Aufwand auch wirklich lohnt und ob man dazu bereit ist, den Verleumder und den Betreiber des sozialen Netzwerkes im Zweifelsfall zu verklagen und eine Löschung und Richtigstellung an gleicher Stelle zu fordern. In der Realität käme ein Gerichtsurteil meistens sowieso viel zu spät, das Unheil wäre ja schon längst angerichtet und die Gegenmaßnahmen wären nicht mehr wirksam.

Sollte man sich dennoch für den Rechtsweg entscheiden, bleibt immer die Möglichkeit, bei der Polizei Anzeige gegen den Urheber eines Rufmords zu erheben.

5.3 Wirksamkeit

Egal, ob man bei der Polizei war oder den Betreiber des Netzes darüber informiert und ihn gebeten hat, die veröffentlichten Inhalte zu löschen und eine Richtigstellung zu veröffentlichen – die Frage ist immer, ob dann nicht schon alles zu spät ist und die Falschinformationen den Ruf bereits dauerhaft geschädigt haben. Hat ein Beitrag im Internet erst eine gewisse Beliebtheit erreicht, ist es beinahe unmöglich, ihn wieder daraus zu entfernen. Zwar kann der ursprüngliche Beitrag gelöscht werden, allerdings werden die Inhalte von Websites von großen Suchmaschinen wie Google oder Bing meist zwischengespeichert, damit sie eine schnelle Vorschau liefern können. Daher kann es vorkommen – und ist auch durchaus an der Tagesordnung –, dass Teile eines Beitrags (oder auch der gesamte Beitrag) nach seiner Löschung noch in Suchergebnissen angezeigt werden. Natürlich ist es auch nie ausgeschlossen, dass andere den Inhalt dieses Beitrags weiterverbreiten.

Selbst wenn eine Richtigstellung veröffentlicht wurde, ist sie oft deshalb wirkungslos, weil die zahlreichen Kopien eines Beitrags, die nach einer gewissen Zeit im Umlauf sind, nicht automatisch mit dem Original abgeglichen werden. Eine Richtigstellung der Originalinformation erreicht also längst nicht wieder alle Leser.

6 Nachwort

Im Lauf dieses Buches wurden die Gefahren der sozialen Netzwerke aufgezeigt. Nun stellt sich natürlich die Frage, ob es nicht besser wäre, ganz auf sie zu verzichten. Die Meinung des Autors zu diesem Thema soll den Lesern hier natürlich nicht vorenthalten werden. Es soll aber noch einmal ausdrücklich darauf hingewiesen werden, dass auch der Verzicht auf soziale Netzwerke unter individuellen Aspekten beurteilt werden muss; dabei es sich handelt zwar gewissermaßen um eine Universalproblemlösung, aber sie ist nicht unbedingt in allen Fällen die beste Lösung.

Meiner Meinung nach ist ein Verzicht auf soziale Netzwerke bei bestimmten Personen durchaus sinnvoll. Es kommt aber ganz auf den Freundeskreis an, ob eine Mitgliedschaft tatsächlich nötig ist. Wenn die meisten Freunde ebenfalls auf die Netzwerke verzichten können und wollen, ist ein Verzicht durchaus ratsam. Wenn der eigene Freundeskreis jedoch intensiven Gebrauch von sozialen Netzwerken macht, würde man sich durch einen Verzicht selbst die Kommunikationsmöglichkeiten beschneiden. Besonders bei Jugendlichen ist aus dieser Perspektive ein Verzicht meist eher nachteilig, da inzwischen nahezu jeder Jugendliche Mitglied sozialer Netzwerke ist und sie auch intensiv nutzt.

6.1 Vorteile des Verzichts

Die wichtigsten Vorteile bei einem Verzicht auf soziale Netzwerke wurden alle im bisherigen Verlauf des Buchs geschildert, sollen hier jedoch der Vollständigkeit halber noch einmal kurz zusammengefasst werden:

- Durch einen Verzicht auf soziale Netzwerke wird ein in letzter Zeit leider verlorengegangener großer Vorteil des Internets wiederhergestellt: die Anonymität in einem Medium, in dem jedermann die Möglichkeit hat, seine Meinung zu verbreiten und sich zu informieren. Gerade durch diese Anonymität wird das Internet zu einem Medium, in dem sich niemand davor fürchten muss, diskriminiert zu werden. Schließlich kann er heute als konservativ eingestellter Fundamentalist auftreten und am nächs-

ten Tag den Eindruck eines lockeren, modernen Menschen erwecken, ohne dass ihn irgendjemand mit seinem Auftreten vom Vortag identifizieren wird.

- Ein Verzicht auf soziale Netzwerke fördert die Anonymität auch im Hinblick auf persönliche Daten. So kann ohne soziale Netzwerke niemand einfach an Daten des Internetnutzers kommen und sie missbrauchen. Persönliche Daten sind in unserer heutigen Gesellschaft ein äußerst wichtiges Gut. Viele Menschen würden alles darum geben, um die Veröffentlichung ihrer persönlichen Daten im Nachhinein rückgängig machen zu können, nachdem sie daraus große Nachteile erlitten haben.
- Ohne soziale Netzwerke würden für viele die Chancen auf einen Arbeitsplatz oder einen Ausbildungsplatz wesentlich besser stehen. Jeder hat seine Fehler, doch üblicherweise kann ein Arbeitgeber die Fehler seiner Bewerber nicht ermitteln. Durch soziale Netzwerke kann er sich aber sehr wohl schon vor dem Vorstellungsgespräch über seine möglichen zukünftigen Beschäftigten informieren und bereits im Voraus anhand ihres Profils eventuelle Einstellungshindernisse ermitteln.

6.2 Nachteile des Verzichts

Durch den vollständigen Verzicht auf soziale Netzwerke können sich natürlich auch einige Nachteile ergeben, die gegen die Vorteile eines Verzichts abgewogen werden sollten.

Die größten Nachteile ergeben sich sicherlich aus den von sozialen Netzwerken bereitgestellten Diensten. So kann der ursprüngliche Zweck sozialer Netzwerke, nämlich die Vernetzung mit den Freunden über das Internet ohne die Mitgliedschaft in einem sozialen Netzwerk nicht mehr genutzt werden. Möchte man dann mit den Freunden über das Internet kommunizieren, muss man nach anderen Möglichkeiten Ausschau halten, die meist aber nicht annähernd so komfortabel wie soziale Netzwerke sein werden.

Außerdem kann es passieren, dass der Netzwerkverzichter ins Abseits gerät, weil seine Freunde Gebrauch von sozialen Netzwerken machen und er sich deshalb ausgeschlossen fühlen wird.

6.2.1 Anschluss zu Freunden

Die Frage, ob man den Anschluss zu Freunden verliert, wenn man nicht Mitglied sozialer Netzwerke ist oder seine Mitgliedschaft bei diesen aufgibt, hängt eng damit zusammen, welcher Benutzergruppe man selbst angehört.

Ein Jugendlicher verliert unter gewissen Umständen eher den Anschluss als ein Erwachsener in einem Alter von über 30 Jahren. Allerdings kann auch dieser Erwachsene den Anschluss verlieren, was aber ganz von seiner Umgebung abhängt. Allerdings sollte man

sich darüber im Klaren sein, dass Freundschaften, die nicht über das Internet gegründet wurden, keine echten Freundschaften sind, wenn sie daran zerbrechen, dass man auf soziale Netzwerke verzichtet.

Betrachten wir einen Jugendlichen, der noch zur Schule geht und bisher regelmäßig in sozialen Netzwerken unterwegs war, um auch dort seine Freunde zu treffen. Er entscheidet sich aufgrund der in diesem Buch aufgeführten Nachteile dazu, soziale Netzwerke in Zukunft nicht mehr zu nutzen. Hier ist aber dennoch nicht davon auszugehen, dass er den Anschluss zu seinen Freunden verlieren wird, weil er schließlich einen großen Teil von ihnen nahezu täglich in der Schule trifft. Den Rest kann er nachmittags nach Schulschluss sehen, wenn er etwas gemeinsam mit ihnen unternimmt. Lediglich virtuelle Freundschaften, die bisher ausschließlich über soziale Netzwerke gepflegt wurden, gehen unter Umständen verloren. Allerdings sind soziale Netzwerke nicht der einzige Ort, an dem virtuelle Freundschaften gepflegt werden und so können sie unter Umständen auch in Foren oder Chatrooms weitergeführt werden und müssen nicht notwendigerweise verloren gehen.

Betrachtet man den selben Nutzer nur wenige Jahre später, kann sich seine Situation erheblich geändert haben. Beispielsweise hat er nach der Schule ein Studium aufgenommen und ist in eine andere Region gezogen. Nun kann er seine alten Schulfreunde nicht mehr täglich treffen und ist auf soziale Netzwerke angewiesen, wenn er Kontakt mit ihnen halten möchte. Nun, wirklich auf soziale Netzwerke angewiesen ist er nicht, schließlich ging es früher ja auch ohne, aber die Gebräuche haben sich dahingehend verändert, dass man Kontakte zu früheren Schulfreunden ohne soziale Netzwerke durchaus verlieren kann. Ein wirkliches K.O.-Kriterium ist das jedoch trotzdem nicht, schließlich kann man durchaus auch auf andere Weise Kontakt zu seinen Freunden aufnehmen, und wenn man wirkliches Interesse an ihnen hat und auch diese die Freundschaft weiter pflegen wollen, verliert man sich gegenseitig nicht so leicht aus den Augen.

Mit der Betrachtung der beiden geschilderten Fälle sind eigentlich schon die Benutzergruppen, bei denen ein Verzicht auf soziale Netzwerke tatsächlich einen Einschnitt darstellen kann, abgedeckt. Die älteren Generationen sind sozialen Netzwerken meist ohnehin nicht so verbunden, dass sie sich ohne diese in ihren Möglichkeiten beschnitten sehen würden.

6.2.2 Informationsmangel

Neben der Frage, ob der Kontakt zu Freunden verloren gehen könnte, muss man sich eine weitere Frage stellen (und beantworten), bevor man sich dazu entschließt, auf soziale Netzwerke zu verzichten: Muss man mit den sozialen Netzwerken auch auf Informationen verzichten, die einem persönlich wichtig sind?

Es kann passieren, dass insbesondere Neugierige beim Ausstieg eine ihrer Hauptinformationsquellen verlieren. Auch wenn das für die meisten wohl kein erhebliches Problem darstellt, sollte man sich als besonders Neugieriger darüber im Klaren sein, dass es zu einer Beschneidung des Informationsflusses kommen wird.

Aber nicht nur jene, die ihren Riecher gerne in fremde Angelegenheiten stecken, können dann an Informationsmangel leiden. Auch der Durchschnittsmensch, der von Natur aus eine gewisse Neugier mitbringt, kann durch den Verzicht auf soziale Netzwerke im Vergleich zu anderen weniger informiert sein. Es hat sich in den letzten Jahren nämlich leider eingebürgert, viele Informationen gar nicht mehr persönlich und mündlich weiterzugeben, sondern an zentraler Stelle schriftlich zu dokumentieren – eben in sozialen Netzwerken. So kann es beispielsweise passieren, dass man von einem recht guten Freund gar nicht erfährt, dass er einen neuen Arbeitsplatz gefunden hat, weil er davon ausgeht, dass es jeder weiß – weil er es ja in einem sozialen Netzwerk veröffentlicht hat.

So kann der Verzicht auf soziale Netzwerke auch für Mitmenschen mit einer gesunden Neugierde einen Einschnitt darstellen, da sie von ihren Freunden nicht mehr alles das erfahren, was sie gerne wissen möchten. Allerdings lohnt es sich in solchen Fällen auch, mit den eigenen Freunden zu reden und diese zu bitten, einem doch etwas mehr zu erzählen, schließlich sei man ja kein Nutzer sozialer Netzwerke mehr und bekomme daher nicht mehr alles mit.

6.3 Ungelöste Probleme

Doch auch durch den Verzicht auf soziale Netzwerke können bestimmte Probleme nicht vollständig gelöst werden.

So ist es beispielsweise nicht möglich, ausschließlich durch den Verzicht auf soziale Netzwerke zu verhindern, dass die Betreiber in den Besitz von persönlichen Daten kommen. Wie bereits erläutert, müssen spezielle Browser-Erweiterungen (Plugins) installiert werden, um die schnüffelnden Betreiber sozialer Netzwerke erfolgreich abzuwehren. Theoretisch gäbe es für die Abwehr der Datenschnüffler auch noch weitere Möglichkeiten wie beispielsweise das Verbot von Cookies oder wenigstens die erhöhte Aufmerksamkeit, was diese anbelangt. Das ist aber fast nicht mehr möglich, da Cookies mittlerweile ein derart wichtiger Bestandteil von Internetangeboten sind, dass das Internet ohne sie einfach keinen Spaß mehr macht und auch Anwendungsgebiete wie das Onlinebanking und ähnliche Dienste ausfallen würden.

Denkbar wäre es theoretisch auch, die Webseite eines sozialen Netzwerkes niemals zu besuchen. Dann hätte dieses niemals die Möglichkeit, ein Cookie auf dem Rechner des Besuchers abzulegen und wäre damit auch nicht in der Lage, ihn auszuspionieren. Allerdings ist dies utopisch. Es ist vielleicht möglich, die Seiten von myspace, XING oder meinVZ beziehungsweise FreundeVZ zu meiden. Die Seiten großer sozialer Netzwerke wie Facebook nie anzusteuern ist dagegen sehr kompliziert und die Seiten von Google zu vermeiden klingt geradezu unmöglich. Der Grund ist, dass nahezu alle Webseiten, die ein größeres Publikum erreichen, Querverlinkungen zu Facebook enthalten, die aber nicht immer als solche ersichtlich sind. So bemerkt man oft erst, wenn man bereits auf der Facebook-Startseite gelandet ist, dass jener Link zu Facebook führte. Die Seiten

von Google zu meiden würde bedeuten, auf alle Dienste, also auch auf die Suchmaschine, zu verzichten. Das ist wirklich unrealistisch.

Auch die Gefahr eines Rufmordes kann durch den Verzicht auf soziale Netzwerke nicht umgangen werden. Ganz im Gegenteil: Die Situation könnte sogar verschärft werden, denn andere können völlig unkontrolliert Gerüchte über Personen verbreiten, die nicht in sozialen Netzwerken registriert sind; nicht registrierte Benutzer können diese Aktivitäten schließlich nicht verfolgen. Ebenso ist es möglich, sich als eine nicht registrierte Person auszugeben und ein Profil unter dem Namen unter ihrem Namen anzulegen und in ihrem Namen alle denkbaren Informationen zu verbreiten. Ein Registrierter bekommt wahrscheinlich Wind davon und hat die Möglichkeit, dagegen vorzugehen. Als nicht registrierter Benutzer bekommt man nicht mit, dass ein anderer unter dem eigenen Namen sein Unwesen treibt, und kann auch nicht dagegen vorgehen.

Diese beiden geschilderten Probleme lassen sich also auch durch einen Verzicht auf soziale Netzwerke nicht lösen. Sie sind vielmehr ein Beweis dafür, dass die Gefahren sozialer Netzwerke jeden Internetnutzer, im Grunde sogar jedermann betreffen. Natürlich bringen soziale Netzwerke auch Vorteile in unser alltägliches Leben, und die eigentliche Idee, die hinter ihnen steckt, ist im Grunde überhaupt nichts Schlechtes. Vielmehr sind es die Betreiber, die mit ihren Leistungen Geld verdienen wollen beziehungsweise müssen und dabei die Nutzer selbst zum Gegenstand ihres Handelns machen. Aber wenigstens außerhalb ihrer Dienstleistungen wäre es angebracht, den Internetnutzer in Ruhe zu lassen und keine zusätzlichen Daten von ihm auszuspionieren.

A Anhang

A.1 Reichweite von „Freunde von Freunden“

Die Reichweite „für Freunde von Freunden sichtbar“ tritt in den verschiedenen sozialen Netzwerken unter unterschiedlichen Namen auf, bedeutet jedoch stets das gleiche: Eine Information, die unter dieser Sichtbarkeit veröffentlicht wurde, erreicht alle Freunde des Autors sowie alle Freunde der Freunde des Autors.

Je nach Autor und seinen Freunden kann die Reichweite einer solchen Information stark schwanken, daher soll später zwischen unterschiedlichen Benutzern unterschieden werden. Dennoch soll an dieser Stelle zunächst eine allgemeingültige Faustregel hergeleitet werden, wie viele Personen durchschnittlich erreicht werden.

Nimmt man an, der Autor hat n Freunde und die Anzahl der Freunde jedes einzelnen Freundes ist mit k_n bezeichnet, wobei n für den n-ten Freund des Autors steht. Nähme man weiter an, dass zwei Freunde des Autors niemals einen gemeinsamen Freund haben und auch der Autor keinen gemeinsamen Freund mit einem seiner Freunde hat, so wäre die Formel zur Berechnung der Reichweite ziemlich trivial.

Gleichzeitig ist diese Formel gültig für den schlimmsten anzunehmenden Fall, also die maximale Reichweite der Information. Um das kurz zu verdeutlichen, gehen wir von einem jugendlichen Facebook-Nutzer aus und berechnen beispielhaft die Reichweite einer von ihm geteilten Information im Worst-Case-Szenario:

$$R = n + \sum_{i=0}^{i=n} (k_i)$$

Ein Jugendlicher, der regen Gebrauch von Facebook macht, hat im Durchschnitt dort zirka 200 Freunde. Von diesen 200 Freunden nutzen zirka 5 Prozent (also 10 Personen) Facebook sehr intensiv und haben im Schnitt selbst wieder zirka 500 Freunde. Der Rest hat wie auch der Facebook-Nutzer selbst durchschnittlich 200 Freunde.

Eingesetzt in die Formel ergibt sich für eine geteilte Information dieses Nutzers also eine Reichweite R von 43200 Personen. Das ist erschreckend!

R = 200 + 10 * 500 + 190 * 200 = 43200

Allerdings ist hier bereits die Benutzergruppe mit der zweitgrößten Reichweite herausgegriffen und die Realität ist deutlich blumiger. Der Hauptgrund für diese große Reichweite ist sicherlich, dass es Überschneidungen in den Freundeslisten der einzelnen Benutzer gibt. Das ist auch nicht weiter verwunderlich, schließlich kennen sich zwei gute Freunde einer Person in der Realität meistens gegenseitig und daher auch in sozialen Netzwerken. Um diese Überschneidung in der obigen Formel zu berücksichtigen, müssen ein paar Mittelwerte herangezogen werden, die jedoch bei den unterschiedlichen Benutzergruppen sehr unterschiedlich ausfallen können. Aus diesem Grund soll zunächst eine allgemeingültige Formel mit mehreren Parametern erarbeitet werden, die Konstanten können dann in einer Tabelle für die Nutzer unterschiedlicher Nutzergruppen abgelesen werden.

Um möglichst exakte Werte für die Reichweite zu erhalten, müssen die Freunde zunächst in Gruppen aufgeteilt werden:

- Enge Freunde haben bis zu 80 Prozent gemeinsame Freunde mit dem Autor.
- Freunde mit gleichen Interessen haben bis zu 60 Prozent gemeinsame Freunde mit dem Autor.
- Bekannte haben etwa 15 bis 30 Prozent gemeinsame Freunde mit dem Autor.
- Entfernte Freunde haben zirka 5 Prozent gemeinsame Freunde mit dem Autor.

Zunächst wollen wir noch einmal vernachlässigen, dass Freunde des Autors untereinander gemeinsame Freunde haben können, da dieser Umstand die Formel äußerst kompliziert gestalten würde.

Die Formel für die Reichweite bei Überlappung auf erster Ebene ist

$$R = n_{ges} + \sum_{i=0}^{i=n_1} (k_{n_1}) \cdot 0{,}2 + \sum_{i=0}^{i=n_2} (k_{n_2}) \cdot 0{,}4 + \sum_{i=0}^{i=n_3} (k_{n_3}) \cdot 0{,}775 + \sum_{i=0}^{i=n_4} (k_{n_4}) \cdot 0{,}95$$

Im Grunde könnte man diese Formel noch weiter verallgemeinern und würde dann eine ähnliche erhalten, die allerdings ein Summenzeichen für jede Anzahl an gemeinsamen Freunden mit einem Freund enthalten würde. Es ist also einfacher, seine Freunde in die angegebenen Kategorien einzusortieren und mit einem genäherten Ergebnis zu rechnen. Diese Formel beruht allerdings immer noch auf der Annahme, dass die Freunde untereinander keine gemeinsamen Freunde haben, und ist daher in der Praxis immer noch ziemlich ungenau.

Wenn man diesen Umstand in seine Berechnungen einbeziehen möchte, muss man aus Aufwandsgründen hier mit Mittelwerten rechnen. Geht man allerdings davon aus, dass eine Person zahlreiche Freunde aus einer bestimmten Region hat, jedoch nur wenige außerhalb dieser Region, so kann man eine nicht zu komplexe Formel finden, nach der sich die Reichweite R näherungsweise berechnen lässt. Kommen alle Freunde aus einer Region, kann man davon ausgehen, dass die Freunde untereinander durchschnittlich je

30 Prozent gemeinsame Freunde haben. Dabei handelt es sich jedoch immer um unterschiedliche Freundeskreise, die diese miteinander gemeinsam haben.

Aus den ermittelten Werten ergibt sich, dass nur etwa 10 Prozent der Freunde von Freunden erreicht werden. Es ergibt sich die folgende Formel:

$$R = n_{ges} + \frac{(\sum_{i=0}^{i=n_1}(k_{n_1})\cdot 0{,}2 + \sum_{i=0}^{i=n_2}(k_{n_2})\cdot 0{,}4 + \sum_{i=0}^{i=n_3}(k_{n_3})\cdot 0{,}775 + \sum_{i=0}^{i=n_4}(k_{n_4})\cdot 0{,}95)}{10}$$

Setzt man in diese Formel realistische Werte ein, kann man die ungefähre Reichweite eines Beitrags ermitteln. Man nehme an, ein Schüler habe insgesamt 250 Freunde. Davon entsprechen 5 Freunde den Anforderungen für enge Freunde im oben definierten Sinne. Etwa 80 Freunde entsprechen den Anforderungen für Freunde mit gleichen Interessen. Dies sind die Mitschüler seiner Stufe, die mehr oder weniger alle untereinander befreundet sind und so einen recht großen Freundeskreis teilen.

Nur etwa 20 Freunde können den entfernten Freunden zugeordnet werden und der Rest, also 145 Freunde, sind Bekannte.

Die mittlere Anzahl der Freunde seiner Freunde beträgt 250 Personen.

Setzt man diese mittlere Anzahl nun in die obige Formel ein, ergibt sich eine Reichweite R von 4348 Personen.

R = 250 +(5 * 250 * 0,2 + 80 * 250*0,4 + 145 * 250 * 0,772 + 20 * 250 * 0,95) / 10

R = 250 + 25 * 5 * (0,2 + 16 * 0,4 + 29 * 0,772 + 4 * 0,95)

R = 250 + 4098,5

R = 4348,5

Diese Anzahl ist zwar deutlich besser zu ertragen als die Reichweite von 43200 Personen aus den ersten Berechnungen. Allerdings ist sie immer noch wesentlich zu hoch, um leichtfertig irgendwelche Informationen an derart viele Leute zu geben. Da die obige Formel relativ kompliziert ist, um damit die Reichweite eines Beitrags schnell bestimmen zu können, soll eine vereinfachte Form dieser Formel als Faustregel gelten:

Die mittlere Reichweite R soll bestimmt werden können aus der Anzahl der eigenen Freunde sowie einer Konstante c, die davon abhängt, welcher Gruppe von Nutzern man angehört. Es gilt also die Formel:

$$R = N_{Freunde} \cdot c$$

Diese Faustregel gilt für die Reichweite eines Beitrags. c muss dabei in Tabelle 7.1 abgelesen werden.

Im eben betrachteten Fall entspricht c einem Wert von zirka 17,5. Für die unterschiedlichen Benutzergruppen können die unterschiedlichen Konstanten der folgenden Tabelle entnommen werden.

TABELLE A.1 Die Werte für die Konstante c in Abhängigkeit vom Benutzertyp

Benutzergruppe	c
Schüler	17,5
Studenten	20
Erwachsene bis ca. 30 Jahre	22,5
Erwachsene bis ca. 50 Jahre	35
Erwachsene ab 50 Jahre	27,5

A.2 Schichten um einen Benutzer

In sozialen Netzwerken bilden sich um einen Benutzer herum gewisse Schichten von anderen Benutzern. Diese Schichten unterscheiden sich darin, wie sie zu dem Benutzer selbst stehen, und können mit den Schichten im realen Leben um eine Person verglichen werden, allerdings mit dem Unterschied, dass die Schichten in sozialen Netzwerken wesentlich näher am Benutzer sind als in der Realität.

In Bild A.1 sind die Schichten um eine reale Person gezeigt und den Schichten um den Nutzer eines sozialen Netzwerkes gegenübergestellt.

Das Schichtenmodell der sozialen Netzwerke ist gegenüber dem Schichtenmodell der Realität deutlich skaliert, außerdem ist die Anzahl der Personen jeder Schicht mit Ausnahme des Partners größer als in der Realität. Aber auch der Partner nimmt in sozialen Netzwerken gegenüber den in Ebene 3 befindlichen Freunden keine Sonderstellung mehr ein, sondern steht dem Nutzer ebenso nahe wie der Rest seiner Freunde.

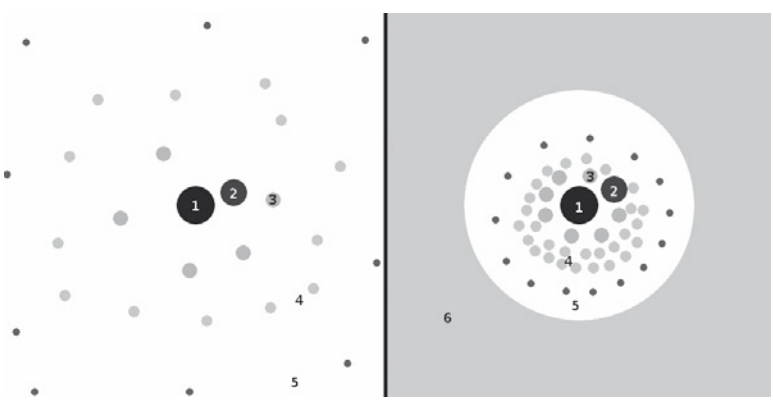

BILD A.1 *Links:* Schichtenmodell der Realität, *rechts:* Schichtenmodell in sozialen Netzwerken. Der Kreis 1 stellt die Person dar, um die es geht, der Kreis 2 stellt den Partner dieser Person dar, die Kreise in Ebene 3 markieren die Freunde, Kreise der Ebene 4 markieren gute Bekannte, Kreise der Ordnung 5 markieren entfernte Bekannte und der Bereich 6 stellt die Öffentlichkeit dar.

Die Öffentlichkeit, die in das Schichtenmodell der Realität aus Platzgründen nicht mehr integriert wurde, steht dem Benutzer in sozialen Netzwerken in etwa so nahe wie die guten Bekannten in der Realität. Dabei sind die Freunde von Freunden, die dem Benutzer unbekannt sind und die in sozialen Netzwerken noch einmal eine Sonderstellung einnehmen, gar nicht in das Schaubild integriert. Sie stehen zwischen den entfernten Bekannten und der Öffentlichkeit.

Aus dem Schaubild geht hervor, wie stark soziale Netzwerke die Privatsphäre reduzieren, wobei es noch die Situation einer relativ gelungen Organisation von Freunden darstellt. Organisiert man seine Freunde nicht weiter in unterschiedliche Gruppen, hätten alle Punkte des Schaubilds den Abstand der Freunde vom Benutzer und könnten alle Informationen, die auch Freunden zugänglich sind, abrufen.

A.3 Browser sichern

Um sich vor der Spionage durch Betreiber sozialer Netzwerke zu schützen, müssen die Browser-Chronik und vor allem die Cookies, die er entgegengenommen hat, regelmäßig gelöscht werden. In diesem Anhang wird erklärt, wie das im Firefox, Safari und im Internet Explorer geht. Andere Browser werden jedoch meist ähnlich bedient, so dass diese Beschreibungen ohne großen Aufwand auch auf sie übertragen werden können.

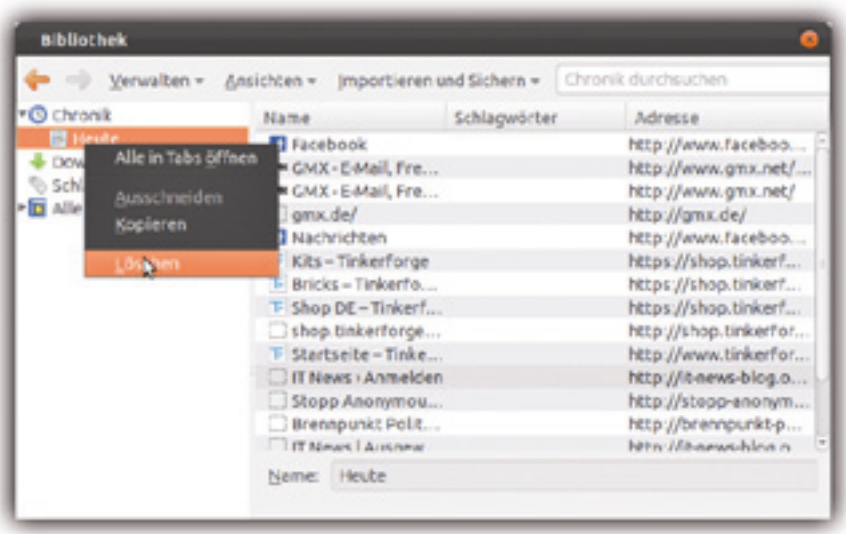

BILD A.2 Das Löschen der Firefox-Chronik

A.3.1 Firefox

Chronik

Die Chronik des Firefox wird in nur sehr wenigen, intuitiven Schritten gelöscht. Bei neueren Firefox-Versionen beginnt man mit einem Klick auf das Firefox-Icon in der linken oberen Bildecke und öffnet die Menüstruktur von Firefox. Dort wählt man den Menüpunkt CHRONIK aus (bei älteren Firefox-Versionen befindet sich das gleichnamige Menü direkt in der Menüzeile im Kopfbereich der Oberfläche) und hat dann in dem daraufhin aufklappenden Menü zwei Möglichkeiten, die Chronik zu löschen.

Die erste besteht darin, auf den Punkt GESAMTE CHRONIK ANZEIGEN zu klicken. Es öffnet sich ein neues Fenster, in dem die einzelnen Einträge der vorhandenen Chronik angezeigt werden; diese werden nach Tagen zusammengefasst. Nun wählt man die Einträge aus, die entfernt werden sollen, und entfernt sie durch Betätigen der [Entf]-Taste.

Die andere Möglichkeit ist erheblich einfacher und mit ihr können im gleichen Schritt auch die Cookies gelöscht werden. Allerdings wird sie in älteren Versionen von Firefox

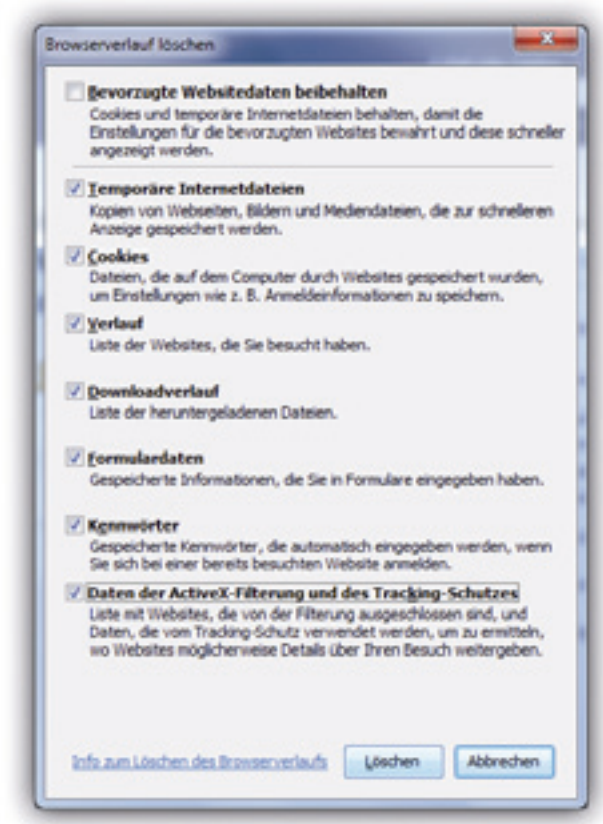

BILD A.3 Das Löschen des Verlaufs im Internet Explorer

nicht angeboten. Hierfür muss im Menü Chronik der Punkt Neueste Chronik löschen ... ausgewählt oder es müssen gleichzeitig die Tasten [Strg]+[Umschalt]+[Entf] gedrückt werden. Anschließend öffnet sich ein Auswahldialog, in dem die zu löschenden Elemente ausgewählt werden können und definiert wird, in welchem Zeitraum sie gelöscht werden sollen. Neben der Chronik an sich können auch Cookies, der Cache und weitere Daten gelöscht werden. Mit einem Klick auf Jetzt Löschen wird der Löschvorgang abgeschlossen.

Cookies

Mit der oben beschriebenen Methode zum Zurücksetzen des Browser-Verlaufs lassen sich auch die Cookies löschen. Allerdings gab es diese Methode wie bereits erwähnt nicht in allen Firefox-Versionen und so muss man vor allem in den älteren Versionen auf folgende Methode zurückgreifen: Man öffnet die Einstellungen von Firefox im gleichnamigen Menüpunkt; in den Firefox-Versionen für Linux befindet sich der Punkt Einstellungen unter dem Menüpunkt Bearbeiten. Nun klickt man auf den Reiter Datenschutz und anschließend auf die Schaltfläche Cookies anzeigen. Jetzt wählt man entweder ein bestimmtes Cookie aus und entfernt es gezielt oder löscht gleich alle Cookies mit einem Klick auf die Schaltfläche Alle Cookies entfernen.

A.3.2 Internet Explorer

Chronik und Cookies

Die Chronik wird beim Internet Explorer als Browser-Verlauf bezeichnet.

Gelöscht wird der Browser-Verlauf in den aktuellen Versionen des Internet Explorers, indem man auf das Zahnrad in der rechten oberen Ecke klickt und anschließend unter dem Punkt Sicherheit die Option Browserverlauf löschen auswählt. Daraufhin öffnet sich ein Fenster, das auch mit der Tastenkombination [Strg]+[Umschalt]+[Entf] aufgerufen werden kann. Dort wählt man die Daten aus, die eigentlich gelöscht werden sollen. Unter anderem sind dies der Verlauf selbst, die Cookies, der Cache (auch als temporäre Internetdateien bezeichnet), gespeicherte Kennwörter, Formulardaten sowie der Downloadverlauf. Sind die gewünschten Punkte ausgewählt, bestätigt man mit einem Klick auf Löschen und schließt den Vorgang damit ab.

A.3.3 Safari

Chronik

Die Chronik von Safari wird aufgerufen, indem man in der rechten oberen Ecke auf das Einstellungssymbol klickt und anschließend den Punkt Verlauf auswählt. Dieser kann auch mit dem gleichzeitigen Betätigen der Tasten [Strg]+H geöffnet werden.

Hier sind die aufgerufenen Seiten des Benutzers aufgelistet, geordnet nach dem Datum ihrer Betrachtung. Durch das Auswählen eines Eintrags oder einer übergeordneten Kategorie und dem anschließenden Betätigen der Taste [Entf] wird dieser aus dem Verlauf des Browsers gelöscht.

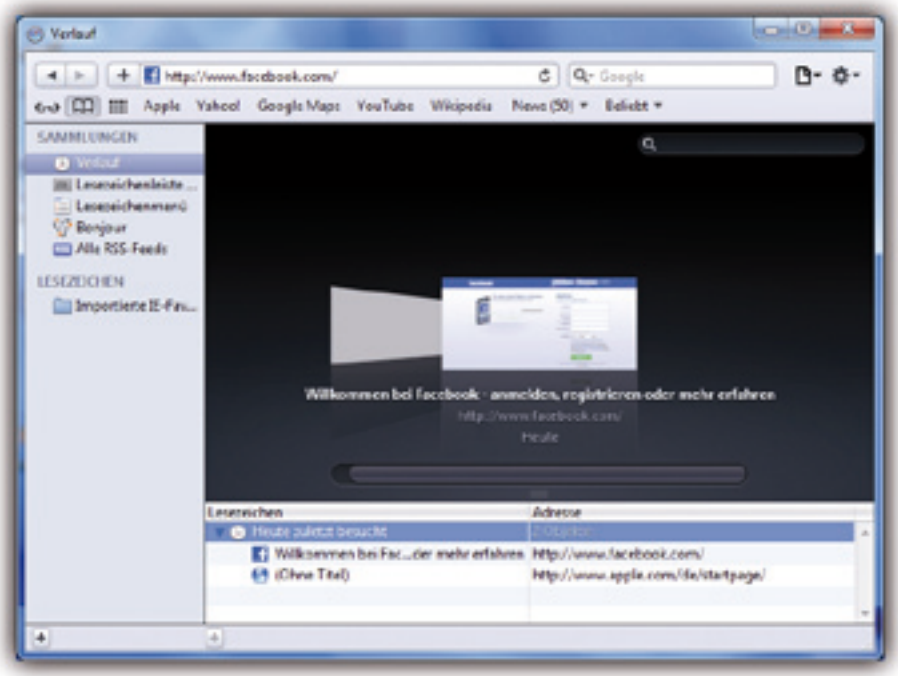

BILD A.4 Der Verlauf in Apple Safari

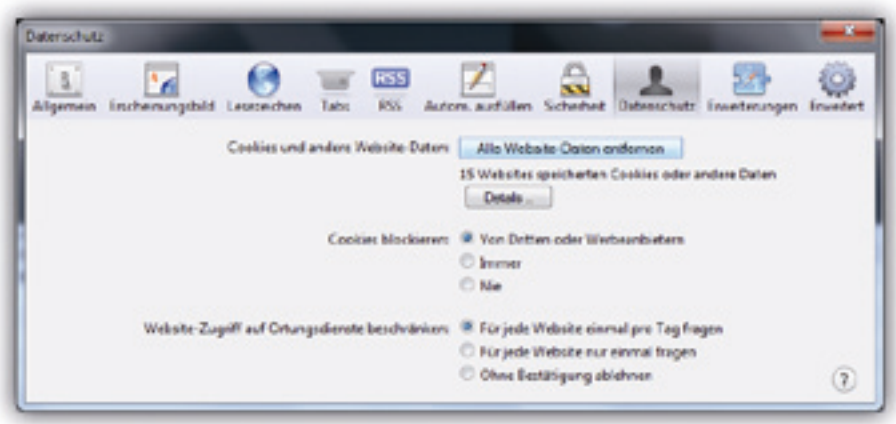

BILD A.5 Cookies im Safari

Cookies

Die Cookies können nur über die Einstellungen von Safari gelöscht werden. Dazu klickt man ebenfalls auf das Einstellungs-Symbol in der rechten oberen Ecke und wählt anschließend die Option EINSTELLUNGEN aus. Alternativ gelangt man zu dem sich daraufhin öffnenden Fenster auch mit der Tastenkombination [Strg]+, (Komma). Dort klickt man auf den Reiter DATENSCHUTZ und dann auf den Button ALLE WEBSITE-DATEN ENTFERNEN, um gespeicherte Cookies zu löschen.

A.4 Neue IP-Adresse erhalten

Über die IP-Adresse ist ein Besucher des Internets eindeutig identifizierbar. Genauer gesagt können die Internetprovider einen Anwender über seine IP-Adresse ermitteln, denn sie weisen einem Privatnutzer täglich seine IP-Adresse zu und sind gesetzlich dazu verpflichtet, zu speichern, welchem ihrer Kunden welche IP-Adresse wann zugewiesen war. Die Idee hinter dieser Gesetzesregelung ist, dass die Polizei bei einem Verdacht auf eine im Internet begangene Straftat den Computer, von dem diese Tat ausging, ermitteln kann.[1] Zwar können nur Behörden bei den Providern anfragen, um welchen Computer es sich bei einer bestimmten IP tatsächlich handelte, allerdings kann man davon ausgehen, dass es sich um die selbe Person handelt, wenn sich innerhalb eines kurzen Zeitraums zwei Benutzer mit der gleichen IP einloggen.

Auf diese Weise könnten auch die Betreiber sozialer Netzwerke schnell erkennen, wenn ein Benutzer mehrere Benutzerkonten betreibt und die Daten dieser Benutzer zusammenführen.

Um diese Transparenz zu verhindern, kann man eine erneute Zuweisung einer IP-Adresse erzwingen, um sich erst danach wieder in einem sozialen Netzwerk einzuloggen.

- *Stecker des Routers ziehen*

  Die einfachste und universell gültige Methode, die Zuweisung einer neuen IP zu erzwingen, ist, den Router kurze Zeit vom Internet zu trennen. Dazu zieht man entweder den DSL-Stecker (selten auch noch ISDN) für kurze Zeit ab und steckt ihn anschließend wieder ein, oder schaltet den Router aus und gleich wieder ein. Da der Router meist eine ganze Weile zum Hochfahren braucht, ist es in der Regel sinnvoller, den „Internetstecker“ abzuziehen und anschließend wieder einzustecken.

  Dabei passiert in etwa folgendes: Der Provider erkennt, dass der Anschluss momentan nicht in Benutzung ist und gibt die IP-Adresse, die diesem Anschluss zugeordnet war, frei. Diese IP-Adresse kann nun einem anderen Anschluss zugewiesen werden.

[1] Allerdings ist es auch anderen unter gewissen Umständen möglich, herauszufinden, wer sich hinter einer IP-Adresse verbirgt.

Beim erneuten Verbinden des Routers mit dem Internet wird dem Anschluss wieder eine IP-Adresse zugewiesen. Dabei ist es sehr unwahrscheinlich, dass man noch einmal die vorherige IP-Adresse erhält und so kann mit neunundneunzigprozentiger Sicherheit davon ausgegangen werden, dass man anschließend eine neue IP-Adresse besitzt.

- *Internetverbindung per Software trennen*

  Das oben geschildertem Verfahren erfordert meistens, sich von seinem Platz zu erheben, zum Router zu gehen, aus einem Kabelgewirr das richtige herauszusuchen, nur um es abzuziehen und anschließend wieder einzustecken, und schließlich wieder zurück zum Arbeitsplatz zu gehen.

  Arbeitet man aber auf der grafische Benutzeroberfläche des Routers, können diese Unbequemlichkeiten umgangen werden. Man muss sich lediglich mit einem Kennwort am Router anmelden, dann per Mausklick die Verbindung zum Internet trennen und sie anschließend per Mausklick wiederherstellen.

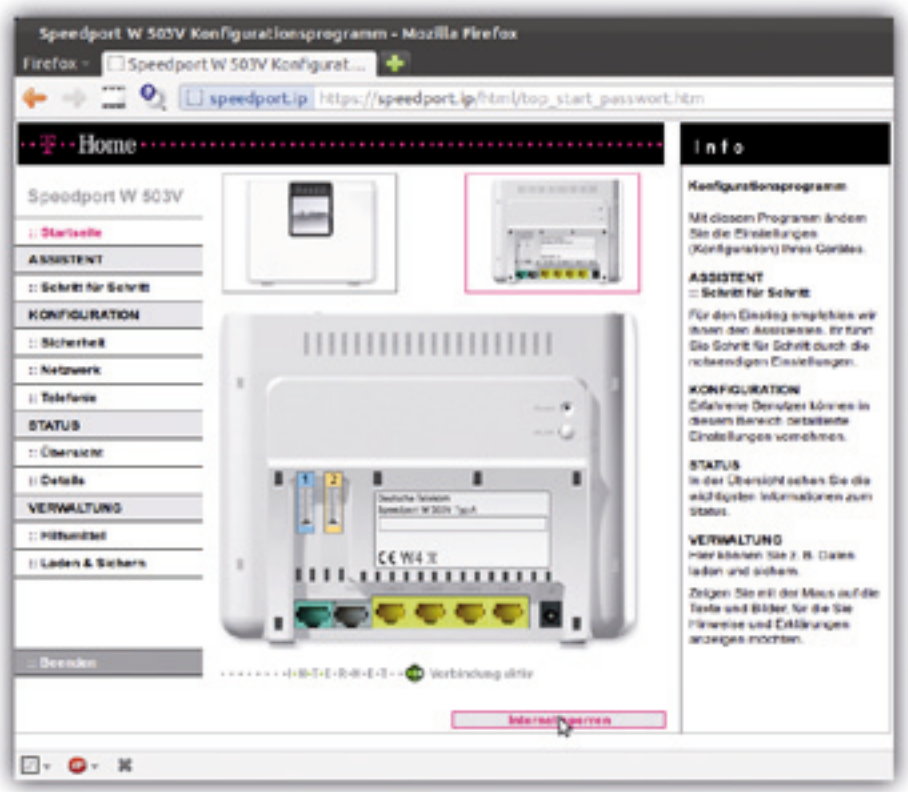

BILD A.6 Trennen der Internetverbindung eines Speedports

Da in den meisten Haushalten der von der Telekom mitgelieferte Speedport-Router in unterschiedlichen Ausführungen anzutreffen ist, soll dieser hier *exemplarisch* erläutert werden. Zusätzlich wird auch das Vorgehen bei einer Fritzbox erklärt, da sie nahezu ebenso weit verbreitet ist. Das Vorgehen bei Routern anderer Hersteller oder Typen unterscheidet sich jedoch meist nicht wesentlich davon. Im Zweifelsfall kann natürlich auch jederzeit das Handbuch des Routers zu Rate gezogen werden.

A.4.1 Speedport

Zur Konfigurationsoberfläche des Speedports gelangt man, indem man in den Webbrowser seiner Wahl die Domain *speedport.ip* eingibt. Auf der jetzt angezeigten Seite klickt man auf die Schaltfläche KONFIGURATION STARTEN, um dann das verlangte Gerätepasswort einzugeben, das sich in der Regel auf der Rückseite des Routers befindet. Anschließend gelangt man zu der Konfigurationsoberfläche des Speedports.

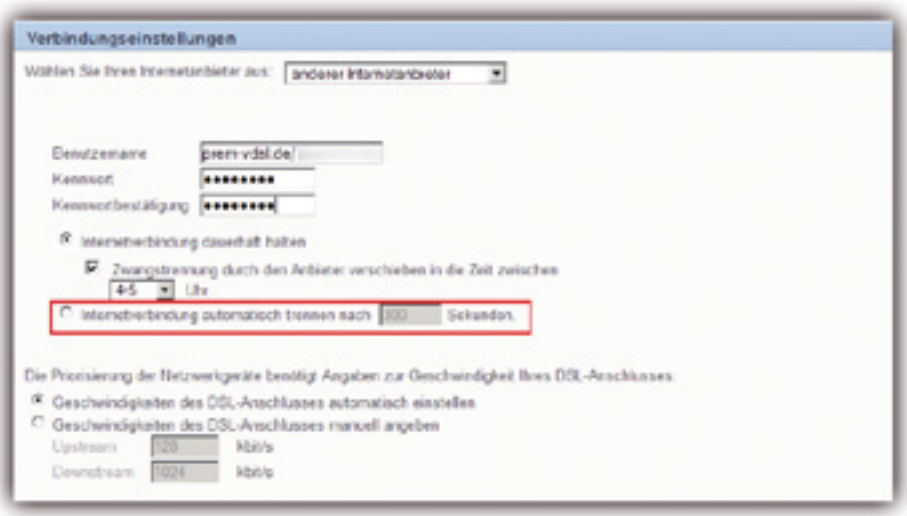

BILD A.7 Das Trennen der Internetverbindung einer Fritzbox mit einem Trick

In der rechten unteren Ecke befindet sich eine Schaltfläche mit der Aufschrift INTERNET SPERREN, mit der die Verbindung zum Internet getrennt wird. Ist die Verbindung getrennt, lässt sie sich mit einem Klick auf INTERNET FREIGEBEN wieder herstellen, so dass man eine neue IP-Adresse zugewiesen bekommt.

A.4.2 Fritzbox

Um die Fritzbox auf der grafischen Oberfläche zu bedienen, benötigt man die Konfigurationssoftware des Routers. Sie liegt dem Router üblicherweise auf einer CD-ROM bei und kann nach den Anweisungen im Handbuch installiert werden. Oder man arbeitet auf dem unter http://fritz.box erreichbaren Webinterface.

Unter dem Punkt System → Zurücksetzen → Neu starten wird die Fritzbox neu hochgefahren, womit man eine neue IP-Adresse erhält.

Eine alternative Möglichkeit bietet ein kleiner Trick:

Unter Internet → Zugangsdaten lässt sich die Option Internetverbindung automatisch trennen auf eine geringe Zeiteinheit, beispielsweise zehn Sekunden einstellen. Anschließend muss man sicherstellen, dass kein Programm in den nächsten zehn Sekunden den Internetzugang anfordert. Danach wird die Verbindung automatisch getrennt.

Anschließend sollte man jedoch wieder Internetverbindung dauerhaft halten auswählen, um auch in Zukunft ungestört surfen zu können.

Stichwortverzeichnis

E

F

G

H

R

S

T

U

V

W

X

Z

Der Autor

Manuel Ziegler begann im Alter von 14 Jahren, sich mit dem Thema IT-Sicherheit zu beschäftigen. Heute studiert er Informatik an der TU München.
Er betreibt mehrere Blogs, u.a. zum Thema Sicherheit, und arbeitet an Lösungen zur Steigerung der Sicherheit in sozialen Netzwerken.

Facebook, Twitter & Co.
Aber sicher!

»Die Urlaubsstimmung ist super, die Selbstporträts an der Poolbar sind es auch – und schwupp, schon sind die Fotos mit Kommentar zum Feriendomizil an 214 Facebook-Freunde verschickt. Pech, wenn auch nur einer dieser Empfänger eben kein Freund ist, sondern in aller Ruhe die verwaiste Wohnung des Absenders ausräumt. […]

Ob verhängnisvolle Arglosigkeit der Nutzer, Spionage, Datenmissbrauch durch Netzbetreiber, Datendiebstahl durch Dritte oder Rufmord: Ziegler sensibilisiert für Risiken und bietet unverzichtbares Know-how. Eine Pflichtlektüre für alle, die die Vorteile sozialer Netzwerke ausschöpfen und dabei auf Nummer sicher gehen wollen.«

Elisabeth Zeitler-Boos, Magazin »büchermenschen«

- Praktischer Ratgeber für alle von 9 bis 99 Jahre
- Mit vielen wichtigen Tipps und alltagsnahen Beispielgeschichten
- EXTRA: Mit kostenlosem E-Book
- Regelmäßig Aktualisierungen und weitere Beiträge finden Sie unter: www.facebook.com/SicherImSozialenNetz

€ 16,90 [D] | € 17,40 [A]
ISBN 978-3-446-43466-0
9 783446 434660

www.hanser-fachbuch.de