Bayerisches Landesamt für
Verfassungsschutz

Soziale Netzwerke

und ihre Auswirkungen auf die Unternehmenssicherheit

Ein gemeinsames Projekt der Hochschule Augsburg und des Bayerischen Landesamts für Verfassungsschutz

Vorwort

Rund 22 Millionen Nutzer hat allein das soziale Netzwerk Facebook derzeit in Deutschland. Ein großer Teil davon sind Arbeitnehmer, die Facebook für die Pflege privater wie beruflicher Kontakte nutzen: Soziale Netzwerke vereinfachen die Kommunikation, sie ermöglichen es, Informationen schnell mit einer großen Anzahl von Freunden, Bekannten, Kollegen und Geschäftspartnern zu teilen.

Facebook und Co. bergen aber auch erhebliche Risiken, derer sich bei weitem nicht alle privaten und professionellen Nutzer bewusst sind: Dabei geht es um Datenverlust und Malware-Infektion, um Produktivitätseinschränkung, Netzwerküberlastung und Reputationsverlust. Auch kriminelle Handlungen werden in sozialen Netzwerken vorbereitet: Dem überwiegenden Teil der Angriffe im Bereich der Wirtschaftsspionage gehen heutzutage „Social Engineering"-Maßnahmen voraus. Das heißt, Angreifer bedienen sich sozialer Netzwerke, um Informationen über Mitarbeiter eines bestimmten Unternehmens zu sammeln und so in einem zweiten Schritt leichter an sensible Unternehmensdaten zu gelangen.

Wirtschaftspionage hat sich seit einigen Jahren zu einer realen Bedrohung für die deutsche Wirtschaft entwickelt. Deutsche Firmen stehen aufgrund ihrer Innovationskraft in nahezu allen Branchen und Forschungsbereichen im Blickfeld ausländischer Nachrichtendienste. Das Bayerische Landesamt für Verfassungsschutz unterstützt mit seinem Dienstleistungsangebot die Wirtschaft bei der Abwehr von Spionageaktivitäten und will auch für einen verantwortungsvollen Umgang mit sozialen Netzwerken sensibilisieren.

Im Rahmen der Präventionsaktivitäten des Bayerischen Landesamts für Verfassungsschutz ist in Zusammenarbeit mit der Hochschule Augsburg dieses Buch entstanden. Führungskräften und Mitarbeitern soll es einen Überblick über das Thema „Soziale Netzwerke und ihre Auswirkungen auf die Unternehmenssicherheit" geben. Die Publikation versteht sich als Kompendium und Nachschlagewerk, in dem die wichtigsten sozialen Netzwerke dargestellt und mögliche Sicherheitsprobleme skizziert sind. Die atemberaubende Geschwindigkeit des technischen Fortschritts im Internet lässt dabei gezwungenermaßen nur eine Momentaufnahme zu.

Mein besonderer Dank gilt den Studierenden Roland Koch, Steffen Wendzel, Florian Forster, Benjamin Kahler, Patrick Branner, Dominik Heimstädt und Franziska Krün der Fakultät für Informatik an der Hochschule Augsburg, die in gemeinsamer Arbeit wesentliche Teile dieses Buches erarbeitet haben. Danken möchte ich zudem Herrn Prof. Dr. Gordon Rohrmair für die Betreuung der Semesterarbeit und die hervorragende Unterstützung bei der Erarbeitung dieser Publikation, der ich viele interessierte Leser wünsche.

Juni 2012

Dr. Burkhard Körner,
Präsident des Bayerischen Landesamts für Verfassungsschutz

Inhalt

Einleitung

Soziale Netzwerke erfreuen sich immer größerer Beliebtheit und sind aus unserem Alltag kaum mehr wegzudenken. Allein Facebook verzeichnet heute weltweit ca. 900 Millionen registrierte Nutzer [1]. Damit wäre Facebook, würde es sich nicht um eine Online-Gemeinschaft handeln, inzwischen das drittgrößte Land der Erde. 50% der Mitglieder nutzen das soziale Netzwerk jeden Tag. Dabei treffen Menschen aufeinander, die in unterschiedlichster Beziehung zueinander stehen: private Bekannte, Angehörige, Arbeitskollegen und Interessensgemeinschaften. Ebenso unterschiedlich wie die Beziehungen ihrer Mitglieder sind die Inhalte, die über soziale Netzwerke ausgetauscht werden. Dabei wird schnell deutlich, dass es einen Konflikt zwischen privaten und unternehmerischen Interessen geben kann, den es bestmöglich aufzulösen gilt.

Da wäre zum einen die Zeit, die Menschen in sozialen Netzwerken verbringen. Sie wird aus unternehmerischer Sicht anders bewertet als aus privater. Ähnlich verhält es sich mit anderen Ressourcen wie beispielsweise der Netzauslastung. Wird etwa ein Video an Freunde, Bekannte oder Arbeitskollegen weitergegeben, kann dies ein Unternehmensnetzwerk schnell in die Knie zwingen. Verletzt ein Mitarbeiter durch die Weitergabe eines Videos eventuell Urheberrechte oder handelt er gegen datenschutzrechtliche Bestimmungen? Findet über das soziale Netzwerk Mobbing von Arbeitskollegen statt? All dies sind Fragen, die Unternehmen neben den Auswirkungen sozialer Netzwerke auf die IT-Sicherheit beantworten müssen. Die Grundaussage aller Antworten auf diese Fragen lautet:

Die negativen Auswirkungen auf die Unternehmenssicherheit sind nur durch eine durchdachte Social-Media-Guideline und intensive Schulungen von Mitarbeitern gering zu halten.

Social Engineering

Eine der erfolgreichsten (vorbereitenden) Angriffstechniken ist das sogenannte Social Engineering. Unter dieser auch „soziale Manipulation" genannten Technik versteht man das Beeinflussen vor Personen, um ein bestimmtes Verhalten hervorzurufen wie beispielsweise die Herausgabe von vertraulichen Informationen.

Menschen werden diese Informationen jedoch freiwillig nur dann herausgeben, wenn sie die Handlung gegenüber sich selbst rechtfertigen können. Genau an dieser Stelle setzen Social Engineers an. Es wird z.B. ein Kennverhältnis vorgetäuscht, um das Vertrauen einer Person zu gewinnen. Dazu benötigt der Angreifer zwingend Informationen über sein Opfer. Soziale Netzwerke bieten mit

ihren vielfältigen personenbezogenen Informationen eine ideale Basis dafür.

Social Engineering kann insbesondere durch zwei Maßnahmen abgewehrt werden:

1. Mitarbeiter müssen wissen, ob die gewünschte Informationsweitergabe oder Handlung gestattet ist oder nicht und
2. die Techniken der Angreifer kennen.

Nicht immer werden Informationen erst über den Umweg des Social Engineering missbraucht. Manchmal genügt schon die Kenntnis über eine Urlaubsreise, um sich in Abwesenheit des Opfers unbemerkt Zutritt zu dessen Räumlichkeiten zu verschaffen.

Reales Risiko in der virtuellen Welt

Soziale Netzwerke stellen ein reales Risiko in der virtuellen Welt dar. Pressemitteilungen über Einbrüche in Firmen-, Industrie- und Regierungsnetzwerke häufen sich inzwischen weltweit und hinterlassen dabei den Eindruck, als ob sich selbst Institutionen mit ausreichenden finanziellen und organisatorischen Möglichkeiten trotz erheblichen technischen Sachverstands immer noch zu wenig gegen Cyber-Angriffe schützen. Die prominentesten Opfer des letzten Jahres sind Sony, RSA, HB Gary, Lockheed-Martin sowie das Pentagon.

Es kann davon ausgegangen werden, dass hinter diesen Angriffen professionelle Hacker stehen, die im Auftrag von Staaten, kriminellen Organisationen oder Institutionen Informationen stehlen (Spionage) oder Schaden anrichten (Sabotage). Um entsprechende Angriffe erfolgreich oder noch erfolgreicher durchführen zu können, werden – wie in der realen Welt auch – Informationen über die Angriffsziele durch das systematische Auswerten von sozialen Netzwerken gewonnen. Auf Grundlage dieser Informationen werden Vertrauensbeziehungen geschaffen, die genutzt werden, um beispielsweise „personalisierte E-Mails“ mit Schadcode im Anhang an den Empfänger im Unternehmen zu senden. Auf diese Weise wird jede Firewall umgangen, da sich der Empfänger durch die perfekt auf ihn zugeschnittene Mail direkt angesprochen fühlt, den Anhang selbstverständlich öffnet und so unbeabsichtigt den Zugang zum Firmennetzwerk ermöglicht, ohne dass dies als Angriff festgestellt werden kann.

Personalisierte E-Mails

Senior Intelligence Analyst Paul Wood hat dies im Symantec Intelligence Report für November 2011 [142] treffend formuliert:

„Jedoch wären ohne das sogenannte Social Engineering beziehungsweise Head-Hacking selbst die technisch ausgereiftesten Angriffe nur wenig erfolgreich. […] Wissen die Täter erst einmal über die Interessen, Hobbys und vor allem das soziale Umfeld Be-

scheid, so können sie den Anwender auf besonders glaubwürdige und überzeugende Weise hinters Licht führen".

In den geschilderten Szenarien werden jeweils veröffentlichte Informationen als Basis für die Angriffe verwendet, deshalb sollte sich jeder Nutzer eines sozialen Netzwerks über die Risiken und Folgen seiner „Postings" bewusst sein. Durch die ins Netz gestellten Informationen gefährdet man eventuell nicht nur sich selbst, Freunde und alle verknüpften Kontakte, sondern auch den Arbeitgeber.

Der Automobilkonzern PORSCHE sperrte laut dem Nachrichtenmagazin Focus im Oktober 2010 den Zugriff auf die Plattform Facebook für seine Mitarbeiter [2]. Dies geschah nicht, weil zu viel Arbeitszeit durch das soziale Netz verloren ging, sondern aus Angst vor Wirtschaftsspionage. Durch die Sperrung sollte verhindert werden, dass ausländische Nachrichtendienste an geheime Firmeninformationen gelangen.

Für den Fall, dass Sie über eine ähnliche Entscheidung nachdenken, sei bemerkt, dass die oben geschilderte Maßnahme für sich allein gesehen nur eingeschränkt wirkt. Ein Verbot kann sich ausschließlich auf die Arbeitszeit beziehen und minimiert damit nur einen Teil der Risiken. Darüber hinaus sollte auf jeden Fall die Sensibilität der Mitarbeiter durch Schulungsmaßnahmen erhöht werden (die das Unternehmen PORSCHE ebenso durchgeführt hat). Schulungen im richtigen Umgang mit sozialen Netzwerken stellen neben durchdachten Regelungen das A und O im Hinblick auf soziale Netzwerke und ihre Auswirkungen auf die Unternehmenssicherheit dar. Dieser sicherheitsorientierte und verantwortungsbewusste Umgang sollte aber – wie oben schon erläutert – nicht nur im Berufsleben, sondern auch im Privatbereich zur Anwendung kommen: schützenswerte Informationen gibt es auf beiden Ebenen – Gefahren ebenfalls.

Schulungen für Mitarbeiter

Unternehmen sollten deshalb Mitarbeiter umfassend informieren, sensibilisieren und den Umgang mit sozialen Netzwerken verbindlich regeln.

Diese Veröffentlichung gibt einen Überblick über die in Deutschland am häufigsten verwendeten sozialen Netzwerke, die Gefahren, die daraus für Unternehmen entstehen, sowie Empfehlungen, wie sich Unternehmen und Privatpersonen vor den Risiken besser schützen können.

Empfehlungen für den Umgang mit sozialen Netzwerken

Für Unternehmen

1. Keine schützenswerten Unternehmens-Informationen publizieren. Es sollte immer das Prinzip gelten: Geheimes bleibt geheim und Internes bleibt intern. Sie sollten sich also die Frage stellen: Wissen alle Mitarbeiter, welche Informationen offen, vertraulich oder streng vertraulich sind?
2. Zurückhaltung mit offensiven persönlichen Meinungen. Wie das Beispiel der Daimler-Mitarbeiter im Zusammenhang mit Stuttgart 21 zeigt [6], können unbedachte Äußerungen über die eigene Firma sehr hohe Wellen schlagen. So wurde in einer Facebook-Gruppe der Vorstandsvorsitzende der Daimler AG als „Spitze des Lügenpacks" beschimpft.
3. Verwenden Sie auf keinen Fall das Firmenpasswort für Ihre Zugänge bei einem sozialen Netzwerk. Diese einfache aber effektive Empfehlung wird nach wie vor zu selten umgesetzt, weil es schlicht bequemer ist, immer das gleiche Passwort zu nutzen. Genau dieser Umstand war ein riesiges Einfallstor für Angreifer in den großen, bekannt gewordenen Sicherheitsvorfällen der vergangenen Monate und Jahre.
4. Erarbeiten Sie eine eigene Position bzw. Strategie zum Thema „Soziale Medien" – angepasst an die individuellen Gegebenheiten in Ihrem Unternehmen – und fixieren Sie diese schriftlich in einer sog. „Social Media Guideline" [5]. Um den Aufwand gering zu halten, können Sie sich Anregungen bei der BITKOM [7] oder in der Policy Database von „Social Media Governance" holen [141].

Des Weiteren haben zahlreiche Unternehmen ihre Social-Media-Guidelines online zur Verfügung gestellt, die kostenlos eingesehen werden können [4][5]. Diese Veröffentlichungen enthalten auch wertvolle Informationen für Mitarbeiter. So wird der Leser in den Microsoft Blogging Guidelines direkt gefragt: „Wenn Sie damit morgen früh auf der Titelseite der New York Times oder Slashdot stehen würden – würden Sie den Beitrag dennoch posten?" [4].

Ihre Social Media Guideline sollte nicht nur den Umgang mit sozialen Netzwerken festlegen, sondern auch regeln, welche Firmeninformationen generell „gepostet" werden dürfen und welche nicht. Dabei sollten „weiche" Formulierungen wie

„interne Informationen“ oder „vertrauliche Projektdaten“ vermieden werden, es sei denn, sie sind als solche gekennzeichnet. Und falls Ihre Mitarbeiter über ihr Unternehmen, ihren Arbeitsbereich oder ein Projekt schwärmen möchten, sollten sie das auch tun – nur nicht mit Betriebsgeheimnissen.

Lassen Sie Ihre Social Media Guideline zum festen Bestandteil Ihrer Unternehmensphilosophie werden und kommunizieren Sie den Inhalt innerhalb des Unternehmens. Schreiben Sie die Richtlinie möglichst nicht nur fest, sondern auch fort und nehmen Sie die Richtlinie als verbindliche Regelung in die Arbeitsverträge mit auf.

Und last but not least:

5. Die Akzeptanz und Bereitschaft der Mitarbeiter, diese Regelungen mitzutragen, wird entscheidend von der Vorbildfunktion der Führungskräfte im Unternehmen bestimmt.

Für Nutzer

1. Vertrauen Sie nicht jeder Anfrage oder Nachricht blind. Oftmals bestätigt man zu schnell eine Freundschaftsanfrage. Dies kann zur Folge haben, dass anschließend diese (ungewollten) „Freunde“ auf wichtige Informationen zugreifen können.
2. Das gleiche gilt für Nachrichten mit ungewöhnlichen Inhalten. Es gibt eine Reihe von Angriffen, die deshalb erfolgreich sind, weil man das Opfer dazu bringt einem Link zu folgen. Gerade bei Twitter ist es üblich, dass Kurzlinks verwendet werden und somit die eigentliche Zieladresse nicht bekannt ist.
3. Veröffentlichen Sie keine allzu privaten oder gar intimen Details oder Bilder – nicht nur um hier keine Angriffsfläche für Social Engineering, Erpressung oder Diffamierung zu bieten. Auch Personalchefs recherchieren heutzutage standardmäßig im Internet, bevor sie jemanden einstellen.
4. Überprüfen Sie Ihre „Privatsphäre“-Einstellungen und regulieren Sie diese entsprechend Ihrer tatsächlichen Nähe zu dem Personenkreis, der Ihre privaten Postings wirklich lesen oder kennen soll.
5. Wer Karrierenetzwerke wie XING als Jobbörse nutzt, sollte darauf achten, sein Profil möglichst aktuell zu halten und so einzustellen, dass sein Name von Suchmaschinen gefunden wird, um für suchende Unternehmen interessant zu bleiben oder zu werden.

6. Um zu überprüfen, was bereits offen über Sie im Netz recherchierbar ist, sollten Sie regelmäßig Ihren eigenen Namen in den verschiedenen Suchmaschinen checken. Zusätzlich kann ein „Google Alert" mit Ihrem Namen dafür sorgen, dass Sie immer sofort informiert werden, wenn online etwas Neues über Sie auftaucht.
7. Halten Sie sich über Neuerungen oder Änderungen Ihres verwendeten sozialen Netzwerks auf dem Laufenden. Sobald Sie durch eine Mail des Betreibers z.B. über eine wichtige Datenschutzänderung informiert worden sind, gilt diese für Sie als verbindlich.
8. Ein Punkt, der viele aufgrund des Aufwandes abschreckt, aber wichtig ist: Machen Sie sich bewusst, welche Rechte Ihrer veröffentlichte Inhalte (Video, Bilder, Texte) an den Betreiber der Plattform übergehen. Mehr dazu finden Sie in den Beschreibungen der einzelnen Netzwerke.
9. Grundsätzlich gilt: Verhalten Sie sich in sozialen Netzwerken den Mitgliedern gegenüber so, wie Sie es auch im realen Leben tun würden.

Populäre soziale Netzwerke

Dieses Kapitel stellt die populärsten sozialen Netzwerke vor und beleuchtet dabei deren Umfang, Grundidee und Funktionalitäten. Im anschließenden Kapitel werden die aus diesen Funktionalitäten resultierenden Risiken analysiert.

Die populärsten sozialen Netze in Deutschland sind laut Vincos [9] Facebook, Twitter und XING.

Der Beliebtheitsgrad einzelner sozialer Netzwerke hängt entscheidend von den lokalen Gegebenheiten ab. So ist beispielsweise die hier kaum bekannte Plattform Vkontakte (http://vkontakte.ru) in Russland Marktführer, während Facebook dort nur einen geringen Marktanteil verzeichnen kann.

Funktionalitäten

Die meisten sozialen Netzwerke bieten ähnliche Funktionen, denn es geht immer um die Interaktion mit anderen Benutzern. Im Detail sind folgende Funktionen fast immer standardmäßig vorhanden [8]:

- Persönliches Profil für jeden Benutzer
- Kontaktliste oder Adressbuch
- Empfang und Versand von Nachrichten an andere Mitglieder
- Empfang von Benachrichtigungen über diverse Ereignisse
- Veröffentlichung von Statusmeldungen
- Such-Funktion

Diese Grundfunktionen sind meist kostenfrei, allerdings werden in fast allen sozialen Netzwerken kostenpflichtige Dienste optional angeboten, für die der zahlende Nutzer erweiterte Funktionalitäten erhält.

Soziale Netzwerke bieten auch für Unternehmen interessante Aspekte, um sich im Internet zu präsentieren oder um an Informationen zu gelangen.

Typischer Inhalt

Der Inhalt eines sozialen Netzwerks besteht hauptsächlich aus Daten, die von den Mitgliedern selbst generiert werden. Dazu gehören Nachrichten, Statusmeldungen, Bilder und Videos sowie Informationen über Themen, die dem Benutzer gefallen.

Spezialportale und Community-Netzwerke

Neben den besonders populären allgemeinen sozialen Netzwerken existieren auch spezielle Online-Communities für kleine Themen- und Personenkreise. Ein Beispiel hierfür ist die Seite www.kress.de, auf der hauptsächlich Journalisten samt persönlichem Werdegang und Geburtsdatum vernetzt sind.

Eine andere, sehr bekannte Webseite ist www.flickr.com, die zwar nicht explizit als soziales Netzwerk gilt, aber eng damit verknüpft ist. Hier handelt es sich um eine Foto-Community, die soziale Aspekte abdeckt. Das Prinzip ist, Fotos für andere Nutzer zur Verfügung zu stellen, die diese bewerten und kommentieren können. Flickr erlaubt seinen Mitgliedern, bereits bestehende Accounts aus anderen sozialen Netzwerken für die Anmeldung wiederzuverwenden, sich also beispielsweise mit seinem Facebook- oder Google-Account einzuloggen.

Soziale Netzwerke als Authentifizierungsmöglichkeit

Fast jeder, der regelmäßig das Internet nutzt, besitzt mittlerweile ein Profil in einem der großen sozialen Netzwerke. Spezielle Schnittstellen ermöglichen es immer öfter, dieses Profil auch auf anderen Seiten für die Anmeldung zu nutzen. Diese Funktionalität wird auch bei bekannten Seiten wie www.bild.de angeboten, die diese Authentifizierung beispielsweise für ihr Kommentarsystem benutzen. Dabei sollte immer beachtet werden, dass durch die Einbindung des Skriptes des sozialen Netzwerks diesem wiederum eigenständig ermöglicht wird, den eigenen Nutzer auch auf anderen Seiten (in diesem Fall www.bild.de) zu „tracken“[1].

Solch eine Drittauthentifizierung bieten unter anderem derzeit Google, Facebook und Twitter an.

1) Verfolgung des Surfverhaltens eines Benutzers

Facebook

Übersicht

Nutzer in Deutschland	22,1 Millionen [27]
Nutzer weltweit	900 Millionen
Hauptsitz	Menlo Park, Kalifornien, USA
Gründungsjahr	Februar 2004
Eigentümer	Mark Zuckerberg (24 %) Chris R. Hughes (12 %) Chris R. Hughes (12 %) Peter Tiel (7 %) Mail.ru Group (6,9 %) Dustin Moskovitz (6 %) Eduardo Saverin (5 %) Microsoft (1,6 %) Goldmann Sachs (0,9 %)[2]
Marktwert nach Börsengang am 18.05.12	ca. 100 Mrd. USD
Hauptbenutzergruppe	Zwischen 45 und 54 Jahren

Quelle: [11]

Kurzbeschreibung

Facebook ist ein kommerzielles soziales Netzwerk der kalifornischen Firma Facebook Inc., das Anfang des Jahres 2004 von den Studenten Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz und Chris Hughes gegründet wurde. Ursprünglich konnte es nur von Studenten der Universität Harvard benutzt werden. Die Anmeldemöglichkeiten dehnten sich jedoch im Lauf der Zeit auf weitere Hochschulen und Länder aus, bis sich schließlich ab dem Jahr 2008 jeder beliebige Nutzer anmelden konnte. Inzwischen ist Facebook in mehr als 80 verschiedenen Sprachen verfügbar und hat weltweit etwa 900 Millionen aktive Mitglieder [1].

Bis zum „größten Börsengang eines Internet-Unternehmens“ am 18.05.2012 konnte der Marktwert von Facebook nur geschätzt werden und lag hier bei etwa 50 Milliarden US-Dollar [28]. Nach der Ausgabe von über 400 Millionen Aktien lag der Marktwert des Unternehmens kurzzeitig bei rund 100 Milliarden US-Dollar.

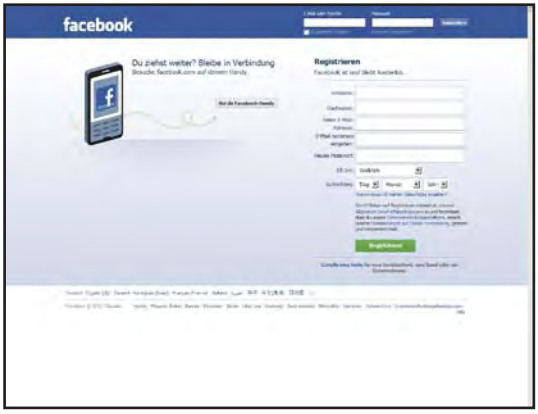
Typischer Inhalt und Kommunikationsmethoden

Wie die meisten sozialen Netzwerke bietet auch Facebook als zentrale Informationsplattform für jeden Nutzer eine Profilseite an, über die Aktivitäten veröffentlicht sowie Fotos und Videos mit anderen Mitgliedern geteilt werden können.

Ein Teil der Profilseite ist dabei die sogenannte Pinnwand. Der Nutzer kann dort Notizen veröffentlichen und Besucher des Profils können Nachrichten hinterlassen. Um mit einem anderen Nutzer

2) Daten vor Börsengang am 18.05.2012

direkt in Kontakt zu treten, können private Nachrichten verschickt werden. Diese sind nur für den Absender bzw. Empfänger zugänglich. Eine Alternative zu den privaten Nachrichten stellt der Facebook-Chat dar. Über diesen können Nutzer mit anderen Mitgliedern in Echtzeit kurze Textnachrichten austauschen. Darüber hinaus hat jeder Nutzer die Möglichkeit, Gruppen, die bestimmte Interessen vertreten, beizutreten oder diese zu gründen.



Vergleichbar mit solchen Gruppen sind sog. Events bzw. Veranstaltungen, die die Möglichkeit bieten, Treffen, wie beispielsweise Geburtstage oder Konzerte, zu organisieren.

Um Profilinformationen mit anderen Nutzern zu teilen oder deren Informationen anzuzeigen, können Freundschaften geschlossen werden. Freunde haben im Unterschied zu unbekannten Nutzern mehr Möglichkeiten mit dem eigenen Profil zu interagieren, indem sie beispielsweise Kommentare zu Bildern, Videos oder Beiträgen hinterlassen. Außerdem ist es ihnen dadurch möglich, bekannte Personen in Bildern oder Videos von Freunden zu markieren und auch zu den Freunden des anderen Nutzers direkt Kontakte zu knüpfen.

Um über die Neuigkeiten auf den Profilseiten befreundeter Nutzer informiert zu werden, gibt es eine Beobachtungsliste auf der Startseite jedes Profils. In dieser werden alle Aktivitäten der Freunde dargestellt.

Eine weitere Funktion von Facebook besteht in kleinen Anwendungen, die von Drittanbietern erstellt werden. Dabei handelt es sich hauptsächlich um Spiele und Kommunikationsanwendungen, die sich nach der Auswahl durch den User in dessen Profilseite integrieren lassen. Allerdings ist zu beachten, dass bei der Nutzung einer Anwendung oft die Genehmigung zum Zugriff auf die Profilinformationen erteilt werden muss.

2009 existierten bereits mehr als 350.000 Anwendungen, die aber selten mehr als 100.000 Benutzer hatten. Am beliebtesten ist derzeit mit 75 Millionen Usern das Spiel „Farmville“. Bedingt durch die schnelle Zunahme von Anwendungen und die daraus resultierende Unübersichtlichkeit des Angebots, benutzt Facebook inzwischen ein „verification program“, um vertrauenswürdige und sichere Anwendungen besser zu platzieren und damit die Auswahl für den Nutzer übersichtlicher zu gestalten [11][12][13].

Der Funktionsumfang von Facebook beschränkt sich nicht nur auf das soziale Netzwerk selbst, sondern wirkt auch auf externe Websites. So gibt es u.a. die Möglichkeit, sich über eine sogenannte „Einmalanmeldung" bei Facebook auch auf anderen Websites zu authentifizieren. Dabei werden die Anmeldedaten des Nutzers an die externen Websites übertragen. So wird vermieden, dass sich der Nutzer dort noch einmal gesondert registrieren muss. Allerdings sind so die Aktivitäten der Nutzer außerhalb des sozialen Netzwerks im Facebook-Profil sichtbar. Die „Einmalanmeldung" wird aktuell beispielsweise von bekannten Seiten wie www.bild.de und www.lufthansa.com unterstützt.

Betreiber externer Websites haben wiederum die Möglichkeit, Plugins[3] von Facebook in ihre Seiten zu integrieren. Dazu gehört z. B. der sogenannte „Like"- oder „Gefällt-mir"-Button, durch dessen Anklicken User signalisieren können, dass sie sich für ein bestimmtes Thema interessieren bzw. dieses gut heißen. Diese Meinungsbekundung auf der externen Website wird ebenfalls im eigenen Facebook-Profil sichtbar[15][16][17].

Auch die mobile Nutzung wird von Facebook unterstützt. So gibt es für jede gängige mobile Plattform, u. a. Windows Mobile, BlackBerry, Apple iPhone/iPod touch, Android und bada, eine Handyanwendung, mit deren Hilfe auf Facebook zugegriffen werden kann[18][11].

Über die Funktionalität „Facebook Orte" (facebook places) können Nutzer Freunden ihren aktuellen Standort mitteilen sowie den Aufenthaltsort ihrer Freunde anzeigen lassen [19].

Um Facebook-Nutzern das Finden von bekannten Personen innerhalb des sozialen Netzwerks zu erleichtern, gibt es eine weitere Funktion namens „Freunde-Finder". Dabei muss der User seine E-Mail-Adresse und das Zugangskennwort angeben und kann so seine E-Mail-Kontakte nach Personen durchsuchen, die in Facebook registriert sind [20].

Finanzierung

Die Nutzung von Facebook ist kostenlos, da es sich hauptsächlich durch Einnahmen aus Werbeeinblendungen finanziert. Den Werbepartnern werden von Facebook weitreichende Informationen über die Nutzer zur Verfügung gestellt, damit die Werbung gezielt auf die jeweilige Person angepasst werden kann. Dazu gehören unter anderem Alter, Geschlecht, Hobbys, Wohnort, politische Überzeugung, Lieblingsbücher und -filme, Bildungsstand sowie Hinweise auf persönliche Beziehungen. In den USA hält Facebook derzeit den größten Anteil an Bannerwerbung [21].

3) Computerprogramm, das in ein anderes Softwareprodukt eingebunden wird und damit dessen Funktionalität erweitert [14]

Seit dem 1. Juli 2011 müssen kostenpflichtige Dienste in Facebook-Anwendungen mit dem von Facebook bereitgestellten Bezahlsystem „Credits" abgewickelt werden können [22]. Facebook behält dabei 30% der Gewinne dieser Online-Währung. Andere Zahlungsmöglichkeiten sind darüber hinaus weiterhin möglich.

Zusätzliche Einnahmen erzielt Facebook durch Investoren, die zum Teil sehr große Summen in das Unternehmen stecken. Die größten Investitionen der letzten Jahre waren:

- 240 Mio. USD von Microsoft (2007)
- 400 Mio. USD von Goldman Sachs (2011)
- 500 Mio. USD von der Mail.ru Group (2009, 2011)

Bisher erhielt Facebook auf diese Weise insgesamt 1.24 Milliarden USD [11].

Vor dem Börsengang am 18.05.12 waren keine genauen Informationen über die Gewinne des Unternehmens bekannt. Ein vertrauliches Dokument an die Investoren lässt aber auf einen Gewinn von 355 Mio. USD in den ersten neun Monaten des Jahres 2010 schließen, bei einem Umsatz von 1.2 Milliarden USD.

Suchmöglichkeiten

Facebook bietet umfangreiche Suchmöglichkeiten, sowohl seitenintern als auch über externe Suchmaschinen[4]. Gesucht werden können generell Personen (inkl. Bildern), Gruppen, Dinge, die Nutzern gefallen (Bands, Hersteller, …), Apps (Anwendungen), Veranstaltungen, Benutzern zugeordnete Institutionen (etwa Hochschulen und Schulen), Beruf(e) einer Person, Firmen, bei denen die Person tätig war, Teile des Lebenslaufs, das „Motto" und weitere Profilelemente.

Die Suche bezieht sich zunächst auf nahe Verbindungen, bevor weiter entfernte Verbindungen analysiert werden. Bei der Suche nach neuen Freunden schlägt Facebook so zunächst Freundes-Freunde vor (je umfangreicher und direkter die Verlinkung mit einer Person ist, desto eher wird sie als Freund vorgeschlagen). Wie bereits erwähnt, besteht ebenfalls die Möglichkeit, E-Mail-Konten nach Kontakten, die Facebook nutzen, zu durchsuchen (vgl. dazu auch Abschnitt Datenschutz & Sicherheit).

Überwachung des Nutzerverhaltens

Eine Verlinkung von Profilen ist über den „Gefällt mir"-Button, Freundschaftsbeziehungen/Partnerschaftsbeziehungen/Familienbeziehungen, Gruppenzugehörigkeiten, Markierungen auf Bildern und in Videos, Verlinkungen innerhalb von Apps (etwa Farmville-Nachbarn) und im Rahmen von Veranstaltungen möglich. Es kann überwacht werden, ob ein Nutzer an einer bestimmten Veranstal-

4) Die Suche durch externe Suchmaschinen, etwa Google oder Yahoo, ist nur für öffentlich zugängliche Profile möglich.

tung teilnimmt. Überträgt ein Nutzer seinen Aufenthaltsort, so ist auch dieser überwachbar. Wie bei den meisten anderen sozialen Netzwerken sind auch bei Facebook sämtliche Beziehungen einer Person einsehbar.

Bei den beliebten „Gefällt-mir"-Buttons ist zu beachten, dass sie unter Umständen persönliche Daten übertragen, ohne dass sie angeklickt wurden [23]. So kann auf der Website von Heise nachgelesen werden: „Konkret kann Facebook [...], während Sie dort angemeldet sind, beobachten welche Webseiten Sie aufrufen, sofern diese einen solchen Like-Button enthalten. [...] Und anders als Statistik-Server wie Google Analytics, die IVW oder auch die Server von Anzeigen-Dienstleistern, die mit anonymisierten Daten oder schlimmstenfalls IP-Adressen arbeiten, kann Facebook diese Daten direkt mit einer realen Person verknüpfen, deren Adresse und Freunde es kennt. Angesichts der einschlägigen Erfahrungen, was Daten und Privatsphäre der Mitglieder angeht, muss man auch davon ausgehen, dass die amerikanische Firma diese Daten auswertet und früher oder später zu Geld macht." [23]. Der „Gefällt-mir"-Button (dies gilt auch für die Kommentarfunktion von Facebook) ist in externe Webseiten integrierbar, was die Gefahr des Missbrauchs von Nutzerinformationen durch Facebook weiter erhöht.

Um zu verhindern, dass Facebook nur durch den Besuch eines Users auf einer Seite dessen Daten erhält, nutzen inzwischen viele Websites eine zweistufige Version des „Gefällt-mir"-Buttons. Dieser muss durch einen Klick aktiviert werden. Erst der zweite Klick veröffentlicht den „Gefällt-mir"-Eintrag auf der Pinnwand des Users.

Administrationsmöglichkeiten für Profile und Konten

Die Administrationsmöglichkeiten für ein Profil sind umfangreich. Standardmäßig sind Facebook-Profile öffentlich, können also z. B. über eine Google-Suche gefunden werden. Dies kann jedoch deaktiviert werden kann. Explizit kann – und sollte – festgelegt werden, welche Personengruppen (etwa Freunde oder Freunde-des-Freunde) welche Profilattribute (etwa politische Einstellung, Freundschaften, Beziehungsstatus, besuchte Orte, das Geburtsdatum usw.) sehen können soll. Ausgewählte Nutzer können auch „geblockt", also vom Profilzugriff ausgesperrt werden. Der Zugriff des Mobiltelefons kann ebenfalls konfiguriert werden.

Seit August 2011 wurde die Administration vereinfacht. Der Nutzer bekommt in seinen Privatsphäre-Einstellungen drei Vorschläge angezeigt, aus denen er auswählen kann:

- öffentlich
- Freunde
- benutzerdefiniert

Die Auswahl der Option „Freunde“ führt z. B. dazu, dass alle Daten des Nutzers nur noch für Freunde sichtbar sind.

Gleichzeitig wurden zudem die Datenschutzeinstellungen erweitert. So können Statusmeldungen inzwischen nicht mehr nur für alle Freunde insgesamt sichtbar veröffentlicht werden, sondern erlauben eine detaillierte Einstellung pro Person, Gruppe oder Freundesliste.

Um die Sicherheit des Profils zu verbessern, können Nutzer in ihren Kontoeinstellungen festlegen, dass die Verbindung zu Facebook SSL-verschlüsselt werden soll. Außerdem können Anmeldebenachrichtigungen aktiviert werden, die den User informieren, wenn von einem Computer oder Handy auf dessen Konto zugegriffen wird, das zuvor noch nie für die Anmeldung verwendet wurde.

Die Löschung des Accounts wird Nutzern von Facebook allerdings nicht leicht gemacht. So findet sich in den Kontoeinstellungen des Profils nur die Möglichkeit, das Konto zu deaktivieren, was Facebook die weitere Speicherung sämtlicher Nutzerdaten erlaubt und dem User die Möglichkeit geben soll, sich jederzeit wieder anzumelden. Das tatsächliche Löschen ist nur über einen Link möglich, der sich ziemlich versteckt innerhalb des Hilfebereichs befindet.

Seit Mitte Dezember 2011 bietet Facebook seinen Nutzern die Möglichkeit über die Funktion „timeline“, die sog. Chronik, ihr Profil als interaktiven Lebenslauf zu präsentieren. Mit inbegriffen in dieser umstrittenen neuen Funktion, die seit 30. März 2012 verpflichtend für alle Nutzer eingeführt wurde, ist ein neues Layout der Profilansicht. Allerdings darf diese schönere und übersichtlichere Darstellung nicht über die damit verbundenen Risiken hinwegtäuschen. Durch die vollständige chronologische Auflistung aller jemals hinterlassenen Informationen, Bilder oder Kommentare können nicht nur peinliche „Jugendsünden“ ans Tageslicht kommen, die dem aktuellen Privat- oder Berufsleben nicht zuträglich sind. Speziell aus datenschutzrechtlicher Sicht ist vor allem bedenklich, dass die Möglichkeit, Daten und Fakten zu recherchieren, zu sammeln und zu verknüpfen, wesentlich vereinfacht wurde – was im Hinblick auf unerwünschte Besucher unangenehme Folgen haben kann. Obwohl die Umstellung auf „timeline“ momentan noch nicht bei allen Nutzer-Profilen erfolgt ist und wohl in der nächsten Zeit erst nach und nach realisiert werden kann, sollte sich jeder bewusst sein, dass eine Deaktivierung der Funktion nicht möglich ist. Angebliche „Tricks“, die seit Monaten im Internet diskutiert werden, sind nach aktueller Einschätzung nicht zur vollständigen Deaktivierung geeignet [143]. Um sich trotz

„timeline“ so weit wie möglich abzusichern, sollten alle jemals eingestellten Inhalte einzeln aufgerufen, auf ihre Schutzwürdigkeit überprüft und im Zweifelsfall gelöscht werden.

Datenschutz und Sicherheit

Facebook fiel in der Vergangenheit immer wieder durch Probleme im Umgang mit persönlichen Daten und der damit zusammenhängenden Implementierung von Schutzmechanismen negativ auf [24].

So gehören die AGB von Facebook zu den am meisten kritisierten aller sozialen Netzwerke. Diese beinhalten u. a. die Klausel, dass für „Inhalte, die unter die Rechte an geistigem Eigentum fallen, wie Fotos und Videos ... vorbehaltlich ... der ... Privatsphäre- und Anwendungseinstellungen ... die folgende Erlaubnis erteilt wird: Ein Benutzer überträgt Facebook ... eine nicht-exklusive, übertragbare, unterlizenzierbare, unentgeltliche, weltweite Lizenz für die Nutzung jeglicher ... Inhalte der genannten Art, die ... auf oder im Zusammenhang mit Facebook ... gepostet werden“ [25].

Dies schließt unter anderem das Recht ein, persönliche Daten von Usern an Dritte zu verkaufen. Im Jahr 2009 änderte Facebook seine Nutzungsbedingungen, so dass es die Daten seiner Nutzer nun zeitlich unbegrenzt verwenden durfte, d. h. auch nach der Deaktivierung oder Löschung des Nutzerkontos. Diese Änderung wurde allerdings nach Protesten von Usern sowie Daten- und Verbraucherschützern wieder zurückgezogen [26].

Ebenfalls ist anzumerken, dass Werber über Facebook persönliche Daten der registrierten Nutzer erhalten können. Bei Benutzung einer Anwendung in Facebook wird nur einmal eine Nachfrage hinsichtlich der Gewährung von Zugriffsrechten auf die Daten des Nutzers gestellt. Ein schnelles „Wegklicken“ gibt der jeweiligen Anwendung Vollzugriff.

Facebook sammelt aber nicht nur Informationen von registrierten Mitgliedern, sondern hat über die Funktion „Freunde-Finder“ auch die Möglichkeit, Daten von Nicht-Mitgliedern zu erhalten. Mit dieser Funktion können Facebook-Nutzer ihre E-Mail-Ordner und Adresslisten nach Personen durchsuchen lassen, die eventuell Mitglieder von Facebook sind. Auch E-Mail-Adressen von Personen, die nicht in Facebook gefunden werden, werden vom sozialen Netzwerk für die eventuelle spätere Verwendung gespeichert. So wird vor dem Import von Kontaktdaten angegeben: „Facebook wird die E-Mail-Adressen, die du importierst, mit niemandem teilen, aber wir werden diese in deinem Namen aufbewahren und eventuell später verwenden, um Freundschaftsvorschläge für dich und andere zu generieren.“

Eine weitere Möglichkeit, über Facebook Daten von Nicht-Mitgliedern zu erhalten, ist eine Handy-Anwendung, die von Facebook-Nutzern verwendet werden kann. Dabei synchronisiert der User seine Handykontakte mit seinen Facebook-Freunden und Facebook kann dadurch Informationen wie Namen, Telefonnummern, E-Mail-Adressen und Geburtstage von Nicht-Mitgliedern speichern. Inzwischen wird von Facebook ein Kontaktformular angeboten, das es nicht im sozialen Netzwerk registrierten Personen ermöglicht, alle Daten, die mit ihrer E-Mail-Adresse verknüpft sind, löschen zu lassen. Dies erzielt allerdings nur dann den gewünschten Effekt, wenn Facebook bereits eine Verknüpfung der Daten mit der E-Mail-Adresse vorgenommen hat [29].

Eine weitere Datenschutzlücke offenbarte sich Ende 2009, als Facebook die Standardeinstellungen für die Privatsphäre änderte. Durch die Änderung waren plötzlich Informationen wie Name, Profilfoto, Freunde und Gruppenzugehörigkeiten öffentlich sichtbar, unabhängig davon, was der User diesbezüglich vorher eingestellt hatte. Dieser Fehler wurde im darauffolgenden Jahr durch eine Vereinfachung der Privatsphäre-Einstellungen behoben, durch die standardmäßig lediglich Name, Profilbild und User-ID öffentlich sichtbar sind [30].

Neben diesen Datenschutzproblemen ist allerdings positiv zu erwähnen, dass Facebook seit einiger Zeit Anstrengungen unternimmt, um seinen Jugendschutz zu verbessern. So gründete es beispielsweise 2009 einen Sicherheitsbeirat und unterzeichnete 2008 Vereinbarungen für einen besseren Jugendschutz. Diese umfassen unter anderem Warnungen an Minderjährige vor dem Austausch persönlicher Daten sowie die Filterung von Inhalten und die Löschung von Links auf pornografische Angebote [31][32].

Durch eine Unachtsamkeit seitens Facebook konnten 2010 Außenstehende Informationen über Facebook-Nutzer auslesen. Diese Sicherheitslücke resultierte aus dem Verhalten des Browsers, der beim Zugriff auf eine URL den sogenannten Referer überträgt, d. h. die URL, von der die Anfrage kommt. Normalerweise ist dies ungefährlich, da die Quell-URL keine personenbezogenen Daten enthält. Bei Facebook-Usern verhält sich dies anders, da sie beim Klicken auf einen Link innerhalb von Facebook ihre User-ID bzw. ihren Usernamen mit übertragen. Für soziale Netzwerke ist dieses Verhalten sinnvoll, da interne Seiten personalisiert, also angepasst auf den jeweiligen User dargestellt werden. Beim Zugriff auf eine externe Seite jedoch könnte der Webserver dieser Site durch die übertragene User-ID herausfinden, welche Person die Anfrage geschickt hat. Um dies zu verhindern, verwendet Facebook eine interne Weiterleitungsseite, sodass die Zielwebsite als Referer nur die URL der Weiterleitungsseite erhält.

Diesen Sicherheitsmechanismus hat Facebook jedoch nur für Links auf externe Seiten benutzt, nicht aber für eingebettete Werbeanzeigen von Dritten.

Inzwischen hat Facebook auf diesen Fehler reagiert und die Art der Werbeeinbettung geändert. Außerdem wurde der Aufbau der internen URLs so umstrukturiert, dass die meisten User-Informationen erst nach einem „#"-Zeichen stehen. Da dieses Zeichen für eine interne Referenz auf einen anderen Seitenabschnitt steht, wird dieser Abschnitt nicht im http-Header übertragen [33][34][35].

Ein weiteres Problem, mit dem Facebook zu kämpfen hat, sind die sogenannten Scams[5] . Dabei werden Nutzer dazu bewegt, Links anzuklicken, die sich daraufhin auf die Pinnwände aller Freunde duplizieren und diese ebenfalls animieren darauf zu klicken, um sich weiter zu verbreiten. Ein bekannter Fall war beispielsweise der Link auf eine angebliche Anwendung, die bei einer Installation anzeigen würde, welche Nutzer sich das eigene Profil angesehen haben. Durch Anklicken duplizierte sich der Link auf die Pinnwände der Freunde und installierte zusätzlich ein Firefox-Plugin, das beim Aufruf der Facebook-Website Pop-up-Fenster einblendete.

Solche Scams könnten auch dazu benutzt werden, um statt Pop-up-Fenstern Schadcode auf dem Rechner des Benutzers zu öffnen und auszuführen [37][38].

Auch gab es immer wieder Würmer, die sich durch Lücken über Facebook verbreiten konnten [39]. Zwar wurden mittlerweile einige Sicherheitsfunktionen implementiert [40], doch fehlt etwa nach wie vor die Unterstützung für permanent SSL-verschlüsselte Verbindungen (die https-Verbindung ist möglich, muss aber explizit vom Benutzer aktiviert werden).

Die indirekte Übertragung von persönlichen Informationen durch eingebettete „Gefällt mir"-Buttons (siehe Abschnitt „Überwachung des Nutzerverhaltens") kann im Firefox-Browser durch das Blockieren von Cookies für Drittanbieter verhindert werden [41].

Facebook für Unternehmen

Facebook ist nicht nur für Privatpersonen interessant. Auch Unternehmen können aus einer Präsenz in dem sozialen Netzwerk Vorteile ziehen. Dafür muss sich ein Unternehmen zunächst als Privatperson registrieren und kann anschließend über diesen Account das Unternehmensprofil anlegen.

5) Die Empfänger werden unter Vorspielung falscher Tatsachen (vgl. Social Engineering) dazu bewegt, an einem Schneeballsystem teilzunehmen [36].

Facebook bietet verschiedene Seitenkategorien, die es einer Vielzahl von unterschiedlichen Einrichtungen ermöglichen, sich zu präsentieren. So gibt es Websites für

- Lokale Unternehmen oder Orte
- Unternehmen, Organisationen oder Institutionen
- Marken oder Produkte
- Künstler, Bands oder öffentliche Personen
- Unterhaltung
- Anliegen oder Gemeinschaften.

Ein Unternehmensprofil kann z. B. dafür genutzt werden, ein positives Markenimage aufzubauen, seine Bekanntheit zu steigern, die Kundenbindung zu erhöhen oder potentielle Mitarbeiter zu rekrutieren. Allerdings sollten auch hier die im Kapitel „Analyse der Gefahren von sozialen Netzwerken" genannten Gefahren (z.B. Negativkampagnen durch Shit-Storms) frühzeitig beachtet werden und ein professioneller Umgang durch einen Unternehmensvertreter sollte gewährleistet sein.

Die Administrationsrechte für das Unternehmen können auf mehrere Facebook-Profile verteilt werden. Wird nach dem Unternehmensnamen gesucht, so zeigt Facebook das entsprechende Profil an. Falls das gesuchte Unternehmen kein Profil besitzt, finden sich bei Facebook in der Regel Informationen aus Wikipedia, sofern dort ein Eintrag zum Unternehmen besteht.

Unternehmensprofile haben dieselben Funktionalitäten wie private Profile. Im Unterschied zu Benutzer-Profilen können sie allerdings „geliked"[6] werden.

Seit dem 30.03.2012 werden auch die Profile von Unternehmen, Organisationen, Vereinen und Bands auf den neuen Timeline-Look (sog. Chronik) umgestellt – analog der Umstellung der privaten Accounts.

6) Englische Bezeichnung für das Klicken auf den „Gefällt mir"-Button

LinkedIn

Übersicht

Nutzer in Deutschland	Über 2 Mio. Mitglieder in der DACH-Region (Deutschland, Österreich, Schweiz) [43]
Nutzer weltweit	Mehr als 150 Millionen (Stand Februar 2012) [43]
Hauptsitz	Mountain View, Kalifornien, USA [42]
Gründungsjahr	Mai 2003 [42]
Eigentümer	Reid Hoffman und weitere Vorstandsmitglieder, Sequoia Capital, Greylock Partners, Bessemer Venture Partners [44]
Hauptbenutzergruppe	Zwischen 35 und 44 Jahren

Kurzbeschreibung

LinkedIn ist das weltweit größte Business-Netzwerk mit über 150 Millionen registrierten Mitgliedern. In Deutschland hat es über eine Million Mitglieder. Gegründet im Mai 2003 in Mountain View, CA USA, gehört es laut dem Serverdienst Alexa [42] zu den 500 weltweit meistbesuchten Websites. Im Dezember 2011 lag LinkedIn weltweit auf Rang 36 der am meisten besuchten Websites [43].

Typischer Inhalt und Kommunikationsmethoden

In Business-Netzwerken wie LinkedIn stellen die Mitglieder im Allgemeinen ihren beruflichen Werdegang dar, geben Auskünfte zu ihrer Bildung und momentanen Stellung sowie teilweise auch über ihren aktuellen Arbeitgeber. Diese Selbstdarstellung ist wie ein Lebenslauf aufgebaut und hilft Unternehmen, auf Nutzer aufmerksam zu werden. Dabei besitzt jedes Profil einen Slogan, der eine Kurzbeschreibung des Nutzers in einem Satz darstellt und für alle sichtbar ist. In der Rubrik „Interests" kann man mithilfe kurzer Schlagworte Interessen eintragen und es dadurch anderen Mitgliedern ermöglichen, das eigene Profil mittels Schlagwortsuche zu finden. Des Weiteren gibt es die Möglichkeit, Profilbilder zu erstellen, seine eigene Webseite zu verlinken oder auch einen Lebenslauf zu veröffentlichen. Mitglieder können sich untereinander empfehlen und Unternehmensprofile erstellen, über die Produkte beworben oder empfohlen werden [45].

Die typische Kommunikationsmethode von LinkedIn besteht darin, Nachrichten an andere Mitglieder über eine private Nachricht (PN) oder per E-Mail zu senden. Die E-Mail-Adressen registrierter Kollegen desselben Arbeitgebers sind dabei einsehbar. Beziehungen zu Firmen, Gruppen und Personen können angelegt und verwaltet werden. Das Versenden von Nachrichten an Mitglieder, die nicht zu den eigenen Kontakten oder Freunden gehören, ist

allerdings kostenpflichtig, falls kein gemeinsamer Kontakt besteht, der die beiden Personen einander vorstellen kann [45].

Finanzierung

Die Einnahmen von LinkedIn kommen zum größten Teil aus Werbeanzeigen und Gebühren, etwa für Personalagenturen. Mitgliedschaften können aber auch bis zu 100 USD im Monat kosten. Am 19.5.2011 ging LinkedIn erfolgreich an die Börse. Die Aktie stieg am ersten Tag von 45 USD bis auf kurzzeitig 112 USD [42]. Der aktuelle Stand der Aktie beträgt 98 USD (Stand 25. Mai 2012) [57]

Suchmöglichkeiten

Allen Mitgliedern steht ein umfangreiches Angebot an Suchfunktionen zur Verfügung, wie z.B. eine Suche nach Personen- bzw. Firmennamen oder Berufsbezeichnung. Für zahlende Mitglieder verbessern sich die Suchfunktionen und -filter. Zudem besteht die Möglichkeit zu Verlinkungen in den Bereichen:

- Gruppen
- Berufssparten und Interessen
- Kollegen / ehemalige Kollegen bei Firma X
- Firmen

Sobald ein Mitglied sich mit einem der oben genannten Punkte identifiziert, ist es gleichartig verlinkten Personen möglich, das jeweilige Profil einzusehen.

Administrationsmöglichkeiten für Profile und Konten

Alle Informationen, die der registrierte Nutzer online stellt, werden von LinkedIn gespeichert und anderen Nutzern zur Verfügung gestellt. Welche Informationen andere Benutzer sehen dürfen, kann in den Profil-Einstellungen festgelegt werden. Dabei sind bestimmte Daten in der Standard-Einstellung öffentlich sichtbar, können aber nachträglich eingeschränkt werden [46][47][48].

Die Administrationsebene für das eigene Konto bietet neben den persönlichen Daten, wie z.B. Telefon, Adresse, Geburtsdatum und E-Mail-Adresse, einige erweiterte Funktionen wie etwa:

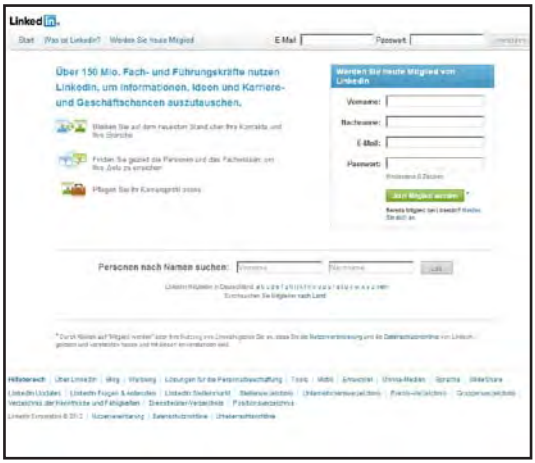
- Empfehlungen erfragen/erteilen
- Fachgebiete oder besondere Auszeichnungen hervorheben
- Jobtitel, Firmen, Firmendaten, Wahl der Informationen, die öffentlich zugänglich sind

Außerdem ist es den Mitgliedern jederzeit möglich, das Erscheinungsbild des Profils zu ändern, da es sich aus verschiedenen Einzelbausteinen zusammensetzt, die frei verschiebbar sind.

Datenschutz und Sicherheit

Alle Daten, die ab dem Zeitpunkt der Anmeldung eingegeben werden, werden von LinkedIn gespeichert und gesammelt, aber man erhält keine Auskunft über alle von LinkedIn gespeicherten Daten.

Es besteht die Möglichkeit, die Daten für den Zugriff von außen (z. B. für externe Suchmaschinen wie Google) zu sperren. Die AGB



von LinkedIn sind vergleichbar mit denen anderer großer sozialer Netzwerke wie z.B. Facebook. Stiftung Warentest hat LinkedIn zusammen mit anderen sozialen Netzwerken getestet und bemängelt beispielsweise: „So schränken Facebook, Myspace und LinkedIn die Rechte der Nutzer stark ein, genehmigen sich selbst aber weitreichende Rechte, vor allem bei der Weitergabe der Daten an Dritte.“[49] Stiftung Warentest kritisiert in diesem Zusammenhang auch die mangelnde Transparenz von LinkedIn sowie Klauseln in den AGB: „Dreist ist auch folgende Klausel: ‚LinkedIn kann die Vereinbarung mit oder ohne Grund, jederzeit, mit oder ohne Mitteilung kündigen.‘“[49]

Vor einigen Monaten wurde eine gravierende Sicherheitslücke bei der Anmeldung von LinkedIn-Mitgliedern gefunden. Diese besteht darin, dass die Authentifizierungs-Token[7] der Mitglieder unverschlüsselt übertragen und gespeichert werden und damit ein Auslesen und anschließendes Übernehmen des Kontos durch den Angreifer erlauben. LinkedIn gibt allerdings an, bereits an einer SSL-verschlüsselten Übertragung der Token zu arbeiten, die das Auslesen verhindert. Eine weitere Gefahr liegt in der Gültigkeit der Token. Sie werden nicht nur unverschlüsselt übertragen, sondern sind auch über einen Zeitraum von einem Jahr gültig. Gelingt es einem Angreifer den Token zu erlangen, bringt dem Nutzer auch eine Änderung seines Passworts nichts, da der Token trotzdem gültig bleibt [50].

LinkedIn für Unternehmen

Unternehmen haben die Möglichkeit eigene Seiten anzulegen. So kann eine Firma zum Beispiel auf ihrer Unternehmensseite Jobangebote exklusiv für Mitglieder des Netzwerks anbieten und sich über Suchfunktionen sofort passende Kandidaten anzeigen lassen und diese benachrichtigen. Zudem können neue Produkte präsentiert werden, die so von Millionen von Fachkräften kommentiert und bewertet werden können.

7) Kurze Textdateien, die auf dem Rechner eines Nutzers abgelegt werden und wie ein Schlüssel arbeiten.

Lokalisten

Übersicht

Nutzer	3,6 Millionen (Stand: Juli 2010) [51]
Hauptsitz	München, Deutschland
Gründungsjahr	Mai 2005
Eigentümer	ProSiebenSat.1 Media, Deutschland (90%), Lokalisten Media GmbH, Deutschland (10%) [52]
Hauptbenutzergruppe	20 - 29 Jahre

Kurzbeschreibung

Lokalisten ist ein in München ansässiges, kommerzielles soziales Netzwerk. Der Großteil der Nutzer kommt aus Bayern. Einnahmen werden durch Werbung und den Verkauf von Fan-Artikeln erzielt. Nach der Gründung im Mai 2005 durch die Lokalisten Media GmbH wurde im Oktober 2009 mit 43,2 Millionen Besuchen die Höchstnutzung erreicht. Inzwischen ist das Interesse an dem sozialen Netzwerk deutlich zurückgegangen: Im März 2012 lag die Anzahl der monatlichen Besuche nur noch bei 5,3 Millionen [56].

Typischer Inhalt und Kommunikationsmethoden

Bei Lokalisten sind hauptsächlich Profile von Privatpersonen gespeichert. Wie in anderen sozialen Netzwerken finden sich auch bei Lokalisten private Informationen der Mitglieder, die sie über „Freundeslisten" anderen Nutzern zugänglich machen können. Mitglieder können so beispielsweise Fotos, Videos, Events und Tagebucheinträge veröffentlichen oder Nachrichten im Gästebuch des Profils eines anderen Nutzers hinterlassen. Für alle gepostenten Veranstaltungen besteht zusätzlich die Möglichkeit, Einträge im Gästebuch des jeweiligen Events zu verfassen.

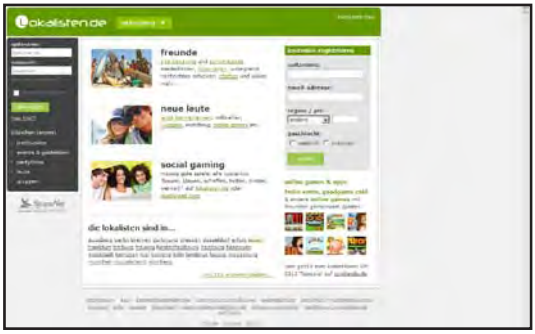
Für die Kommunikation in Echtzeit steht ein Chat zur Verfügung. Darüber hinaus gibt es die Möglichkeit, einem Mitglied eine private Nachricht zu schicken, in dessen Gästebuch zu schreiben oder seine Fotos, Alben oder Videos zu kommentieren. Für eine allgemeinere Kommunikation gibt es Gruppen, in denen sich Benutzer mit gemeinsamen Interessen oder Mottos zusammenschließen können. Nutzer können Gruppen gründen, ihnen beitreten oder sie wieder verlassen. Innerhalb der Gruppen gibt es Gruppenbeiträge, ähnlich einem Forum, in dem sich die Mitglieder untereinander austauschen können.

Bei Lokalisten gibt es ein eigenes Belohnungs-System für aktive Nutzer. Sie steigen je nach Aktivität im Level (1-100) und erhalten im Anschluss jeden Samstag ein Gehalt in Form von „Talern". Diese Taler können dazu verwendet werden, „Geschenke" in Form von kleinen Grafiken bzw. Cliparts zu kaufen und diese an andere Lokalisten-Nutzer zu verschicken. Eine Art öffentliches Tagebuch

stellen die Blogs dar. Einträge, die hier verfasst werden, können anschließend von jedem Mitglied gelesen und kommentiert werden. Auch „Kleinanzeigen“, sonst aus Tageszeitungen bekannt, können erstellt werden. Eine Kommentarfunktion gibt es hier nicht.

Über das Profil kann jeder Nutzer Einträge in seinem Tagebuch verfassen. Diese sind je nach Einstellung für alle Besucher des eigenen Profils, nur für Freunde oder Freundes-Freunde sichtbar. Auch bei Lokalisten gibt es sogenannte „Apps“, zu denen hauptsächlich Spiele auf Flash-Basis gehören. Ähnlich wie bei anderen sozialen Netzwerken können diese Anwendungen auf öffentliche Profilinformationen (Spitzname, Lokalisten-ID, Profilbild) des Nutzers sowie seiner Freunde zugreifen, um diese Informationen im Spiel darzustellen. So kann man zum Beispiel sehen, welcher Freund dasselbe Spiel spielt.

Eine etwas andere Form der Kommunikation zwischen Mitgliedern bietet der Prepaid-Karten-Tarif „Lokalisten fon“ an. Für 10 Euro kann ein Startpaket mit 5 Euro Startguthaben bestellt werden. Inhaber dieser Prepaid-Karte können untereinander zu einem günstigeren Tarif kommunizieren. Das mobile Surfen auf der Lokalisten-Webseite (erreichbar unter m.lokalisten.de) innerhalb Deutschlands ist damit kostenlos.



Das Lokalisten-Netzwerk verfügt neben der Web-Darstellung auch über Anwendungen für Smartphones mit Apple iOS und Google Android Betriebssystem. Diese Anwendungen sind sowohl im App Store als auch im Android Market kostenlos zu beziehen.

Finanzierung

Anfangs wurde das Netzwerk ausschließlich durch die Gründungsmitglieder finanziert. Die Firma SpaceNet AG unterstützt das Netzwerk bei Serverwartung und Hosting. Einnahmen durch Werbung wurden anfänglich von den Gründern abgelehnt. Seit der Übernahme durch die ProSiebenSat.1 Media hat sich dies jedoch geändert. Gegenwärtig verwendet das Lokalisten-Netzwerk Werbeeinblendungen. Nach Angaben des Unternehmens wird diese Werbung teilweise personalisiert, also auf Alter, Geschlecht und Aufenthaltsort des jeweiligen Nutzers angepasst [53]. Weitere Einnahmen werden durch den Verkauf von T-Shirts, Lokalisten-Dirndln und ähnlichen Artikeln im Lokalisten-Fan-Shop sowie mit Partyveranstaltungen erzielt [52].

Suchmöglichkeiten

Die Mitgliedersuche bietet die Möglichkeit, nach vielfältigen Kriterien zu suchen. Diese decken sich mit den im Profil gespeicherten Informationen (Spitzname, Name, E-Mail, Alter, Geschlecht, Ort, Sportarten, Hobbys, usw.).

Daneben gibt es die Möglichkeit zu „stöbern". Dabei werden Suchanfragen mit vorgefertigten Kriterien abgeschickt. Zur Auswahl stehen „Neue Mitglieder (mit Fotos)", „Jungs/Mädels in meiner Homebase"[8] und ähnliches. Über die „Ausbildungssuche" lassen sich Mitglieder herausfiltern, die bestimmte Schulen, Ausbildungsplätze oder Hochschulen besuchen oder besucht haben. Über die sog. „Trefferbox" kann nach bestimmten Kriterien (Geschlecht, mit Foto, online), der Homebase und dem Beziehungsstatus gesucht werden. Die „Treffer" können direkt kontaktiert oder auf eine Merkliste gesetzt werden, die nur für den aktuellen Benutzer einsehbar ist. Zu einem „Volltreffer" kommt es, wenn sich beide Mitglieder gegenseitig auf ihre Merklisten gesetzt haben – dazu erfolgt dann eine automatische Information.

Auf der Startseite findet jeder Nutzer das so genannte „Spotlight". Hier werden Profilbilder samt Kurznachrichten von Mitgliedern angezeigt, die sich mit ihren Talern ins Spotlight „eingekauft" haben.

Administrationsmöglichkeiten für Profile und Konten

Das eigene Profil kann auf vielfältige Art und Weise bearbeitet werden. Dabei kann unter anderem eingestellt werden, ob

- die Lokalisten-ID über Suchmaschinen auffindbar ist
- Aktivitäten für andere Mitglieder sichtbar sind
- Kontakte in einem bestimmten Altersbereich liegen müssen
- die Sichtbarkeit der Profil-Informationen variiert wird.

Datenschutz und Sicherheit

Laut den AGB §6 ff. räumt ein Nutzer den Lokalisten nicht-ausschließliche, zeitlich und räumlich unbeschränkte Rechte ein, vom Nutzer eingestellte Inhalte anderen Nutzern zugänglich zu machen. Darunter fällt auch „das Recht, die eingestellten Inhalte zu bearbeiten, um alle technisch erforderlichen Anpassungen (z.B. Änderung der Auflösung von Fotos und Videos...) vorzunehmen" [54]. Diese Rechte erlöschen, sobald der Nutzungsvertrag des betreffenden Mitglieds endet oder die Inhalte aus dem Lokalisten-Netzwerk entfernt werden. Weiter garantiert das Mitglied, über alle erforderlichen Rechte an den von ihm eingestellten Inhalten zu verfügen. Sollte es zu einem Rechtsstreit aufgrund fehlender Rechte kommen, trägt das Mitglied die volle Verantwortung. Nach eigenen Angaben werden keine Nutzerdaten an Dritte weitergegeben [55].

8) Homebase: Enspricht einer Anpassung der Lokalisten-Seite an eine bestimmte Region der Stadt.

Lokalisten für Unternehmen

Die Darstellungsmöglichkeiten für Unternehmen sind bei den Lokalisten sehr begrenzt, weil Firmen-Profile nicht möglich sind.

Zu Marketingzwecken lassen sich sogenannte „Events“ erstellen, zu denen sich andere Lokalisten-Mitglieder anmelden können. Dies wird zum größten Teil zur Eigenwerbung von Diskotheken genutzt. Dabei lassen sich auch „Specials“ erstellen, bei denen angemeldete Mitglieder beispielsweise Rabatte auf den Eintritt oder andere Vergünstigungen erhalten.

Eine weitere Möglichkeit ist, mithilfe der „Gruppen“-Funktion eine „Fangruppe“ zu erstellen und darüber Informationen an potentielle Kunden weiterzugeben.

Twitter

Übersicht

Nutzer in Deutschland	4,1 Millionen (Stand: März 2012) [144]
Nutzer weltweit	140 Millionen (Stand: März 2012) [97]
Hauptsitz	San Francisco, Kalifornien, USA
Sitz der Daten	Salt Lake City, Utah, USA
Gründungsjahr	März 2006
Unternehmensform	Kapitalgesellschaft
Hauptbenutzergruppe	Zwischen 35 und 44 Jahren

Quelle: [58-60]

Kurzbeschreibung

Twitter ist ein soziales Netzwerk, das im Jahr 2006 von Jack Dorsey, Biz Stone und Evan Williams gegründet wurde. Es wird oft auch als „öffentliches Tagebuch" im Internet bezeichnet. Nutzer verwenden Twitter zum „Bloggen"[9] von kurzen Textnachrichten, die maximal 140 Zeichen umfassen können. Der Nutzer entscheidet dabei, ob er die Nachricht jedem Nutzer oder nur seinen Freunden zur Verfügung stellen möchte. Das Veröffentlichen dieser Nachrichten wird als „Twittern" bezeichnet und dient dem Austausch von Gedanken oder der öffentlichen Meinungsäußerung zu einem bestimmten Thema. Auf jede dieser Nachrichten („Tweets") kann geantwortet werden [58].

Typischer Inhalt und Kommunikationsmethoden

Für die Nutzung von Twitter ist eine Anmeldung mit Namen, E-Mail und Passwort notwendig. Danach kann man sich mit E-Mail-Adresse und Passwort einloggen. Jeder Account hat die Möglichkeit, verschiedenen Personen oder Institutionen zu folgen (sog. „Following"). Das bedeutet, dass danach alle Tweets einer Person oder Institution auf der eigenen Startseite erscheinen. Auf jede Nachricht kann man antworten oder sie an einen Freund (sog. „Follower") weiterleiten. Außerdem kann der Tweet als Favorit markiert werden, damit man ihn später schneller wiederfinden kann.

Durch die Maximalanzahl von 140 Zeichen in einer Textnachricht beschränken sich die Nutzer bei der Verbreitung von Informationen auf das Wesentliche. Da via Twitter Informationen in Echtzeit einem großen Publikum verfügbar gemacht werden und das Prinzip der Weiterleitung die Verbreitung von Nachrichten fördert, ist dieses Medium vor allem bei Politikern und Prominenten beliebt: Der japanische Premierminister informierte 2011 über Twitter zur

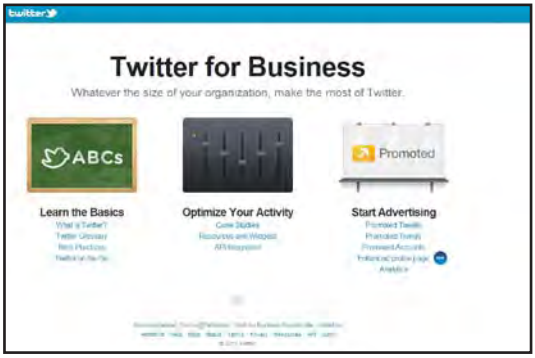
9) Veröffentlichen von Nachrichten im Internet.

aktuellen Lage in Fukushima. Beim Aufstand in Ägypten 2011 wurde Twitter zur Verbreitung politischer Meinungen genutzt.

Hier wird auch der Unterschied zu Facebook deutlich. Während Facebook vorwiegend der Kommunikation unter Freunden dient, ist Twitter eher ein Informationsnetz [61].

Twitter kann mittlerweile auch auf allen gängigen mobilen Geräten genutzt werden, so z.B. über iPhone, Android, iPad, Blackberry und Windows Phone 7. Damit können von unterwegs Nachrichten versendet oder empfangen werden. Außerdem bietet Twitter einen SMS-Service an, der es Nutzern ermöglicht, Twitter-Nachrichten zu empfangen, auch wenn sie keines der genannten Smartphones besitzen.

Außerdem bietet Twitter einen SMS-Service an, der es Nutzern, die keines der oben genannten Smartphones besitzen, ermöglicht, Twitter-Nachrichten empfangen zu können.



Des Weiteren können Twitter-Buttons auf der eigenen Homepage platziert werden, um neue Follower zu gewinnen. So sieht man beispielsweise auf www.bild.de am Ende eines jeden Artikels die Möglichkeit, diesen zu „twittern". Es wird also ein „Tweet" mit dem Link des Artikels erstellt, der den eigenen „Followern" zur Verfügung gestellt wird. Besitzt der Nutzer eine eigene Webseite, so kann er auf dieser seine aktuellen „Tweets" mit Hilfe eines von Twitter zur Verfügung gestellten Widgets[10] einbinden [62].

Finanzierung

Twitter finanziert sich bislang hauptsächlich aus Risikokapital und Investitionen der Unternehmen Union Square Ventures, Digital Garage, Spark Capital und Bezos Expeditions [63]. Andere Einnahmequellen besitzt Twitter kaum, sodass die Zukunft des sozialen Netzwerks unsicher ist. Um mehr finanzielle Sicherheit zu schaffen, entschloss sich Twitter im April 2010, Werbeflächen an Unternehmen zu verkaufen. Diese wurden so realisiert, dass nun vereinzelt Tweets mit der Markierung „promoted" in der Seite der Twitter-Suchergebnisse angezeigt werden. Im Juli 2011 wurde der Wert des Unternehmens auf ca. 4,9 Milliarden USD geschätzt [61][64].

10) Ein Widget ist meist eine Komponente der Benutzeroberfläche und kann in verschiedenen Anwendungen integriert werden.

Such-möglichkeiten

Twitter bietet verschiedene Möglichkeiten um Kontakte zu finden. Zum einen kann man über die E-Mail-Adresse oder den Twitter-Benutzernamen suchen. Zum anderen können unterschiedliche Mail-Anbieter wie Gmail, Yahoo, Hotmail & MSN Messenger und AOL durchsucht werden. Durch Angabe der Login-Daten gewährt man Twitter Zugriff auf seine Kontakte, die so automatisch zum eigenen Twitter-Account hinzugefügt werden.

Überwachung des Nutzerverhaltens

Jeder Tweet kann mit einer Ortsangabe versehen werden. Damit ließe sich beispielsweise ermitteln, ob jemand im Urlaub ist, falls dieser aus einem Internetcafé vom Urlaubsort twittert. Um die eigene Privatsphäre zu schützen, sollten deshalb die Ortsangaben bei neuen Tweets in den Einstellungen deaktiviert werden. Außerdem können im Profil eines Twitter-Nutzers auch Wohnort, Biografie oder Webauftritt gespeichert werden. Besonders durch Angabe eines Webauftritts können dort weitere Informationen gesammelt werden. Aber auch die Inhalte der Tweets können Informationen über den zugehörigen User preisgeben.

Administrations-möglichkeiten für Profile und Konten

Die Nutzer von Twitter können ihr Profil nach eigenen Vorstellungen anpassen, indem sie z.B. die Ortsangabe bei neuen Tweets generell deaktivieren, ihre Tweets vor der öffentlichen Einsicht schützen oder unbekannte Follower blockieren. Zusätzlich können die Benutzer einstellen, dass ihnen Twitter nur noch über eine sichere, https-verschlüsselte, Internetverbindung angezeigt wird.

Datenschutz und Sicherheit

Gemäß dem Kapitel „Die Rechte des Benutzers“ in den AGB von Twitter liegen die Rechte für alle Inhalte beim Nutzer. Dennoch räumt sich Twitter die nicht-exklusive, gebührenfreie und weltweite Erlaubnis ein, die Inhalte in sämtlichen jetzt bekannten oder später entwickelten Medien oder Vertriebsmethoden zu benutzen, zu kopieren, zu vervielfältigen, zu verarbeiten, anzupassen, zu verändern, zu veröffentlichen und zu übertragen. Darüber hinaus dürfen alle Inhalte von Twitter an Gesellschaften, Organisationen sowie Personen für die Versendung, Verbreitung oder Veröffentlichung in anderen Medien und Services, die gemäß den Geschäftsbedingungen verbunden sind, weitergegeben werden. Die Verwendung aller Materialien ist ohne Anspruch auf Entschädigung für den besagten Inhalt gestattet. Weiterhin trägt der Nutzer die Verantwortung für die Verwendung seiner Inhalte durch ihn oder durch dritte Parteien, die ein Partnerschaftsverhältnis mit Twitter haben [65].

Im Abschnitt „Einschränkungen der Inhalte und Nutzung der Services“ in den AGB wird der Zugriff auf die Daten geregelt. Demnach behält sich Twitter das Recht auf Zugang sowie Aufbewahrung und Offenlegung jeglicher Informationen vor. In Übereinstimmung mit den Geschäftsbedingungen dürfen auch persön-

liche Daten von Nutzern an Dritte weitergegeben werden [65]. Außerdem behält sich Twitter das Recht vor, nutzerbezogene Daten an Dritte zu verkaufen, falls das Unternehmen den Eigentümer wechselt [66].

In der Vergangenheit wurde das soziale Netzwerk aufgrund von Sicherheitslücken bereits zum Ziel von Angriffen. So nutzte im Jahr 2007 ein Angreifer die Möglichkeit, die Absenderangabe einer SMS als Authentifizierung für das Benutzerkonto zu verwenden, um Nachrichten im Namen eines anderen zu verbreiten [67]. Ein Fehler im Twitter-Dienst „t.co" führte 2010 zu einer automatisierten Verbreitung von Nachrichten unter den Followern der Betroffenen. Diese Sicherheitslücke betraf nur Nutzer, die Twitter über die Weboberfläche und nicht mit Hilfe von Client-Programmen verwendeten [68].

Twitter für Unternehmen

Twitter ist auch für Unternehmen eines der beliebtesten sozialen Netzwerke. Während des Anmeldevorgangs gibt es keinen Unterschied zwischen Privatperson und Unternehmen. Im Vergleich zu Facebook ist die Anmeldung bei Twitter mit weniger Aufwand verbunden.

Unternehmen schätzen den Vorteil, dass jeder an ihrem Nachrichtenstream teilhaben kann. Außerdem können sie auf Nachrichten wie z.B. Neuerscheinungen von Produkten oder Veranstaltungen als Twitter-Nutzer antworten, sodass eine direkte Kommunikation zwischen Unternehmen und Kunden ermöglicht wird. Als weiteren Vorteil bewerten viele Firmenvertreter und Kunden die Kürze der Twitter-Nachrichten, die auf 140 Zeichen begrenzt sind. Damit beschränken sich die Beiträge auf das Wesentliche. Gegebenenfalls lassen sich Beiträge um einen Link für weitere Informationen erweitern.

Twitter besitzt zudem eine Schnittstelle, die die Anbindung von externen Anwendungen (z.B. FourSquare) erlaubt [69].

VZ-Netzwerke

Übersicht

Nutzer in Deutschland	Ca. 16 Millionen [70] (Stand November 2011)
Hauptsitz	London, England [71]
Gründungsjahr	Oktober 2005 [71]
Umsatz	Ca. 30 Millionen Euro [71] (Stand Dezember 2011)
Eigentümer	VZnet Netzwerke Ltd.
Hauptbenutzergruppe:	
StudiVZ	Studenten und ehemalige Studenten
SchülerVZ	Schüler und Auszubildende zwischen 12 und 21 Jahren
FreundeVZ	Soziales Netzwerk für alle Zielgruppen

Kurzbeschreibung

Die kostenfreien VZ-Netzwerke bestehen aus den sozialen Netzwerken StudiVZ, FreundeVZ und SchülerVZ, wobei zwischen den beiden erstgenannten ein Datenaustausch möglich ist. Die unterschiedlichen Plattformen sind auf verschiedene Zielgruppen ausgelegt.

Das soziale Netzwerk StudiVZ zielt auf Studenten und ehemalige Studenten ab, während SchülerVZ als reines Schülernetzwerk für Kinder und Jugendliche ab 12 Jahren gedacht ist. Das für junge Erwachsene von 18-29 Jahren konzipierte MeinVZ wurde im September 2011 in FreundeVZ umbenannt und umgestaltet. Nachdem die Nutzerdaten der VZ-Netzwerke – vermutlich zugunsten von Facebook – kontinuierlich und im großen Umfang zurückgehen, ist aktuell geplant, StudiVZ und FreundeVZ zusammenzulegen.

Typischer Inhalt und Kommunikationsmethoden

Die Nutzerinformation in den VZ-Netzwerken besteht meist aus

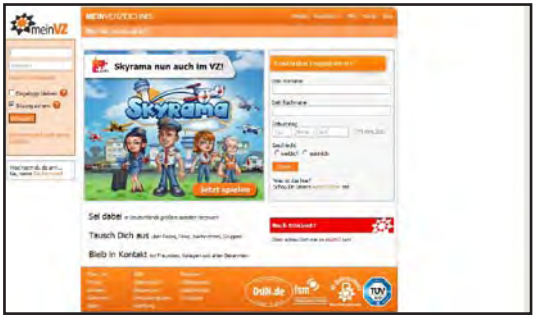
- einem gegliederten Profil mit allgemeinen Informationen,
- den Kontaktdaten,
- dem Arbeitsplatz,
- Persönlichem sowie
- einem Profilbild und/oder Fotoalben.

Neben der standardmäßigen Kommunikationsform mittels persönlicher Nachricht besteht die Möglichkeit, Einträge auf der „Pinnwand“ von anderen Nutzern zu hinterlassen bzw. Einträge anderer zu bekommen.

Wenn Nutzer Personen auf Bildern erkennen, können sie diese innerhalb des Bildes markieren, d. h. das Profil dieser Person mit dem entsprechenden Bildbereich verlinken. Für andere ist dann erkennbar, wer auf dem Bild zu sehen ist. Bilder können zusätzlich zu den Markierungen kommentiert werden, indem andere Nutzer einen kurzen Text hinterlassen. Dies könnte zum Beispiel eine Erklärung zur Entstehung des Fotos sein.

Die bereits erwähnte Schnittstelle zwischen StudiVZ und FreundeVZ soll es Nutzern dieser beiden Netzwerke ermöglichen, sich gegenseitig zu finden. Eine Schnittstelle zu SchülerVZ besteht aus Jugendschutzgründen nicht [72]. Die Nutzer sehen, welchen Gruppen ihre Freunde beigetreten sind, welche sogenannten „Edelprofile" (Profile von prominenten Personen) sie gut finden, bzw. welche Nachrichten auf den Pinnwänden hinterlassen wurden und wer mit wem Freundschaft geschlossen hat. Diese Mitteilungen laufen über den sogenannten „Buschfunk".

Dies ist ein Dienst, der das Versenden von Nachrichten mit einer Maximallänge von 140 Zeichen erlaubt und diese auf den Pinnwänden aller Freunde anzeigt. Neben Nachrichten werden dort auch Freundes-Aktivitäten wie das Hochladen von Fotos oder der Neuerwerb von Apps angezeigt. Eine Kommentarfunktion erlaubt allen Freunden die Veröffentlichung von Beiträgen zu den Buschfunk-Mitteilungen. Zudem besteht eine Schnittstelle zu Twitter, um Tweets im Buschfunk veröffentlichen zu können oder umgekehrt [72][73].



Finanzierung

StudiVZ finanziert sich zum einen über eine Reihe von Privatpersonen und Unternehmen, zu denen u. a. erfolgreiche Internet-Unternehmen und die beiden Venture Capital Funds European Founders Found GmbH und Holtzbrinck Ventures GmbH gehören [74].

Um weiterhin die kostenlose Nutzung des sozialen Netzwerks zu gewährleisten, finanziert sich StudiVZ zusätzlich durch die Einnahmen aus Werbeeinblendungen [74]. Hinzu kommen noch Einnahmen aus dem Verkauf von bedruckten Kleidungsstücken durch die Marketing-Abteilung der VZ-Netzwerke.

Außerdem erhält SchülerVZ eine Gewinnbeteiligung an der Nutzung von Apps[11] mit kostenpflichtigen Inhalten, die von Dritten innerhalb des sozialen Netzwerks bereitgestellt werden. Obwohl

11) Externe Anwendungen

die Apps in der Regel kostenlos sind, können sogenannte Premium-Inhalte, wie zusätzliches virtuelles Geld oder Güter, durch eine Bezahlung freigeschaltet werden. Damit ist es dann u. a. möglich weiterführende Level zu erreichen. Die Bezahlung erfolgt per Handy mithilfe der Firma Mindmatics, d. h. der Betrag wird von der Handyrechnung oder dem Prepaid-Guthaben abgebucht. Dabei wird allerdings sichergestellt, dass ein monatlicher Maximalbetrag von 30 Euro nicht überschritten wird [75].

Suchmöglichkeiten

Die Suche nach einer Person lässt sich auf verschiedene Weise durchführen: nach Namen mit einer einfachen Suchmaske, nach allen Feldern aus dem allgemeinen Profilteil mit der sogenannten „Super-Suche", oder nach einzelnen Feldern wie z.B. der politischen Einstellung aus dem persönlichen Profilteil. Mit den Standardeinstellungen ist es möglich, Profile der Freunde sowie von Freundes-Freunden anzusehen. Andere Profile sind nicht öffentlich.

Überwachung des Nutzerverhaltens

Öffentliche Profile können von jedem angemeldeten Nutzer gesehen werden. Dadurch lässt sich auch das Nutzerverhalten ableiten, z.B. welchen Gruppen er beigetreten ist oder welche Freunde oder Interessen er hat. Benachrichtigungen über das Nutzerverhalten von Freunden (wie z.B. bei Facebook) lassen sich über die Funktion „Buschfunk" einstellen. Diese kann jederzeit über die Profileinstellungen deaktiviert werden.

Administrationsmöglichkeiten für Profile und Konten

Die Einstellungen zur Privatsphäre können mit vielen Optionen individuell angepasst werden. Es können Voreinstellungen in den Kategorien gewählt werden (d.h. jeder Besucher darf entweder alles, nichts oder Teile vom eigenen Profil sehen). Es gibt allerdings auch die Möglichkeit, die Privatsphäre-Einstellungen selbst zu definieren. Dies ist aber wegen des Funktionsumfangs sehr aufwändig, da bei jeder Funktionalität, die das VZ-Netzwerk bietet, entschieden werden muss, ob (und welche) privaten Daten generell unsichtbar, oder nur für Freunde sichtbar sein sollen.

Die Apps, die von externen Anbietern innerhalb der VZ-Netzwerke zur Verfügung gestellt werden, bieten ein sogenanntes Visitenkartensystem, um den Nutzern die differenzierte Einstellung ihres Datenschutzes zu ermöglichen. Dabei können User für jede App eine Visitenkarte anlegen, in der individuell festgelegt werden kann, welche Informationen dieser App zugänglich gemacht werden. Zusätzlich kann für jede App eingestellt werden, ob sie auf dem Profil sichtbar ist oder nicht [79].

Datenschutz und Sicherheit

In den AGB der VZ-Netzwerke ist festgelegt, dass die Rechte an hochgeladenen Inhalten nicht an die VZ-Netzwerke übertragen werden. Die Nutzer müssen sich aber vor dem Hochladen von Bilddateien etc. vergewissern, dass sie selbst die Urheberrechte

besitzen. Die VZ-Netzwerke übernehmen in einem gegenteiligen Fall keine Haftung (vgl. [80]).

Vor drei Jahren führten die VZ-Netzwerke neue AGB ein, um die Verwendung von personalisierter Werbung zu ermöglichen. Dies führte in mehrfacher Hinsicht zu Kritik seitens der Medien und der Nutzer. Zum einen wurden diese dazu gezwungen, den neuen AGB zuzustimmen, da sie ansonsten aus ihrem (für andere Nutzer immer noch zugänglichen) Profil ausgesperrt wurden. Dieses Vorgehen wurde von einigen Rechtsanwälten sogar als rechtswidrig eingestuft. Zum anderen wurden durch die Verwendung der personalisierten Werbung Nutzerdaten (wenn auch anonymisiert) an Dritte übertragen [71].

Viele Mitglieder wollten dies nicht hinnehmen und verließen daraufhin das soziale Netzwerk. In diesem Zusammenhang unterzeichnete StudiVZ nach einer Abmahnung vom Bundesgerichtshof zusammen mit anderen sozialen Netzwerken wie Facebook und Lokalisten eine Unterlassungserklärung, die den Nutzern einen größeren Schutz ihrer privaten Daten gegenüber den Anbietern einräumt [81].

Die Einführung der neuen AGB ermöglichte den VZ-Netzwerken aber auch die Lösung eines Konflikts, der durch die Verpflichtung zur Herausgabe von Daten an Ermittlungsbehörden entstand. Gesetzlich sind soziale Netzwerke dazu verpflichtet, einer solchen Anfrage nachzukommen, wenn ein begründeter Verdacht gegen den jeweiligen Nutzer besteht. Dagegen verbietet das Telemediengesetz jedoch das Speichern von Nutzerdaten gegen den ausdrücklichen Willen der User. Durch die Änderung der AGB waren die Nutzer nun gezwungen, der Speicherung ihrer Daten zuzustimmen und ermöglichten es den VZ-Netzwerken somit, diese notfalls legal an Ermittlungsbehörden weitergeben zu können [82].

Wie viele soziale Netzwerke haben auch die VZ-Netzwerke Schwierigkeiten damit, ihre Nutzerdaten vor unberechtigtem Zugriff zu schützen. So wurden beispielsweise im Dezember 2006 über eine Million StudiVZ-Profile heruntergeladen, um damit eine Analyse der Profilinformationen durchzuführen. Da der unrechtmäßige Zugriff auf Profildaten in den VZ-Netzwerken immer wieder mit Programmen (sogenannten Crawlern) automatisiert wurde, setzte vor allem SchülerVZ ab Dezember 2006 verstärkt auf den Einsatz von Captchas[12], um dieses Vorgehen zu erschweren.

12) Captchas dienen der Festzustellung, ob es sich bei einem Benutzer um einen Menschen oder eine Maschine handelt. Sie verlangen oftmals die Eingabe eines Textes, der vorher durch einen Bildfilter verzerrt wurde und somit für Menschen einfach, für Programme aber sehr schwer zu lesen ist.

Im Februar 2007 musste SchülerVZ sogar so weit gehen, die Passwörter aller User zurückzusetzen und die Website einige Stunden vom Netz zu nehmen, da es einem Angreifer gelungen war, sich Zugriff auf die Datenbank des Netzwerks zu verschaffen, wodurch er nicht veröffentlichte Daten wie Passwörter und E-Mail-Adressen auslesen konnte.

Als dann 2009 ein Programm veröffentlicht wurde, mit dem die Captchas innerhalb der VZ-Netzwerke automatisch gelesen werden konnten, wurden diese auf den VZ-Websites wieder entfernt, da sie keinen praktischen Nutzen mehr zur Abwehr von Angriffen brachten und damit die Benutzung der Website nur erschwerten.

Im selben Jahr tauchte eine Datensammlung von etwa 100.000 Datensätzen auf, die durch verschiedene Sicherheitslücken in den VZ-Netzwerken zusammengestellt worden war. Daraufhin soll der Angreifer den VZ-Netzwerken angeboten haben, diese könnten die Daten von ihm zurückkaufen. Die genaueren Umstände der Tat konnten nie geklärt werden, da der Verdächtige wenig später in der Untersuchungshaft Selbstmord beging. [71][83][84][85]

VZ-Netzwerke für Unternemen

Unternehmen können die VZ-Netzwerke, insbesondere StudiVZ, für die Personalsuche nach Absolventen bestimmter Hochschulen nutzen. Es besteht ebenfalls die Möglichkeit, ein Edelprofil z.B. für Geschäftsführer oder Vorstandsmitglieder anzulegen. Dies kann für einen zusätzlichen Werbeeffekt sorgen.

Google+

Übersicht

Nutzer in Deutschland	3,6 Millionen (Stand Januar 2012) [76]
Nutzer weltweit	Mehr als 170 Millionen (Stand April 2012) [77]
Hauptsitz	Mountain View, Kalifornien, USA
Gründungsjahr	Juni 2011 [86]
Eigentümer	Google Inc.
Hauptbenutzergruppe	Zwischen 20 und 29 Jahren

Kurzbeschreibung

Bei Google+ handelt es sich um ein soziales Netzwerk, das von der Google Inc. betrieben wird. Google+ ermöglicht eine Integration von sozialen Elementen in andere Google-Produkte wie die Google-Websuche oder Google-Mail. Dadurch werden z.B. bei der Suche Treffer bevorzugt, die von Bekannten in dem sozialen Netzwerk bereits markiert worden sind. Vor der Veröffentlichung startete Google+ in einer geschlossenen Beta-Phase, in der nur mit einer Einladung von einem auf Google+ vertretenen Nutzer die Anmeldung möglich war. Die ersten Einladungen verschickte Google nach dem Zufallsprinzip.

Schätzungen zufolge hatte Google+ nach zwei Wochen Laufzeit schon über zehn Millionen Nutzer [87]. Dies stellt allerdings noch keine ernstzunehmende Konkurrenz für bereits etablierte soziale Netzwerke wie beispielsweise Facebook dar. In der Presse wurde Google+ als Angriff von Google auf Facebook gewertet. Ob Google+ wirklich ebenso erfolgreich wird wie sein Konkurrent, ist derzeit noch nicht abzusehen.

Typischer Inhalt und Kommunikationsmethoden

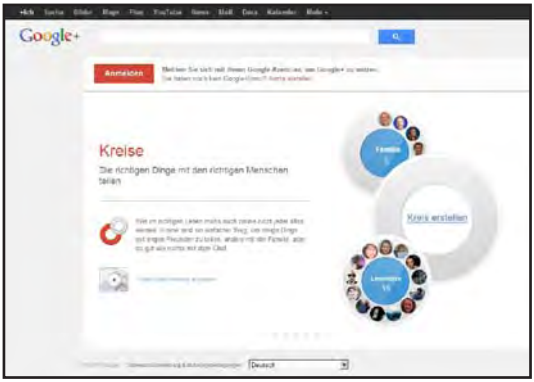
Was Google+ von anderen sozialen Netzwerken unterscheidet, ist die Einteilung von Freunden in „Kreise“. Diese können als Gruppen angesehen werden, wie z. B. Freunde und Familie. Beim Hinzufügen eines Users zu einem Kreis wird dem Nutzer nicht mitgeteilt, in welchen Kreis er eingeordnet wurde. Der Aufbau von Kontakten funktioniert, ähnlich wie bei Twitter, asynchron. Das bedeutet, man kann jeden beliebigen Nutzer der Plattform zu seinen Kreisen hinzufügen. Der Gefundene muss dies seinerseits aber nicht tun. Momentan kann auch nicht verhindert werden, dass man selbst zu einem Kreis eines anderen Nutzers hinzugefügt wird.

Das Senden von Nachrichten verläuft bei Google+ ebenfalls etwas anders als bei den übrigen sozialen Netzwerken. Statt jemandem eine private Nachricht zu schicken – wie etwa in Facebook –

schreibt man einen neuen Eintrag und teilt diesen nur mit der Person, für die die Nachricht gedacht ist. So kann explizit ausgewählt werden, wer die Nachricht lesen kann.

Folgende Unterstufen können eingestellt werden:

- Person (eine oder mehrere)
- Kreis (einer oder mehrere)
- „Meine Kreise" (alle Personen die sich in einem meiner Kreise befinden)
- „Erweiterte Kreise" (alle Personen, die sich in einem meiner Kreise befinden oder in einem Kreis von Personen, die zu meinen Kreisen gehören)
- Öffentlich (jeder kann die Nachricht lesen)



Dabei ist zu beachten, dass sich „Öffentlich" nicht nur auf das soziale Netzwerk selbst bezieht, sondern bedeutet, dass jeder Internetnutzer die Seite aufrufen und die Nachricht lesen kann, ohne dafür einen Google+ Account zu benötigen.

Google bezeichnet diese Kommunikationsform als „Stream". In der Startseite von Google+ bekommt jeder Nutzer einen für sich angepassten „Stream" angezeigt. Dieser kann auch benutzerdefiniert sortiert werden, z.B. nach bestimmten Kreisen, um nur Nachrichten von ausgewählten Personen anzuzeigen.

Als Nachrichten-Typen sind Nachricht, Video, Link, Foto und Standort vorgesehen. Darüber hinaus besitzt Google+ die Funktion „Sparks", die anzeigt, dass man an einem bestimmten Thema Interesse hat. Für den Nutzer führt der Klick auf einen „Spark" zur Auflistung aktueller Nachrichten aus verschiedenen Quellen zu einem bestimmten Thema.

In jeder Art von Nachricht können andere Nutzer verlinkt werden. So kann eine Person auf einem Foto markiert oder direkt im Text verlinkt werden. Dabei ist zu beachten, dass das Verlinken einer Person in einer privaten Nachricht dazu führt, dass der Betroffene über seine Erwähnung in der Nachricht informiert wird. Den Inhalt der Nachricht kann er jedoch nicht einsehen. Darüber hinaus verfügt Google+ über erweiterte Kommunikationsmöglichkeiten. So gibt es einen Videochat, mit dessen Hilfe bis zu zehn Personen gleichzeitig miteinander kommunizieren können.

Die Auswahl der Kommunikationspartner erfolgt dabei nach demselben Prinzip wie bei den Nachrichten.

Finanzierung

Google+ bietet seinen Mitgliedern eine kostenfreie Nutzung. Um dies zu ermöglichen, verwendet es – wie viele andere soziale Netzwerke auch – Werbeeinblendungen, die auf den User angepasst sind. Die Auswahl und Darstellung der jeweiligen Werbeanzeigen erfolgt mittels der Google-Anwendungen AdWords und AdSense [88][89].

Suchmöglichkeiten

Die Suchfunktion von Google+ ist angebunden an die Echtzeit-Suche von Google. Damit können Inhalte von Nachrichten durchsucht werden. Natürlich kann auch nach Personen gesucht werden.

Administrationsmöglichkeiten für Profile und Konten

Die Administrationsmöglichkeiten des eigenen Google+-Profils sind umfangreich. So kann etwa eingestellt werden, dass der „+1"-Button, der das Google-Äquivalent zum „Gefällt-mir"-Button von Facebook darstellt, von Google nicht dafür verwendet werden darf, um Inhalte oder Werbung auf Websites Dritter zu personalisieren. Dies ist auch die Standardeinstellung.

Außerdem können E-Mail-Benachrichtigungen für eine Vielzahl von Aktivitäten im Google+-Netzwerk eingestellt werden, z.B. wenn ein Beitrag kommentiert wird, den der Nutzer erstellt hat. Des Weiteren können Standortinformationen für neu hochgeladene Alben und Fotos aktiviert oder das Herunterladen von Fotos untersagt werden.

Interessant ist zudem die Option, eine Sicherung seiner Profilinformationen, Fotos, Kontakte, Kreise, Stream-Beiträge u. ä. zu erstellen und lokal auf seinem Rechner zu speichern.

Weiterhin kann man die Sichtbarkeit der Kreise und darin enthaltenen Personen, die Beiträge, die innerhalb des Streams angezeigt werden sollen, und die Personen, die die Erlaubnis erhalten, den User auf Fotos zu markieren, definieren.

Datenschutz und Sicherheit

Wie alle sozialen Netzwerke speichert Google+ die persönlichen Daten seiner Nutzer. Hinzu kommen Informationen, die der Nutzer an Google schickt, beispielsweise in Form von E-Mails, SMS oder Suchanfragen, Daten über den Standort des Users oder personenbezogene Informationen, die an Partner-Websites von Google übermittelt werden [90]. Um dem Nutzer einen Überblick über die im Zusammenhang mit seinem Google+-Konto gespeicherten Daten zu ermöglichen, stellt Google eine Anwendung namens „Google Dashboard" bereit. Dies ist eine Website, innerhalb der die Nutzer ihre Daten verwalten und teilweise auch entfernen können [91].

Nach eigenen Angaben gibt Google sensible personenbezogene Daten nur nach ausdrücklicher Genehmigung des Nutzers weiter. Darin nicht eingeschlossen ist die Weitergabe dieser Informationen an externe Unternehmen, die von Google mit der Verarbeitung dieser Daten beauftragt werden. Dabei stellt Google jedoch die Bedingung: „Diese Parteien sind insbesondere verpflichtet, diese Informationen nur gemäß unseren Weisungen und unter Einhaltung dieser Datenschutzbestimmungen sowie anderer maßgeblicher Vertraulichkeits- und Sicherheitsmaßnahmen zu verarbeiten." [90] Google gibt jedoch ebenfalls zu bedenken, dass in bestimmten Fällen die Offenlegung der Userdaten auch ohne Genehmigung der Betroffenen möglich ist.

Dazu zählen:

- Verstöße gegen gesetzliche Bestimmungen
- Anordnungen in gerichtlichen Verfahren
- Untersuchung von Verstößen gegen die Nutzungsbedingungen
- Bekämpfung von Betrug oder technischen Problemen
- Die „[...] Rechte, das Eigentum oder die Sicherheit von Google, seinen Nutzern und der Öffentlichkeit, soweit dies gesetzlich zulässig oder erforderlich ist, vor drohendem Schaden zu schützen." [90]]

Da Google+ erst seit Kurzem besteht, ist noch nichts über etwaige Sicherheitslücken oder Angriffe bekannt. Lobenswert ist aber, dass die Datenübertragung im sozialen Netzwerk zu jedem Zeitpunkt SSL-verschlüsselt erfolgt [78].

Google+ für Unternehmen

Zum jetzigen Zeitpunkt sieht Google+ noch keine speziellen Funktionen für Unternehmen vor. Für diejenigen, die sich trotzdem anmelden, besteht die Gefahr, dass deren Account gelöscht wird. Für Unternehmen ist es – ähnlich wie bei Facebook – möglich, sich mit einem eigenen Profil auf der Plattform zu präsentieren

XING

Übersicht

Nutzer D-A-CH	5,51 Millionen [92]
Nutzer weltweit	12,1 Millionen (2012) [93]
Hauptsitz	Hamburg, Deutschland [93]
Gründungsjahr	2003 [93]
Eigentümer	XING AG [93]
Umsatz	66,2 Millionen EUR (2011) [93]
Hauptbenutzergruppe	Zwischen 31 und 40 Jahren [94]

Kurzbeschreibung

Bei XING handelt es sich um ein deutsches soziales Netzwerk mit einer starken Ausrichtung auf die Berufswelt. Es wurde im Jahr 2003 von Lars Hinrichs gegründet und trug zu diesem Zeitpunkt noch den Namen OpenBC (Open Business Club). Seine Hauptfunktionen sind das Suchen nach Stellenangeboten bzw. Bewerbern und der Aufbau eines Business-Netzwerks.

Momentan zählt es weltweit etwa 12,1 Millionen Mitglieder, wovon 5,51 Millionen Nutzer aus dem deutschsprachigen Raum (Deutschland, Österreich, Schweiz) stammen.

Typischer Inhalt und Kommunikationsmethoden

Das Besondere an XING ist, dass es als einziges soziales Netzwerk in Deutschland auf ein Premium-Modell setzt. So erhalten Nutzer, die eine monatliche Gebühr bezahlen, erweiterte Funktionen.

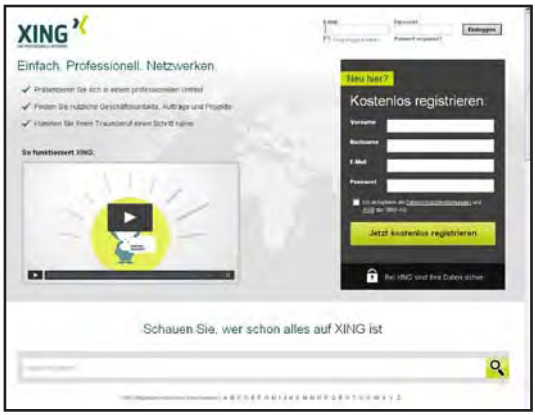
Es gibt folgende Arten von Nutzerkonten:

- normaler Nutzer
- Premium-Mitgliedschaft (erweiterte Funktionen)
- Recruiter-Mitgliedschaft (Premium mit zusätzlichen Suchfiltern)

Mitglieder können in ihrem Profil sowohl private als auch berufliche Informationen veröffentlichen. Beispielsweise ist es möglich, den schulischen und beruflichen Werdegang in Form eines Lebenslaufs einzutragen. Wie die meisten sozialen Netzwerke dient auch XING dazu, Kontakte aufzubauen. Nach einer Kontaktanfrage ist es notwendig, dass die Gegenseite diese bestätigt.

Eine wichtige Funktion von XING sind die Gruppen. Diese können öffentlich (jeder kann beitreten) oder auch geschlossen sein (Aufnahme nur mit Einladung oder Bewerbung). Typische Gruppen sind zum Beispiel regionale Gruppen (Augsburg, München usw.) oder auch Interessengebiete (PHP-Programmierung, Musizieren, Reisen usw.). Um das Knüpfen von persönlichen Kontakten zu erlauben, veranstalten regionale Gruppen auch häufig lokale Tref-

fen. Zudem besitzt XING eine Kalenderfunktion, die dem Nutzer die Organisation von privaten und geschäftlichen Termin erlaubt. Dieser Kalender kann ebenfalls für öffentliche Veranstaltungen genutzt werden.



XING bietet außerdem Möglichkeiten zum Nachrichtenaustausch. An Nicht-Kontakte eine Nachricht zu schicken ist nur als Premium-Mitglied möglich (bis zu 50 Nachrichten am Tag). Außerdem können Nachrichten auch an mehrere Teilnehmer gleichzeitig gesendet werden. Das Chat- und VoIP[13] - Programm Skype kann über XING genutzt werden und dient damit ebenfalls der Kommunikation mit anderen Nutzern des sozialen Netzwerks.

Für die aktive Stellensuche bietet XING eine Jobbörse an. In dieser können Nutzer sowohl nach freien Stellen suchen als auch selbst Angebote einstellen.

Finanzierung

XING finanziert sich hauptsächlich durch sein Premium-Modell. Nach der Gründung 2003 erhielt das soziale Netzwerk Risikokapital von Business Angels und strategischen Partnern [93]. Zwei Jahre später investierte das Unternehmen Wellington Partners weitere 5,7 Mio. Euro in XING. Seit Dezember 2006 werden die Aktien des sozialen Netzwerks an der Börse gehandelt [93].

Eine zusätzliche Einnahmequelle von XING ist die Jobbörse, da das Einstellen von Stellenangeboten kostenpflichtig ist. Die Gebühr für die Anzeige ist dabei keine Pauschalsumme, sondern berechnet sich aus der Anzahl von Aufrufen durch die Nutzer.

Suchmöglichkeiten

Die Suchfunktion von XING bietet interessante Möglichkeiten. Beispielsweise kann nicht nur per Name nach Personen gesucht werden, sondern auch nach bestimmten Fähigkeiten. Zusätzlich können Unternehmen gesucht werden. Allerdings können nur zahlende Mitglieder die volle Funktionalität der Suche nutzen.

Administrationsmöglichkeiten für Profile und Konten

Benutzer können innerhalb ihres XING-Kontos einstellen, welche ihrer Profilinformationen für andere Nutzer sichtbar sein sollten. Außerdem können sie beispielsweise verhindern, dass ihre Profile und Beiträge in offenen Gruppen für Suchmaschinen oder RSS-Feeds abrufbar sind.

13) Voice over IP bezeichnet das Telefonieren über Computernetzwerke

Da jedes XING-Profil standardmäßig auch für Nicht-Mitglieder zugänglich ist, sollten User diese Funktion in ihren Privatsphäre-Einstellungen ebenfalls deaktivieren. Auch die Sichtbarkeit der Kontaktliste und der Gruppen kann hier abgeschaltet werden. Falls Nutzer keine unerwünschten Einträge in ihrem Gästebuch wollen, besteht in den Kontoeinstellungen die Möglichkeit dies zu deaktivieren.

Datenschutz und Sicherheit

Funktionen, die nur für zahlende Mitglieder verfügbar sind, haben in der Vergangenheit immer wieder zu Kritik an XING geführt. Dazu gehört u.a. die Möglichkeit, dass Nutzer sehen können, welche Personen ihre Kontaktseite aufgerufen haben.

Noch stärker in der Kritik steht eine Funktionalität namens „Neues aus meinem Netzwerk", die den Usern Änderungen anzeigt, die andere Nutzer an ihrem Profil vorgenommen haben, beispielsweise neue Kontakte oder geänderte Arbeitgeber. Bei einigen dieser Informationen können Nutzer verhindern, dass sie anderen angezeigt werden. Dies ist jedoch nicht für alle Profilinformationen möglich [95].

Um seinen Usern eine gefahrlose Nutzung des sozialen Netzwerks zu gewährleistet, wird auch bei XING die Datenverbindung SSL-verschlüsselt. Trotz dieser Sicherheitsmaßnahme kam es im Jahr 2009 zu einem sicherheitskritischen Vorfall. Dabei fälschten Angreifer die Systemmails von XING und schickten diese als Kontaktanfrage getarnten Nachrichten an XING-User. Darin befand sich die Frage, ob es sich bei dem ebenfalls in der Mail verlinkten Bild um das des – persönlich angesprochenen – Nutzers handelte. Klickte dieser nun auf den Link, lud sich eine exe-Datei herunter, die Schadsoftware enthielt und den Angreifern den Zugang zum Rechner des Opfers gewähren sollte [96].

XING für Unternehmen

Unternehmen können XING nicht nur für die Suche nach potentiellen Mitarbeitern nutzen, sondern sich dort auch selbst präsentieren. Dafür kann auf der XING-Plattform jede Person ein neues Unternehmen anlegen.

Analog zu den Benutzerprofilen gilt, dass es auch hier ebenso eine kostenlose wie eine kostenpflichtige, erweiterte Variante gibt.

Legt ein Unternehmen kein eigenes Profil an, so werden bei der Suche nach diesem die Mitarbeiter gelistet, die das Unternehmen als Arbeitgeber angegeben haben.

Fazit

Die Inhalte und Kommunikationsmöglichkeiten populärer sozialer Netzwerke unterscheiden sich abhängig von deren Ausrichtung (Privat/Business) zum Teil beträchtlich. Twitter bietet beispielsweise vergleichsweise geringe Features im Vergleich zu Facebook. Die Gefahren, die aus der Verlinkung und der Preisgabe persönlicher und geschäftlicher Informationen resultieren, werden im nächsten Kapitel genauer analysiert. Dabei wird darauf eingegangen, was diese Gefahren für Unternehmen bedeuten und wie versucht werden kann, diese zu minimieren.

Analyse der Gefahren von sozialen Netzwerken

Dieses Kapitel befasst sich mit den möglichen Gefahren, die aus der Verwendung sozialer Netzwerke für Mitarbeiter und Unternehmen resultieren können. Es wird dabei auf verschiedene Szenarien eingegangen, die öffentliche Attribute (etwa Ansehen) und/oder interne Attribute (etwa Arbeitszeiten und Geschäftsgeheimnisse) eines Unternehmens negativ beeinflussen können.

Verlust von Ansehen

Soziale Netzwerke sind speziell für das Ansehen von Unternehmen eine Herausforderung und dürfen in ihrer Bedeutung nicht unterschätzt oder gar ignoriert werden. Nicht nur, ob oder wie sich ein Unternehmen in sozialen Netzwerken darstellt, sondern vor allem, welche Informationen andere über das Unternehmen einstellen, ist von elementarer Bedeutung.

Durch die enge Vernetzung von Kontakten in einem sozialen Netzwerk werden scheinbar unwichtige Nachrichten bereits durch die einfache Statusmeldung eines Benutzers schnell verbreitet. So kann bereits ein einziger negativer Beitrag das Ansehen eines Unternehmens nachhaltig schädigen. Es muss auch davon ausgegangen werden, dass jede noch so unwichtige Kleinigkeit an die Öffentlichkeit getragen werden kann.

Klassische Gegenmaßnahmen keine effektive Lösung

Klassische Gegenmaßnahmen wie etwa eine Pressemitteilung stellen für sich gesehen keine effektive Lösung mehr dar. Auch sollte bedacht werden, dass lokale Probleme durch die rasche Verbreitung schnell ein überregionales Ausmaß annehmen können.

So führte ein Youtube-Video, in dem Ratten durch eine Filiale des Franchise-Systemgastronomie-Unternehmens Kentucky Fried Chicken liefen, zu einem enormen Ansehensverlust [98] für das Unternehmen.

Des Weiteren sind folgende Szenarien denkbar bzw. bereits eingetreten:

Mitarbeiter eines Unternehmens veröffentlichen (Status-) Meldungen in der Art von „Jetzt bringen wir schon wieder ein nicht ausgereiftes Produkt auf den Markt, mein Chef denkt nur ans Geld und nicht an die Kunden“. Solche Postings von unzufriedenen Mit-

arbeitern werfen ein unprofessionelles Licht auf den Mitarbeiter und schaden darüber hinaus dem Ruf des Unternehmens.

Öffentlich zugängliche Mitteilungen zu kontroversen politischen Themen können, wie es sich in der Vergangenheit gezeigt hat, ebenfalls zum Ansehensverlust führen. So hinterließ der Geschäftsführer einer Stuttgarter Werbeagentur im Internet einen Kommentar, den er später bereute. Er konnte ihn jedoch nicht mehr entfernen, und so liefert eine Suche nach seinem Namen den unliebsamen Beitrag noch heute [99].

Auch das „Like-" Verhalten einiger Mitarbeiter kann zu einem Ansehensverlust in der Öffentlichkeit führen. Dies hat sich vor kurzem bei Daimler gezeigt [6]. Mitarbeiter hatten mit einem Klick auf den „Gefällt mir"-Button einer Facebook Seite gezeigt, dass sie dem Inhalt dieser Seite zustimmen. Auf der Seite wurden u. a. Mitglieder des Daimler-Vorstands als „Lügenpack" bezeichnet. Für Außenstehende wirkt so ein Verhalten von Mitarbeitern illoyal und schadet dem Ansehen des Unternehmens.

Schnell und effektiv auf unerwünschte Inhalte reagieren

Nutzer, die einen Groll gegen ein Unternehmen hegen, können Gruppen in sozialen Netzwerken eröffnen, um z. B. gegen die Firmenpolitik zu demonstrieren [100]. Auch Konkurrenten können zielgerichtet falsche Gerüchte streuen, um den Ruf eines Unternehmens zu schädigen [101]. Unternehmen sollten schon aus diesen Gründen aktiv Eigen- oder Fremddarstellungen im Internet beobachten. Nur so kann schnell und effektiv auf unerwünschte Inhalte reagiert werden.

Entscheidet sich ein Unternehmen dafür, in sozialen Netzwerken aktiv zu werden, müssen vorher Zuständigkeiten geklärt und Verantwortlichkeiten geschaffen werden. Ein Auftritt muss durchgehend gepflegt und aktualisiert werden, und es muss mit den Benutzern interagiert werden. Elementar wichtig ist die richtige, professionelle und vor allem schnelle Reaktion bei konzertierten Negativ-Kampagnen gegen ein Unternehmen, einen Unternehmensangehörigen oder ein Produkt. Diese sog. „Shit-Storms" haben in der Vergangenheit namhafte Unternehmen wie Adidas, Siemens oder Sky in ernsthafte Bedrängnis gebracht und gezeigt, dass Fluch und Segen durch soziale Netzwerke eng beeinander liegen [115].

Zufriedene Mitarbeiter, regelmäßig überprüfte Firmenprofile und Löschungen von zweifelhaften Postings in sozialen Netzwerken sowie notfalls auch das Sperren dieser Netzwerke können das Unternehmen vor Ansehensverlust schützen. Zusätzlich bieten die gängigen Netzwerke Mechanismen zum Melden und Sperren von unerwünschten Inhalten.

Belästigungen und Mobbing über soziale Netzwerke

Soziale Netzwerke führen online zu einer kontinuierlichen Verschmelzung des persönlichen und geschäftlichen Bekanntenkreises. Dies und der nachgewiesene Umstand, dass Hemmschwellen online wesentlich niedriger liegen [102], führt dazu, dass sich Mobbing von der physischen Welt in die virtuelle ausbreitet und dort Mitarbeiter auch weit über ihre Arbeitszeit hinaus belasten kann. Mittlerweile sind sogar Fälle bekannt, bei denen dieser Umstand auch von Führungspersonen gezielt ausgenutzt wurde, um Angestellte zu einer kostengünstigen Kündigung zu bewegen [103].

Mobbing in sozialen Netzwerken ist ein immer häufiger [104] auftretendes Phänomen. Experten schätzen, dass Mobbing alleine in Deutschland jährlich zu einem volkswirtschaftlichen Schaden von über 6 Milliarden Euro führt [105]. Mobbing, das über soziale Netzwerke betrieben wird, ist weitreichender, denn es kann nach einem Wechsel des Arbeitgebers fortgeführt werden, da sich Inhalte z.T. nur mit erheblichem Aufwand löschen lassen.

Hemmschwellen online wesentlich niedriger

Durch die geringe Online-Hemmschwelle und den technisch minimalen Aufwand ist es auch ohne Probleme möglich, die Kollegen des Mobbing-Opfers beim neuen Arbeitgeber in laufendes Mobbing einzubinden oder Gerüchte zu streuen. Nicht nur einfache Angestellte sind Opfer von Cyber-Mobbing. Über soziale Netzwerke können auch schädigende Gerüchte über Vorgesetzte und Unternehmensvorstände gestreut werden [106].

Die Konsequenzen des Cyber-Mobbings sind nahezu deckungsgleich mit denen des Mobbings in der physischen Welt:

- Verschlechterung des Arbeitsklimas
- Minderung der Produktivität [107]
- Überdurchschnittlich viele Krankheitstage von Mitarbeitern
- Imageschaden für die Firma, da die Informationen nicht nur für Kollegen sichtbar sind [108]

Verbreitung von Viren und Malware

Die Nutzer von sozialen Netzwerken kommen immer wieder mit verschiedenen Bedrohungen für ihre IT-Sicherheit in Kontakt. Diese reichen von einfachen Spam-Nachrichten bis hin zu komplexen Betrugs-Szenarien.

Die Ziele der Angriffe können dabei sein:

- Besucher auf eine Webseite zu locken, um Profit durch Werbung zu generieren

- Besucher auf eine manipulierte Webseite zu locken, um einen Virus oder Trojaner auf dem Rechner des Nutzers zu installieren
- Diebstahl der Konto- oder Kreditkartendaten
- Nachrichten im Namen des Nutzers zu veröffentlichen

Dabei muss sich der Benutzer bewusst sein, dass sein Handeln nicht nur ihn selbst in Gefahr bringt, sondern auch seine „Freunde" in den sozialen Netzwerken. Wird in seinem Namen ein Link auf eine potentiell gefährliche Seite veröffentlicht, so werden die Kontakte, die ihm trauen, mit hoher Wahrscheinlichkeit auch auf diesen Link klicken.

Die Angriffe auf den Anwender können dabei auf verschiedenste Weise stattfinden. Folgende sind am meisten verbreitet:

Phishing

Bei diesem Angriff wird versucht, den Benutzer auf eine der Seite des sozialen Netzwerks gleichende aber gefälschte Webseite zu locken. Gibt der Nutzer anschließend seine Daten ein, hat der Angreifer vollen Zugriff auf dessen Konto und persönliche Informationen.

Passwort-Diebstahl

Hier wird versucht, die Login-Informationen des Benutzers zu stehlen, meist mit Hilfe eines Wurms oder Trojaners. Besonders bekannt wurde der Wurm Koobface [109], der Benutzerdaten von verschiedenen sozialen Netzen sammelt.

Download von Malware

Oft werden Schwachstellen in nicht-aktuellen Browser-Versionen genutzt, um Schadsoftware auf einen Computer zu bringen.

Damit diese Angriffe für die Benutzer nicht offensichtlich sind, werden so genannte Kurzlinks[14] eingesetzt. Speziell Nutzer der Plattform Twitter werden immer wieder Opfer dieser Vorgehensweise. Die Tatsache, dass die Zieladresse nicht mehr erkennbar ist, wird von Kriminellen ausgenutzt, um ahnungslose Nutzer auf infizierte Webseiten zu leiten [110].

Häufig geht die Gefahr nicht von den sozialen Netzwerken selbst aus, sondern von Werbeeinblendungen oder Anwendungen von Drittanbietern, die in diese Seiten integriert sind und Schwachstel-

14) Ermöglicht es, eine lange URL bei einem externen Anbieter abzuspeichern, welche dieser über eine kurze Adresse weiterleitet.

len des jeweiligen Browsers oder Systems ausnutzen. Ein stets aktueller Antivirenschutz sowie eine aktuelle Browsersoftware ist daher für jeden Nutzer ein Muss.

Verlust von Geschäftsgeheimnissen

Über soziale Netzwerke können Geschäftsgeheimnisse ungewollt an die Öffentlichkeit gelangen und zum Nachteil des Unternehmens verbreitet werden. Eine typische „Falle" ist die Verwendung sozialer Netzwerke als Kommunikationsmittel der Mitarbeiter, um firmeninterne Nachrichten oder Daten auszutauschen. Dies führt dazu, dass alle Informationen, die verschickt werden, an den Anbieter, der sich auch außerhalb der nationalen Grenzen befinden kann, übertragen werden. Dabei hat der Nutzer des sozialen Netzwerks keine Gewissheit darüber, was mit seinen Daten passiert und wer sie mitliest.

Eine andere Methode ist das absichtliche oder unabsichtliche Veröffentlichen einer internen Nachricht über ein soziales Netzwerk. So veröffentlichte ein Mitarbeiter der Suchmaschine Google unabsichtlich einen internen Bericht auf der eigenen Plattform „Google+" [111]. Dies konnte geschehen, weil Google dieselbe Plattform mit anderen Accounts für die firmeninterne Kommunikation verwendet, und der Mitarbeiter versehentlich seinen „externen" Account genutzt hatte. Die Veröffentlichung kann aber auch indirekt durch ein (Status-) Posting wie „Mein Chef will schon wieder, dass X klappt, damit Y erreicht wird – wie nervig" geschehen.

Solche Informationsweitergaben kommen oft bei unzufriedenen Mitarbeitern vor [112]. Loyalitätsbildende Maßnahmen und ein gutes Verhältnis zwischen Mitarbeitern und Führungskräften spielen gerade in Zeiten sozialer Netzwerke eine wesentliche Rolle.

Verlust von Arbeitszeit

Soziale Netzwerke sind häufig so gestaltet, dass ein angemeldeter Benutzer sie häufig besuchen muss, um sich auf dem aktuellen Stand zu halten. Außerdem gehört es zu den Geschäftsprinzipien der meisten Netzwerke, den Benutzer durch verschiedene psychologisch geschickt integrierte Mechanismen möglichst lange auf der Plattform zu halten.

Dabei entgeht dem Unternehmen Arbeitszeit in zweifacher Hinsicht:

Zum einen kann der Arbeitnehmer selbstverständlich während der Zeit, die er auf der sozialen Plattform verbringt, nicht seiner eigentlichen beruflichen Tätigkeit nachgehen. Zum anderen wurde

in mehreren Studien nachgewiesen, dass eine Unterbrechung der Arbeit durch einen nicht unmittelbar mit der aktuellen Beschäftigung verbundenen Einfluss die Arbeitsleistung noch über einen Zeitraum von bis zu 15 Minuten hinweg negativ beeinflussen kann [113]. Häufig ist erst nach dieser Zeit wieder derselbe Grad an Produktivität erreicht wie vor der Störung. Solche Störungen können kurze Anrufe, Popups auf dem Bildschirm, E-Mail-Benachrichtigungen oder Kurzbesuche auf Seiten sozialer Netzwerke sein.

Zusammenfassend kann man sagen, dass Unternehmen auf diesem Weg pro Mitarbeiter und Tag eine Stunde Arbeitszeit verloren geht [114].

Verlust von Firmenkontakten durch Firmenwechsel eines Mitarbeiters

Nutzt ein Angestellter seinen Account auf einer Business-Plattform wie XING oder LinkedIn für Firmenzwecke, stellt dies eine Herausforderung für den Arbeitgeber dar. Es muss geklärt werden, was mit dem Account sowie den zugehörigen Kontakten passiert, falls der Arbeitnehmer die Firma verlässt. Es können folgende Problemkonstellationen auftreten:

- Der Arbeitnehmer wechselt zu einer Konkurrenzfirma und nutzt seine bisherigen Kontakte weiter.
- Der Arbeitgeber hat keinen Zugriff mehr auf die bisherigen geschäftlichen Kontakte seines Arbeitnehmers, nachdem dieser die Firma verlassen hat.

Eine Vereinbarung über die zusätzliche Pflege der Kontaktdaten innerhalb eines Informationssystems der Firma kann solchen Risiken vorbeugen.

Überwachung von Mitarbeitern durch externe Personen

Die Nutzer von sozialen Netzwerken können von ihren „Freunden" überwacht werden. Dabei genügt es, mit einer Person befreundet zu sein. Hat diese Person ihre Privatsphäre-Einstellungen nicht entsprechend angepasst, kann jeder Freund (oder im schlimmsten Fall: jeder andere Nutzer des sozialen Netzwerks) Status-Nachrichten lesen, Fotos sehen und weitere private Details entnehmen.

Eine besondere Rolle spielen hierbei die so genannten „location-based services", also Dienste, die ortsgebundene Benutzerdaten auswerten. Dabei stellt der Benutzer meist seinen aktuellen Standort zur Verfügung. Angefangen hat dies mit Gowalla (inzwischen eingestellt) und Foursquare [116]. Mittlerweile bieten aber

auch Google mit „Google Places“ [117] sowie Facebook mit „Facebook Places“ (in Deutschland „Facebook Orte“) [119] entsprechende Dienste an. Auch Twitter hat seine mobile Anwendung um den Standort des Benutzers erweitert [120]. Mit Smartphones ist die Nutzung der ortsgebundenen Dienste mithilfe eingebauter GPS-Module und WLAN-basierter Netzwerk-Lokalisierung auch außerhalb des Arbeitsplatzes oder des eigenen Zuhauses möglich. Sind die Orte im System registriert, kann man in diesen Orten „einchecken“. Je nach Dienst kann somit beispielsweise ein Restaurant bewertet werden. Auch kann man sehen, welche Freunde gerade an bestimmten Orten sind beziehungsweise diese Orte regelmäßig besuchen. Bei Google und Facebook gibt es die Möglichkeit, über die persönlichen Einstellungen diese „Location Updates“ zu deaktivieren. Dienste wie Foursquare leben jedoch von diesen Daten und bieten deshalb nicht die Möglichkeit einer Deaktivierung.

Ortung deaktivieren

Um auf die gravierenden Datenschutz-Probleme von öffentlichen Location Updates hinzuweisen, ist die Seite „Please Rob Me“ entstanden. Diese scannt automatisch Twitter- und Foursquare-Updates, um zu erkennen, wann eine Person nicht zu Hause ist und demzufolge ausgeraubt werden könnte [121]. Die Seite soll natürlich keine Aufforderung sein, Personen auszurauben, sondern will auf die Missbrauchsmöglichkeiten von location-based services aufmerksam machen. Mittlerweile haben die Betreiber den Dienst eingestellt.

Gerade Mitarbeiter mit Schlüsselpositionen in Unternehmen sollten ihren aktuellen Standort nicht aller Welt zugänglich machen, da ein Dritter auf diese Weise leicht ermitteln kann, wann z.B. der Sicherheitschef nicht vor Ort ist.

Durch die Nutzung dieser Dienste lassen sich Bewegungsprofile erstellen, die Aufschluss auf Wohnort, Arbeitsplatz, Freizeitaktivitäten und Reisen geben [122]. Diese Informationen können sowohl im privaten als auch im wirtschaftlichen Umfeld leicht missbraucht werden. Zum Schutz vor einem möglichen finanziellen Schaden durch den Missbrauch der Daten dient das Bundesdatenschutzgesetz (BDSG). Die Informationen über den Aufenthaltsort einer Person unterliegen dem Schutz personenbezogener Daten und erfordern in jedem Fall das Einverständnis des Benutzers [123]. Aus diesem Grund müssen sich auch entsprechende Dienste leicht ein- und ausschalten lassen.

Identitätsdiebstahl

Eine weitere Gefahr besteht im sogenannten „Identitätsdiebstahl". Anders als in der realen Welt ist es in der digitalen Welt sehr einfach, die Rolle einer anderen Person für sich zu beanspruchen. Hat Person X in einem bestimmten sozialen Netzwerk noch kein Profil, könnte sich ein Angreifer als diese Person ausgeben und ein Profil erstellen. Um die Validität des Profils zu verbessern, könnte er neben dem Namen zusätzlich ein Foto und eine gültige E-Mail-Adresse des Opfers verwenden. Nicht alle sozialen Netzwerke setzen die Bestätigung der Kontaktdaten als zwingend voraus. Gerade bei bekannten Personen sind E-Mail-Adressen und Profilfotos schnell gefunden. Ein Angreifer könnte dann negative Kommentare über Produkte, Konkurrenten u. ä. mithilfe dieser Identität streuen [124].

Ebenfalls kritisch ist, dass der Angreifer mit der gestohlenen Identität andere Nutzer des sozialen Netzwerks, die diese Person kennen, als Freunde hinzufügen kann und so weitere Informationen über diese Person erhält. Wenn der Angreifer es durch eine gestohlene Identität schafft, sich die Freundschaft eines Opfers zu erschleichen, wird der Schutz, den ein gewissenhaft gesicherter Account gegen unbekannte Personen bietet, ausgehebelt. Außerdem ist denkbar, dass eine Person auch einen fremden Nutzer als Freund akzeptiert, falls dieser bereits einen oder mehrere seiner Freunde täuschen konnte und deshalb in deren Freundesliste steht [125]. Um einen solchen Angriff vorzubereiten, genügt es, die Freundesliste des Opfers einsehen zu können. Dabei können erste Erkenntnisse über die Beziehungen zu anderen Personen gesammelt werden. Daraus lässt sich später die Vertrauensbasis aufbauen, um das Opfer zur Annahme einer Freundschaftsanfrage zu bewegen.

Automatisierter Angriff

Um zu zeigen, dass dieses Szenario nicht nur rein theoretisch ist, hat das Projektteam Saafan das JAVA-Tool „Facebook Pwn" [126] entwickelt. Dieses Tool automatisiert einen Angriff auf der Facebook-Plattform fast vollkommen. Der Angreifer muss lediglich einen gefälschten Account erstellen und das potentielle Opfer auswählen. Anschließend stellt das Tool an alle Freunde des Opfers eine Freundschaftsanfrage. Ist dies geschehen, bietet das Tool an, die Identität eines Users, der die Freundschaftsanfrage angenommen hat, auf das gefälschte Profil zu übertragen. Dazu kopiert es Namen und Bild eines der Profile, mit denen mittlerweile eine Freundschaftsbeziehung besteht. Ist dieser Schritt abgeschlossen, stellt „Facebook Pwn" automatisiert eine Freundschaftsanfrage an das ausgewählte Opfer. Sobald dieser die Freundschaft bestätigt, kopiert „Facebook Pwn" alle Daten, die es erlangen

kann, auf die Festplatte, um zu verhindern, dass der Zugriff auf die Daten verloren geht, wenn der Angreifer den Schwindel durchschaut.

Durch solche Tools sind auch umfangreichere Angriffe für unerfahrene Nutzer ohne technisches Verständnis problemlos möglich. Um dies zu erschweren, ist es unumgänglich, die Nutzer solcher Plattformen für mögliche Gefahren zu sensibilisieren.

Ablauf typischer Angriffe

Wie bereits erörtert, sind soziale Netzwerke ein Mittel, um Informationen über Unternehmen und deren Mitarbeiter zu erlangen. Angreifer können diese Informationen nutzen, um tiefer in die Unternehmensstruktur einzudringen. Die weiterführenden Erkenntnisse können genutzt werden, um eine Social-Engineering-Attacke oder einen Hacking-Angriff zu starten. Dieser erfolgt in der Regel mit dem Ziel, Daten des Unternehmens (z.B. Patente, Kundendateien, Baupläne) zu entwenden, zu löschen oder zu manipulieren.

Wie werden Informationen beschafft?

In Kapitel „Populäre soziale Netzwerke" wurden bereits die in Deutschland bekanntesten sozialen Netzwerke beschrieben. Jedes bietet für seine Mitglieder die Möglichkeit, den Beruf sowie den Arbeitgeber anzugeben. Möchte man nun beispielsweise einen Mitarbeiter einer bestimmten Firma finden, bietet es sich an, nach allen Personen zu suchen, die den Namen des Unternehmens in ihrem Profil angegeben haben.

Um den Angriff zu präzisieren, werden im Anschluss die Profile der potentiellen Opfer gefiltert. Es werden diejenigen herausgesucht, die für einen Angriff am erfolgversprechendsten erscheinen, d. h. am meisten Daten über ihre Person, ihre Aufgaben im Betrieb und das Unternehmen als Ganzes eingestellt haben. Dabei variiert die Auswahl der Opfer je nach ihrem Aufgabengebiet. Gibt zum Beispiel ein Mitarbeiter der IT-Abteilung an, Fachwissen in der Administration von Windows-Servern zu besitzen und an Projekten mit diesem Schwerpunktthema teilgenommen zu haben, lassen sich daraus Schlussfolgerungen auf die Beschaffenheit des Unternehmens-Netzwerks ziehen. Vor allem das Netzwerk XING bietet sich für solche Angriffe an, da hier viele und teils sehr detaillierte Informationen über Unternehmen gespeichert sind.

Wie geht es weiter?

Reichen die Informationen nicht aus bzw. erscheinen sie für einen erfolgreichen Angriff auf ein Unternehmen noch unvollständig, wird ein Angreifer versuchen, an zusätzliche Daten zu kommen und diese geschickt miteinander zu verknüpfen. Selten sind Personen in sämtlichen sozialen Netzwerken aktiv. Diesen Umstand macht sich der Angreifer zu Nutze. Erkennt er, dass Person A mit Person B in XING befreundet ist, jedoch B keinen Account auf

Facebook hat, kann er sich dort unter Angabe des Namens von B anmelden und Informationen über B hinterlegen, welche in XING frei einsehbar sind, zum Beispiel den Arbeitgeber und das XING-Profilbild.

Anschließend schickt er A eine Freundschaftsanfrage, die dieser vermutlich annehmen wird, da er den vermeintlichen B ja bereits kennt. Der Angreifer hat nun Zugriff auf die Daten, die A nur unter Freunden teilt, und kann somit sein Wissen über A erweitern und noch bestehende Lücken schließen. Zudem kann er Nachrichten im Namen von B versenden, ohne dass Argwohn entsteht – im Gegenteil: A kennt ja B und vertraut ihm.

Wie können diese Informationen ausgenutzt werden?

Ist der Awareness-Grad der Mitarbeiter eines Unternehmens zu niedrig, kann sich ein Angreifer über typische Social-Engineering-Methoden glaubhaft als „Mitarbeiter" oder „Befugter" ausgeben und so von „Kollegen" in gutem Glauben firmeninterne, schützenswerte Daten oder Informationen erhalten. So wird ein Angreifer kaum Probleme haben z.B. eine Kundendatei anzufordern, wenn er sich glaubhaft als Außendienstmitarbeiter ausgeben kann, der die eigentlich vertraulich zu behandelnde Datei momentan dringend vor Ort braucht und ansonsten nicht weiterarbeiten kann.

Außerdem besteht über diese Social-Engineering-Methoden relativ leicht die Möglichkeit, gezielt Schadcode in das Unternehmensnetz zu schmuggeln, um das Firmennetz im Anschluss auszuforschen, zu schädigen oder für Erpressungsversuche zeitweise lahmzulegen. Häufig reicht der Klick auf den E-Mail-Anhang eines vertrauenswürdig wirkenden Absenders.

Fallbeispiele

Im Rahmen einer Evaluation konnte festgestellt werden, dass der Awareness-Grad selbst in IT-Abteilungen großer Unternehmen nicht sehr hoch ist. Zusätzlich ließ sich feststellen, dass Personen in beruflichen Netzwerken wie XING offenbar viel mehr über sich preisgeben als z.B. in Facebook.

Der Grund dafür dürfte in der immer wiederkehrenden Medienberichterstattung über Datenschutzlücken bei Facebook liegen. Viele Anwender stellen ihr Profil mittlerweile so ein, dass der Großteil der Informationen nur für registrierte Freunde zugänglich ist. Außerdem liegt es in der Natur von Netzwerken wie XING, dass dort viele berufliche und private Informationen öffentlich gemacht werden.

Eine weitere Feststellung der durchgeführten Untersuchung ist, dass sich erfolgreiche Attacken kaum mit Informationen aus nur einem Netzwerk durchführen ließen. Es handelte sich meist um eine Kombination von Daten aus verschiedenen sozialen Netzwerken, privaten Homepages, Firmenwebseiten und whois-Abfragen.

Beispiel 1 - Adresse des Wohnorts

Über das Netzwerk XING konnte der Systemadministrator eines Unternehmens ausfindig gemacht werden, indem nach allen registrierten Mitarbeitern dieses Unternehmens gesucht wurde. Dieser hatte zusätzlich ein Facebook-Profil, auf dem einige Hobbys angegeben waren. Eine Suchanfrage in Google mit vollem Namen und Hobbys führte zur privaten Webseite der Person, über deren Impressum wiederum die Privatadresse ausfindig gemacht werden konnte. Der private Abfall des Administrators wäre für die Angreifer der nächste Schritt bei der Jagd nach wertvollen Informationen.

Beispiel 2 - Informationen über das Netzwerk

Der Systemadministrator eines Unternehmens wurde über XING ausfindig gemacht. Der Mitarbeiter bezeichnet sich selbst als Linux-Experte im Bereich von Web-, Datenbank-, und Virtualisierungsservern sowie der Spam-Bekämpfung und Netzwerksicherheit im Linux-Umfeld. Aus diesen Angaben kann ein Angreifer Informationen über das Netzwerk des Unternehmens gewinnen. So könnten die Angreifer nun mit hoher Wahrscheinlichkeit davon ausgehen, dass es sich bei den o.g. Servern um Linux-Server han-

delt und dass die gängigen Security-Produkte (Firewalls etc.) des Unternehmens auf Linux basieren.

Beispiel 3 - Personen mit geringer Security Awareness

Über XING konnte ein Mitarbeiter eines Unternehmens gefunden werden. Die Suche bei Facebook ergab ein Profil mit gleichem Namen aber ohne Arbeitgeber. Über die Profilbilder konnte darauf geschlossen werden, dass die beiden Profile zur selben Person gehören. Im Facebook-Profil wurde festgestellt, dass die Person sog. Likejacking-/Clickjacking-Seiten angesehen und auf den „Gefällt Mir"-Button geklickt hat. Ein Angreifer kann diese Tatsache als Angriffspunkt auf die Person ausnutzen, indem er ihr auf Facebook selbst erstellte Likejacking-/Clickjacking-Seiten schickt, welche beim „Liken" zu einer Seite weiterleiten, die Code auf dem Rechner des Opfers ausführt.

Beispiel 4 - Indirekte Informationen ausnutzen

Über XING wurde die Führungskraft eines Unternehmens gefunden, die zusätzlich noch mit einem Twitter-Profil verlinkt war. Dort fiel auf, dass die Person eine Reihe von Koordinaten ihrer Fahrradtouren hochgeladen hatte. Das genauere Betrachten der Koordinaten zeigte, dass die Touren immer am gleichen Ort starteten bzw. endeten. Da sich dieser Punkt in einer Ortschaft befand, ließ sich daraus schließen, dass dies der Wohnort der Person ist. Falls die Touren zusätzlich regelmäßig stattfinden, könnte ein Angreifer daraus ableiten, wie der Tagesablauf der Person aussieht und sogar, wann diese außer Haus ist.

Bekannte Beispiele aus der Öffentlichkeit

In den letzten Jahren ereigneten sich einige aufsehenerregende Vorfälle, die im Zusammenhang mit der Sicherheit von sozialen Netzwerken standen. Diese Ereignisse steigerten in der Öffentlichkeit das Bewusstsein für die jeweiligen Gefahren enorm. Dieser Abschnitt präsentiert kurz einige der bekanntesten Fälle.

Fall 1: Barack Obama und Britney Spears

Der Spiegel berichtete im Januar 2009: „Eigentümliche, teils sehr pubertäre Botschaften von US-Prominenten konnten Nutzer des Social-Networking-Dienstes Twitter an diesem Montag lesen, wenn sie zu den Abonnenten der Promi-Accounts im Angebot gehörten" [127]. Diese Meldung bezog sich auf Twitter-Kanäle von Barack Obama, Britney Spears und anderen amerikanischen Pro-

minenten, die von Angreifern übernommen wurden. Die Angreifer versendeten Nachrichten im Namen der Opfer. So twitterte „Barack Obama" etwa, man könne an einer Umfrage teilnehmen, bei der es Benzin im Wert von 500 USD zu gewinnen gäbe [127].

Fall 2: Sarah Palin

Im Jahr 2008 wurde der E-Mail-Account der amerikanischen Politikerin Sarah Palin gehackt. Sarah Palin war zu diesem Zeitpunkt die designierte Vizekandidatin des republikanischen Präsidentschaftsbewerbers John McCain.

Vor dem Angriff wurde bekannt, dass Palin Amtsgeschäfte über eine private E-Mail-Adresse bei Yahoo abgewickelt hatte. Daraufhin fand ein Hacker namens Rubico einen Account mit der Adresse gov.palin@yahoo.com. Damals konnten sich User nicht nur durch ein Passwort, sondern auch anhand dreier Fragen bei Yahoo identifizieren. Der Hacker fand aus öffentlich zugänglichen Informationen den Geburtstag, die Postleitzahl und die Antwort auf die Sicherheitsfrage der Politikerin heraus. Danach ersetzte er Palins Passwort durch ein eigenes.

Es wurden zwar keine verfänglichen Informationen gefunden, dennoch wurden private E-Mails und Fotos veröffentlicht [128, 129].

Fall 3: RSA und Lockheed Martin

Der Hack von RSA und Lockheed Martin im Jahr 2011 ist ein Musterbeispiel für einen sog. Advanced Persistent Threat (APT)[15] . Es wird davon ausgegangen, dass sich die Quelle des Angriffs auf die amerikanischen Unternehmen im Ausland befand und das Ziel die Gewinnung von Informationen zum Zweck der Wirtschaftsspionage war. Bei Lockheed Martin handelt es sich um einen US-amerikanischen Rüstungskonzern.

Zum Zugriff auf das Netzwerk nutzte Lockheed Martin sog. RSA SecurID-Token zur Netzwerkauthentifizierung. Jeder Benutzer verwendet dabei ein Gerät in Form eines Schlüsselanhängers, an das, in einem zeitlichen Intervall von 60 Sekunden, ein SecureID-Token gesendet wird. Dieser Token basiert auf einem geheimen, von RSA entwickelten, Algorithmus. Die Angreifer verschafften sich zuerst Zugang zum Netzwerk der Firma RSA. Dann erfolgte

15) Advanced Persistant Threat beschreibt eine Bedrohung, die von einer Gruppe (z.B. Staaten) ausgeht, die sowohl die Fähigkeit als auch die Absicht hat, ein Ziel effektiv und nachhaltig anzugreifen. In aller Regel bezieht sich der Ausdruck auf Bedrohungen im Cyberraum, insbesondere auf internetbasierte Spionage.

der Angriff in Form einer E-Mail mit Excel-Anhang, die an Angestellte der Firma RSA gesandt wurde. Es ist anzunehmen, dass sich die Hacker vorher auch in sozialen Netzwerken über die Angestellten der Firma RSA informiert haben, da die Mail gezielt an einen bestimmten Empfängerkreis und jeweils eine Kopie an drei weitere Personen gesendet wurde. Es war also bekannt, dass die insgesamt vier Personen zueinander in Beziehung standen. In den Excel-Anhang betteten die Angreifer einen sog. Flash-Code ein. Bei der Ausführung des Flash-Codes wurde eine Schwachstelle im Adobe Flash Player ausgenutzt, um eine „Backdoor“[16] zu schaffen. Durch diese Backdoor war es dem Programm möglich, sich mit dem Server der Domain good.mincesur.com zu verbinden. Sobald die Verbindung aufgebaut war, verfügte der Angreifer über volle Systemkontrolle von außen. Im weiteren Verlauf des Angriffs verschaffte sich der Angreifer die notwendigen Rechte im Netzwerk zum Zugriff auf den geheimen Algorithmus. Die gewonnenen Informationen dienten zum Zugang in das Intranet von Lockheed Martin [130][131][132].

16) Hintertür in IT-Systemen, durch die ein Angreifer externen Zugriff auf ein System erlangt.

Umgang mit sozialen Netzwerken

In den vorherigen Kapiteln wurden die sozialen Netzwerke an sich und die davon ausgehenden Gefahren behandelt. Dieses Kapitel beschäftigt sich nun damit, wie Unternehmen und Mitarbeiter mit den potentiellen Gefahren umgehen können. Darüber hinaus finden Sie Handlungsanweisungen, die im Unternehmen umgesetzt und etwa in einer Policy abgebildet werden können.

Administrativer Umgang mit sozialen Netzen

Regelmäßig sollte über News-Seiten wie www.heise.de nach bekannten und insbesondere offenen Sicherheitslücken in Social-Networking-Portalen Ausschau gehalten werden. Neue Sicherheitsprobleme können an Mitarbeiter über Mailverteiler gemeldet werden, damit sich diese neuer Risiken bewusst werden.

Ein Blockieren entsprechender Webseiten im Unternehmen durch die IT-Abteilung schafft nur bedingt Abhilfe, da Mitarbeiter auch von zuhause aus soziale Netzwerke nutzen. Wirklichen Schutz bieten vor allen Dingen Awareness-Maßnahmen, wie sie im Weiteren aufgezeigt werden.

Grundprinzipien

Wie beschrieben, ist es nicht generell schlecht, einem sozialen Netzwerk anzugehören; schließlich ist mit sozialen Netzwerken eine gewisse persönliche und berufliche Vernetzung verbunden, die zunehmend wichtiger wird. Allerdings ergeben sich dadurch auch Nachteile, u.a. die genannten Gefahren, derer sich jeder Nutzer bewusst sein sollte. Der richtige und verantwortungsvolle Umgang mit sozialen Netzwerken ist daher von elementarer Bedeutung.

Die Webseiten www.focus.com und cio.wisc.edu schlagen eine Reihe von Verhaltensrichtlinien vor [133][134], wobei den Benutzern nahegelegt wird, diskret, skeptisch (hinsichtlich Geschäftsinformationen und -angeboten aus solchen Netzwerken), durchdacht und professionell zu handeln, sowie die Privatsphäre-Einstellungen sicher zu konfigurieren.

Aus den dargestellten Gefahren lassen sich entsprechend weitere Verhaltensweisen ableiten, etwa, dass keine firmeninternen Informationen (auch nicht indirekt) in sozialen Netzwerken veröffentlicht werden.

Mit von Dritten erhaltenen Informationen sollte ebenfalls vorsichtig und eher misstrauisch umgegangen werden, da diese möglicherweise nicht von der Person stammen, als die sich der Absender ausgibt.

Das Bereitstellen von möglichst wenig persönlichen Informationen ist ein Grundprinzip des sicheren Umgangs mit sozialen Netzwerken. Zusätzlich zum Schutz des Unternehmens im Allgemeinen kann so auch für jeden Einzelnen das Risiko z.B. eines Identitätsdiebstahls reduziert werden [125][133].

Awareness von Mitarbeitern und privater Umgang mit sozialen Netzen

Es ist von besonderer Bedeutung, Mitarbeiter durch Schulungen über die vorgestellten Gefahren zu unterrichten. Hierbei sollte darauf geachtet werden, dass auch die Familienangehörigen von Mitarbeitern entsprechend informiert werden. Denn wenn ein Mitarbeiter seine eigenen Daten aus beruflichen Gründen schützt, sein Lebenspartner / seine Lebenspartnerin aber das gesamte Privatleben veröffentlicht, kann ein Angreifer auch über diesen Weg Informationen sammeln. Beispielsweise zu welchem Zeitpunkt ein Sicherheitschef nicht vor Ort ist, da er laut Facebook-Nachricht seiner Frau gerade mit ihr im Urlaub ist.

Schulungen in diesem Bereich können entweder von externer Seite oder innerhalb des Unternehmens durchgeführt werden. Hierzu zählt nicht nur die Bereitstellung von Informationsmaterial, sondern vielmehr die Vermittlung der Thematik im direkten, möglichst persönlichen Kontakt mit den Mitarbeitern. Es sollten dabei nicht nur die oftmals sehr technischen Aspekte der Angriffsmöglichkeiten vermittelt, sondern vielmehr ein Gefühl für die Wichtigkeit dieser Gefahren transportiert werden. Dabei ist es – wie bereits erwähnt – auch wichtig, über die Zusammenhänge von Beruf und Privatleben und die möglichen wechselseitigen Auswirkungen zu sprechen.

Periodische Awareness-Schulungen

Im zweiten Schritt sollten Verhaltensrichtlinien vereinbart werden. Darüber hinaus gilt: Awareness-Wissen eines so schnelllebigen Themenfeldes veraltet schnell. Deshalb werden periodische Awareness-Schulungen empfohlen, um die Kenntnisse in diesem Bereich ständig auf dem aktuellen Stand zu halten. E-Learning-Systeme können dabei den Aufwand überschaubar halten.

Beispiele für Policies

Firmen setzen immer häufiger Richtlinien bzw. Policies ein, mit denen man Mitarbeitern verständlich machen möchte, welche Folgen bestimmte Handlungen im Web 2.0 mit sich bringen können. Bei der Einführung solcher Policies ist darauf zu achten, dass dem Mitarbeiter nicht nur mit erhobenem Zeigefinger ein Verbot ausgesprochen wird, sondern verständlich gemacht wird, wes-

halb ein bestimmtes Verhalten notwendig ist. Beispiele für entsprechende Policies verschiedenster namhafter Unternehmen finden sich unter http://socialmediagovernance.com/policies.php [141].

Schutz der Firma und des Mitarbeiters

Zu begrüßen ist die Policy der Firma IBM [136], die nicht nur zum Schutz der Firma, sondern auch des Mitarbeiters gedacht ist. Die Guideline wird in regelmäßigen Abständen überarbeitet und gepflegt, sodass sie auch technische Neuerungen berücksichtigt. Mitarbeiter werden dazu angehalten, sich in sozialen Netzwerken aufzuhalten, um Ideen zu sammeln. Allerdings werden auch rechtliche Aspekte und Gefahren, sogar für den privaten Bereich, dargelegt. Dies beinhaltet Hinweise darauf, dass sämtliches Material, das ins Internet gestellt wird, für eine sehr lange Zeit einsehbar ist und es nahezu unmöglich ist, entsprechende Informationen nachträglich wieder zu entfernen. Zudem sollte bei der Verbreitung von Material auf entsprechende Urheberrechte und mögliche Rechtsverletzungen geachtet werden. Falls in sozialen Netzwerken Themen diskutiert werden, die die Firma direkt betreffen, sollte man sich als Mitarbeiter der Firma zu erkennen geben und dies – wenn nötig – sogar mit der genauen Stellung im Betrieb. Dabei sollte ein Mitarbeiter aber dennoch verdeutlichen, dass er für sich spricht, und nicht für den Betrieb. Gewarnt wird auch davor, zu viel Persönliches preiszugeben, um die eigene Sicherheit zu wahren. Weiterhin verbietet die Policy die Weitergabe vertraulicher Informationen und das Zitieren von Geschäftspartnern ohne deren explizit eingeholte Erlaubnis.

Auch der Umgangston wird von der IBM-Policy bedacht: So ist zu vermeiden, besonders emotionale oder gar beleidigende Inhalte zu publizieren. Unter diese Beschränkung fallen im Übrigen auch politische Inhalte.

Speziell dieser Punkt wird auch von besonders stark mit der öffentlichen Meinung in Verbindung stehenden Organisationen gefordert. So steht etwa in der Policy der BBC: „The personal use of the internet by BBC staff must be tempered by an awareness of the potential conflicts that may arise“ [137]. Reuters hat in eine entsprechende Veröffentlichung zudem die Anmerkung eingefügt, im Internet gesichtete Informationen auf Falschmeldungen (sog. Hoaxes) zu untersuchen, bevor diese einer Weiterverwendung zugeführt werden dürfen [138].

Speziell finden sich bei Reuters auch Hinweise zur Verwendung von Twitter. Dabei wird gefordert, vor der professionellen Verwendung von Twitter Absprache mit dem jeweiligen Vorgesetzten zu halten. Auch wird für diesen Fall darum gebeten, den Namen des Unternehmens im Twitter-Profil anzugeben sowie zu persönliche

und nicht relevante Inhalte von professionellen Inhalten zu trennen [138].

Eine weitere lobenswert übersichtliche Policy (die man ebenfalls unter dem oben angegebenen Link findet) ist die der Daimler AG. Diese Policy beinhaltet u. a. 10 Punkte, die relativ kurz und knapp alles zusammenfassen, was hinsichtlich des Umgangs mit sozialen Netzwerken von Bedeutung ist. Im Großen und Ganzen stimmt sie inhaltlich mit der IBM-Policy überein.

Ein explizites Ablaufschema für den Umgang mit Online-Postings bietet (auf einer einzigen Seite zusammengefasst) die US Air Force [139].

Auch die Firma Intel unterhält „Social Media Guidelines". Es wird den Mitarbeitern geraten, sich an ihr jeweiliges Fachgebiet zu halten, wenn sie Auskunft geben. Außerdem sollen sie klar machen, dass es sich um ihre persönliche, individuelle Meinung handelt. Die verfassten Beiträge sollen sinnvoll und respektvoll sein, auch dürfen geheime und vertrauliche Informationen nicht weitergegeben werden. Überstürztes Antworten auf Beiträge und Kommentare ist untersagt – eine angemessene „Denkpause" vor der Beantwortung wird explizit gefordert („Always pause and think before posting."). In der gleichen Art und Weise soll höflich auf andere Meinungen reagiert und die Nützlichkeit eigener Beiträge überprüft werden. Weiterhin wird auf den „Intel Code of Conduct" und die „Intel Privacy Policy" verwiesen [140].

Zusammenfassung

Die bekannten Richtlinien für den Umgang mit sozialen Netzwerken unterscheiden sich von Unternehmen zu Unternehmen. Einheitliche Standards wurden in diesem Bereich noch nicht geschaffen, doch lässt die Recherche der bisherigen Policies erkennen, dass die Wichtigkeit des Themas von den großen Unternehmen bereits erkannt wurde. Deren Policies enthalten in der Regel etwa zehn wichtige Punkte, die aber nicht immer vollständig alle Gefährdungen abdecken. Daraus kann geschlossen werden, dass eine Kombination der wichtigsten Regeln bekannter Unternehmen (speziell IBM, Daimler, BBC und Reuters) eine gute Grundlage für die Policy eines deutschen Unternehmens bilden kann. Die in diesem Kapitel genannten Punkte erheben keinen Anspruch auf Vollständigkeit, sollten aber die wichtigsten Fakten gelistet und erläutert haben.

Die zentrale Empfehlung lautet, soziale Netzwerke nicht nur von administrativer Seite zu blocken, sondern das Bewusstsein sämtlicher Mitarbeiter (inkl. Führungspersonal) für die Gefahren von sozialen Netzwerken – ggf. auch mit externer Hilfe – zu wecken und in geeigneten Schulungsmaßnahmen den richtigen Umgang zu vermitteln.

Quellenverzeichnis

1. Facebook News: Key Facts, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22, (2012).
2. Focus Online: Porsche verhängt Facebook-Verbot für Mitarbeiter, http://www.focus.de/finanzen/karriere/berufsleben/wirtschaftsspionage-porsche-verhaengt-facebook-verbot-fuer-mitarbeiter_aid_560720.html (2010).
3. BITKOM: Soziale Netzwerke – Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet (2011).
4. BITKOM: Leitfaden Social Media (2010).
5. Digitalpublic.de: 100 Social Media Guidelines, http://www.digitalpublic.de/25-social-media-guidelines (2011).
6. Legal Tribune Online: Illoyale Arbeitnehmer - Gefährliches Netzwerken bei Daimler, http://www.lto.de/de/html/nachrichten/3386/illoyale_arbeitnehmer_gefaehrliches_netzwerken_bei_daimler/ (2011).
7. BITKOM: Social Media Guidelines, Tipps für Unternehmen (2011).
8. Wikipedia: Soziales Netzwerk (Internet) – Wikipedia, Die freie Enzyklopädie, http://de.wikipedia.org/w/index.php?title=Soziales_Netzwerk_(Internet)&oldid=91554675 (2011).
9. World Map of Social Networks, http://www.vincos.it/world-map-of-social-networks/ (2011).
10. Pingdom: Royal Pingdom Study: Ages of social network users, http://royal.pingdom.com/2010/02/16/study-ages-of-social-network-users/.
11. Wikipedia: Facebook – Wikipedia, http://de.wikipedia.org/wiki/Facebook.
12. Haugen, A.: The Facebook Blog, http://blog.facebook.com/blog.php?topic_id=222173789127 (2010).
13. Weigert, M.: Die Ära der Facebook-Applikationen ist vorbei, http://netzwertig.com/2008/12/14/die-aera-der-facebook-applikationen-ist-vorbei/ (2008).
14. Wikipedia: Plug-in – Wikipedia, http://de.wikipedia.org/wiki/Plugin.
15. Zuckerberg, M.: Facebook Across the Web, http://blog.facebook.com/blog.php?post=41735647130 (2008).
16. Becker, A.: Meedia: Bild.de vernetzt sich mit Facebook, http://meedia.de/internet/bildde-vernetzt-sich-mit-face-

book/2009/04/16.html?tx_veguestbook_pi1%5Bpointer%5D=1&cHash=f619dd815814e33ab6c66231ca486a20 (2009).
17. Roth, P.: Facebook Social Plugins: Like Button, Recommendations, Activity Feed, Like Box usw. – Die neuen und alten Plugins im Überblick, http://allfacebook.de/connect/facebook-social-plugins-like-button-recommendations-activity-feed-like-box-usw-die-neuen-und-alten-plugins-im-uberblick (2010).
18. Facebook: Facebook-Handy, http://www.facebook.com/mobile/.
19. What is Facebook Places? - Facebook Hilfebereich, http://www.facebook.com/help/?faq=223406984336119#What-is-Facebook-Places?
20. Stiftung-Warentest: Soziale Netzwerke - Datenschutz oft mangelhaft - Test - Stiftung Warentest, http://www.test.de/themen/computer-telefon/test/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-1855785/ (2010).
21. comScore: U.S. Online Display Advertising Market Delivers 22 Percent Increase in Impressions vs. Year Ago - comScore, Inc, http://www.comscore.com/Press_Events/Press_Releases/2010/11/U.S._Online_Display_Advertising_Market_Delivers_22_Percent_Increase_in_Impressions (2010).
22. Liu, D.: The Next Step for Facebook Credits, https://developers.facebook.com/blog/post/451 (2011).
23. Heise-Security: Das verrät Facebooks Like-Button, http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html (2011).
24. Heise-Security: Facebook Apps verraten Zugangsdaten, http://www.heise.de/security/meldung/Facebooks-Apps-verraten-Zugangsdaten-1241261.html (2011).
25. Facebook: Terms of Service, http://www.facebook.com/legal/terms (2011).
26. Walters, C.: Facebook's New Terms Of Service: „We Can Do Anything We Want With Your Content. Forever." The Consumerist. http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html (2009).
27. Allfacebook: Facebook Nutzerzahlen 2012, http://allfacebook.de/news/facebook-nutzerzahlen-2012-in-deutschland-und-weltweit (2012).
28. Süddeutsche Zeitung: Facebook eröffnet Rekordjagd, http://www.sueddeutsche.de/wirtschaft/geplanter-boersengang-facebook-eroeffnet-die-rekord-jagd-1.1359896 (2012).

29. Bager, J.: heise online - Was Facebook über Nicht-Mitglieder weiß, http://heise.de/-921350 (2010).
30. Klaß, C.: Facebook: Neue Privatsphäre-Einstellungen sind da (Update) - Golem.de, http://www.golem.de/1005/75376.html.
31. Wilkens, A.: heise online - Facebook gründet Sicherheitsbeirat, http://heise.de/-878471.
32. Wilkens, A.: heise online - Facebook verschreibt sich besserem Jugendschutz, http://heise.de/-206824.
33. Bright, P.: Understanding the latest Facebook privacy train wreck, http://arstechnica.com/web/news/2010/05/understanding-the-latest-facebook-privacy-train-wreck.ars (2010).
34. Balachander Krishnamurthy, C.E.W.: On the Leakage of Personally Identifiable Information Via Online Social Networks, http://www2.research.att.com/~bala/papers/wosn09.pdf (2010).
35. jeremy: Referrer URLs and Privacy Risks, http://blog.rapleaf.com/blog/2010/10/17/referrer-urls-and-privacy-risks/ (2010).
36. Wikipedia: Vorschussbetrug – Wikipedia, http://de.wikipedia.org/wiki/Scam.
37. Wueest, C.: Firefox Extension Used in Facebook Scam | Symantec Connect Community, http://www.symantec.com/connect/blogs/firefox-extension-used-facebook-scam (2011).
38. Sebayang, A.: Social Engineering: Facebook-Scam mit Firefox-Erweiterung, http://www.golem.de/1103/82241.html (2011).
39. Heise-Security: Würmer breiten sich ungehindert aus, http://www.heise.de/security/meldung/Facebook-Wuermer-breiten-sich-ungehindert-aus-1021650.html (2010).
40. Heise-Security: Facebook mit 2-Faktor-Login, http://www.heise.de/security/meldung/Facebook-mit-2-Faktor-Login-und-weiteren-Sicherheitsverbesserungen-1242500.html, (2011).
41. Mozilla: Cookies von Drittanbietern blockieren, http://support.mozilla.com/de/kb/Cookies%20von%20Drittanbietern%20blockieren.
42. Wikipedia: LinkedIn – Wikipedia, Die freie Enzyklopädie, http://de.wikipedia.org/w/index.php?title=LinkedIn&oldid=91155515, (2011).
43. LinkedIn Pressebereich: Über uns – LinkedIn Fakten, http://de.press.linkedin.com/about (2012)
44. LinkedInsider Deutschland: Eigentümer von LinkedIn, http://linkedinsiders.wordpress.com/2011/02/23/linkedin2011/ipo-diagramm-5.

45. Koß, S.: Was ist eigentlich LinkedIn? Ein Erklärungsversuch…, http://linkedinsiders.wordpress.com/2011/01/09/was-ist-linkedin/.
46. LinkedIn: LinkedIn User Agreement, http://www.linkedin.com/static?key=user_agreement&trk=hb_ft_userag.
47. LinkedIn: LinkedIn Privacy Policy, http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv.
48. LinkedIn: LinkedIn Copyright Policy, http://www.linkedin.com/static?key=copyright_policy&trk=hb_ft_copy.
49. Stiftung Warentest.: Soziale Netzwerke - Datenschutz oft mangelhaft, http://www.test.de/themen/computer-telefon/test/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-1855785/.
50. Zeit Online: Datenschutz: Sicherheitslücke bei LinkedIn entdeckt, http://www.zeit.de/digital/datenschutz/2011-05/LinkedIn-Datenschutz.
51. lokalisten media gmbh: lokalisten community: freunde, chat, online games & partyfotos, http://www.lokalisten.de/press/open/showPress.do.
52. Wikipedia: Lokalisten (Netzwerk) — Wikipedia, Die freie Enzyklopädie, http://de.wikipedia.org/w/index.php?title=Lokalisten_(Netzwerk)&oldid=91070055 (2011).
53. lokalisten media gmbh: Kurz und Bündig, http://vermarktung.lokalisten.de/2011_09_05/08_11_Lokalisten_Keyfacts.pdf.
54. lokalisten media gmbh: Allgemeine Geschäftsbedingungen der Lokalisten media GmbH, http://www.lokalisten.de/common/closed/showAgb.do#rights (2011).
55. lokalisten media gmbh. media: lokalisten community: freunde, chat, online games & partyfotos, http://www.lokalisten.de/press/open/showPress.do.
56. statista.com: Soziale Netzwerke – Besucherzahlen Deutschland, http://de.statista.com/statistik/daten/studie/209595/umfrage/entwicklung-der-visits-der-deutschen-social-networks (2012)
57. Yahoo Deutschland – Finanzen, http://de.finance.yahoo.com/q?s=LNKD
58. Wikipedia: Twitter — Wikipedia, Die freie Enzyklopädie, http://de.wikipedia.org/w/index.php?title=Twitter&oldid=91906720 (2011).
59. ZDNet.de: Umzug des Twitter-Rechenzentrums klappt nicht wie geplant, http://www.zdnet.de/news/digitale_wirtschaft_internet_ebusiness_umzug_des_twitter_rechenzentrums_klappt_nicht_wie_geplant_story-39002364-41551247-1.htm.

60. Spiegel.de: So verdienen die Web-Riesen im Netz, http://www.spiegel.de/netzwelt/web/0,1518,745755,00.html.
61. FAZ.NET: 5 Jahre Twitter - 20 Millionen Meinungsmacher, http://www.faz.net/s/Rub4C34FD0B1A7E46B88B0653D-6358499FF/Doc~E10F7D939A60E4BDD9C4F4109468FE823~ATpl~Ecommon~Scontent.html.
62. Twitter Inc.: Twitter Widgets, http://twitter.com/about/resources/widgets.
63. Chubby Team: Twitter Investors – Venture Capital, Private Equity and Mutual Fund Heavyweights, http://www.chubbybrain.com/blog/twitter-investors-venture-capital-heavyweights/.
64. Arthur, C.: Twitter unveils 'promoted tweets' ad plan, http://www.guardian.co.uk/technology/2010/apr/13/twitter-advertising-google.
65. Twitter Inc.: Twitter Terms of Service, http://twitter.com/tos.
66. Twitter Inc.: Twitter Datenschutzbestimmungen, http://twitter.com/privacy.
67. Dhanjani, N.: Twitter and Jott Vulnerable to SMS and Caller ID Spoofing, http://www.dhanjani.com/blog/2007/04/twitter-and-jot.html.
68. Cluley, G.: Twitter 'onMouseOver' security flaw widely, http://nakedsecurity.sophos.com/2010/09/21/twitter-onmouseove
69. handelsblatt.com: Warum Unternehmen twittern müssen, http://www.handelsblatt.com/unternehmen/mittelstand/warum-unternehmen-twittern-muessen/3345572.html?p3345572=6.
70. Offizielle Daten und Fakten über die VZ Netzwerke, http://www.StudiVZ.net/l/about_us/1/.
71. VZnet Netzwerke – Wikipedia, http://de.wikipedia.org/wiki/VZnet_Netzwerke.
72. StudiVZ – Wikipedia, http://de.wikipedia.org/wiki/StudiVZ.
73. StudiVZ: Buschfunk, http://www.StudiVZ.net/l/buschfunk.
74. Dittes, A.: Finanzierung von StudiVZ liegt jetzt offen, http://dittes.info/die-finanzierung-vom-StudiVZ-liegt-jetzt-offen/.
75. Informationen für Eltern und Lehrer, http://www.schuelervz.net/l/parents/1/.
76. Steuer, Ph. für Google+inside, http://googleplusinside.de/so-sieht-der-deutsche-google-plus-nutzer-aus/ (28.01.2012)
77. Google-Produkt-Blog, http://google-produkte.blogspot.de/2012/04/google-wird-einfacher-und-immer.html
78. PHP-Magazin, http://it-republik.de/php/news/Google%2B-und-die-Browser-Sicherheit-060154.html

79. VZ-Netzwerke präsentieren einmaliges Open-Social-Konzept mit umfassender Datenschutzlösung | VZblog, http://blog.StudiVZ.net/2009/12/07/vz-netzwerke-prasentieren-einmaliges-opensocial-konzept-mit-umfassender-datenschutzlosung.
80. Offizielle AGB VZ Netzwerke, http://www.StudiVZ.net/l/terms.
81. Datenschutz: StudiVZ, Xing und Co. unterzeichnen Unterlassungserklärungen - SPIEGEL ONLINE - Nachrichten - Netzwelt, http://www.spiegel.de/netzwelt/netzpolitik/0,1518,660863,00.html.
82. StudiVZ-Boss Riecke: "Gott sei Dank dürfen wir bei Ermittlungsersuchen Daten jetzt herausgeben" - SPIEGEL ONLINE - Nachrichten - Netzwelt, http://www.spiegel.de/netzwelt/web/0,1518,537622,00.html.
83. heise online - Erneute Datenschutzpanne bei SchülerVZ [Update], http://www.heise.de/newsticker/meldung/Erneute-Datenschutzpanne-bei-SchuelerVZ-Update-992435.html.
84. heise online - SchülerVZ-Datenklau: Verdächtiger begeht Selbstmord, http://www.heise.de/newsticker/meldung/SchuelerVZ-Datenklau-Verdaechtiger-begeht-Selbstmord-847178.html.
85. StudiVZ | klartext, http://www.StudiVZ.net/Newsroom/Detail/fce0360b56ca70b6/backPg/4.
86. Wikipedia: Google+ — Wikipedia, Die freie Enzyklopädie, http://de.wikipedia.org/w/index.php?title=Google%2B&oldid=95049618, (2011).
87. Allen, G.: Google+ To Pass 10,000,000 Users Tomorrow (on 7/12), https://plus.google.com/117388252776312694644/posts/bGJPTALDkDe, (2011).
88. die-medienblogger.de: Heilsbringer Google+? – Die Medienblogger, http://www.die-medienblogger.de/722/heilsbringer-google.
89. Google: Werbung und Datenschutz – Google Datenschutz-Center, http://www.google.com/intl/de/privacy/ads/.
90. Google: Datenschutzbestimmungen - Google Datenschutz-Center, http://www.google.com/intl/de/privacy/privacy-policy.html.
91. Google: Dashboard, https://www.google.com/dashboard/?hl=de.
92. .:tobesocial TREFF, httpXing VS. LinkedIn: Eine Analyse der größten Businessnetzwerke in Deutschlandhttp://tobesocial.de/category/tags/nutzerzahlen-xing/.
93. XING – Wikipedia, http://de.wikipedia.org/wiki/XING.

94. Rittig, A.: XING Generations | XING Blog, http://blog.xing.com/2009/04/xing-generations/.
95. Wilkens, A.: heise online - Neue Xing-Funktion weckt Datenschutzbedenken, http://www.heise.de/newsticker/meldung/Neue-Xing-Funktion-weckt-Datenschutzbedenken-167585.html.
96. datensicherheit.de: XING-Gruppen-Newsletter http://www.xing.com/net/fischernetz/newsletter-archiv-19807/gruppen-newsletter-achtung-gefalschte-xing-mails-im-umlauf-24514207/.
97. Twitter-Blog, http://blog.twitter.com/2012/03/twitter-turns-six.html
98. Bell, J.H.: Corporate Reputation in the Social Age, http://www.yoursocialmediascore.com/downloads/b_repmanagement.pdf.
99. Digital, P.: Der bezahlbare Ruf, http://politik-digital.de/der-bezahlbare-ruf.
100. ZDNet: Mitmachen oder verbieten: Soziale Netzwerke in Unternehmen, http://www.zdnet.de/magazin/41536177/mitmachen-oder-verbieten-soziale-netzwerke-in-unternehmen.htm.
101. Rundschau, F.: Schmutz und Blut, http://www.fr-online.de/kultur/medien/schmutz-und-blut/-/1473342/8446884/-/.
102. paradisi.de: Online-Kriminalität: Hemmschwelle bei Jugendlichen sehr niedrig, http://www.paradisi.de/Freizeit_und_Erholung/Gesellschaft/Jugendkriminalitaet/News/15987.php.
103. Spiegel.de: Der Chef stichelt gezielt mit, http://www.spiegel.de/unispiegel/jobundberuf/0,1518,269981,00.html.
104. stuttgarter-nachrichten.de: Cyber-Mobbing immer häufiger Web-gemobbt, http://content.stuttgarter-nachrichten.de/stn/page/2208354_0_6327_-cyber-mobbing-immer-haeufiger-web-gemobbt.html.
105. welt.de: Mobbing und Burn-out kosten jährlich 6,5 Milliarden, http://www.welt.de/wirtschaft/karriere/article3659218/Mobbing-und-Burn-out-kosten-jaehrlich-6-5-Milliarden.html.
106. heise.de: "Mobbing-Vorstand" der Telekom Austria verliert Zuständigkeit für Personal, http://www.heise.de/jobs/meldung/Mobbing-Vorstand-der-Telekom-Austria-verliert-Zustaendigkeit-fuer-Personal-201122.html.
107. DiePresse.com: Facebook und Twitter kosten eine Woche Arbeit pro Jahr, http://diepresse.com/home/techscience/internet/517564/Facebook-und-Twitter-kosten-eine-Woche-Arbeit-pro-Jahr?from=rss.
108. pressetext.deutschland: Arbeitgeber hadern mit Social Networks, http://www.pressetext.com/news/20090925034.

109. Wikipedia: Koobface — Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=Koobface&oldid=451225447, (2011).
110. Nemey, A.K. und C.: 5 Bedrohungen bei Social Media, http://www.cio.de/knowledgecenter/security/2277766/index.html.
111. Miller, M.: Google Engineer Publishes, Then Deletes Opinionated Google+ Rant, http://searchenginewatch.com/article/2117162/Google-Engineer-Publishes-Then-Deletes-Opinionated-Google-Rant.
112. W&S: Zufriedene Kollegen wahren Geschäftsgeheimnisse, http://www.sicherheit.info/SI/cms.nsf/si.ArticlesByDocID/1103258?Open.
113. pressemitteilungen-online.de: E-Mail Benachrichtigungen während der Arbeitszeit stören Konzentration, http://www.pressemitteilungen-online.de/index.php/e-mail-benachrichtigungen-waehrend-der-arbeitszeit-stoeren-konzentration/.
114. Sicking, M.: Facebook & Co verursachen Millionen-Schäden in Unternehmen, http://www.heise.de/resale/artikel/Faceboo Co-verursachen-Millionen-Schaeden-in-Unternehmen-1251956.html.
115. Handelsblatt: „Explosive Grüße aus dem Netz", http://www.handelsblatt.com/unternehmen/it-medien/soziale-netzwerke-explosive-gruesse-aus-dem-netz/6089176.html (26.01.12)
116. foursquare: foursquare, https://de.foursquare.com/.
117. Google: Google places, http://www.google.com/places/.
118. mobile-location-services-to-the-next-level/.
119. Stern.de: "Facebook Orte" ist hier: Deutschland, http://www.stern.de/digital/online/neuer-dienst-places-facebook-orte-ist-hier-deutschland-1610627.html.
120. Twitter.com: How To With Use the Location Feature on Mobile Devices, http://support.twitter.com/groups/34-mobile/topics/171-twitter-s-mobile-website/articles/118492-how-to-tweet-with-your-location-on-mobile-devices.
121. TechCrunch.com: Please Rob Me Makes Foursquare Super Useful For Burglars, http://techcrunch.com/2010/02/17/please-rob-me-makes-foursquare-super-useful-for-burglars/.
122. Grimme-Institut: Hier und jetzt im Netz, http://www.grimme-institut.de/imblickpunkt/pdf/imblickpunkt-hier-und-jetzt-im-netz.pdf (2011).
123. BRD: BDSG-§4, http://dejure.org/gesetze/BDSG/4.html (2009).

124. Arrington, M.: Being Eric Schmidt (On Facebook), http://techcrunch.com/2010/10/10/being-eric-schmidt-on-facebook/.
125. Siciliano, R.: Identity Theft Committed Using Social Networks, http://www.huffingtonpost.com/robert-siciliano/identity-theft-commited-u_b_243305.html.
126. Saafan: fbpwn - A cross-platform Java based Facebook social engineering framework, http://code.google.com/p/fbpwn/.
127. C.S.Online: Microblogging-Dienst Twitter. Kanäle von Britney Spears und Barack Obama gehackt, http://www.spiegel.de/netzwelt/web/0,1518,599699,00.html (2009).
128. Heise.de: Sarah Palin: Der Mail-Hack, der keiner war, http://www.heise.de/security/meldung/Sarah-Palin-Der-Mail-Hack-der-keiner-war-207052.html (2008).
129. Heise.de: Sarah Palins E-Mail-Account wurde gehackt, http://www.heise.de/newsticker/meldung/Sarah-Palins-E-Mail-Account-wurde-gehackt-Update-206516.html (2008).
130. Heise.de: RSA-Hack könnte Sicherheit von SecurID-Tokens gefährden, http://www.heise.de/security/meldung/RSA-Hack-koennte-Sicherheit-von-SecurID-Tokens-gefaehrden-1210245.html (2011).
131. Heise.de: Hacker steigen bei Lockheed Martin ein, http://www.heise.de/ct/meldung/Hacker-steigen-bei-Lockheed-Martin-ein-1251902.html, (2011).
132. f-secure.com: How We Found the File That Was Used to Hack RSA, http://www.f-secure.com/weblog/archives/00002226.html, (2011).
133. CIO and V.P. for I.T. at the University of Wisconsin-Madison: Protect your identity, http://www.cio.wisc.edu/security-identity.aspx.
134. Focus.com: The Security Risks of Social Networks, http://www.focus.com/fyi/security-risks-social-networks/.
135. Broecker, D.S.: Wie sich das Sicherheitsbewußtsein entwickelt – IT-Security-Awareness in Zeiten von Social Media und Datenverlusten, http://www.searchsecurity.de/specials/security_corner/management/articles/276485/.
136. IBM: Social Computing Guidelines. Blogs, wikis, social networks, virtual worlds and social media, http://www.ibm.com/blogs/zz/en/guidelines.html.
137. BBC: Social Networking, Microblogs and other Third Party Websites: Personal Use, http://www.bbc.co.uk/guidelines/editorialguidelines/page/guidance-blogs-personal-summary, (2010).

138. Reuters: Reporting from the internet, http://handbook.reuters.com/index.php/Reporting_From_the_Internet_And_Using_Social_Media, (2012).
139. Force, U.A.: Air Force Web Posting Response Assessment V.2, http://www.globalnerdy.com/wordpress/wp-content/uploads/2008/12/air_force_web_posting_response_assessment-v2-1_5_09.pdf.
140. Corporation, I.: Intel Social Media Guidelines, http://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html.
141. Social Media Governance: Policy Database, http://socialmediagovernance.com/policies.php, (2012).
142. Wood, P.: Symantec Intelligence Report für November 2011, http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20111207_01
143. Lerg, A. auf T-Online.de, http://computer.t-online.de/facebook-timeline-deaktivieren-geht-das-/id_54030330/index
144. Focus Online, Netzökonomie-Blog, http://www.focus.de/digital/internet/netzoekonomie-blog/social-media-twitter-durchbricht-die-4-millionen-marke-in-deutschland_aid_740627.html (2012)

Kontakt

Bayerisches Landesamt für Verfassungsschutz

Knorrstraße 139 I 80937 München
Telefon Wirtschaftsschutz: 089 31201-500

E-Mail: wirtschaftsschutz@lfv.bayern.de
Internet: www.wirtschaftsschutz.bayern.de
www.verfassungsschutz.bayern.de

Hochschule Augsburg
Fakultät für Informatik

Friedberger Straße 2 I 86161 Augsburg
Telefon: 0821 5586-3450

E-Mail: info@informatik.hs-augsburg.de
Internet: www.hs-augsburg.de

Impressum

Herausgeber:	Bayerisches Landesamt für Verfassungsschutz, Knorrstr. 139, 80937 München
	Hochschule Augsburg, Friedberger Straße 2, 86161 Augsburg
Druck:	Bayerisches Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie
Bildnachweis:	Titelbild: almagami/Shutterstock.com
	Internet-Screenshots: S. 16: facebook.de I S. 27: linkedin.com S. 29: lokalisten.de I S. 33: twitter.com I S. 37: meinvz.net S. 42: plus.google.com I S. 46: xing.com

Wollen Sie mehr über die Arbeit der Bayerischen Staatsregierung erfahren?

BAYERN I DIREKT ist Ihr direkter Draht zur Bayerischen Staatsregierung.

Unter Telefon **089 122220** oder per E-Mail unter **direkt@bayern.de** erhalten Sie Informationsmaterial und Broschüren, Auskunft zu aktuellen Themen und Internetquellen sowie Hinweise zu Behörden, zuständigen Stellen und Ansprechpartnern bei der Bayerischen Staatsregierung.

Hinweis:

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit der Bayerischen Staatsregierung herausgegeben. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern im Zeitraum von fünf Monaten vor einer Wahl zum Zwecke der Wahlwerbung verwendet werden.

Dies gilt für Landtags-, Bundestags-, Kommunal- und Europa wahlen. Missbräuchlich ist während dieser Zeit insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken und Aufkleben von parteipolitischen Informationen oder Werbemitteln. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung. Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die Druckschrift nicht in einer Weise verwendet werden, die als Parteinahme der Staatsregierung zugunsten einzelner politischer Gruppen verstanden werden könnte. Den Parteien ist gestattet, die Druckschrift zur Unterrichtung ihrer eigenen Mitglieder zu verwenden.

Die Druckschrift wurde mit großer Sorgfalt zusammengestellt. Gewähr für die Richtigkeit und Vollständigkeit des Inhalts kann dessen ungeachtet nicht übernommen werden.

Initiative Wirtschaftsschutz

Eine gemeinsame Aktion des Bayerischen Staatsministeriums des Innern und des Bayerischen Staatsministeriums für Wirtschaft, Infrastruktur, Verkehr und Technologie