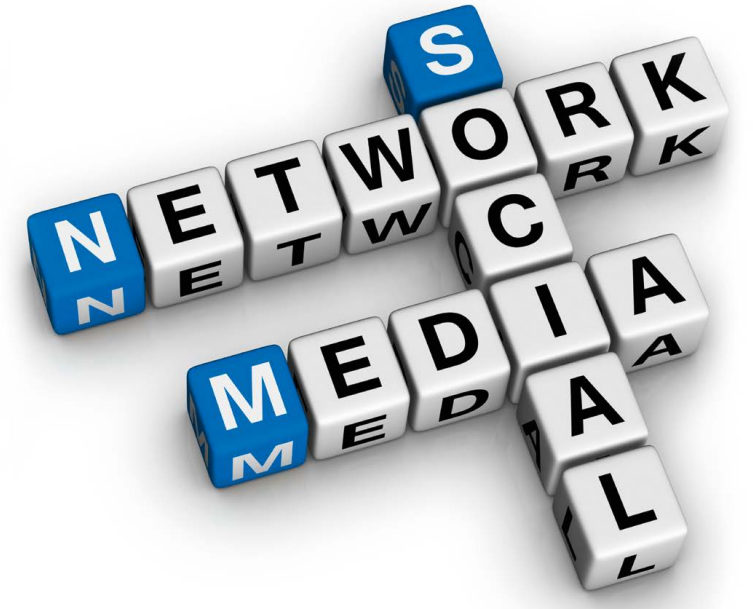
Bayerisches Landesamt
für Verfassungsschutz

Soziale Netzwerke

und ihre Auswirkungen auf die Unternehmenssicherheit



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

2. überarbeitete Auflage

Kontakt

Bayerisches Landesamt
für Verfassungsschutz
Knorrstraße 139 I 80937 München
Telefon Wirtschaftsschutz: 089 31201-500
E-Mail: wirtschaftsschutz@lfv.bayern.de
www.wirtschaftsschutz.bayern.de

Cyber-Allianz-Zentrum Bayern
Hotline: 089 31201-222
E-Mail: caz@lfv.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

INHALTSVERZEICHNIS

VORWORT

Rund 28 Millionen Nutzer hat allein das soziale Netzwerk [1] 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.

Wirtschaftsspionage hat sich 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 Präventionsarbeit hat das Bayerische Landesamt für Verfassungsschutz zusammen mit der Hochschule Augsburg bereits 2012 eine Publikation erstellt. Weil Entwicklungsprozesse im Internet in rasantem Tempo ablaufen und sich seit der Erstausgabe sowohl Nutzungsverhalten als auch Regelungen und Möglichkeiten in sozialen Netzwerken erheblich verändert haben, wurde die Broschüre nun einer umfassenden Aktualisierung unterzogen. Damit verschafft diese Neuauflage auch weiterhin Füh-

rungskräften und Mitarbeitern einen umfassenden und möglichst aktuellen Überblick über das Thema „Soziale Netzwerke und ihre Auswirkungen auf die Unternehmenssicherheit". Sie finden darin Informationen zu den wichtigsten sozialen Netzwerken und zu möglichen Sicherheitsproblemen.

Mein besonderer Dank gilt Herrn Prof. Dr. Gordon Rohrmair und Herrn Sebastian Kraemer von der Fakultät für Informatik an der Hochschule Augsburg, für die hervorragende Unterstützung bei der Erarbeitung und Aktualisierung dieser Edition, der ich viele interessierte Leser wünsche.

August 2016
Dr. Burkhard Körner
Präsident des Bayerischen Landesamts
für Verfassungsschutz

EINLEITUNG

Ein soziales Netzwerk ist per Definition ein „Beziehungsgeflecht, das Menschen mit anderen Menschen und Institutionen sowie Institutionen mit anderen Institutionen verbindet“ [1]. Dieses Eingebundensein in ein „soziales Netz“ ist ein menschliches Grundbedürfnis und erleichtert auch heute noch unser tägliches Leben. Durch das Web 2.0 wurden diese Mechanismen von der realen in die virtuelle Welt übernommen: So entstanden die sogenannten „internetbasierten social networks“, die wir im Folgenden der Einfachheit halber als „soziale Netzwerke“ bezeichnen.

Veränderte Bedeutung und gesellschaftspolitische Entwicklungen

Die Bedeutung sozialer Netzwerke geht inzwischen weit über diesen ursprünglichen Sinn hinaus. Nicht nur im privaten oder beruflichen Bereich steigen Vernetzungsgrad und Einfluss auf den Einzelnen. Die Generation der sogenannten „Native User“ kann sich ein Leben ohne Internet nicht mehr vorstellen – und daher auch nicht mehr ohne Smartphones, die nicht nur als „lebensnotwendig“ sondern quasi als „Teil des Körpers“ wahrgenommen werden [2]. Ihre persönlichen Daten geben die „Digital Natives“ bereitwillig preis, über Datenschutz machen sie sich kaum Gedanken.[3]

Native User/ Digital Natives: Erste Generation, die von klein auf mit der digitalen Technik aufwächst.

Auch auf gesellschaftspolitischer Ebene spielt das „Social Web“ zunehmend eine Rolle – mit positiven wie negativen Auswirkungen. Wichtige politische Entwicklungen der vergangenen Jahre wie z.B. der „Arabische Frühling“ wurden maßgeblich über Facebook und Twitter initiiert und beeinflusst [4]. Sowohl von politischen Systemen als auch von Extremisten wurden und werden soziale Netzwerke auch als Manipulationswerkzeuge missbraucht. Überwachung, Zensur und Infiltration sind in Ländern wie China an der Tagesordnung. Nutzer liefern sich dort ein „Katz-und Maus-Spiel“ mit den Regierungen, um diese Einschränkungen zu umgehen. Die salafistisch-jihadistische Terrororganisation Islamischer Staat (IS) wiederum nutzt soziale Netzwerke, um Mitglieder zu rekrutieren und ihre Terrorbotschaften in den Ländern des Westens zu verbreiten.

Im privaten oder beruflichen Alltag

Zurück zu unserem Alltag: Die Nutzung von „Online-Communities" wird nicht nur zunehmend beliebter, sondern auch immer vielfältiger und umfassender. Viele Menschen können sich einen Alltag ohne soziale Netzwerke nicht mehr vorstellen. Diese Communities ermöglichen es Teilnehmern mit gleichen Interessen, sich mit anderen auszutauschen, Beziehungen zueinander herzustellen, zu vertiefen und durch die Freundes-Freund-Verbindung auch neue Kontakte zu knüpfen. Allein Facebook verzeichnet heute weltweit ca. 1,7 Milliarden registrierte Nutzer. [5] Damit wäre Facebook, würde es sich nicht um eine Online-Gemeinschaft handeln, inzwischen das größte Land der Erde [6].

In sozialen Netzwerken 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 hier ausgetauscht werden. Dabei wird schnell deutlich, dass es einen Konflikt zwischen privaten und unternehmerischen Interessen geben kann, den es bestmöglich zu lösen gilt. Dies gelingt nur, wenn man sich der Gefahren bewusst ist und über die Möglichkeit verfügt, frühzeitig präventive Maßnahmen im Sinne der Unternehmenssicherheit zu implementieren.

Ein weiterer relevanter Faktor ist die Zeit, die Mitarbeiter 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 stark belasten. 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 grundsätzliche Antwort auf diese Fragen lautet: Soziale Netzwerke können durchaus eine positive Auswirkung für Unternehmen haben. Allerdings bedarf es dazu durchdachter Social Media Guidelines und intensiver Mitarbeiter-Schulungen, um die notwendige Awareness und deren Umsetzung zu gewährleisten.

Social Media Guidelines: Richtlinien für den Umgang mit sozialen Netzwerken.

Social Media Intelligence (SMI)
Um den Überblick über die Milliarden von Online-Nachrichten und Social-Media-Inhalten nicht zu verlieren, ist eine frühzeitige und umfassende Beobachtung, Auswertung und Reaktion sinnvoll. Immer mehr Unternehmen nutzen daher die Möglichkeiten des sog. „Social Media Intelligence" (SMI), um hier auf dem Laufenden zu bleiben, vorausschauend planen und agieren zu können sowie bei Bedarf lageangepasst reagieren zu können. Nicht nur im Hinblick auf die Reputation des eigenen Unternehmens im Netz, sondern auch als Grundlage für Managemententscheidungen sind geeignete Tools für SMI heutzutage unerlässlich. Auch im Rahmen der Wettbewerbsbeobachtung sowie bei der Bewertung anderer Unternehmen, Institutionen und Personen lässt sich SMI zielgerichtet einsetzen und liefert zeitnah detaillierte Informationen.

Social Engineering
Eine der erfolgreichsten Angriffstechniken ist das sogenannte Social Engineering. Unter dieser auch „soziale Manipulation" genannten Technik versteht man das Beeinflussen von 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.

Schulungen für Mitarbeiter
Social Engineering kann insbesondere durch drei Maßnahmen abgewehrt werden:

Mitarbeiter müssen
- wissen, ob die gewünschte Informationsweitergabe oder Handlung gestattet ist oder nicht
- die Techniken der Angreifer kennen
- durch Schulungen und Vorträge für diese Thematik und den richtigen Umgang sensibilisiert werden

Schulungen 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 nicht nur im beruflichen, sondern auch im privaten Bereich zur Anwendung kommen: Schützenswerte Informationen gibt es auf beiden Ebenen – Gefahren ebenfalls.

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 kaum noch gegen Cyber-Angriffe schützen können. Zu den prominentesten Opfern der letzten Jahre gehören Sony Pictures, Ebay, Apple, Paypal und die Nato.

Personalisierte E-Mails

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 Informationen über die Angriffsziele u.a. durch systematisches Auswerten sozialer Netzwerke 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. Der Empfänger fühlt sich durch die perfekt auf ihn zugeschnittene Mail direkt angesprochen, öffnet den Anhang oder den enthaltenen Link wie selbstverständlich und ermöglicht dem Angreifer so unbeabsichtigt den Zugang zum Firmennetzwerk.

Senior Intelligence Analyst Paul Wood hat dies im Symantec Intelligence Report für November 2011 [7] 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 Bescheid, so

können sie den Anwender auf besonders glaubwürdige und überzeugende Weise hinters Licht führen". Daher sollte sich jeder Nutzer eines sozialen Netzwerks über die Risiken und Folgen seiner „Postings" bewusst sein. Durch die ins Netz gestellten Informationen gefährdet er eventuell nicht nur sich selbst, sondern auch seine Freunde, alle verknüpften Kontakte und ggf. sogar den Arbeitgeber.

Der Automobilkonzern Porsche sperrte laut dem Nachrichtenmagazin Focus im Oktober 2010 den Zugriff auf die Plattform Facebook für seine Mitarbeiter [8]. Dies geschah nicht, weil zu viel Arbeitszeit durch das soziale Netz verloren ging, sondern aus Angst vor Wirtschaftsspionage. Durch die Sperrung – die bis heute Bestand hat – 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).

Diese Veröffentlichung gibt einen Überblick über einige der wichtigsten sozialen Netzwerke, die Gefahren, die daraus für Unternehmen entstehen sowie Empfehlungen, wie sich Unternehmen und Privatpersonen vor den Risiken besser schützen können.

POPULÄRE SOZIALE NETZWERKE

Dieses Kapitel stellt die populärsten sozialen Netzwerke vor und beleuchtet deren Umfang, Grundidee und Funktionalität. Zudem erfolgt eine Bewertung des jeweiligen Netzwerks unter Sicherheitsaspekten. Im anschließenden Kapitel werden die daraus resultierenden Risiken analysiert.

Die populärsten sozialen Netzwerke in Deutschland sind laut dem Portal Statista[9] Facebook, Google+ und Twitter.

Der Beliebtheitsgrad einzelner sozialer Netzwerke hängt entscheidend von den lokalen Gegebenheiten ab. Während Facebook europaweit unangefochtene Nr. 1 ist, kann es in anderen Regionen der Welt nur einen geringen Marktanteil verzeichnen. Gründe hierfür sind neben kulturellen oder sozialen Unterschieden die Tatsache, dass in einigen Ländern die Nutzung bestimmter sozialer Netzwerke verboten ist bzw. technisch unterbunden wird. Eigene, landesspezifische Gemeinschaftsportale treten dann an die Stelle von Facebook.[10]

Funktionalitäten und typischer Inhalt
Die meisten sozialen Netzwerke bieten ähnliche Funktionen: Es geht um die Interaktion mit anderen Benutzern. Erfahrungsgemäß sind folgende Funktionen standardmäßig vorhanden: [11]

- 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
- Suchfunktion

Diese Grundfunktionen sind meist kostenfrei, allerdings werden regelmäßig kostenpflichtige Dienste optional angeboten, für die der zahlende Nutzer erweiterte Funktionalitäten erhält.

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 Nutzer 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 vernetzt sind, die hier u.a. ihren persönlichen Werdegang darstellen.

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 Gemeinschaftsportalen für die Anmeldung wiederzuverwenden, sich also beispielsweise mit seinem Facebook- oder Google+-Account einzuloggen.

Der Messaging-Dienst WhatsApp [12] bietet den meist jugendlichen Benutzern [13] eine Vielzahl von Anwendungsmöglichkeiten, die größtenteils kostenfrei sind. So können nicht nur Kurznachrichten, Fotos und Videos zwischen zwei oder — mittels speziell angelegter Gruppen — mehr Personen ausgetauscht werden; auch internetbasiertes Telefonieren ist möglich. Seit April 2016 ist WhatsApp in der neuesten Version Ende-zu-Ende-verschlüsselt, d.h. Nachrichten und Anrufe können nur noch von Sender und Empfänger entschlüsselt und gelesen werden. Der beliebte Messaging-Dienst ist seit 2014 in der Hand von Facebook und hatte im Jahr 2016 über eine Milliarde Nutzer — Tendenz steigend. [14]

Eine zunehmende Rolle spielen auch Dating-Portale und Partnerbörsen wie „AdultFriendFinder“ oder „Parship“. Aufgrund der von den Nutzern dort veröffentlichten, höchst sensiblen privaten Daten und Fotos eröffnen sich für Angreifer auf solchen Portalen besonders weitreichende Missbrauchsmöglichkeiten.

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 zu „tracken".

tracken: Verfolgen des Surfverhaltens.

Solch eine Dritt-Authentifizierung bieten unter anderem derzeit Google+, Facebook und Twitter an.

Soziale Netzwerke als Recruiting-Instrument
Während Facebook als typisches „privates" soziales Netzwerk gilt, haben Portale wie Xing oder LinkedIn einen beruflich orientierten Zweck. Die von den Nutzern dort veröffentlichten Informationen sind gezielt darauf abgestimmt, sich mit dem eigenen beruflichen Werdegang möglichst positiv zu präsentieren, um von Personal suchenden Unternehmen gefunden zu werden bzw. sich beruflich verbessern zu können. Auswirkungen auf Einstellungschancen können aber auch jene Informationen haben, die öffentlich zugänglich in anderen sozialen Netzwerken publiziert werden. Immer mehr Personalstellen beziehen diese Informationen in den Auswahlprozess mit ein.

FACEBOOK

Netzwerk	Facebook [15]
URL	http://www.facebook.com
Nutzer weltweit	1,7 Milliarden (Stand Juli 2016)[16]
Nutzer in Deutschland	28 Millionen (Stand Februar 2016)[17]
Hauptsitz	Menlo Park, Kalifornien, USA
Gründungsjahr	Februar 2004

Facebook ist ein kommerzielles soziales Netzwerk der kalifornischen Firma Facebook Inc., das Anfang 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 Laufe 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 1,7 Milliarden aktive Mitglieder. Damit ist es in fast allen Ländern der Welt das größte soziale Netzwerk — mit Ausnahme von China und Russland, wo lokale Anbieter dominieren.[18]

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.

Typischer Inhalt und Kommunikationsmethoden
Ein Teil der Profilseite ist dabei die sogenannte „Timeline“ (in Deutschland: „Chronik“). Nutzer und Besucher, die dafür freigeschaltet sind, können dort Kommentare, Fotos, Links, Videos etc. veröffentlichen. Um mit einem anderen Nutzer direkt in Kontakt zu treten, können private Nachrichten verschickt werden (Facebook-Messenger). Diese sind nur für Absender und Empfänger zugänglich. Darüber hinaus hat jeder Nutzer die Möglichkeit, verschiedensten Interessens-Gruppen beizutreten oder diese zu gründen.

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

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 (Freundes-Freunde) direkt Kontakte zu knüpfen.

Eine weitere gern genutzte und für Facebook äußerst lukrative Funktion sind Apps, 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. Häufig setzt die Installation aber voraus, dass der Benutzer der App bestimmte Berechtigungen gewährt, z.B. die Erlaubnis, in dessen Namen Kommentare zu veröffentlichen oder auf ausgewählte Profildaten zuzugreifen.

Der Funktionsumfang von Facebook beschränkt sich nicht nur auf das soziale Netzwerk selbst. So gibt es u.a. die Möglichkeit, sich über die sogenannte „Einmalanmeldung“ (single-sign-on) bei Facebook auch auf anderen Webseiten oder Apps zu authentifizieren. Anstelle einer zusätzlichen Anmeldung und Authentifizierung wird auch dort das Facebook-Konto für den Login genutzt.

Betreiber externer Websites haben wiederum die Möglichkeit, Plugins [19] 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 gutheißen. Diese Meinungsbekundung auf der externen Website wird ebenfalls im eigenen Facebook-Profil sichtbar. [20, 21, 22]

Auch die mobile Nutzung wird von Facebook unterstützt. So gibt es für jede gängige mobile Plattform eine Anwendung, mit deren Hilfe auf Facebook zugegriffen werden kann. [23]

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

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. [24]

Finanzierung

Die Nutzung von Facebook ist kostenlos, da es sich hauptsächlich durch Einnahmen aus Werbung finanziert. Den Werbepartnern stellt Facebook weitreichende Informationen über die Nutzer zur Verfügung, damit die Einblendungen gezielt auf die jeweilige Person angepasst werden können. Dazu gehören unter anderem Alter, Geschlecht, Hobbys, Wohnort, politische Überzeugung, Lieblingsbücher und -filme, Bildungsstand sowie Hinweise auf persönliche Beziehungen.

Zusätzliche Einnahmen erzielt Facebook durch Investoren, die zum Teil sehr große Summen in das Unternehmen stecken.

Seit dem Börsengang 2012 hat Facebook alle Markterwartungen übertroffen. Vor allem die mobilen Nutzer sorgten für steigende Umsätze und Gewinne. Der Erfolg an der Börse und die hohen Werbeeinnahmen ermöglichen es Facebook, sich auch in anderen Geschäftsbereichen aufzustellen, was z.B. die Übernahmen

des Fotodienstes Instagram, des Messenger-Dienstes WhatsApp sowie des 3D-Brillenspezialisten Oculus VR belegen. [25]

Suchmöglichkeiten
Facebook bietet umfangreiche Suchmöglichkeiten, sowohl seitenintern als auch über externe Suchmaschinen. Gesucht werden können generell Personen (inkl. Bildern), Gruppen, Dinge, die Nutzern gefallen (Bands, Hersteller, …), Apps, 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 direkt auf der Facebook-Seite bezieht sich zunächst auf nahe Verbindungen, bevor weiter entfernte Verbindungen analysiert werden. Bei der Suche nach neuen Freunden schlägt Facebook zunächst Freundes-Freunde vor (je umfangreicher und direkter die Verlinkung mit einer Person ist, desto eher wird sie als Freund vorgeschlagen). Zudem besteht die Möglichkeit, E-Mail-Konten nach Kontakten, die Facebook nutzen, zu durchsuchen (vgl. dazu auch Abschnitt Datenschutz & Sicherheit).

Facebook bietet zudem eine als Graphensuche bezeichnete Funktion an. Diese Suchanfrage muss als (englischer) Satz formuliert werden, wie z.B. „People who are older than 50 and work at Freistaat Bayern" oder „My friends who like dogs". Die Graphensuche ermöglicht das Durchsuchen großer Datenmengen mit sehr spezifischen Informationen in sehr kurzer Zeit. Zur Ausführung der Suche werden die vom Nutzer öffentlich bereitgestellten Informationen herangezogen.

Überwachung des Nutzerverhaltens
Durch die große Anzahl von Informationen, die die jeweiligen Nutzer bereitstellen, können teilweise sehr weitgehende Rückschlüsse gezogen werden. Je nach Art der Information ist dies nicht nur für Facebook selbst, sondern auch für andere Teilnehmer des Netzwerks möglich. Bewusst bereitgestellte Informationen können z.B. Beziehungen zwischen Profilen (Familienmitgliedschaften, Freundschaften, Likes, öffentliche Kommentare), die Teilnahme an Veranstaltungen oder der Besuch bestimmter Orte sein.

Zu den häufig unbewusst bereitgestellten Informationen gehören beispielsweise besuchte Webseiten außerhalb von Facebook. Bei den beliebten „Gefällt-mir"-Buttons ist zu beachten, dass diese unter Umständen persönliche Daten übertragen, ohne angeklickt worden zu sein. So kann Facebook u.a. nachvollziehen, welche Seiten ein Benutzer besucht, wenn diese über einen „Gefällt-mir"-Button oder die Facebook-Kommentarfunktion verfügen. [26]

Eine Anfang Januar 2015 veröffentlichte großangelegte Studie der Universität Cambridge kam zu dem Ergebnis, dass bereits zehn geklickte „Like-Buttons" präzise Angaben zur eigenen Persönlichkeit in den Kategorien Offenheit, Pflichtbewusstsein, Verträglichkeit, Impulsivität und Geselligkeit ermöglichen. Dies ergab die Auswertung von 86.000 Facebook-Profilen und einer Befragung von 32.000 Versuchsteilnehmern, die selbst 100 Fragen zur eigenen Persönlichkeit beantworteten. Diese eigenen Angaben wurden mit einem anhand der Like-Buttons berechneten Persönlichkeitsprofil und dem Persönlichkeitsprofil, das Angehörige und Bekannte von dem jeweiligen Versuchsteilnehmer angegeben hatten, verglichen. Das Ergebnis brachte Überraschendes zutage: Bereits ab zehn „Gefällt mir"-Angaben konnte die Computersoftware die Persönlichkeit eines Probanden besser einschätzen als ein Arbeitskollege. 70 „Likes" reichten der Software aus, um zu einer besseren Einschätzung zu kommen als ein Freund oder Mitbewohner. Um Eltern oder Geschwister zu überflügeln waren 150 geklickte „Likes" nötig — für den Ehepartner mehr als 300. Der überraschend präzise Algorithmus der Software belegt, dass so künftig profilgemäße bzw. maßgeschneiderte Werbung gezielt platziert werden kann. Dass ein solch detailliertes Persönlichkeitsprofil auch für andere, im Zweifelsfall kriminelle Absichten bzw. für Zwecke der Spionage genutzt werden kann, sollte dabei nicht übersehen werden. [27]

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. Die indirekte Übertragung von persönlichen Informationen durch eingebettete „Gefällt mir"-Buttons kann im Firefox-Browser durch das Blockieren von Cookies für Drittanbieter verhindert werden. [28]

Neben den typischen Nutzer-Funktionen stellt Facebook auch eine umfangreiche Programmierschnittstelle bereit. Dadurch sind Anwendungsentwickler in der Lage, eigene Applikationen zu entwickeln und dabei auf Facebook-Daten zuzugreifen oder diese zu verändern. Dazu muss der Benutzer seine Einwilligung erteilen, die er allerdings zu jedem späteren Zeitpunkt widerrufen kann. Wenn die Einwilligung erteilt ist, kann die Software im Rahmen der erteilten Berechtigungen Daten lesen und schreiben. Der Nutzer erhält hierüber keine gesonderte Meldung mehr.

Administrationsmöglichkeiten für Profile und Konten
Die Administrationsmöglichkeiten für ein Profil sind umfangreich und auf verschiedene Positionen innerhalb der Plattform verteilt.

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

Durch die Einführung der „Timeline" wurden nicht nur die Funktionalitäten erweitert, sondern auch die Nutzer animiert, noch mehr Persönliches über sich preiszugeben. So entsteht ein virtueller und multimedialer Lebenslauf, der von Geburt bis zur Gegenwart reichen und Facebook ein noch effizienteres Zuschneiden von Werbe-Angeboten ermöglichen soll. Durch die vollständige chronologische Auflistung aller jemals hinterlassenen Informationen, Bilder oder Kommentare können z.B. 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. Die Privatsphäre-Einstellungen sollten hier ganz bewusst genutzt werden: zum einen, um einzuschränken, wer was sehen darf, zum anderen, um einzelne Beiträge gemäß ihrer Schutzwürdigkeit auf bestimmte Nutzer zu

beschränken bzw. aus der Chronik zu löschen. Eine aufmerksame Auswahl und Auslese ist grundsätzlich jedem privaten Nutzer empfohlen. Für Unternehmen, die ein Facebook-Profil betreiben, sollte es selbstverständlich sein, die veröffentlichten Informationen so einzustellen und zu pflegen, dass es ihrem Image dient und negative Rückmeldungen (im schlimmsten Fall Shit-Storms) vermieden werden.

Shit-Storm:
In sehr kurzer Zeit und großer Anzahl eingehende massive, aggressive Kritik.

Um die Sicherheit des Profils zu verbessern, 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 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.

Datenschutz und Sicherheit

Die AGB von Facebook gehören 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“.[29]

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.[30]

Seit Januar 2015 gelten neue Datenschutzbedingungen. Diese wurden bereits vor Ihrer Einführung stark kritisiert, da sie laut Auffassung mehrerer Studien gegen geltendes Europäisches Recht verstoßen. Die Vorwürfe weist Facebook allerdings zurück und verweigert bislang eine Korrektur. [31]

So sammelt Facebook weiterhin nicht nur Informationen von registrierten Mitgliedern, sondern hat z.B. 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." [31]

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. [32]

Eines der wichtigsten und aus Sicht des Datenschutzes fragwürdigsten Instrumente für Facebook bleibt die Datenerhebung für Werbezwecke. Durch die neuen AGB kann Facebook anhand der Standortdaten gezielt Werbeanzeigen schalten — zum Beispiel von nahegelegenen Geschäften oder Restaurants. Dies kann lediglich durch eine Deaktivierung der GPS-Verbindung oder einer Zugriffsblockade der Facebook-App auf das GPS-Modul des Smartphones umgangen werden. Darüber hinaus kann Facebook

künftig auch auswerten, welche anderen Webseiten die Nutzer im Netz besuchen und welche Apps sie verwenden. Wer dann beispielsweise online Wanderschuhe kauft, kann Werbung für Wanderurlaub oder weitere Outdoor Bekleidung erhalten.

Ziel des Unternehmens ist ferner, es dem User durch einen neu installierten „Kaufen"-Button zu ermöglichen, künftig auch direkt über das Facebook-Konto Waren zu bestellen. So kann Facebook neben den Nutzerdaten und Einkaufsgewohnheiten auch Zahlungsdaten der Kunden und mithin ein noch umfassenderes Personenprofil erhalten.

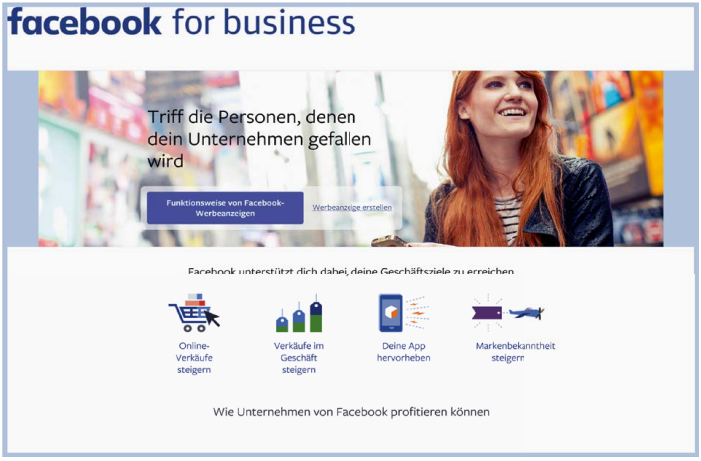
Durch die neuen AGB soll es den Nutzern zudem leichter gemacht werden, selbst zu entscheiden, wer ihre Inhalte sieht — dieses Datenschutzinstrument muss jedoch eigenständig aktiviert werden und betrifft nur sichtbare Daten gegenüber anderen Nutzern, nicht gegenüber Facebook selbst. Darüber hinaus können Nutzer durch einen Button in Werbeanzeigen herausfinden, warum eine Werbeanzeige gerade an sie gerichtet wurde. [33]

In der Vergangenheit gab es immer wieder Schadsoftware, die sich durch Sicherheitslücken über Facebook verbreiten konnte. Um dem vorzubeugen, wurde mit „Facebook Security" ein Sicherheitsteam etabliert, das zeitnah auf ungewöhnliche Vorfälle reagiert [34].

Auch für die Themen Jugendschutz [35] und Hass-Botschaften im Netz [36] hat Facebook in den letzten Jahren Verbesserungen vorgenommen. Mit „Facebook Safety" [37] wurde ein eigener Sicherheitsbereich für Familien geschaffen. Speziell für Krisenfälle wie Naturkatastrophen, Terroranschläge oder Amokläufe wurde 2015 die Funktion „Safety Check" [38] eingeführt. Damit können Facebook-Nutzer untereinander abfragen oder mitteilen, ob und wer sich innerhalb eines bestimmten Umkreises um den betroffenen Ort in Sicherheit befindet.

Facebook für Unternehmen
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 potenzielle Mitarbeiter zu rekrutieren. Allerdings sollten auch hier die im Kapitel „Analyse der Risiken und Gefahren von sozialen Netzwerken“ genannten Punkte (z.B. Negativkampagnen durch Shit-Storms) frühzeitig beachtet werden und ein professioneller Umgang durch einen verantwortlichen Unternehmensvertreter 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, fin-

den sich bei Facebook in der Regel Informationen aus Wikipedia, sofern dort ein Eintrag zum Unternehmen besteht.

Unternehmensprofile sind etwas anders strukturiert und haben etwas andere Funktionalitäten als private Profile. Um auf dem Laufenden zu bleiben, kann jede Privatperson ein Unternehmensprofil „liken" und wird so fortlaufend über die jeweiligen Neuerungen informiert. Auch eine Unternehmens-Seite kann eine andere „liken" — ein Einverständnis des Gegenübers (wie bei einer Freundschaftsanfrage) ist dazu nicht nötig.

Seit Januar 2015 testet eine Handvoll ausgewählter Unternehmen eine geplante neue Funktion: „Facebook at Work" [39]. Diese ist nicht dazu gedacht, das Unternehmen in Facebook zu präsentieren oder gar Business-Netzwerken wie Xing Konkurrenz zu machen. Es geht rein um die Vernetzung von Nutzern innerhalb eines Unternehmens, um aktiv die Zusammenarbeit zwischen Kollegen zu fördern und das Arbeitsgeschehen zu vereinfachen. Die Anmeldung soll allein Mitarbeitern eines für diesen (kostenpflichtigen) Dienst lizenzierten Unternehmens vorbehalten sein.

GOOGLE+

Netzwerk	Google+
URL	https://plus.google.com
Nutzer weltweit	3.091 Millionen registrierte Nutzer (Stand April 2016) [40], davon monatlich ca. 300 Millionen aktive Nutzer (Stand Juni 2016) [41]
Nutzer in Deutschland	Ca. 2 Millionen Nutzer (Stand Juni 2016) [42]
Hauptsitz	Mountain View, Kalifornien, USA
Gründungsjahr	Juni 2011 [43]

Bei Google+ handelt es sich um ein soziales Netzwerk, das von der Google Inc. betrieben wird. Es 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.

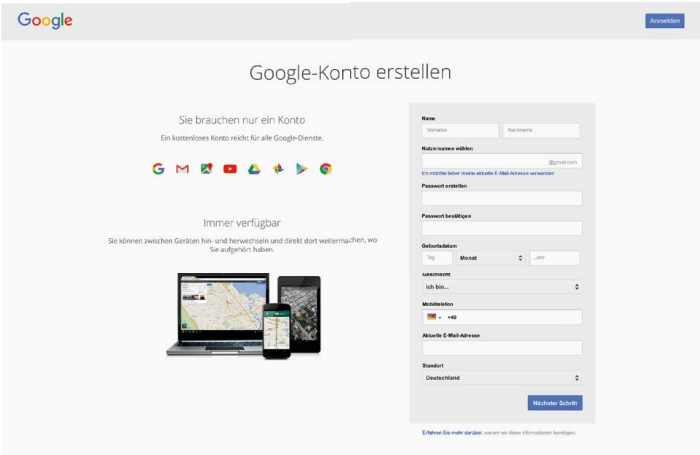
Google+ wurde in seiner Anfangszeit von der Presse als Angriff von Google auf Facebook gewertet. Allerdings bleiben die Nutzerzahlen von Google+ bis heute weit hinter den Erwartungen zurück. An der marktbeherrschenden Position von Facebook hat sich durch die Gründung von Google+ nichts geändert.

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 allerdings nicht mitgeteilt, in welchen Kreis er eingeordnet wurde. Der Aufbau von Kontakten funktioniert, ähnlich wie bei Twitter, asymmetrisch. 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.

Für das Senden von Nachrichten existiert bei Google+ seit 2013 die Funktion „Handouts" — eine Kombination aus den bisherigen Funktionen „Google Talk" und „Google+ Messenger". Dieses vollwertige Chatprogramm unterstützt auch Videotelefonie und ist

u.a. in Google Chrome und Android integriert. Nachrichten können an verschiedene Empfängerkreise adressiert 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. In jeder Art von Nachricht können andere

Nutzer verlinkt werden. So kann eine Person auf einem Foto markiert oder direkt im Text verlinkt werden. Darüber hinaus verfügt Google+ über eine Videochat-Funktion, die es ermöglich, dass bis zu zehn Personen gleichzeitig miteinander kommunizieren. 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 [44, 45].

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 z. B. 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.

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 die darin enthaltenen Personen, die Beiträge, die innerhalb des Streams ange-

zeigt werden sollen, und die Personen, die die Erlaubnis erhalten, den User auf Fotos zu markieren, definieren.

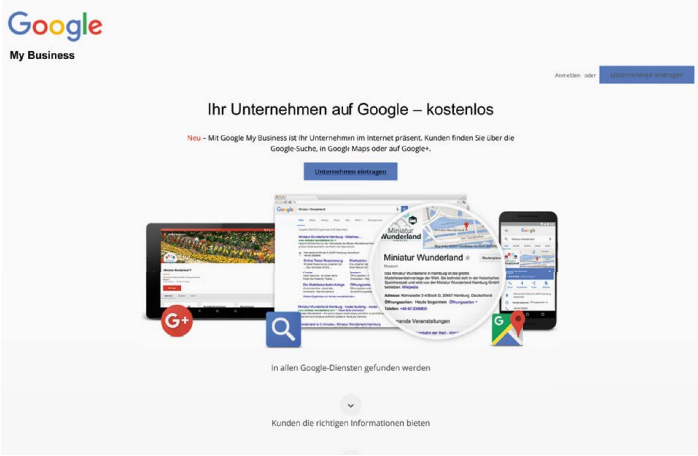
Datenschutz und Sicherheit

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.[46] 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.[47] 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."[47a] Google gibt jedoch ebenfalls zu bedenken, dass in bestimmten Fällen die Offenlegung der Userdaten auch ohne Genehmigung der Betroffenen möglich ist. Dazu zählen unter anderem:

- Verstöße gegen gesetzliche Bestimmungen,
- Anordnungen in gerichtlichen Verfahren,
- die Untersuchung von Verstößen gegen die Nutzungsbedingungen,
- die Bekämpfung von Betrug oder
- die Behebung technischer Probleme.

Des Weiteren behält sich Google das Recht auf Weitergabe der Daten vor, um „das Eigentum oder die Sicherheit von Google, seinen Nutzern und der Öffentlichkeit, soweit dies gesetzlich zulässig oder erforderlich ist, vor drohendem Schaden zu schützen".[48]

Wie bei allen Google-Services ist der Datentransport zwischen Benutzer und Google mittels SSL verschlüsselt. [49]



Google+ für Unternehmen

Mit „Google My Business“ bietet Google Unternehmen die Möglichkeit, sich über Google zu präsentieren. Unternehmen können somit für ihre Kunden in der Google-Suche, auf Google Maps und auf Google+ präsent sein, um so zusätzlich unternehmensspezifische Informationen anzubieten. Über eine Bewertungsplattform können Kunden dann das Unternehmen hinsichtlich ihrer Zufriedenheit bewerten. Die „Google+ für Unternehmen“-Seiten ähneln den personenspezifischen Google+-Seiten.

TWITTER

Netzwerk	Twitter
URL	https://twitter.com/
Nutzer weltweit	ca. 3,7 Mrd. (Stand März 2016) [50]
Nutzer in Deutschland	320 Millionen (Stand: Februar 2016) [51]
Hauptsitz	San Francisco, Kalifornien, USA
Gründungsjahr	März 2006

Twitter ist ein Mikroblogging-Dienst, der im Jahr 2006 von Jack Dorsey, Biz Stone und Evan Williams gegründet wurde. Oft als „öffentliches Tagebuch" im Internet bezeichnet, können Nutzer hier in Echtzeit telegrammartige Kurznachrichten mit maximal 140 Zeichen verbreiten. Als Kommunikationsplattform und soziales Netzwerk wird Twitter von Privatpersonen, Unternehmen und Organisationen genutzt. Das Veröffentlichen von Nachrichten („Tweets") wird als „Twittern" bezeichnet und dient dem Austausch von Gedanken oder der öffentlichen Meinungsäußerung zu einem bestimmten Thema. [52]

Typischer Inhalt und Kommunikationsmethoden

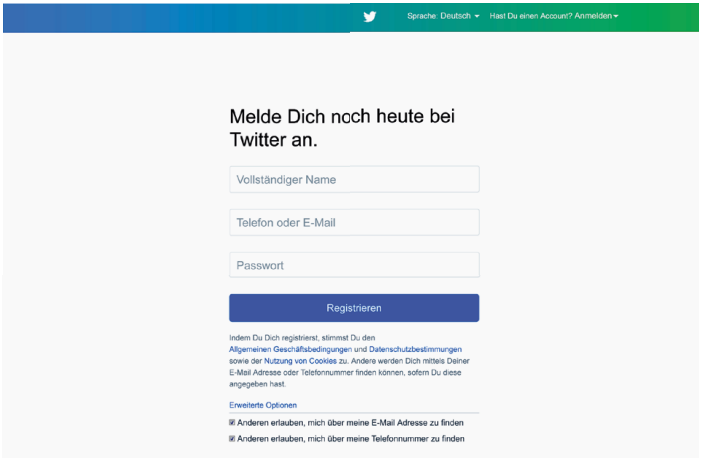
Für die Nutzung von Twitter ist eine Anmeldung mit Namen, E-Mail und Passwort notwendig. Danach kann man sich alternativ mit E-Mail-Adresse, Telefonnummer und Benutzername und Passwort auf dem Portal selbst oder einer der Apps für mobile Endgeräte einloggen. Jeder Account hat die Möglichkeit, verschiedenen Personen oder Institutionen zu folgen (sog. „Following"). Dies 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 (sogenannter „Follower") weiterleiten. Außerdem kann der Tweet als Favorit markiert werden, was dem „Liken" bei Facebook ähnelt. Der Nutzer kann (und sollte) jeweils entscheiden, ob er die Nachricht jedem Nutzer oder nur seinen Followern zur Verfügung stellen möchte.

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, Prominenten und Pres-

severtretern beliebt: Der japanische Premierminister informierte 2011 über Twitter zur aktuellen Lage in Fukushima. Beim Aufstand in Ägypten 2011 wurde Twitter zur Verbreitung politischer Meinungen genutzt. Auch beim Amoklauf in München am 22. Juli 2016 wurde Twitter von der Münchner Polizei gewinnbringend eingesetzt, um die Bürger zeitnah und in mehreren Sprachen über die Vorkommnisse zu informieren.[53]

Hier wird auch der Unterschied zu Facebook deutlich. Während Facebook vorwiegend der Kommunikation im Bekanntenkreis dient, ist Twitter eher ein Informationsnetz [54], das mehr und mehr auch gesellschaftspolitische Bedeutung gewinnt.

Twitter kann mittlerweile auch auf allen gängigen mobilen Geräten genutzt werden, so z.B. über iPhone oder Android. Außerdem bietet Twitter einen SMS-Service an, der es Nutzern ermöglicht, Nachrichten zu empfangen, auch wenn sie keines der genannten Smartphones besitzen.



Um neue Follower zu gewinnen, können Twitter-Buttons auf Homepages platziert werden. Auf den Internetpräsenzen vieler Medien besteht 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 einbinden.[55]

Finanzierung
Während sich Twitter zu seinen Anfangszeiten fast ausschließlich durch Risikokapital finanzierte, stützt sich das Unternehmen mittlerweile nahezu vollständig auf Werbeeinnahmen. Der Börsengang im November 2013 brachte Twitter 2,1 Milliarden USD ein. Obwohl die Zahl der Nutzer weltweit steigt, kämpft Twitter mit dem Rückgang der Umsatzzahlen und sinkendem Börsenwert.

Suchmöglichkeiten
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 und MSN Messenger 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 in den Einstellungen deaktiviert werden. Außerdem können im Profil eines Twitter-Nutzers 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.

Administrationsmöglichkeiten 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 öffentlicher Einsicht schützen, anderen Nutzern erlauben oder verbieten, den eigenen Account in Fotos zu taggen oder unbekannte Follower blockieren. Die Kommunikation zwischen dem Anwender und der Twitter-Seite ist standardmäßig verschlüsselt.

taggen:
Das eigene Profil auf Fotos verknüpfen.

Datenschutz und Sicherheit

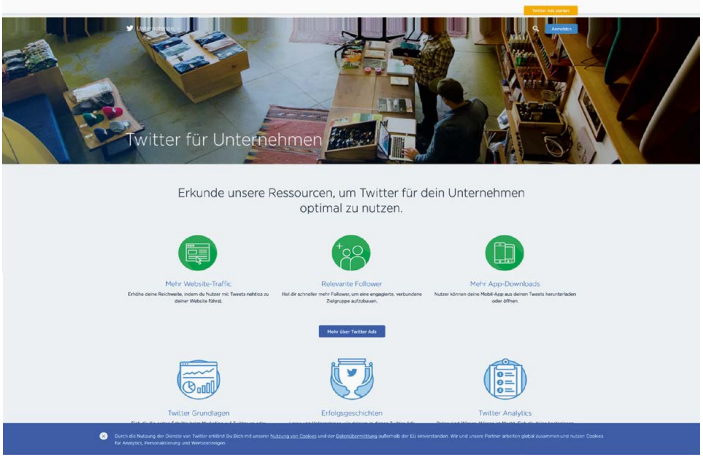
Gemäß dem Kapitel „Ihre Rechte" in den AGB von Twitter liegen die Rechte für alle Inhalte beim Nutzer. Dennoch räumt sich Twitter die nicht-exklusive, gebührenfreie und weltweite Erlaubnis ein, die Inhalte in sämtlichen jetzt bekannten oder später entwickelten Medien oder Vertriebsmethoden zu benutzen, 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. [56]

Im Abschnitt „Austausch und Offenlegung von Informationen" in der Twitter-Datenschutzrichtlinie 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 persönliche Daten von Nutzern an Dritte weitergegeben werden. In der Vergangenheit wurde Twitter aufgrund von Sicherheitslücken bereits mehrfach 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. [57] Ein Fehler im Twitter-Dienst „t.co" führte 2010 zu einer automatisierten Verbreitung von Nachrichten unter den Followern der Betroffenen. [58]

In den darauffolgenden Jahren verschoben sich die Sicherheitslücken in Richtung der Anwendung „TweetDeck", die wie eine Nachrichtenzentrale funktioniert, in der alle Tweets, Messages und Gruppen eines Nutzers sortiert und suchfähig dargestellt werden. Hier war es beispielsweise im April 2012 möglich, ohne weiteres Zutun auf die Konten anderer Teilnehmer zuzugreifen oder im Juni 2014 fremden JavaScript-Code auf der Plattform ausführen zu lassen.

Twitter für Unternehmen
Bei Unternehmen ist Twitter eines der beliebtesten sozialen Netzwerke.

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, so dass eine direkte Kommunikation zwischen Unternehmen und Kunden ermöglicht wird. Als weiteren Vorteil bewerten viele Firmenvertreter und Kunden die Kürze der Twitter-Nachrichten. Damit beschränken sich Beiträge auf das Wesentliche und lassen sich gegebenenfalls um einen Link für zusätzliche Informationen erweitern. [59]



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

FourSquare: Standortbasierter Empfehlungsdienst für Restaurants und andere Orte.

LINKEDIN

Netzwerk	LinkedIn
URL	https://de.linkedin.com/
Nutzer weltweit	Ca. 400 Millionen (Stand Juli 2016) [60]
Nutzer in Deutschland	Ca. 8 Millionen Nutzer (Stand Juli 2016) [60]
Hauptsitz	Mountain View, Kalifornien, USA [61]
Gründungsjahr	Mai 2003 [61]

LinkedIn ist das weltweit größte Business-Netzwerk mit ca. 400 Millionen registrierten Mitgliedern — ca. 8 Millionen davon im deutschsprachigen Raum. Auf LinkedIn können sich sowohl Arbeitnehmer als auch Firmen und Arbeitgeber präsentieren, Kontakte knüpfen und networken. Zudem existieren viele technische Möglichkeiten, die das Recruiting innerhalb der Plattform für entsprechende Accounts erheblich vereinfachen. LinkedIn vereint somit die Merkmale eines klassischen Business-Netzwerks mit denen einer Recruiting- und Jobvermittlungsplattform.

Seit 2006 bietet das internationale Netzwerk seine Dienste auch auf Deutsch an. Gegenüber dem rein national ausgerichteten Konkurrenten XING punktet LinkedIn mit seiner Internationalität und wird auch in Deutschland immer beliebter.

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 sowie ihre persönlichen Interessen.

Diese Selbstdarstellung ist wie ein Lebenslauf aufgebaut und hilft Unternehmen, auf Bewerber aufmerksam zu werden. Mittels Schlagworten können Nutzer ihre Interessen benennen, die unter der gleichnamigen Rubrik abgelegt und für andere somit suchfähig sind. Zusätzlich gibt es die Möglichkeit, Profilbilder zu erstellen, seine eigene Webseite und Instant-Messanger-Konten zu verlinken, einen Lebenslauf zu veröffentlichen oder weitere persönliche Merkmale wie Zertifizierungen oder ehrenamtliches Engagement anzugeben. Mitglieder können sich untereinander empfehlen und Unternehmensprofile erstellen, über die Produkte beworben oder empfohlen werden. [62]

Die Kommunikation der Mitglieder untereinander kann auf verschiedenen Wegen erfolgen. Am häufigsten wird die auf der Plattform integrierte Nachrichtenfunktion verwendet. So können gegenseitig Nachrichten versandt werden, ohne dass Dritte mitlesen. Alternativ stehen themenspezifische Gruppen zur Kommunikation und Diskussion zur Verfügung. Zudem können mittels der sogenannten „Pulse-Funktion" Äußerungen veröffentlicht und so von anderen Mitgliedern eingesehen, kommentiert, bewertet und empfohlen werden.

Eine Besonderheit von LinkedIn ist das „Persönliche Netzwerk", dessen Auf- und Ausbau gezielt gefördert wird. Zum einen können nicht-zahlende Mitglieder umfangreicher mit Mitgliedern interagieren als mit „Fremden". Dazu zählt beispielsweise auch das Versenden von Nachrichten oder das Einsehen bestimmter Profilbereiche.

Zum anderen bietet LinkedIn verschiedene Möglichkeiten, um persönliche Bekannte oder Geschäftskontakte zu entdecken. So können z.B. Listen mit Mailadressen an die Plattform übermittelt werden, die dann mit registrierten Nutzern abgeglichen werden. Alternativ lassen sich auch die eigenen Mail-Daten hinterlegen, so dass LinkedIn die Online-Konten der angemeldeten Nutzer damit abgleicht, um Treffer aufzuspüren. Unter anderem werden folgende Informationen der Mitglieder gespeichert: Name, Geburtsdatum, Geschlecht, Wohnort, Jobbezeichnung, Mail-Adressen, Telefonnummern, Webseiten und Notizen.

Finanzierung
Die Einnahmen von LinkedIn kommen zum größten Teil aus Werbeanzeigen und Gebühren, etwa für Personalagenturen. Das Angebot zahlungspflichtiger Mitgliedschaften für Profile mit erweiterten Funktionen macht den kleineren Teil aus. Seit 19.5.2011 ist LinkedIn an der Börse.

Suchmöglichkeiten
Allen Mitgliedern steht ein umfangreiches Angebot an Suchfunktionen zur Verfügung wie z.B. eine Suche nach Personen- bzw. Firmennamen oder Berufsbezeichnung, nach Hochschulen und Ausbildungsstätten. 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
- Karrierestufen
- Unternehmensgrößen

Sobald ein Mitglied sich mit einem der oben genannten Punkte identifiziert, ist es gleichartig verlinkten Personen möglich, das jeweilige Profil direkt einzusehen. LinkedIn ergänzt (sofern möglich) die jeweiligen Profildarstellungen um einen Graphen, aus dem ersichtlich ist, auf welchem Weg die Profile miteinander verbunden sind (gemeinsame Freunde, Firmen, Freundes-Freunde, etc.).

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. Hier kann zwischen „alle", „nur Kontakte" (bis zu einem vorgegebenen Grad), „Netzwerk" und „Niemand" ausgewählt werden. Dabei sind bestimmte Daten in der Standard-Einstellung öffentlich sichtbar, können aber nachträglich eingeschränkt werden. [63, 64, 65]

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:

- Einstellungen für Zahlungsmodalitäten kostenpflichtiger Profile
- Einstellungen für die Privatsphäre auf der Plattform
- Werbe-Einstellungen
- Einstellungsmöglichkeiten für Daten, die Dritten auf dem eigenen Profil angezeigt werden können
- Grafische Anpassungen des eigenen Profils

Mitglieder können eine Liste der Daten, die LinkedIn über sie erhoben hat und die auf keinem anderen Weg abgefragt werden können, unter einem speziellen Link beantragen und sich per Mail zusenden lassen.

Überwachung des Nutzerverhaltens
Ähnlich wie bei anderen sozialen Netzwerken werden Informationen über Änderungen am eigenen Profil automatisch an die jeweiligen Kontakte übermittelt und dort als Benachrichtigung angezeigt. In den Privatsphäre-Einstellungen besteht allerdings die Möglichkeit, dies zu ändern. LinkedIn macht selbständig Vorschläge, wann das sinnvoll sein kann (z.B. „Sie sollten diese Funktion eventuell deaktivieren, wenn Sie auf Stellensuche sind und nicht möchten, dass Ihr derzeitiger Arbeitgeber sieht, dass Sie ihr Profil aktualisieren").

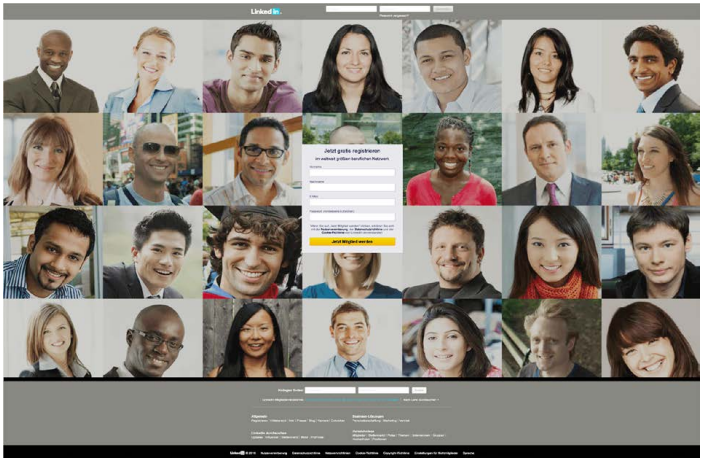
Durch weitere Einstellungen im Privatsphäre-Menü kann differenziert werden, welche Gruppe von Profilbesuchern auf welche Bereiche des Profils Zugriff erhält. Bei einer unzureichenden Konfiguration stehen die Daten sonst einer unbeabsichtigt großen Menge an Personen zur Verfügung.

Datenschutz und Sicherheit
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." 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". [66]

Im Mai 2011 wurde eine gravierende Sicherheitslücke bei der Anmeldung von LinkedIn-Mitgliedern gefunden. Diese bestand darin, dass die Authentifizierungs-Token der Mitglieder unverschlüsselt übertragen und gespeichert wurden. Erhielt ein Angreifer darauf Zugriff, konnte er das betreffende Konto übernehmen. 2012 gelang es einem Hacker, 6,5 Millionen Accounts zu knacken und die zu schwach verschlüsselten Passwörter in Untergrundforen zu veröffentlichen (sog. „LinkedIn-Hack"). Um Hürden für Angreifer zu schaffen, führte LinkedIn im Mai 2013 die Zwei-Faktor-Authentifi-

Zwei-Faktor-Authentifizierung: Nutzer-Identitätsnachweis mittels der Kombination zweier unabhängiger Komponenten/Faktoren.

zierung ein. Sofern vom Nutzer aktiviert, ist hier die Eingabe eines per SMS versendeten Codes notwendig, wenn der Nutzer sich von einem bislang noch nie verwendeten Gerät aus anmelden will.



Die schwerwiegenden und weitreichenden Folgen des Hacks aus 2012 zeigten sich erst vier Jahre später: Seit Mai 2016 werden ca. 117 Millionen entschlüsselte LinkedIn-Passwörter im Darknet zum Verkauf angeboten (pro Stück ca. 5 Bitcoins/2000 Euro). [67]

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.

XING

Netzwerk	XING
URL	https://www.xing.com
Nutzer weltweit	Mehr als 15 Millionen (Stand März 2015) [68]
Nutzer in Deutschland, Österreich, Schweiz	10 Millionen (Stand Juli 2016) [69]
Hauptsitz	Hamburg, Deutschland
Gründungsjahr	2003

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 die Suche nach Stellenangeboten bzw. Bewerbern und der Aufbau eines Business-Netzwerks.

Momentan zählt XING weltweit etwa 15 Millionen Mitglieder, wovon ca. 10 Millionen Nutzer aus dem deutschsprachigen Raum (Deutschland, Österreich, Schweiz) stammen.

Typischer Inhalt und Kommunikationsmethoden
Wie viele andere Netzwerke setzt XING auf das sogenannte „Freemium-Modell", d.h. die Basismitgliedschaft wird gratis angeboten, — Erweiterungen sind nur in der kostenpflichtigen Premiummitgliedschaft (monatliche Gebühr) enthalten.

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

Treffen. 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. Um die Kommunikation zwischen den Teilnehmern weiter auszubauen, wurde das Programm Skype in die XING-Oberfläche integriert. Dadurch können andere Nutzer erkennen, ob der jeweils gewünschte Gesprächspartner momentan online erreichbar ist.

Für die aktive Stellensuche bietet XING eine Jobbörse an. In dieser können Nutzer sowohl nach freien Stellen suchen als auch selbst Angebote einstellen. Umgekehrt können als Recruiter registrierte Personen Profile gezielt nach definierten Kriterien durchsuchen.

Recruiter: Personalvermittler

Finanzierung

XING finanziert sich hauptsächlich durch sein Premium-Modell. Nach der Gründung 2003 erhielt das soziale Netzwerk Risikokapital von Business Angels und strategischen Partnern. Zwei Jahre später investierte das Unternehmen Wellington Partners weitere

5,7 Mio. Euro. Seit Dezember 2006 werden die Aktien des sozialen Netzwerks an der Börse gehandelt. [70]

Eine zusätzliche Einnahmequelle von XING sind verschiedene kostenpflichtige Dienste wie die Jobbörse „Xing Stellenanzeigen", das Premium-Zusatzpaket ProJobs oder das E-Recruiting. [71, 72]

Suchmöglichkeiten
Mitglieder können in der XING-Datenbank nach anderen Mitgliedern, Unternehmen, Gruppen, Neuigkeiten, Veranstaltungen und Stellenangeboten suchen. Für Gratis-Mitglieder sind die Suchmöglichkeiten allerdings stark eingeschränkt. Komplexere Suchanfragen mit Kriterien wie bisherige oder aktuelle Arbeitgeber, Beschäftigungsart, Wohnort und berufliche Position sind nur für zahlende Nutzer möglich.

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.

Zu den konfigurierbaren Optionen gehören unter anderem: Sichtbarkeit der eigenen Kontaktliste für andere Mitglieder, erlaubte Absendergruppen für Nachrichten, Inhalt und Sichtbarkeit der eigenen Aktivitäten auf der Plattform und die Zugehörigkeit zu verschiedenen Gruppen. Eine vollständige Liste aller Privatsphäre-Einstellungen finden angemeldete Mitglieder unter: https://www.xing.com/app/settings?op=privacy. Da jedes XING-Profil standardmäßig auch für Nicht-Mitglieder zugänglich ist, sollten User diese Funktion in ihren Privatsphäre-Einstellungen ebenfalls deaktivieren. Falls Nutzer keine unerwünschten Einträge in ihrem Gästebuch wollen, besteht in den Kontoeinstellungen die Möglichkeit dies zu deaktivieren.

Zur Einschätzung, welche Einstellungen sich auf andere Teilnehmer auswirken, bietet XING eine Ansicht des eigenen Profils aus „Sicht eines Nicht-Kontakts" an.

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.[73]

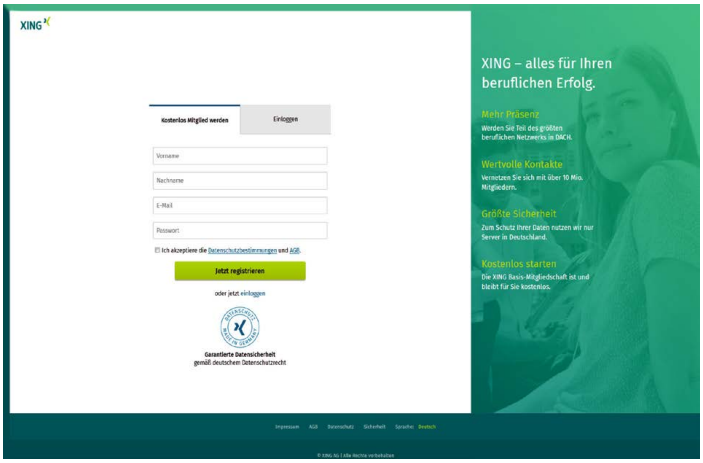
Um seinen Usern eine gefahrlose Nutzung des sozialen Netzwerks zu gewährleistet, wird auch bei XING die Datenverbindung SSL-verschlüsselt. Trotz dieser Sicherheitsmaßnahme kam es im Jahr 2009 zu einem sicherheitskritischen Vorfall. Dabei fälschten Angreifer die Systemmails von XING und schickten diese 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. [74]

Die von XING genutzten Rechenzentren für die unmittelbare Datenverarbeitung befinden sich ausschließlich in Deutschland. Daten, die im Auftrag von XING, weiterverarbeitet werden, bleiben laut eigenen Angaben „innerhalb der EU". Zusätzlich zur Verschlüsselung überwacht XING das Verhalten von Nutzern und die Registrierung auf „ungewöhnliches oder angriffsähnliches Verhalten".

Überwachung des Nutzerverhaltens
Je nach Konfiguration der Privatsphäre-Einstellungen können Dritte sehr weitreichende Informationen über den Nutzer erhalten. Dies gilt insbesondere dann, wenn dieser Dritte in der Kontaktliste des Nutzers steht. In diesem Fall besteht sogar die Möglichkeit, sich automatisiert über Änderungen im Profil informieren zu lassen. Diese Funktion kann in den Einstellungen unter „Ihre Aktivitäten" deaktiviert werden.

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.

SINA WEIBO

Netzwerk	Sina Weibo
URL	http://www.weibo.com
Nutzer weltweit	600 Mio. registriert , 261 Mio. aktive Nutzer (Stand Mai 2016)
Nutzer in Deutschland	Nicht bekannt
Hauptsitz	Peking [76]
Gründungsjahr	2009 [77]

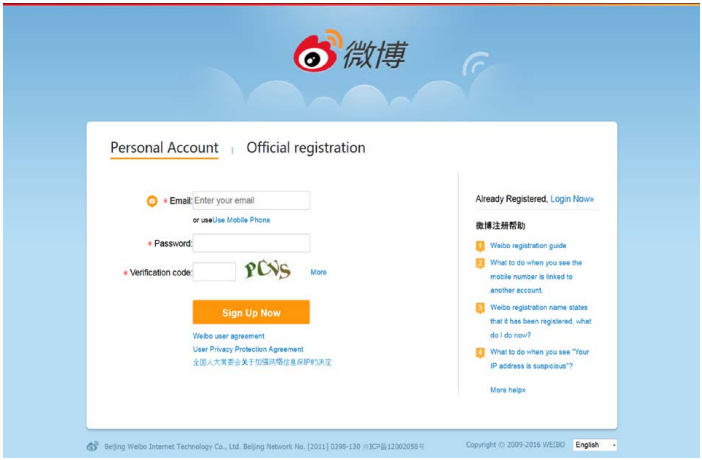
Sina Weibo ist das chinesische Äquivalent zu Twitter. Der chinesischsprachige Mikroblogging-Dienst wurde im Jahr 2009 von der Sina Corporation gegründet, nachdem soziale Netzwerke wie Facebook oder Twitter von der chinesischen Regierung vollständig gesperrt worden waren.[77] Das Netzwerk verfügt neben der Kernfunktion zum Veröffentlichen und Austauschen von Kurznachrichten auch über wenige Möglichkeiten der sozialen Interaktion. Auf der Plattform können sich sowohl Personen als auch Unternehmen und Institutionen präsentieren.

Laut Angaben des Netzwerks selbst waren zwischen 2009 und 2013 mehr als 500 Millionen Nutzer registriert. Diese Zahlen wurden nach einer Untersuchung von Forschern der Universität Hongkong angezweifelt. Die Überprüfung von 30.000 zufällig ausgewählten Profilen hatte ergeben, dass über 57% ohne Inhalt oder erkennbare Aktivität waren. [78]

Typischer Inhalt und Kommunikationsmethoden
Sina Weibo wird aufgrund der strengen Zensur in der VR China von der Regierung selbst überwacht und kontrolliert. Die Kommunikationsmethoden ähneln denen von Twitter stark. Nutzer können Kurznachrichten mit bis zu 140 Zeichen publizieren und mit diesen an öffentlichen Diskussionen teilnehmen. Sowohl die Farbgebung als auch die Möglichkeiten mit „@“ Nutzer zu verlinken oder mit „#“ ein Hashtag zu publizieren, ähneln dem verbotenen westlichen Konkurrenten.

Zusätzlich können zwei oder mehr Nutzer über die private Chat-Funktion miteinander kommunizieren.

Suchmöglichkeiten
Die primäre Suche funktioniert über E-Mail-Adresse oder Handynummer — dies kann vom Nutzer aber relativ einfach deaktiviert werden. In den Profilen können u. a. Informationen zu Geschlecht, Beziehungsstatus und Blutgruppe bis hin zu Bildung, Beruf und postalischer Anschrift eingestellt werden.



Administrationsmöglichkeiten für Profile und Konten
Nutzer von Sina Weibo haben verschiedene Einstellungsmöglichkeiten, um ihre Außenwirkung oder die Kommunikation mit anderen individuell anzupassen. Neben der Auswahl, ob das jeweilige Profil über die E-Mail-Adresse oder die Handynummer gefunden werden kann, ist auch die Veröffentlichung der Ortsangabe bei Nachrichten zu- oder abschaltbar. Unerwünschte Nutzer oder Kommentare können mittels „Blacklist“ ausgeschlossen werden. Auf gleiche Weise können auch Inhalte mit bestimmten Schlüsselwörtern oder Drittanbieter-Apps blockiert werden.

Das kostenpflichtige „VIP-Programm“ bietet darüber hinaus weitere Filtermöglichkeiten.

Überwachung des Nutzerverhaltens
Wie alle chinesischen sozialen Netzwerke unterliegt auch Sina Weibo dem Einfluss der staatlichen Zensur, die fortwährend ausgebaut wird. Dies zwingt die Nutzer u.a. dazu, ihre Klarnamen auf der Plattform zu hinterlegen. So können die ca. 40.000 auf den verschiedenen Plattformen angemeldeten Zensurbeamten sehr einfach Urheber von Nachrichten identifizieren. Accounts, Nachrichten oder Verknüpfungen zu zensierten Themen werden schnellstmöglich gesperrt oder gelöscht.

Zusätzlich existieren technische Zensur-Vorrichtungen, mit denen z.B. die Suche nach bestimmten Schlagwörtern oder Posts mit unerwünschtem Inhalt unterbunden werden kann. Im März 2012 wurde so zur Eindämmung von Gerüchten über einen Putschversuch sogar die themenspezifische Kommentarfunktion plattformübergreifend für 5 Tage komplett gesperrt. [79]

Datenschutz und Sicherheit
Nichts bekannt

VK

Netzwerk	VK
URL	https://vk.com [80]
Nutzer weltweit	Über 300 Millionen registrierte Nutzer (Stand Juni 2015) [81]
Nutzer in Deutschland	Über 10 Millionen Nutzer (Stand Juni 2015) [82]
Hauptsitz	Russland
Gründungsjahr	2006

VK ist das russische Äquivalent zu Facebook. Mehrheitseigner und Besitzer von VK (bis Jan. 2012 Vkontakte.ru) ist mail.ru Mit seinen über 300 Millionen registrierten Nutzern bildet VK die am zweithäufigsten besuchte Seite in Russland und belegt im weltweiten Ranking Platz 22. Optik und Funktionsumfang sind sehr stark an Facebook angelehnt. Eine Besonderheit an VK ist die Möglichkeit für User, sich online Videos, Bilder und sogar komplette Filme direkt auf der Plattform anzusehen.

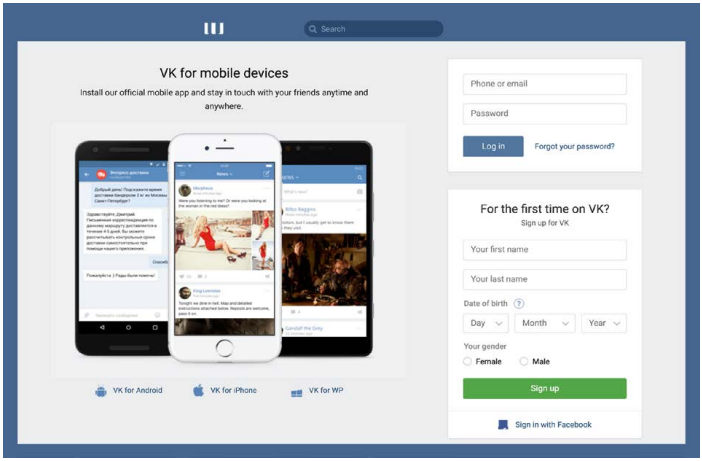
Typischer Inhalt und Kommunikationsmethoden
Auch die Kommunikationsmethoden ähneln dem Vorbild und Konkurrenten Facebook. VK bietet seinen Nutzern die Möglichkeit, sich untereinander durch private oder Gruppen-Chats auszutauschen, Nachrichten innerhalb der Plattform zu versenden oder sich in Gruppen mit angeschlossenen Foren zu organisieren. Es können „Events" oder Ereignisse erstellt und andere Teilnehmer dazu eingeladen werden.

Pinnwandeinträge, Ereignisse, Fotos und andere Objekte können mit anderen Nutzern geteilt werden. Bei Bildern besteht zusätzlich die Möglichkeit, andere Personen darauf zu markieren bzw. auf das Bild oder einen Fließtext zu verlinken.

Eine Besonderheit, mit der sich VK von anderen sozialen Netzwerken abhebt, ist die Synchronisations-Funktion. Über diese Verknüpfung des VK-Profils mit anderen sozialen Netzwerken (z.B. mit Facebook oder Twitter) werden veröffentlichte Inhalte auch dort geteilt und Kommentare oder Antworten, die dort eingehen, ebenso auf dem Ursprungs-Profil angezeigt.

Finanzierung
Die Finanzierung des börsennotierten Unternehmens erfolgt sowohl über den Verkauf von Aktien als auch zu einem wesentlich geringeren Teil durch Werbung.

Am 16. September 2014 gewann der russische Internetkonzern Mail.ru nach längeren Auseinandersetzungen die vollständige Kontrolle über VK. Die Übernahme der verbliebenen 48,01% kostete Mail.ru umgerechnet 1,47 Milliarden USD. Hinter dem Kauf steht der russische Mehrheitseigner Alisher Usmanov. Der milliardenschwere Oligarch gilt als enger Freund von Präsident Putin. Menschenrechtsorganisationen werteten daher den Kauf als weiteren Beleg für eine Ausweitung der Internetkontrolle und Beschneidung der Meinungsfreiheit in Russland.



Der Gründer und ehemalige Chef von VK wurde bereits im April 2014 als CEO abgesetzt, nachdem er sich eigenen Aussagen zufolge weigerte, dem russischen Inlandsgeheimdienst FSB Nutzerdaten zu übermitteln. [83]

Suchmöglichkeiten
Ähnlich wie in vergleichbaren Netzwerken kann gezielt nach veröffentlichten Profil-Attributen anderer Nutzer gesucht werden:

- Land/Region
- Schule/Universität
- Alter/Geschlecht
- Beziehungsstatus
- Religion
- Prioritäten, Tabak- und Alkoholkonsum
- Adresse (Land, Stadt, Straße)
- Arbeit/Rang
- Militärdienst (Land & Diensteintritt)
- Geburtsdatum

Die Suche ermöglicht eine Verknüpfung der Attribute, sodass sich relativ einfach große Personengruppen gezielt durchsuchen und filtern lassen.

Administrationsmöglichkeiten für Profile und Konten
Die Administrationsoberfläche des Nutzerkontos ermöglicht es dem Anwender, festzulegen, welche Benutzergruppen Zugang zu welchen Informationen des Profils haben dürfen. Der Zugriff auf folgende Inhalte kann eingeschränkt werden:

- Profil: Profil, Fotos, Videos, Communities, Audiodaten, Geschenke, Orte, Freunde
- Einträge: Kommentare auf Pinnwand lesen/schreiben, Kommentare zu Einträgen lesen/schreiben
- Kontakt- Möglichkeiten: Nachrichten, Anrufe, Einladen in Communities, Einladungen zu Apps, Freundschaftsanfragen
- Benutzergruppen können sein: Jeder, Freunde, Freundesfreunde, Alle außer, nur bestimmte Personen (jeder außer Suchmaschinen)

Durch die Vielzahl an Möglichkeiten wird der Anwender in die Lage versetzt, die Sichtbarkeit seines Profils sehr individuell und feingranular an die eigenen Bedürfnisse anzupassen.

Datenschutz und Sicherheit
Nichts bekannt

ANALYSE DER RISIKEN UND GEFAHREN VON SOZIALEN NETZWERKEN

Dieses Kapitel befasst sich mit den möglichen Risiken und 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 Faktoren (wie Arbeitszeiten und Geschäftsgeheimnisse) eines Unternehmens negativ beeinflussen können.

Verlust von Ansehen

Soziale Netzwerke sind speziell für das Ansehen von Unternehmen eine Herausforderung und sollten in ihrer Bedeutung nicht unterschätzt oder gar ignoriert werden. Nicht nur, ob oder wie sich ein Unternehmen in sozialen Netzwerke 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 Nutzers 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 sind keine effektive Lösung

Pressemitteilungen oder andere klassische Gegenmaßnahmen 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 für das Unternehmen.[84]

Des Weiteren sind folgende Szenarien denkbar bzw. bereits eingetreten: Mitarbeiter eines Unternehmens veröffentlichen (Sta-

tus-) 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 Mitarbeitern werfen ein unprofessionelles Licht auf Unternehmensangehörige 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.[85]

Auch das „Like-“Verhalten einiger Mitarbeiter kann zu einem Ansehensverlust in der Öffentlichkeit führen. Dies hat sich im Jahr 2011 bei Daimler gezeigt[86]. 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[87]. Auch Konkurrenten können zielgerichtet falsche Gerüchte streuen, um den Ruf eines Unternehmens zu schädigen.[88] Unternehmen sollten schon aus diesen Gründen aktiv und möglichst „rund um die Uhr“ Eigen- oder Fremddarstellungen im Internet beobachten. Nur so kann schnell und effektiv auf unerwünschte bzw. schädliche Inhalte reagiert werden.

Entscheidet sich ein Unternehmen dafür, in sozialen Netzwerken aktiv zu werden, müssen vorher Zuständigkeiten geklärt und Verantwortlichkeiten geschaffen werden. Ein solcher Internetauftritt muss durchgehend gepflegt und aktualisiert werden und die Interaktion mit den Nutzern muss gewährleistet sein. 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 beieinander liegen.[89]

Unternehmen sollten alle Möglichkeiten nutzen, sich gegen einen Ansehensverlust durch die Nutzung sozialer Netzwerke zu schützen: Zufriedene Mitarbeiter, regelmäßig überprüfte Firmenprofile und Löschungen von zweifelhaften Postings sowie notfalls auch das Sperren dieser Netzwerke sind nur einige davon. Zusätzlich bieten die meisten 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 [90], 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.[91]

Mobbing in sozialen Netzwerken ist ein immer häufiger auftretendes Phänomen. [92] Experten schätzen, dass Mobbing alleine in Deutschland jährlich zu einem volkswirtschaftlichen Schaden von über 6 Milliarden Euro führt.[93] 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 sind online wesentlich geringer

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.[94]

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

- Verschlechterung des Arbeitsklimas
- Minderung der Produktivität [95]
- Überdurchschnittlich viele Krankheitstage von Mitarbeitern
- Imageschaden für die Firma, da die Informationen nicht nur für Kollegen sichtbar sind [96]

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 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[97], 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 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.[98]

Kurzlinks: Speicherung einer langen URL bei einem externen Anbieter, welcher diese über eine kurze Adresse weiterleitet.

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

Präparierte Apps oder Links

Mit Apps wie „Wer hat mein Profil angesehen“ können sich z.B. Facebook-Nutzer durch einen Klick mit Malware infizieren. Nach Bestätigung der AGB verschickt die App unbemerkt Nachrichten, die für Phishing, Betrugs- sowie Spam- und Malware-Aktionen genutzt werden. Nach dem gleichen Prinzip funktionieren präparierte Links, die den Nutzer mit vermeintlichen Werbegeschenken, Verlosungen, Gutscheinen oder angeblichen Benachrichtigungen zu Erweiterungen oder Updates locken.[99]

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+“.[100] 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.[101] 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 Nutzer sie häufig besuchen muss, um sich auf dem aktuellen Stand zu halten. Außerdem gehört es zu den Geschäftsprinzipien der meisten Netzwerke, den Nutzer 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.[102] Häufig ist erst nach dieser Zeit wieder derselbe Grad an Produktivität erreicht wie vor der Störung. Sol-

che 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.[103]

Verlust von Firmenkontakten durch Wechsel 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 Gemeinschaftsportals) Status-Nachrichten lesen, Fotos sehen und weitere private Details entnehmen.

Eine besondere Rolle spielen hierbei die so genannten „locationbased services", also Dienste, die ortsgebundene Nutzerdaten auswerten. Dabei stellt der Nutzer meist seinen aktuellen Standort zur Verfügung. Angefangen hat dies mit Gowalla (inzwischen eingestellt) und Foursquare[104]. Mittlerweile bieten aber auch Google mit „Google Places" [105] sowie Facebook mit „Facebook Places" (in Deutschland „Facebook Orte") [106] entsprechende Dienste an. Auch Twitter hat seine mobile Anwendung um den Standort des Nutzers erweitert.[107] 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.

Ortung deaktivieren

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.

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.[108] 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, dass z.B. der Sicherheitschef nicht vor Ort ist. Zudem besteht die Gefahr, dass aus Ortsdaten bestimmter Personen Rückschlüsse auf strategische Unternehmensentscheidungen gezogen werden können: Die häufige Präsenz von Entscheidungsträgern an bestimmten Orten könnte beispielsweise auf Verhandlungen mit einer dort ansässigen Firma hinweisen.

Durch die Nutzung dieser Dienste lassen sich Bewegungsprofile erstellen, die Aufschluss über Wohnort, Arbeitsplatz, Freizeitaktivitäten und Reisen geben.[109] 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 Bundesdatenschutz-

gesetz (BDSG). Die Informationen über den Aufenthaltsort einer Person unterliegen dem Schutz personenbezogener Daten und erfordern in jedem Fall das Einverständnis des Benutzers.[110] Aus diesem Grund müssen sich auch entsprechende Dienste leicht ein- und ausschalten lassen.

Erpressung
Die Fälle von Online-Erpressung mittels sozialer Netzwerke mehren sich. Die Erpresser legen es dabei zunächst darauf an, kompromittierendes Bildmaterial ihrer Zielperson zu erlangen. Dazu wird beispielsweise über Dating-Portale ein Erstkontakt hergestellt, der dann durch Video-Chats (z.B. über Skype) weiter ausgebaut wird. Dem Opfer werden dabei Videoaufnahmen vorgeführt, die seine vermeintliche Online-Bekanntschaft in erotischen Posen zeigen. Zugleich wird er aufgefordert, sich seinerseits ebenfalls vor der Webcam zu entblößen. Das Video-Telefonat wird heimlich aufgezeichnet und später als Grundlage für eine Erpressung genutzt. Dazu wird dem Opfer ein noch nicht frei gegebener Youtube-Link mit der Aufzeichnung geschickt und die Überweisung eines Geldbetrages gefordert, um zu verhindern, dass das Video veröffentlicht wird. Wer bezahlt, muss damit rechnen, wiederholt mit Forderungen in zunehmender Höhe konfrontiert zu werden.[111]

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 zu übernehmen.

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.[112]

Ebenfalls kritisch ist, dass der Angreifer mit der gestohlenen Identität andere Nutzer des sozialen Netzwerks, die diese Person ken-

nen, 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 [113]. 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, entwickelte 2011 ein Team von Sicherheitsexperten das JAVA-Tool „Facebook Pwn“ [114]. 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 es 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 das Tool automatisiert eine Freundschaftsanfrage an das ausgewählte Opfer. Sobald dieser die Freundschaft bestätigt, kopiert „Facebook Pwn“ alle Daten, die es erlangen kann, auf die Festplatte. Dies soll verhindern, dass der Zugriff auf die Daten verloren geht, wenn das Opfer den Schwindel durchschaut. Durch solche Tools sind auch umfangreichere Attacken für Angreifer ohne technisches Verständnis problemlos möglich.

ABLAUF TYPISCHER ANGRIFFE

Soziale Netzwerke sind eine Möglichkeit, um unbemerkt und unerkannt Informationen über Unternehmen und deren Mitarbeiter zu erlangen. Angreifer können diese Informationen nutzen, um tiefer in die Unternehmensstruktur einzudringen. Die weiterführenden Erkenntnisse werden oft missbraucht, um eine Social-Engineering-Attacke oder einen Hacking-Angriff zu starten. Dies erfolgt in der Regel mit dem Ziel, Daten des Unternehmens (z.B. Patente, Kundendateien, Baupläne) zu kopieren, zu löschen oder zu manipulieren.

Wie werden Informationen beschafft?
Im Kapitel „Populäre soziale Netzwerke" wurden einige der bekanntesten sozialen Netzwerke beschrieben. Gerade die teilweise oder überwiegend beruflich genutzten Netzwerke basieren auf Angaben zu Beruf, fachlicher Qualifikation, persönlichem Werdegang und aktuellem Arbeitgeber. 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 die Ergebnisse zu präzisieren, werden anschließend die Profile herausgesucht, die für einen Angriff am erfolgversprechendsten erscheinen, d.h. am meisten Daten über die Person, ihre Aufgaben im Betrieb und das Unternehmen als Ganzes veröffentlicht 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 XING bietet sich für solche Attacken an, da hier umfangreiche und teils sehr detaillierte Informationen gespeichert sind.

Wie geht es weiter?
Erscheinen die erlangten Informationen für einen erfolgreichen Angriff auf ein Unternehmen noch unvollständig, wird ein Hacker versuchen, an zusätzliche Daten zu kommen und diese geschickt miteinander zu verknüpfen. Dafür wird häufig ein bekannter Trick

angewendet: Da Menschen selten in sämtlichen sozialen Netzwerken aktiv sind, macht sich der Angreifer diesen Umstand zu Nutze und erstellt im Namen des Opfers einen der fehlenden Accounts. Da er aus den Vorrecherchen weiß, dass Person A mit Person B beispielsweise über XING befreundet ist, B jedoch keinen Facebook-Account hat, kann er sich dort unter Angabe des Namens von B anmelden und Informationen über B hinterlegen (die Informationen stammen aus den frei einsehbaren XING-Daten, zum Beispiel Arbeitgeber und 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 Awarenessgrad 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 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 Methoden relativ leicht die Möglichkeit, gezielt Schadcodes in das Unternehmensnetz zu schmuggeln. Häufig reicht der Klick auf den E-Mail-Anhang eines vertrauenswürdig wirkenden Absenders um das Firmennetz im Anschluss auszuforschen, zu schädigen oder für Erpressungsversuche zeitweise lahmzulegen.

FALLBEISPIELE

Der Awarenessgrad ist selbst in IT-Abteilungen oder Führungsetagen großer Unternehmen nach wie vor nicht überall ausreichend hoch. Während die Sensibilität im Umgang mit Facebook gewachsen ist, geben viele Berufstätige in überwiegend beruflich genutzten Netzwerken wie XING immer wieder Informationen preis, die von Angreifern missbraucht werden können.

Erfolgreiche Attacken lassen sich kaum mit Informationen aus nur einem Netzwerk durchführen - meist werden Daten aus verschiedenen sozialen Netzwerken, privaten Homepages, Firmenwebseiten und whois-Abfragen zusammengeführt und kombiniert, so dass ein umfassendes und präzises Bild über das Opfer entsteht.

Beispiel 1 - Adresse des Wohnorts
Über XING konnte der Systemadministrator eines Unternehmens ausfindig gemacht werden. 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 ebenfalls auf XING gefunden. Dort bezeichnete er sich selbst als Linux-Experte im Bereich von Web-, Datenbank-, und Virtualisierungsservern sowie der Spambekämpfung und Netzwerksicherheit im Linux-Umfeld. Aus diesen Angaben kann ein Angreifer wertvolle Informationen über das Netzwerk des Unternehmens gewinnen. So kann er mit hoher Wahrscheinlichkeit davon ausgehen, dass dort mit dem Betriebssystem Linux gearbeitet wird.

Beispiel 3 - Personen mit geringer Security-Awareness
Ein Mitarbeiter eines Unternehmens hatte einen Account bei XING. 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

gehörten. Im Facebook-Profil wurde festgestellt, dass die Person sog. Likejacking-/Clickjacking-Seiten angesehen und auf den „Gefällt mir"-Button geklickt hatte. Ein Angreifer kann diese Tatsache als Angriffspunkt auf die Person ausnutzen, indem er ihr auf Facebook selbst erstellte Likejacking-/Clickjacking-Seiten schickt, die beim „Liken" zu einer Seite weiterleiten, die wiederum Schadcodes auf dem Rechner des Opfers ausführt.

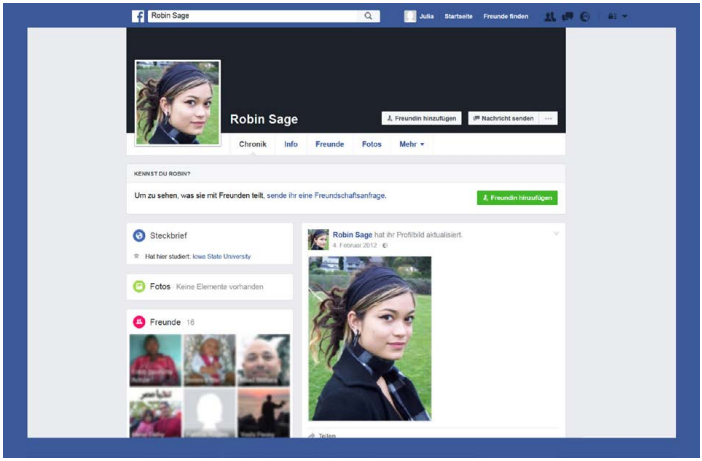
Beispiel 4 - Indirekte Informationen ausnutzen
Die Führungskraft eines Unternehmens hatte einen XING-Account, der zusätzlich u.a. mit einem Twitter-Profil verlinkt war. Dort fiel auf, dass die Person eine Reihe von Koordinaten ihrer Fahrradtouren hochgeladen hatte. Die genauere Analyse dieser Daten zeigte, dass die Touren immer am gleichen Ort starteten bzw. endeten. Da sich dieser Punkt in einer Ortschaft befand, war der Rückschluss auf den Wohnort der Person naheliegend. Eine langfristige Auswertung regelmäßig durchgeführter Touren ermöglichte zudem Hinweise auf den Tagesablauf der Person und ließ Rückschlüsse zu, wann diese außer Haus ist.

Beispiel 5 — Kompromittierende Aufnahmen
Ein leitender Mitarbeiter eines renommierten Unternehmens war bei einer Partnerbörse angemeldet. Eine Frau, die er dort kennengelernt hatte, motivierte ihn dazu, sich selbst bei sexuellen Handlungen zu filmen. Diese kompromittierenden Aufnahmen wurden als Grundlage für eine Erpressung verwendet. Da die Aufnahmen später auf Youtube eingestellt und eine gewisse Zeit recherchierbar waren, wurden sowohl der Name des Mitarbeiters als auch des Arbeitgebers bekannt. Nachdem die Situation sowohl für den Mitarbeiter als auch für das Unternehmen untragbar wurde, verständigte man sich auf die einvernehmliche Beendigung des Beschäftigungsverhältnisses.

Bekannte Beispiele aus der Öffentlichkeit
In den letzten Jahren ereigneten sich einige aufsehenerregende Vorfälle, die deutlich aufzeigen, wie weitreichend Angriffe unter Zuhilfenahme sozialer Netzwerke oder darin enthaltener Informationen sein können.

Fall 1: Das Experiment

2009 erstellte der New-Yorker-Sicherheitsspezialist Thomas Ryan unter dem fiktiven Namen „Robin Sage“ eine virtuelle Identität, die er mit einem beeindruckenden Lebenslauf und dem Foto einer attraktiven, jungen Frau ausstattete und für die er in mehreren sozialen Netzwerken Profile einrichtete.[115] Die fiktive Person wurde dargestellt als „25-jährige Absolventin des Massachusetts Institute of Technology (MIT) und Analystin für Cyber-Sicherheit bei der US-Marine“. Über ihre Profile nahm sie gezielt Kontakt zu einem großen Personenkreis auf — überwiegend aus den Bereichen Militär, Wirtschaft und Rüstung. Nach einem Monat beendete Thomas Ryan das Experiment. In dieser Zeit hatte sich sein fiktiver Charakter mit über 300 Personen angefreundet (davon über 80% Männer) und eine unerwartet große Menge teilweise sogar als geheim eingestufter Informationen bekommen (Kontonummern, Standorte und Bilder von Militäreinrichtungen u.ä). Zudem waren Jobangebote von mehreren großen Unternehmen aus der IT- und Rüstungsbranche eingegangen.



Das Experiment zeigte: Durch geschickte Manipulation ist es ohne großen Aufwand und innerhalb kürzester Zeit möglich, auch Personen, bei denen berufsbedingt eine erhöhte Vorsicht zu erwarten ist, dazu zu bringen, internes Wissen preiszugeben.[116]

Fall 2: Phishing (CEO-Fraud)

Einer der „teuersten" Cyber-Betrugsfälle der letzten Jahre ereignete sich Anfang 2015 in den USA. Hier brachten Betrüger einen Manager dazu, sukzessive 17,2 Millionen Dollar auf ein chinesisches Bankkonto zu überweisen. Mittels Social-Engineering war dem Mann suggeriert worden, dass es sich hier um einen direkten Auftrag seines Geschäftsführers handelte und von dieser Transaktion außer ihm niemand wissen dürfte. Als „Beweis" sollte sich der Manager beim angeblichen Mitarbeiter einer Rechnungsprüfungsgesellschaft rückversichern — dessen Daten lieferten die Betrüger in der gefälschten E-Mail gleich mit. Da es sich bei der geheimen Transaktion angeblich um die Übernahme einer chinesischen Firma handelte, überwies der Manager die Summe in drei Teilbeträgen auf ein Konto in China. Eine kurze Rücksprache mit dem Geschäftsführer als vermeintlichem Auftraggeber war dem Manager nicht rechtzeitig in den Sinn gekommen, hätte dem Unternehmen aber nicht nur den finanziellen Schaden, sondern auch einen Reputationsverlust erspart.[117]

Fall 3: Dating-Portal gehackt

Mit rund 40 Millionen Mitgliedern ist „AdultFriendFinder" das größte Datingportal weltweit. Hackern gelang es im Mai 2015, knapp 4 Millionen Datensätze zu stehlen — darunter auch Profile, die bereits gelöscht sein sollten. In die Hände der Cyber-Kriminellen gelangten dadurch nicht nur die Identitäten der jeweiligen Nutzer, sondern auch intimste Informationen aus deren Privatleben [118]. Innerhalb kürzester Zeit wurden die entwendeten Daten veröffentlicht und teilweise für Spam- und Phishing-Attacken genutzt. Zu befürchten ist zudem, dass die gestohlenen Daten auch für Erpressungsversuche genutzt werden, möglicherweise mit dem Ziel, wirtschaftliche, politische oder militärische Geheimnisse zu erfahren.

Fall 4: „Facebook-Gate"

Bis in die 90er Jahre waren alle Informationen rund um den Chef des englischen Geheimdienstes MI6 als „top secret" eingestuft — sogar dessen Name sollte nicht bekannt werden, so dass die Kurzbezeichnung „C" (für „Chief") geschaffen wurde. Ganz anders im Jahr 2009: Zum Amtsantritt des neuen „C", John Sawers, wurde ein ganzes Portfolio an privaten Informationen und Fotos öffentlich. Sawers' Frau, eine begeisterte und offensichtlich

ahnungslose Facebook-Nutzerin, teilte ihre Postings nicht nur mit „Freunden“ sondern bedenkenlos mit der gesamten Öffentlichkeit. Fotos in Badehose, Freundschaften mit mehr oder weniger fragwürdigen Personen sowie die Informationen über persönliche Vorlieben brachten John Sawers beruflich in höchste Bedrängnis.[119]

Fall 5: RSA und Lockheed Martin

Der Hack von RSA und Lockheed Martin im Jahr 2011 ist ein Musterbeispiel für einen sog. Advanced Persistent Threat (APT). 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.

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.

Für den Zugriff auf sein Netzwerk nutzte Lockheed Martin sog. RSA SecurID-Token zur Netzwerkauthentifizierung. Jeder Benutzer verwendet dabei ein Gerät in Form eines Schlüsselanhängers, das, in einem zeitlichen Intervall von 60 Sekunden, einen eindeutigen und für Außenstehende nicht vorhersagbaren SecureID-Token generiert. Dieser Token basiert auf einem geheimen, von RSA entwickelten Algorithmus, den sich die Angreifer durch einen Zugang zum RSA-Netzwerk verschafften mussten. Dazu wurden E-Mails mit Excel-Anhang an ausgewählte Angestellte der Firma verschickt.

Da die Mails gezielt an einen bestimmten Empfängerkreis und jeweils in Kopie an drei weitere Personen gesendet wurde, ist davon auszugehen, dass sich die Hacker vorher auch in sozialen Netzwerken über die Angestellten der Firma RSA informiert hatten.

In den Excel-Anhang betteten die Angreifer einen sog. Flash-Code ein. Bei der Ausführung dieses Flash-Codes wurde eine Schwachstelle im Adobe Flash Player ausgenutzt, um eine „Backdoor“ zu schaffen. Dadurch war es dem Programm möglich, sich mit dem Server der Domain good.mincesur.com zu verbinden und so dem Angreifer volle Systemkontrolle von außen zu eröffnen. Im weiteren Verlauf des Angriffs verschaffte sich der Angreifer die notwendigen Rechte im Netzwerk, um auf den geheimen Algorithmus zuzugreifen, der so den Zugang in das Intranet von Lockheed Martin ermöglichte. [120, 121, 122]

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

EMPFEHLUNGEN FÜR DEN 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 Handlungsempfehlungen, die im Unternehmen kommuniziert, umgesetzt und 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 diese auch von zuhause aus ansurfen. Effektiveren Schutz versprechen vor allem Awareness-Maßnahmen, wie sie im Weiteren aufgezeigt werden.

Grundprinzipien

Soziale Netzwerke ermöglichen eine persönliche und berufliche Vernetzung, die zunehmend wichtiger wird und deren Vorteile jeder ganz individuell nutzen kann. Allerdings ergeben sich dadurch auch Risiken, derer sich ebenso jeder Nutzer bewusst sein sollte — ob im privaten oder beruflichen Kontext. Der verantwortungsvolle Umgang mit sozialen Netzwerken ist daher von elementarer Bedeutung.

Verhaltensweisen

Die Webseiten www.focus.com[123] und cio.wisc.edu[124] schlagen eine Reihe von Verhaltensrichtlinien vor, mit deren Hilfe Benutzern nahegelegt wird, diskret, skeptisch (hinsichtlich Geschäftsinformationen und -angeboten aus solchen Netzwerken), durchdacht und professionell zu handeln sowie Privatsphäre-Einstellungen sicher zu konfigurieren.

Aus den dargestellten Risiken und Gefahren lassen sich entsprechend weitere Verhaltensweisen ableiten, u.a. keine firmeninternen Informationen (auch nicht indirekt) in sozialen Netzwerken zu veröffentlichen. Mit Informationen, die von Dritten erhalten werden, sollte ebenfalls mit Vorsicht und einem gesunden Misstrauen umgegangen werden, da diese möglicherweise gar nicht von der Person stammen, für die sich der Absender ausgibt. Die Datensparsamkeit, bzw. das Einstellen möglichst weniger persönlicher Informationen ist ein Grundprinzip im sicheren Umgang mit sozialen Netzwerken. Als positiver Nebeneffekt, zusätzlich zum Schutz des Unternehmens, kann so auch für jeden Einzelnen das Risiko eines Identitätsdiebstahls reduziert werden.[125, 126]

Awareness von Mitarbeitern und privater Umgang mit sozialen Netzwerken

Es ist von besonderer Bedeutung, Mitarbeiter durch Schulungen über die bekannten Gefahren zu sensibilisieren und dabei auch Familienangehörige entsprechend mit einzubeziehen. Dadurch soll verhindert werden, dass Angreifer an schützenswerte Informationen gelangen, wenn ein Mitarbeiter, der seine eigenen Daten aus beruflichen Gründen schützen muss, einen Lebenspartner hat, der das gesamte Privatleben veröffentlicht. Beispielsweise kann ein möglicher Angreifer leicht herausfinden, zu welchem Zeitpunkt ein Sicherheitschef nicht vor Ort ist, wenn er sich laut Facebook-Nachricht gerade im Ausland aufhält oder seine Frau gemeinsame Urlaubsfotos vom Strand postet.

Schulungen in diesem Bereich können entweder von externer Seite oder unternehmensintern durchgeführt werden. Die Bereitstellung von Informationsmaterial allein reicht jedoch nicht aus. Die Vermittlung der Thematik im direkten, möglichst persönlichen Kontakt mit den Mitarbeitern mit der Möglichkeit Fragen zu stellen und einzelne Problemstellungen zu erörtern, wird dringend empfohlen. Dabei sollten nicht nur die oftmals sehr technischen Aspekte der Angriffsmöglichkeiten vermittelt, sondern vielmehr ein Gefühl für die Bedeutung dieser Gefahren transportiert werden. Wichtig ist, über die Zusammenhänge von Beruf und Privatleben sowie die möglichen wechselseitigen Auswirkungen zu sprechen. Im zweiten Schritt sollten Verhaltensrichtlinien vereinbart werden.

Periodische Awareness-Schulungen

Wissen in einem so schnelllebigen Themenfeld veraltet schnell. Deshalb werden periodische Awareness-Schulungen empfohlen, um Kenntnisse in diesem Bereich auf dem aktuellen Stand zu halten. E-Learning-Systeme können dabei den Aufwand überschaubar halten.

Beispiele für Richtlinien

Firmen setzen immer häufiger Richtlinien bzw. Policies ein, mit denen Verhaltensweisen in Bezug auf die Nutzung sozialer Netzwerke geregelt werden, aber auch um Mitarbeitern verständlich zu machen, 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, weshalb ein bestimmtes Verhalten notwendig ist. Beispiele für entsprechende Policies verschiedenster namhafter Unternehmen finden sich unter: http://socialmediagovernance.com/policies.php [127].

Schutz der Firma und des Mitarbeiters

Als positives Beispiel ist die Policy der Firma IBM hervorzuheben, da sie nicht nur dem Schutz des Unternehmens, sondern auch dem der Mitarbeiter dient.[128] Diese Guideline wird in regelmäßigen Abständen überarbeitet und gepflegt, so dass darin auch technische Neuerungen berücksichtigt sind. Mitarbeiter werden mit der Richtlinie 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. Beim Versand von Video- Bild-, und Tonmaterial sollte auf entsprechende Urheberrechte und mögliche Rechtsverletzungen geachtet werden. Falls in sozialen Netzwerken Themen diskutiert werden, die in direktem Bezug zum Unternehmen stehen, 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 ist in der Policy der BBC ausgeführt: „The personal use of the internet by BBC staff must be tempered by an awareness of the potential conflicts that may arise“[129]. Die Nachrichtenagentur Reuters hat in einer entsprechenden Veröffentlichung zudem die Anmerkung eingefügt, Informationen aus dem Netz auf Falschmeldungen (sog. Hoaxes) zu untersuchen, bevor diese einer Weiterverwendung zugeführt werden dürfen. Speziell finden sich bei Reuters auch Hinweise zur Verwendung von Twitter. Dabei wird gefordert, vor der professionellen Verwendung von Twitter Rücksprache 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.[130]

Eine weitere, bemerkenswert übersichtliche Policy ist die der Daimler AG.[131] Sie 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.[132]

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. Vor überstürztem Antworten auf Beiträge und Kommentare wird hier gewarnt — 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.[133]

Handlungsempfehlungen

Für Unternehmen

1. Keine schützenswerten Unternehmensinformationen publizieren. Es sollte das Prinzip gelten: Geheimes bleibt geheim - Internes bleibt intern. Sie sollten sich die Frage stellen: Wissen alle Mitarbeiter, welche Informationen offen, vertraulich oder streng vertraulich sind und kennen alle Mitarbeiter den entsprechenden Umgang?

2. Zurückhaltung mit offensiven persönlichen Meinungen. Wie das Beispiel der Daimler-Mitarbeiter im Zusammenhang mit Stuttgart 21 zeigt, 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.[134]

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 immer wieder 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". Um den Aufwand gering zu halten, können Sie sich Anregungen bei der BITKOM[135] oder in der Policy Database von „Social Media Governance" holen.[127]

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

Des Weiteren haben zahlreiche Unternehmen ihre Social Media Guidelines online zur Verfügung gestellt, die kostenlos eingesehen werden können.[136] Diese Veröffentlichungen enthalten auch wertvolle Informationen für Mitarbeiter. So wird der Leser in den Apple Blogging Guidelines darauf hingewiesen, achtsam bei der Nutzung sozialer Netzwerke zu sein, da die Grenzen zwischen privater und beruflicher Sphäre sich dort schnell vermischen.[137]

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 oder allzu vielen internen Details.

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 diese als verbindliche Regelung in die Arbeitsverträge mit auf.

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. Ähnliches 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 einen Bewerber einstellen.

4. Überprüfen Sie Ihre „Privatsphäre"-Einstellungen und regulieren Sie diese entsprechend Ihrer tatsächlichen Nähe zu dem Personenkreis, der Ihre Veröffentlichungen 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. Dabei sollten möglichst wenig Details über die derzeitige Tätigkeit eingestellt werden, um hier keine Angriffspunkte zu bieten.

6. Um zu überprüfen, was bereits offen über Sie im Netz recherchierbar ist, sollten Sie regelmäßig Ihren eigenen Namen in den verschiedenen Suchmaschinen überprüfen. 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.

Grundsätzlich gilt:
Verhalten Sie sich in sozialen Netzwerken den Mitgliedern gegenüber so, wie Sie es auch im realen Leben tun würden.

FAZIT

Die bekannten Richtlinien für den Umgang mit sozialen Netzwerken unterscheiden sich ganz individuell von Unternehmen zu Unternehmen. Einheitliche Standards wurden in diesem Bereich noch nicht geschaffen, doch lässt die Recherche der bisherigen Policies erkennen, dass die Wichtigkeit der Thematik 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 (können).

Daraus kann geschlossen werden, dass eine Kombination der wichtigsten Regeln bekannter Unternehmen (speziell IBM, Daimler, BBC und Reuters) als Basis für die Erstellung einer für das eigene Unternehmen angepassten Policy genutzt werden kann.

Jedes Unternehmen, das selbst in sozialen Netzwerken aktiv ist, sollte nach Möglichkeit eine 24/7-Betreuung des eigenen Profils sowie der dort von anderen Nutzern hinterlassenen Postings gewährleisten.

Die zentrale Empfehlung lautet, die Nutzung sozialer Netzwerke während der Arbeitszeit nicht nur von administrativer Seite zu untersagen, sondern das Bewusstsein sämtlicher Mitarbeiter (inkl. Führungspersonal) für die aus sozialen Netzwerken resultierenden Risiken und Gefahren zu schärfen. Der richtige und „unternehmenskonforme“ Umgang sollte klar festgeschrieben, innerhalb des Unternehmens kommuniziert und in geeigneten Schulungsmaßnahmen vermittelt werden — ggf. auch mit externer Hilfe. Mögliche Folgen bei Zuwiderhandlungen im Rahmen der privaten Nutzung sollten ebenso klar und nachvollziehbar sein.

QUELLENVERZEICHNIS

1 www.sign-lang.uni-hamburg.de/projekte/slex/seitendvd/konzepte/l53/l5385.htm

2 https://hinsehen.net/2015/05/01/smartphone-also-bin-ich

3 Deloitte-Studie – „Datenland Deutschland — Die Generationenlücke“: http://www2.deloitte.com/de/de/pages/presse/contents/datenland-deutschland-2015.html

4 www.bpb.de/internationales/afrika/arabischer-fruehling/52420/die-rolle-der-neuen-medien

5 http://de.newsroom.fb.com/company-info

6 https://de.wikipedia.org/wiki/Liste_der_Staaten_der_Erde

7 Wood, P.: Symantec Intelligence Report für November 2011: https://www.synabtec.com/de/de/about/news/release/article/jsp?prid=201111007_01

8 Focus Online – Porsche verhängt Facebook-Verbot für Mitarbeiter: https://www.focus.de/finanzen/karriere/berufsleben/wirtschaftsspionage-porsche-verhaengt-facebook-verbot

9 Statista.com – Soziale Netzwerke-Besucherzahlen Deutschland: http://de.statista.com/statistik/daten/studie/209595/umfrage/entwicklung-der-vistits-der-deutschen-social-networks

10 http://de.statista.com/statistik/daten/studie/244178/umfrage/aktiven-twitter-nutzerzahlen-weltweit-prognose

11 Wikipedia – Soziales Netzwerk (Internet): https://de.wikipedia.org/wiki/Soziales_Netzwerk_(Internet)

12 WhatsApp: https://de.wikipedia.org/wiki/WhatsApp

13 Nutzerzahlen WhatsApp: http://sueddeutsche.de/digital/messenger-whatsapp-hat-mehr-als-eine-milliarde-nutzer-1.2845262

14 Altersstruktur der WhatsApp Nutzer in Deutschland: http://www.de.statista.com/statistik/daten/studie/510985/umfrage/anteil-der-nutzer-von-whatsapp-nach-altersgruppen-in-deutschland

15 Facebook: https://de.wikipedia.org/wiki/Facebook

16 Soziale Netzwerke – Nutzerzahlen: http://www.socialmedia-institute.com/übersicht-aktueller-social-media-nutzerzahlen

17 Facebook Nutzer Deutschland: http://www.allfacebook.de/zahlen_fakten/erstmals-ganz-offiziell-facebook-nutzerzahlen-fuer-deutschland

18 Ranking der größten Social Networks und Messenger nach Anzahl der monatlich aktiven Nutzer (MAU): https://www.de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user

19 Wikipedia – Plug-in: http://de.wikipedia.org/wiki/Plugin

20 Zuckerberg, M.: Facebook Across the Web: http://blog.facebook.com/blog.php?post=41735647130

21 Becker, A.: Meedia – Bild.de vernetzt sich mit Facebook: http://meedia.de/internet/bildde-vernetzt-sich-mit-facebook/2009/04/16.html?tx_veguestbook_pi1%5Bpointer%5D=1&cHash=f619dd815814e33ab6c66231ca486a20

22 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

23 Facebook – Facebook-Handy: http://www.facebook.com/mobile/

24 Stiftung Warentest.: Soziale Netzwerke - Datenschutz oft mangelhaft: http://www.test.de/themen/computer-telefon/test/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-1855785/

25 Facebook im Shopping-Wahn – Alle Übernahmen auf einen Blick: https://t3n.de/news/facebook-kaufrausch-infografik-social-media-547027

26 Heise-Security – Das verrät Facebooks Like-Button: http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html

27 Holger Bleich – Globaler Abhörwahn, Wie digitale Kommunikation belauscht wird: http://www.heise.de/ct/artikel/Globaler-Abhoerwahn-1913829.html

28 Mozilla – Cookies von Drittanbietern blockieren: http://support.mozilla.com/de/kb/Cookies%20von%20Drittanbietern%20blockieren

29 Facebook – Terms of Service: http://www.facebook.com/legal/terms

30 Datenschutzbedingungen bei Facebook verstoßen gegen EU-Recht: http://www.haertig.de/neuigkeit/faq-safe-harbor

31 Bager, J.: heise online – Was Facebook über Nicht-Mitglieder weiß: http://heise.de/-921350

32 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

33 Neue Nutzungsbedingungen – Das müssen Facebook-Nutzer wissen: www.stern.de/digital/online/neue-agb-bei-facebook-das-muessen-sie-wissen-html

34 Facebook Security: https://de-de.facebook.com/security

35 Wilkens, A.: heise online – Facebook verschreibt sich besserem Jugendschutz: http://heise.de/-206824

36 Facebook gründet „Initiative für Zivilcourage Online“: http://www.heise.de/newsticker/meldung/Facebook-gruendet-Initiative-fuer-Zivilcourage-Online-3074600.html

37 Facebook Safety: https://www.facebook.com/safety

38 Facebook Safety Check: www.rp-online.de/digitales/internet/facebook-wie-funktioniert-der-safety-check-aid-1.5560017

39 Facebook at work: http://www.spiegel.de/netzwelt7web/facebook-at-work-soziales-netzwerk-fuer-firmen-a-1012946.htm

40 Registrierte Nutzer der Jahre 2012-2016 weltweit bei Google+: http://www.de.statista.com/themen/651/google

41 Monatlich aktive Nutzer bei Google+ (Stand Juni 2016): http://www.de.statista.com/themen/651/google

42 Google + Nutzer Deutschland: www.construktiv.de/blog/social-media/aktuelle-nutzerzahlen-fuer-die-social-media-landschaft-in-deutschland-2016

43 Wikipedia: Google+ — Wikipedia, Die freie Enzyklopädie: http://de.wikipedia.org/w/index.php?title=Google%2B&oldid=95049618

44 die-medienblogger.de – Heilsbringer Google+?, Die Medienblogger: http://www.die-medienblogger.de/722/heilsbringer-google

45 Google: Werbung und Datenschutz — Google Datenschutz-Center: http://www.google.com/intl/de/privacy/ads/

46 Google – Datenschutzbestimmungen, Google Datenschutz-Center: http://www.google.com/intl/de/privacy/privacy-policy.html

47 Google: Dashboard, https://www.google.com/dashboard/?hl=de

47a https://www.google.de/intl/de/policies/privacy/archive/20101003-20111020/

48 Google vs. Verbraucherschützer: www.cloud.irights.info/artikel/google-vs-verbraucherschuetzer-kleingedrucktes-bleibt-vorerst-beharrlich/19888

49 HTTPS – Google markiert bald alle Websites ohne SSL-Verschlüsselung: www.t3n.de/news/httsp-google-markiert-bald-alle-675146

50 Twitter.com — Nutzer weltweit: www.statista.com/statistic/daten/studie/2340/umfrage/monatlich-aktive-nutzer-von-twitte-weltweit

51 Twitter.com — Nutzer Deutschland: www.projeter.de/blog/social-media/aktuelle-nutzerzahlen-sozialer-netzwerke-2016

52 Twitter — Wikipedia, Die freie Enzyklopädie: https://de.wikipedia.org/wikipedia.org/wiki/Twitter

53 www.augsburger-allgemeine.de/comunity.profile/27315/Facebook-Twitter-und-Co-und-der-Amoklauf-in-Muenchen

54 FAZ.NET – 5 Jahre Twitter – 20 Millionen Meinungsmacher: http://www.faz.net/s/Rub4C34FD0B1A7E46B88B0653D6358499FF/Doc~E10F7D939A60E4BDD9C4F4109468FE823~ATpl~Ecommon~Scontent.html

55 Twitter Inc – Twitter Widgets: http://twitter.com/about/resources/widgets

56 Twitter Inc – Twitter Terms of Service: http://twitter.com/tos

57 Dhanjani, N.: Twitter and Jott Vulnerable to SMS and Caller ID Spoofing: http://www.dhanjani.com/blog/2007/04/twitter-and-jot.html

58 Cluley, G.: Twitter 'onMouseOver' security flaw widely: http://nakedsecurity.sophos.com/2010/09/21/twitter-onmouseove

59 handelsblatt.com – Warum Unternehmen twittern müssen: http://www.handelsblatt.com/unternehmen/mittelstand/warum-unternehmen-twittern-muessen/3345572.html?p3345572=6

60 Nutzer LinkedIN weltweit: https://socialmedia-institute.com/uebersicht-aktueller-social-media-nutzerzahlen

61 https://de.wikipedia.org/wiki/Linedln

62 Koß, S.: Was ist eigentlich LinkedIn? Ein Erklärungsversuch… : http://linkedinsiders.wordpress.com/2011/01/09/was-ist-linkedin/

63 LinkedIn – LinkedIn User Agreement: http://www.linkedin.com/static?key=user_agreement&trk=hb_ft_userag

64 LinkedIn – LinkedIn Privacy Policy: http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv

65 LinkedIn – LinkedIn Copyright Policy: http://www.linkedin.com/static?key=copyright_policy&trk=hb_ft_copy

66 Stiftung Warentest – Soziale Netzwerke – Datenschutz oft mangelhaft: http://www.test.de/themen/computer-telefon/test/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-1855785/

67 LinkedIn – Hack: https://www.basicthinking.de/blg/2016/05/26/linkedin-hack-sicherheit

68 Nutzer XING weltweit: https://recruting.xing.com/ce/daten-und-fakten

69 www.http://socialmedia-institute.com/übersicht-aktueller-social-media-nutzerzahlen

70 XING – Wikipedia: http://de.wikipedia.org/wiki/XING

71 XING ProJobs: https://www.xing.com/upsell/projobs

72 XING E-Recruiting: https://recruiting.xing.com

73 Wilkens, A.: heise online – Neue XING-Funktion weckt Datenschutzbedenken: http://www.heise.de/newsticker/meldung/Neue-Xing-Funktion-weckt-Datenschutzbedenken-167585.html

74 datensicherheit.de – XING-Gruppen-Newsletter: http://www.xing.com/net/fischernetz/newsletter-archiv-19807/gruppen-newsletter-achtung-gefalschte-xing-mails-im-umlauf-24514207/

75 Übersicht der aktuellen Nutzer von Sina Weibo: http://expandedramblings.com/index.php/weibo-user-statistics

76 Sina Corporation: https://de.wikipedia.org/wiki/Sina_Corporation

77 Sina Weibo: https://de.wikipedia.org7wiki/Sina_Weibo

78 Untersuchung der Uni Honkong – mehr als die Hälfte der Sina Weibo Profile sind inaktiv: www.spiegel.de/netzwelt/web./bei-chinas-twitter-klon-sina-weibo-finden-sich-viele-pseudo-profile

79 Gezielte Unterdrückung unliebsamer Blogger: www.Epochtimes.de/china/china-politik/das-hat-die-zensur-aus-chinas-twitter-sina-weibo-gemacht

80 vk.com: https://de.wikipedia.org/wiki/Vk.com

81 Vk.com – Über 300 Millionen Mitglieder weltweit: http://eurusky.ru/2015/06/vk-com-die-vielversprechende-russische-facebookalternative

82 Vk.com – Nutzer Deutschland: www.http://meedia.de/2015/0619/die-10-groessten-sozialen-netzwerke-der-welt-und-deutschlands

83 Gründer von VKontakte verweigert die Schließung von Gruppen bei VK: https://de.wikipedia.org/wiki/Pawel_Walerjewitsch_Durow

84 Bell, J.H.: Corporate Reputation in the Social Age: http://www.yoursocialmediascore.com/downloads/b_repmanagement.pdf

85 Digital, P.: Der bezahlbare Ruf: http://politik-digital.de/news/der-bezahlbare-ruf

86 Legal Tribune Online – Illoyale Arbeitnehmer – Gefährliches Netzwerken bei Daimler: www.lto.de/recht/hintergruende/h/illoyale-arbeitnehmr-gefaehrliches-netzwerken-bei-daimler/

87 ZDNet – Mitmachen oder verbieten – Soziale Netzwerke in Unternehmen: www.zdnet.de/41536177/mitmachen-oder-verbieten-soziale-netzwerke

88 Rundschau, F.: Schmutz und Blut: www.fr-online.de/medien/facebook-schmutz-und-blut14733428446884.html

89 Handelsblatt – „Explosive Grüße aus dem Netz“: www.handelsblatt.com/unternehmen/it-medien/soziale-netzwerke-explosive-gruesse-aus-dem-netz

90 paradisi.de – Online-Kriminalität: https://www.paradisi.de/Freizeit_und_Erholung_/Gesellschaft/Jugendkriminalität/News

91 Spiegel.de: www.spiegel.de/unispiegel/jobundberuf/mobbing-der-chef-stichelt-gezielt-mit-a-269981.html

92 stuttgarter-nachrichten.de: www.stuttgarter-nachrichten.de/inhalt.cyber-mobbing-immer-haeufiger-web-gemobbt

93 welt.de: http://www.welt.de/wirtschaft/karriere/article3659218/Mobbing-und-Burn-out-kosten-jaehrlich-6-5-Milliarden.html

94 heise online: www.heise.de/newsticker/meldung/Mobbing-Vorstand-der-Telekom-Austria-verliert-Zustaendigkeit-fuer-Personal-201122.html

95 Die Presse.com – Facebook und Twitter kosten eine Woche Arbeit pro Jahr: http://www.die presse.com/home/techscience/internet/517564

96 pressetext.deutschland – Arbeitgeber hadern mit Social Networks: http://www.pressetext.com/news/20090925034

97 Wikipedia – Koobface — Wikipedia, The Free Encyclopedia: https://en.wikipedia.org/wiki/Koobface

98 Nemey, A. K. und C.: 5 Bedrohungen bei Social Media: http://www.cio.de/knowledgecenter/security/2277766/index/html

99 Präparierte Apps und Links: www.praxistipps.chip.de/wer-hat-mein-facebook-profil-besucht-kann-man-das-sehen

100 Miller, M.: Google Engineer Publishes –Then Deletes Opinionated Google+ Rant: http://searchginewatch.com/article/2117162/Google-Engineer-Publishes-Then-Deletes-Optionated-Google-Rant

101 W & S – Zufriedene Kollegen wahren Geschäftsgeheimnisse: http:// www.sicherheit.info/SI/cms.nsf/si.ArticlesByDocID/1103258?Open

102 pressemitteilungen-online.de: http://www.pressemitteilungen-online.de/index.php/e-mail-benachrichtigungen-waehrend-der-arbeitszeit-stoeren-konzentration

103 Sicking, M.: http://www.heise.de/resale/artikel/Facebook-Co-verursachen-Millionen-Schaeden-in-Unternehmen-1251956.html

104 https://de.foursquare.com

105 http://www.google.com/places

106 Stern.de – „Facebook Orte" ist hier: Deutschland: http://www.stern.de/digital/online/neuer-dienst-places-facebook-orte-ist-hier-deutschland-1610627.html

107 Twitter.com: http://support.twitter.com/groups/34-mobile/topics/171-twitter-s-mobile-website/articles/118492-how-to-tweet-with-your-location-on-mobile-devices

108 http://techcrunch.com/2010/02/17/please-rob-me-makes-foursquare-super-useful-for-burglars

109 Grimme-Institut – Hier und jetzt im Netz: https://www.grimme-institut.de/imblickpunkt/pdf/imblickpunkt-hier-und-jetzt-im-netz.pdf

110 BRD – BDSG-§4: https://dejure.org/gesetze/BDSG/4.html

111 Erpressung nach erotischem Video-Chat: https://www.watchlist.internet.at/liebesbetrug/fallbeispiel-erpressung-nach-erotischem-video-chat

112 Arrington, M.: Being Eric Schmidt (On Facebook): http://techcrunch.com/2010/10/10/being-eric-schmidt-on-facebook

113 Siciliano, R.: Identity Theft Committed Using Social Networks: http://www.huffingtonpost.com/robert-siciliano/identity-theft-commited-u_b_243305.html

114 Saafan: fbpwn – A cross-platform Java based Facebook social engineering framework: http://code.google.com/p/fbpwn

115 Das Experiment – Robin Sage: https://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage

116 Die gängigsten Fallen im Netz: http://blog.emisoft.com/de/2015/04/16/so-verwenden-sie-facebook-sicher-und-vermeiden-die-top-5-betrugereien

117 Social Engineering: https://www.focus.de/finanzen/news/unternehmen/nun-ist-er-seinen-job-los-manager-trottel-amerikaner-ueberweist-chinesischen-betruegern.17-2-millionen-dollar-id-4466355.html

118 SaferInternet.at: https://m.saferinternet.at/news/article/erpressung-per-webcam-der-sex-scam-417 (2014)

119 http://www.welt.de/wirtschaft/webwelt/article4062801/Londons-Spionage-Chef-in-Badehose-auf-Facebook.html

120 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

121 Heise.de – Hacker steigen bei Lockheed Martin ein: http://www.heise.de/ct/meldung/Hacker-steigen-bei-Lockheed-Martin-ein-1251902.html

122 Identitätsdiebstahl im Internet – Wie er funktioniert und wie man sich schützen kann: http://irights.info/artikel/identittsdiebstahl-im-internet

123 Focus.com – The Security Risks of Social Networks: http://www.focus.com/fyi/security-risks-social-networks (letzter Zugriff: 22.06.2016)

124 CIO and V.P. for I.T. at the University of Wisconsin-Madison – Protect your identity: http://www.cio.wisc.edu/security-identity.aspx (letzter Zugriff: 22.06.2016)

125 Siciliano, R.: Identity Theft Committed Using Social Networks: http://www.huffingtonpost.com/robert-siciliano/identity-theft-commited-u_b_243305.html. (letzter Zugriff: 11.08.2016)

126 Focus.com –The Security Risks of Social Networks: http://www.focus.com/fyi/security-risks-social-networks/ (letzter Zugriff: 11.08.2016)

127 Social Media Governance – Policy Database: http://socialmediagovernance.com/policies.php

128 IBM – Social Computing Guidelines. Blogs, wikis, social networks, virtual worlds and social media: http://www.ibm.com/blogs/zz/en/guidelines.html

129 BBC – Social Networking, Microblogs and other Third Party Websites: Personal Use: http://www.bbc.co.uk/guidelines/editorialguidelines/page/guidance-blogs-personal-summary

130 Reuters – Reporting from the internet: http://handbook.reuters.com/index.php/Reporting_From_the_Internet_And_Using_Social_Media

131 DAIMLER – Data Protection Policy – Privacy Statement: www.com/privacy/

132 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

133 Corporation, I.: Intel Social Media Guidelines: http://www.intel.com/content/www/us/en/legal/intel-social-media-guidelines.html

134 Legal Tribune Online – Illoyale Arbeitnehmer – Gefährliches Netzwerken bei Daimler: http://www.lto.de/de/html/nachrichten/3386/illoyale_arbeitnehmer_gefaehrliches_netzwerken_bei_daimler/

135 BITKOM – Studie Social Media in deutschen Unternehmen: https://www.bitkom.org/Bitkom/Publikationen/Studie-Social-Media-in-deutschen-Unternehmen.html

136 Digitalpublic.de – 100 Social Media Guidelines: http://www.digitalpublic.de/25-social-media-guidelines

137 Apple Retail Blogging and Online Social Media Guidelines Leaked: modmyi.com/forums/mac-news/790947-apple-retail-blogging-online-social-media-guidelines-leaked-html

Impressum

Herausgeber
Bayerisches Landesamt für Verfassungsschutz,
Knorrstr. 139, 80937 München

Hochschule Augsburg,
Friedberger Straße 2, 86161 Augsburg

Druck
Schmid Druck & Medien, Kaisheim

Bildnachweis
Titelbild: almagami/Shutterstock.com
Internet-Screenshots:
S. 17, S. 25: facebook.de,
S. 28, S. 31: plus.google.com,
S. 33, S. 36: twitter.com,
S. 41: linkedin.com,
S. 29: lokalisten.de,
S. 43, 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.

BAYERN | DIREKT
www.bayern.de Tel. 089 12 22 20

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, für Bau und Verkehr und des Bayerischen Staatsministeriums für Wirtschaft und Medien, Energie und Technologie