Preprint. Erscheint als: Langheinrich, M., & Karjoth, G. (2010). Soziale Netzwerke als Risiko für Unternehmen. *Digma - Zeitschrift Für Datenrecht Und Informationssicherheit*, 10(2): 50–55.

Soziale Netzwerke als Risiko für Unternehmen

Trotz der verbundenen Gefahren spielen Soziale Netzwerke auch für Unternehmen eine zunehmend wichtige Rolle

Lead (5 Zeilen, ca. 150 Zeichen)
Soziale Netze eröffnen für Unternehmen neue Möglichkeiten für Werbung, Wissensmanagement und Mitarbeiterbindung. Doch sie bergen auch neue Gefahren.

Wie schon das World Wide Web vor knapp mehr als 10 Jahren die Welt im Sturm eroberte, so schritt in den letzten Monaten die Verbreitung „Sozialer Netzwerke“ voran. Allein in den USA verdoppelte sich die Zahl der Teilnehmer am weltgrössten sozialen Netzwerk, Facebook, innert des letzten Jahres von 56 Millionen auf über 114 Millionen (Stand: April 2010). In der Schweiz waren im April 2010 laut Facebook ganze 2.1 Millionen Nutzer aktiv - das wäre mehr als ein Viertel der Schweizer Bevölkerung![1]

Aus der Sicht des Einzelnen wurde bereits ausführlich über die Vorteile und Gefahren dieser zunehmenden „Vernetzung“ des Einzelnen im öffentlichen und halböffentlichen Raum berichtet.[2] Doch auch für Unternehmen spielen Soziale Netzwerke eine zunehmend wichtige Rolle, auch wenn diese „juristischen Personen“ wohl kaum auf diese Weise „Freundschaften“ etwa mit anderen Firmen pflegen dürften. Immerhin sollen inzwischen fast 7% des gesamten betrieblichen Internetaufkommens durch den Besuch von Facebook-Seiten verursacht werden (Stand: April 2010).[3]

Tatsächlich eröffnen soziale Netzwerke Firmen neue Möglichkeiten der Kundenwerbung und -bindung, erleichtern den Wissenstransfer innerhalb der Unternehmen und können das Betriebsklima positiv beeinflussen. Auch können sie gezielt zur Stellenankündigung und zum Bewerberscreening eingesetzt werden. Auf der negativen Seite können Soziale Netzwerke allerdings auch blitzschnell ein über Jahre mühsam aufgebautes Markentingimage durch eine sich im Lauffeuer ausbreitende Grassrootskampagne zerstören. Auch birgt die Freigabe sozialer Netzwerke am Arbeitsplatz Gefahren einer übermässigen Nutzung durch den Mitarbeiter und kann gesetzliche Archivierungspflichten unterlaufen. Selbst das „Befreunden“ von Mitarbeitern durch Vorgesetzte kann bei Kündigungen schnell Arbeitsrechtsklagen nach sich ziehen mit dem Vorwurf, dass hier gesammeltes privates Material eine Rolle gespielt hätte. Eifrig „netzwerkende“ Mitarbeiter können auch schnell einmal Unternehmensinterna ausplaudern, die nicht für die Öffentlichkeit gedacht waren. Und nicht zuletzt ergeben sich für Hacker völlig neue Angriffsvektoren, sobald einmal genügend "Freundschaften" zu Firmenmitarbeitern geschlossen wurden.

Soziale Netze als Werbeplattform

Die Werbung der Zukunft ist persönlich. Zunächst einmal „personalisiert“, d.h. von einem Unternehmen speziell auf den einzelnen Kunden ausgerichtet, aber mehr und mehr auch in Form privater Tips und Empfehlungen – von Freunden für Freunde.

Erste Ansätze dieser neuen Art der Werbung sind die sogenannten „viralen Marketing“ Kampagnen im Web: Ein Unternehmen spielt beispielsweise einem bekannten Blog scheinbar unauthorisierte Fotos, Videos oder andere Informationen über ein noch nicht erschienenes Produkt zu, von wo aus sichdiese Informationen idealerweise in windeseile über „Mund-zu-Mund“ Propaganda ausbreiten. Bestes Beispiel ist das Ende April 2010 angeblich von einem Apple-Mitarbeiter verlorene iPhone der 4. Generation, welches das sonst so verschwiegene Unternehmen kurz nach dem abklingendne iPad-Hype erneut auf allen Kanälen erscheinen liess.[4]

Auch Plattformen wie Amazon, Tripadvisor oder Netflix bieten Unternehmen – in Tripadvisors Falle zum Beispiel Hotels und Restau-

rants, bei Amazon Bücher oder Filme – eine völlig neue Art der Kundenwerbung: Statt vorgefertigter Slogans vom Marketing Department schreiben bestehende Kunden Reviews, die auf ihren persönlichen Erfahrungen basieren. Diese besitzen bei potentiellen Kunden eine weit höhere Glaubwürdigkeit als Hochglanzprospekte.

Soziale Netze treiben diese Entwicklung nun einen Schritt weiter: Statt Reviews und anderen Informationen von Unbekannten zu erhalten, kommen werberelevante Nachrichten (z.B. Erfahrungsberichte oder auch einfach nur die Tatsache einer Kaufentscheidung) in einem Sozialen Netzwerk typischerweise von Freunden, die man persönlich kennt und deren Geschmack man möglicherweise schätzt.

Facebook's „Beacon" Programm versuchte diese Art Mundpropaganda in sozialen Netzwerken vor einigen Jahren (zunächst erfolglos) zu automatisieren: Sobald ein Facebook Nutzer auf einer Website eines teilnehmenden Händlers ein Produkt online erwarb, wurde diese Information an das gesamte in Facebook angelegte Freundesnetz weitergegeben. So erfuhr man ohne weiteres Zutun sofort, welcher Freund wann welches Buch oder welche DVD bei Amazon einkaufte. Das Beacon Programm scheiterte allerdings an seiner dilettantischen Einführung: Statt dieses als einen leicht ein- bzw. ausschaltbaren optionalen Service anzubieten, wurden diese Informationen in den meisten Fällen praktisch ohne das Wissen des Facebook Nutzers gesammelt und weitergegeben – schnell hatte so das bei Amazon scheinbar heimlich gekaufte Geschenk sich selbst beim beschenkten Freund bzw. der Freundin angekündigt. Keine 9 Monate nach der mit viel Fanfare gestarteten Einführung beendete Facebook das Programm im September 2007 unter einer Flut beinah ausnahmslos negativer Berichterstattung.[5]

Inzwischen wurde – quasi als überarbeitetes Beacon Programm – im April 2010 der „Like"-Button eingeführt, welcher es beliebigen Webseitenbetreibern erlaubt, an Facebook's sogenannten „OpenGraph" teilzunehmen und nicht nur Informationen in Facebook einzuspeisen, sondern auch abzurufen. Sobald ein Nutzer z.B. auf der Website des Unternehmens den (prominent platzierten) „Like"-Button betätigt, wird diese Vorliebe nicht nur seinem gesamten sozialen Netz mitgeteilt sondern auch allen am Facebook-Advertising-Programm beteiligten Firmen. Die Beliebtheit eines Produkts oder einer Marke lässt sich bald nicht mehr wie bei Google anhand des Grades der Verlinkung ablesen, sondern ganz persönlich an der Anzahl der Facebook Nutzer, die hier den „Like"-Button betätigten. Können Unternehmen es sich leisten im Sozialen Netzwerk der Zukunft nicht mit dabei zu sein?

Auch das virale Marketing erfährt mittels der stark vernetzten sozialen Netzwerke eine neue Dimenson. Ähnlich des Phänomens der sogenannten „Flash-Mobs" – spontanen über das Internet und SMS organisierten Zusammenkünfte sich gegenseitig weitgehend unbekannter Personen zu meist dadaistisch angehauchten Themen – erlauben es Soziale Netzwerk Plattformen, schnell und unkompliziert Interessengruppen zu Produkten und/oder Ereignissen zu bilden. Inzwischen gibt es kaum ein Produkt, welches keine dedizierte „Facebook Gruppe" vorweisen kann: vom VW Golf über Kitkat Schokoriegel, vom Zürcher Traditionsrestaurant Hiltl bis hin zum Produkt „Facebook" selbst. Die im April 2010 angekündigten Facebook Neuerungen erlauben inzwischen sogar die „Befreundung" von Orten und Ideen!

Während solche Produktgruppen ein ungeahntes Potenzial für nicht nur kostengünstige sondern auch extrem zielgerichtete und effektive Werbung darstellen, die quasi „von selbst" läuft, so lassen sie sich um so weniger steuern und können so schnell der scheinbaren Kontrolle ihrer „Erzeuger" entgleiten. Solches musste Nestlé im März 2010 erfahren, als es in der Kitkat-Schokoriegel Fangruppe nach einem kritischen Greenpeace Artikel über die Verwendung von lebensraumzerstörendem Palmöl, was in Kitkat Verwendung finden soll, von Boykottaufrufen nur so wimmelte.[6] Da die Zugehörigkeit zu solchen Fangruppen prinzipiell jedem Facebook Nutzer offensteht, können Aktivisten schnell eine bis dato beschauliche Fangruppe im Handstreich in einen wütenden Mob verwandeln. Nestlé verschärfte den Konflikt weiter, indem es als Fangruppen-Erzeuger von seinem „Hausrecht" gebraucht machte und unliebsame Einträge löschte – dies entfachte den

Zorn der „Fans“ erst recht. Die erste Adresse für Fans der Schokolade wurde schnell zur ersten Adresse für Kritiker.

Natürlich können Kritiker auch gleich eine ganz eigene „Fangroup“ erzeugen – wie im Falle des britischen MusicStar-Äquivalents X-Factor. Um dem alle Jahre wiederkehrenden Phänomen Einhalt zu bieten, dass der X-Factor Gewinner im einträglichen britischen Weihnachtsgeschäft den Titel der meistverkauften Single erhält, machten im Jahr 2009 Kritiker der Sendung in einer eigens dafür geschaffenen Facebook Gruppe mobil und schafften es tatsächlich, genügend „Fans“ zu motivieren, durch den Kauf einer anderen Single den scheinbar vorprogrammierten Nummer Eins Hit um knappe 50‘000 verkaufte Exemplare am Weihnachtstag zu schlagen. Auch hier waren die X-Factor Macher überrascht, wie es eine mit einfachsten Mitteln und ohne finanzielle Ausgaben auskommende Facebook Gruppe schaffte, ihre gut eingespielte und mit teurem Geld finanzierte Werbemaschinerie zu übertrumpfen.

Soziale Netze und ihre Eignung zum höchst virales Marketing sind also ein zweischneidiges Schwert: sie erlauben ungeahnte Verbreitung bei minimalen Kosten, doch bleiben sie auch unkontrollierbar und können so schnell in negative Publicity umschlagen. Ebenso nivellieren sie den „Wettkampf“ zwischen Werbern und möglichen Unternehmenskritikern, die über soziale Netzwerke höchst effektive Kampagnen quasi zum Nulltarif betreiben können.

Soziale Netzwerke und Mitarbeiterführung

Soziale Netzwerke können nicht nur die Kommunikation mit bestehenden und potentiellen Kunden eines Unternehmens verbessern, sie können auch die Kommunikation innerhalb eines Unternehmens positiv beeinflussen.

Auch ohne eine offizielle Strategie der Unternehmensführung besteht wohl in den meisten Unternehmen bereits heute ein grosses Interesse unter Mitarbeitern, vom Arbeitsplatz aus ihr (privates) Facebook Profil zu pflegen und Updates von Freunden zu verfolgen. Ein gutes Beispiel ist der Fall der Zürcher Stadtverwaltung, welche im März 2010 bei über sieben Millionen täglichen Facebook-Zugriffen durch ihre 24‘000 Mitarbeiter die Notbremse zog: Nachdem ein Apell zur freiwilligen Selbstbeschränkung kaum einen Effekt hatte, beschloss der Stadtrat die Sperrung der Seite.[7] Weitere Schweizer Firmen, wie z.B. Credit Suisse oder die SBB, haben bereits den Zugriff auf Facebook von Dienstcomputern gesperrt. In den USA sollen inzwischen knapp 40% aller Firmen den Zugriff auf Soziale Medien jeglicher Art sperren.[8] Andere setzen auch weiterhin auf Eigenverantwortung, wie etwa der Kanton Zürich. Sicherlich ist ein uneingeschränkter Webzugriff in der heutigen Zeit ein „Perk“, der positiv zum Betriebsklima beitragen kann. Doch wann beginnt ein Motivationsinstrument zum Zeitkiller zu werden?

Eine Option ist die Adoption von Facebook als ein Instrument zur Mitarbeiterführung. Manager „befreunden“ ihre Teammitglieder und schaffen so eine scheinbar lockere Atmosphäre. Reguläre Status-Updates innerhalb einer solchen Facebook Gruppe können helfen, Arbeit zu koordinieren und ein Bewusstsein für die Aktivitäten der einzelnen Teammitglieder zu schaffen. Doch Anwälte warnen inzwischen davor, dass eine solche Vermischung im Falle von Konflikten schnell arbeitsrechtliche Probleme schaffen kann: Inwieweit wurde z.B. im Falle einer Kündigung privates Material von der Facebook Seite des Mitarbeiters verwendet? Gerade im klagefreudigen Amerika kann eine solche Verbindung schnell den Vorwurf des „sexual harassment“ mit sich bringen.[9]

Mitarbeiterwerbung und -screening

Nach einer von Microsoft im Dezember 2009 veröffentliche internationale Studie[10] mit 1200 befragten Recruitern ist – neben der klassischen Suche in Suchmaschinen (78%) – die Nutzung sozialer Netzwerke inzwischen fester Bestandteil des Mitarbeiterscreenings geworden (63%), zusammen mit Photosharing Plattformen wie Flickr (59%) und professionellen Business Netzwerken wie etwa Xing oder LinkedIn (57%). Im Vorjahr hatte eine Harris Interactive Studie[11] für die Nutzung sozialer Netzwerke noch eine Quote von nur 45% gefunden.

Seit Facebook im April 2010 die im öffentlichen Profil zugänglichen Informationen umfassend (und in den meisten Fällen ohne Wissen der Profilebesitzer) erweitert hat,

können potentielle Arbeitgeber auch ohne vorherige Freundschaft einen detaillierten Blick auf die Interessen und Beziehungen eines Bewerbers verschaffen. Vor allem die Tatsache, dass Gruppenzugehörigkeiten und jegliche Vorlieben bzw. Interessen (z.B. Bücher, Filme) durch die Umwandlung in „Connections“ nun immer öffentlich sind, hat bereits erste Aktivisten dazu inspiriert, Mitglieder unliebsamer Gruppen aufzufinden und als „Spammer“ anzuschwärzen, um so eine automatische Blockierung ihres Accounts zu erreichen.[12] Doch wie bereits erwähnt müssen Kündigungen, die in Folge von unliebsamen Kommentaren auf sozialen Netzwerken ausgesprochen wurden, typischerweise private Handlungen von solchen, die den veröffentlichten Firmenregeln explizit widersprechen, klar trennen können. So konnte in 2005 Google einen frisch angestellten Product Manager innert 11 Tagen wieder feuern, nachdem dieser entgegen den schriftlich festgehaltenen Richtlinien auf seinem Blog betriebsinterne Informationen verbreitet hatte.[13]

Natürlich können Soziale Netzwerke von Unternehmen nicht nur zur Produktwerbung sondern auch zur Selbstbewerbung als potentieller Arbeitgeber eingesetzt werden. Dabei kann ein Einsatz solcher Dienste ein frisches und weltgewandtes Image erzeugen, vor allem bei eher konservativ wahrgenommenen Unternehmen. So startete unlängst die französche Katholische Kirche im Rahmen ihrer „Pourquois pas moi?“ Recruitment Kampagne eine Facebook-Gruppe, in der sich junge Menschen über den Berufswunsch Priester austauschen können.[14] Professionelle Netzwerke wie LinkedIn und Xing sind sogar speziell darauf zugeschnitten, Bewerber mit bestimmten Qualifikationen bzw. Interessen gezielt aufzufinden, um dann schnell und unkompliziert mit ehemaligen Arbeitgebern und Managern in Kontakt treten zu können, um detaillierte Informatione über frühere Aufgabenbereiche bzw. Tätigkeiten zu erhalten. Natürlich gilt gleiches auch für das Abwerben ihrer bestehenden Mitarbeiter durch Konkurrenzunternehmen.

Mitarbeiter in sozialen Netzwerken

Die Teilnahme der eigenen Mitarbeiter an sozialen Netzwerken kann nicht nur die produktive Arbeitszeit einschränken und sie „anfällig“ machen für Abwerbungsversuche der Konkurrenz – es kann schnell auch direkten Einfluss auf die Unternehmenssicherheit nehmen.

Statistische Einblicke

Die meisten Unternehmen veröffentlichen keinerlei detaillierten Informationen über Arbeitsgruppen, deren Mitglieder bzw. deren Projekte. Durch die oben erwähnte Zwangsveröffentlichung jeglicher „Connections“ in Facebook könnten Aussenstehende leicht einen ungewollten Einblick in interne Betriebsstrukturen erhalten. Unvergessen ist hier der Medienrummel, als vor einigen Jahren Amazon aggregierte Kaufmuster („Purchase Circles“) seiner Kunden veröffentlichte – aufgeschlüsselt nicht nur nach Ländern und Städten, sondern auch nach Unternehmen.[15] Zwar achten Soziale Netzwerkplattformen sehr darauf, dass ihre Datensammlungen nicht im grossen Stile automatisiert „abgegrast“ werden,[16] doch sind solche Details oft Bestandteil der Marketing-Werkzeuge, die sie Werbetreibenden zum Einstellen von Werbung zur Verfügung stellen.[17]

Selbst individuelle Einträge können bereits sensitive Einblicke gewähren, wenn z.B. ein Relationship Manager seine Kunden auf seine Freundesliste setzt. Nicht nur wären solche Informationen für die Konkurrenz interessant, in vielen Fällen fallen sie auch unter die betriebliche Geheimhaltungspflicht. Auch hinreichend auf betriebsinterne „Freunde“ beschränkte private Chats können aufgrund der globalen Verfügbarkeit der Plattformen bei etwaigen Systemfehlern schnell ungewollt weltweit lesbar sein. So waren bei dem am 5. Mai 2010 entstandenen „Preview my Profile“-Bug auf Facebook sowohl private Chat Aufzeichnungen sowie pendente Freundesanfragen kurzzeitig öffentlich zugänglich gewesen.[18]

Plaudereien

Nicht zu unterschätzen ist darüber hinaus auch das in der Natur des Menschen liegende Mitteilungsbedürfnis. Schnell kann es Mitarbeiter, die aktiv an sozialen Netzwerken oder sozialen Medien teilnehmen dazu verleiten, bewusst oder unbewusst nicht nur private Informationen preis zu geben, sondern auch betriebliche Geheimnisse. So wurde beispielsweise die Wiederwahl des deutschen Bundespräsidenten bereits vor der offiziellen

Bekanntgabe des Ergebnisses von einigen Abgeordneten über Twitter „verraten“.[19] Im März 2010 musste die israelische Armee einen geplanten Überraschungsangriff in der West Bank abblasen, nachdem ein Soldat in seinem Facebook Status mit seiner Teilnahme an dem bevorstehenden Einsatz geprahlt hatte[20]. Auch können geringschätzende Kommentare von Mitarbeitern gegenüber Kunden schnell ungewollt nach aussen dringen und so das Unternehmensimage nachhaltig schädigen (wie beispielsweise im Falle von Domino’s Pizza oder der Fluglinie Virgin.[21]

Selbst wenn Postings und Chat Nachrichten der Mitarbeiter nicht nach aussen dringen, bleibt dennoch die Frage nach dem rechtlichen Status der in einem Sozialen Netzwerk verbreiteten Informationen, insbesondere wenn diese Geschäftsdaten betreffen. Es ist deshalb sehr wichtig, die Allgemeinen Geschäftsbedingungen des Netzwerkbetreibers zu kennen. Da diese jedoch sehr häufig geändert werden, muss das Risiko einer totalen Offenlegung dieser Nachrichten mitberücksichtigt werden.

Phishing und andere Angriffe

Die in sozialen Netzwerken verfügbaren persönlichen Informationen von Mitarbeitern stellen für Hacker eine wichtige Quelle für das Eindringen in gesicherte Firmennetze dar.

Zunächst einmal können die bei der Registration verwendeten und meist öffentlich zugänglichen privaten Informationen von Mitarbeitern dazu verwendet werden, sich gegenüber schlecht gesicherten Helpdesks oder IT-Mitarbeitern auszuweisen: Schnell lassen sich nicht nur Name und Abteilung herausfinden, sondern auch Geburtsdatum und firmeninterne Telefonnummer – Informationen, die oftmals als Identifikation am Telefon ausreichen.

Ebenso können öffentlich zugängliche Bilder dazu verwendet werden, eine falsche Identität anzulegen und so vermeintliche Kollegen zu befreunden, die dann nichtsahnend Firmeninterna weitergeben können. Eine „Freundschaftsanfrage“, die das richtige Foto, die richtige Abteilung und Namen aufweist, wird in den meisten Fällen kaum Verdacht auslösen, vor allem wenn ausserhalb des sozialen Netzwerks kein direkter Kontakt besteht (z.B. bei Mitarbeitern an unterschiedlichen Standorten). So fand ein Report der Sicherheitsfirma Sophos in 2009, dass 46% der Facebook Nutzer sogar Freundschaftanfragen von ihnen völlig unbekannten Personen bestätigten.[22]

Professionelle „Phishing“ Angriffe erkunden zunächst die oft von Mitarbeitern angelegten öffentlichen Unternehmensgruppen und treten diesen dann mit einer falschen Identität und einer falschen Abteilung bei.[23] So können sie eine Liste der Mitarbeiter und deren Abteilungen erstellen, welche sie dann in einem zweiten Schritt im eigentlichen Phishing-Angriff ins Visir nehmen. Dazu wird eine dem Firmennamen ähnliche Domäne reserviert und mit einer im Unternehmensdesign gestalteten Webseite geschmückt, die einen möglichst allgemeingehaltenen Service anbietet, z.B. eine Human Resources Seite bzw. eine Betriebsversicherungs. Die Phishing Email – an einem Sonntagabend verschickt damit sie in der Email Flut am Montag Morgen weniger auffällt – fordert dann die im ersten Schritt identifizierten Mitarbeiter auf, sich auf dem vermeintlich neuen Portal mit ihrem gewohnten Usernamen und Passwort einzuloggen. Dieses wird dann mit einem generischen „Under Construction“ quittiert, während die eingegebenen Daten nun direkt für den eigentlichen Angriff auf das Firmennetz verwendet werden können.

Solch ein gezieltes Anschreiben von Mitarbeitern im Einklang mit ihrer Aufgabe und Rolle innerhalb der Firmenhierarchie wird als „Spear-Fishing“ bezeichnet, da es im Gegensatz zu herkömmlichen „Phishing“ Angriffen keine Massen-Emails verschickt, sondern sich gezielt die lohnensten Opfer aussucht. Hier spielen soziale Netzwerke und professionelle Netzwerke eine signifikante Rolle, da sie die Professionalität solcher gefälschten Anschreiben durch Hintergrundwissen erheblich steigern können.[24] Schaffen es Hacker sogar, in den Sozialen Netzwerk-Account des Vorgesetzten einzubrechen (wie unlängst in den eines Facebook Aufsichtsratsmitglieds) und in seinem Namen Nachrichten zu verschicken, können hunderte von Mitarbeitern schnell in die Phishing-Falle tappen.[25] Vor allem die bei Internetdiensten oft unumgänglichen, meist aber trivialen „Sicherheitsabfragen“, die im Falle eines Passwortverlusts das Neusetzen erleichtern sollen, erleichtern Ha-

ckern die Arbeit ungemein. So konnte ein College Student im September 2008 den Yahoo Email Account der US-amerikanischen Präsidentschaftskandidaten, Sarah Palin, durch das Beantworten der Frage „Wo haben Sie Ihren Ehepartner kennengelernt?“ übernehmen – die Antwort lieferte ihm eine kurze Internetsuche (auf der Highschool: „Wasilla high“).[26]

Darüber hinaus kann durch den Gebrauch Sozialer Netzwerke auf dem Firmen-Laptop oder der mobilen Nutzung solcher Dienste auf dem dienstlichen Smartphone die Wahrscheinlichkeit für Hacking-Angriffe aller Art steigen. Wird das gleiche Passwort für das Firmennetz auch bei den i.A. schlechter gesicherten Sozialen Netzwerken verwendet, ergeben sich schnell grosse Sicherungslücken. Auch die bei den oft in ihrer Länge stark beschränkten Status-Nachrichten verwendeten Kurz-URLs können leicht ungewollte Links verstecken – und auf mobilen Endgeräten werden diese oft nur teilweise angezeigt.

Archivierungspflichten und Online-Chats

Nicht zu unterschätzen sind schliesslich die Probleme beim Gebrauch von sozialen Netzwerken und sozialen Medien wie etwa Twitter wenn es um *Corporate Compliance* geht. In regulierten Industrien sowie im öffentlichen Sektor bestehen oftmals Vorschriften, dass die gesamte Kommunikation aufbewahrt werden muss. Während dies bei der Verwendung von Email inzwischen Unternehmensweit gewährleistet werden kann, befinden sich Soziale Medien hier oft „unter dem Radar“ und unterlaufen so gesetzliche Vorgaben. Prominentes Beispiel ist der Deputy Chief Technology Officer des US-amerikanischen Präsidenten, Andrew McLaughlin. Der ehemalige Google Mitarbeiter nutzte wie selbstverständlich den im Februar 2010 von Google neu gestarteten sozialen Netzwerkdienst „Buzz“ – und unterlief damit ungewollt die für amerikanische Regierungsmitarbeiter strikte Archivierungspflicht, da der gesamte im Amt anfallende Mailverkehr aufbewahrt werden muss.[27] Existierende Lösungen für *Records Management* und Digitale Archivierung unterstützen den Informationsaustausch über soziale Netzwerkplattformen (noch) nicht.

Fazit

Hat ein Unternehmen entschlossen sich des neuen Mediums Soziale Netzwerke zu bedienen, wie kann es den möglichen Gefahren begegnen? Bereits 2007 hat ENISA einen Katalog mit 19 Empfehlungen für Betreiber und Nutzer von sozialen Netzwerken aufgestellt.[28] Ähnliche Empfehlungen gibt es inzwischen auch für öffentliche Behörden, aufgestellt z.B. durch die britische Regierung, um behördliche Aktivitäten in Sozialen Medien zu verbessern.[29] Ganz oben stehen in jedem Falle die Schulung (der Mitarbeiter) sowie Überprüfung und Neubewertung der gesetzlichen Rahmenbedingungen. Auch eine offizielle Firmenpolicy zur Nutzung Sozialer Netzwerke kann Mitarbeitern helfen, diese Art von Diensten produktiv und sicher zu nutzen – laut einer Erhebung der Zeitarbeitsfirma Manpower vom Februar 2010 haben bisher erst knapp 11% der Europäischen Unternehmen solch eine policy aufgestellt.[30]

Auf der technischen Seite stehen die Verwendung von sicheren Einstellungen für das Nutzerprofil, Gegenmassnahmen zur Firmenspionage, und Vorkehrungen zur Missbrauchentdeckung und Reporting. Schlussendlich ist es notwendig, dass die Betreiber von sozialen Netzwerkplattformen die Anforderungen von Unternehmen untertützen. Dies reicht von stabilen Allgemeinen Geschäftsbedingungen mit gutem Datenschutz bis zur Realisierung stärkerer Authentifikationsmechanismen und Zugriffskontrollen. Dann würden vielleicht auch die Meldungen weniger, dass es wieder gelungen ist, Millionen von Nutzerprofilen von einer sozialen Netzwerkplattform abzuziehen.[31]

Kurz & bündig ((ca. 820 Zeichen))

Soziale Netzwerke eröffnen Unternehmen neue Möglichkeiten der Kundenwerbung und -bindung, erleichtern den Wissenstransfer innerhalb der Firma und können das Betriebsklima positiv beeinflussen. Allerdings können sie auch blitzschnell ein über Jahre mühsam aufgebautes Marketingimage durch eine sich im Lauffeuer ausbreitende Grassroots-Kampagne zerstören. Die Freigabe sozialer Netzwerke am Arbeitsplatz birgt Gefahren einer übermässigen Nutzung durch den Mitarbeiter und kann gesetzliche Archivierungspflichten unterlaufen. Eifrig „netzwerkende“ Mitarbeiter können auch schnell einmal Unternehmensinterna ausplaudern, die nicht für die Öffentlichkeit gedacht waren. Und nicht zuletzt ergeben sich für Hacker völlig neue Angriffsvektoren, sobald einmal genügend "Freundschaften" zu Firmenmitarbeitern geschlossen wurden. Der vorliegende Artikel analysiert die Vorteile und Gefahren dieser Entwicklung für Unternehmen sowie erste Empfehlungen auszusprechen.

Literatur

- T. HILLENBRAND, Die Facebook-Falle. Der Spiegel, 16. April 2010 http://www.spiegel.de/netzwelt/web/0,1518,688975,00.html
- G. HOGBEN, Best Practices for Social Networks. digma 2008(3) 120-122.
- M. LANGHEINRICH und G. KARJOTH, Das «persönliche» Internet. digma 2007(4) 134-138.
- A. MARTÍNEZ-CABRERA, Spear-Phishing an Effective Tool for Scammers. San Francisco Chronicle, 22. Februar 2010. http://www.chron.com/disp/story.mpl/business/6880273.html
- CH. STÖCKER, Google Buzz blamiert Obamas Internet-Berater. Der Spiegel, 13. April 2010 http://www.spiegel.de/netzwelt/netzpolitik/0,1518,688794,00.html
- S. STRICKER, Die schöne Facebook-Freundin der Elitesoldaten. Der Spiegel, 17. Mai 2010 http://www.spiegel.de/politik/ausland/0,1518,694582,00.html
- E. TAYLOR-SMITH und R. LINDNER, Social Networking Tools Supporting Constructive Involvement throughout the Policy-Cycle. In: Prosser, A.; Parycek, P. (eds.): EDEM 2010 – Conference on Electronic Democracy 2010. (erscheint demnächst).
- J. WORTHAM, Facebook Glitch Brings New Privacy Worries , New York Times, 6. Mai 2010 http://www.nytimes.com/2010/05/06/technology/internet/06facebook.html

Autor(in)

Marc Langheinrich, Prof. Dr., Università della Svizzera italiana, Lugano
langheinrich@acm.org

Günter Karjoth, Dr., IBM Forschungslabor Zürich, Rüschlikon karjoth@acm.org

[1] http://www.nickburcher.com/2010/03/facebook-usage-statistics-march-2010.html
[2] LANGHEINRICH & KARJOTH (2007)
[3] http://www.network-box.com/node/533
[4] http://www.examiner.com/x-14552-Social-Media-Examiner~y2010m4d20-Who-is-Gary-Powell-Part-of-an-Apple-iPhone-4G-publicity-stunt-AppleGate-2010
[5] Vgl. http://www.handelsblatt.com/technologie/it-internet/facebook-stoppt-beacon;2459165
[6] Vgl. HILLENBRAND (2010)
[7] http://www.tagesanzeiger.ch/zuerich/stadt/Stadt-Zuerich-will-ihren-Angestellten-Zugang-auf-Facebook-verbieten/story/14353055
[8] http://www.emarketer.com/Article.aspx?R=1007670
[9] http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202434893818
[10] http://www.microsoft.com/privacy/dpd/research.aspx
[11] http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants/?emc=eta1

[12]http://www.readwriteweb.com/archives/facebooks_new_policies_make_harrassment_easy.php

[13] http://news.cnet.com/Google-blogger-has-left-the-building/2100-1038_3-5567863.html

[14] http://www.google.com/hostednews/ap/article/ALeqM5ibLAsFG8ZdF1r4iMyd9qaYqvqQ6QD9FCOVD80

[15] http://www.internetnews.com/ec-news/article.php/190431/Amazon+Modifies+Purchase+Circles+Following+Controv.htm

[16] http://scobleizer.com/2008/01/03/ive-been-kicked-off-of-facebook/

[17] Siehe http://www.facebook.com/advertising/

[18] WORTHAM (2010)

[19] http://www.stern.de/politik/deutschland/koehler-wahl-twitter-affaere-beschaeftigt-bundestagspraesidium-701884.html

[20] Vgl. http://thelede.blogs.nytimes.com/2010/03/03/israeli-raid-canceled-after-facebook-leak/ und auch STRICKER (2010)

[21] http://abcnews.go.com/Business/PersonalFinance/facebook-firings-employees-online-vents-twitter-postings-cost/story?id=9986796

[22] http://origin-www.sophos.com/security/topic/facebook.html

[23] http://www.darkreading.com/blog/archives/2010/03/facebook_as_a_s.html

[24] MARTÍNEZ-CABRERA (2010)

[25] http://news.cnet.com/8301-13577_3-20004549-36.html

[26] http://www.wired.com/threatlevel/2008/09/palin-e-mail-ha/

[27] STÖCKER (2010)

[28] HOGBEN (2008)

[29] TAYLOR-SMITH & LINDNER (2010)

[30] http://www.emarketer.com/Article.aspx?R=1007493

[31] http://abcnews.go.com/Technology/facebook-accounts-sold-russian-hacker-kirllos-user-logins/story?id=10461717