Link: http://www.computerwoche.de/a/print/noimages/2533455

Facebook, Twitter & Co. im Business

Die Gefahr im Social Web wächst

Datum: 13.03.2013
Autor(en): Stanislav Wittmann

Social Media sind längst mehr als reine Kommunikationskanäle: Mit ausgeklügelten Methoden schöpfen Cyberkriminelle dort Betriebs- und Geschäftsgeheimnisse unvorsichtiger Anwender ab. Die Folgen für Unternehmen können verheerend sein.

Richtig eingesetzt, eröffnen Facebook, Twitter, Google+, Xing, LinkedIn und Co. Anwendern bisher ungeahnte Möglichkeiten - im Marketing, der Kundenbindung, der Kontaktpflege und der internen Kommunikation. Einige Unternehmen experimentieren mit **Social-Enterprise**[1]-Lösungen, andere wie der französische IT-Dienstleister Atos versprechen sich gar eine **komplette Ablösung der E-Mail**[2]. Ihre Stärken ausspielen können soziale Anwendungen besonders auch in Kombination mit mobilen Geräten, deren Nutzung im Business-Umfeld kontinuierlich zunimmt.

Wer hat den Datenschutz im Griff?

Je beliebter die Plattformen werden, desto attraktiver werden sie aber auch für die "dunkle Seite der Macht" - Cyberkriminelle, Social Engineers und die Spione der Konkurrenz. Darüber hinaus drohen Konflikte mit geltenden Datenschutzgesetzen, wenn beispielsweise keine klaren Richtlinien zur Nutzung von Social Media erlassen worden sind. Denn was passiert, sobald es ein Unternehmen seinen Mitarbeitern erlaubt, Facebook oder Xing während der Arbeitszeit zu nutzen? Ist sichergestellt, dass in einem lockeren Facebook-Chat keine Firmeninterna ausgeplaudert werden? Das müssen nicht Betriebs- oder Geschäftsgeheimnisse sein. Es reicht bereits, wenn Namen, Adressen oder andere personenbezogene Daten von Arbeitskollegen weitergegeben werden. Die Telefonnummer oder Wohnadresse ist schließlich schnell versendet. Oder wie sorgenfrei klickt ein Mitarbeiter auf einen nicht als solchen erkennbaren Malware-Link, der ihm via Twitter von einem vorgeblichen Kollegen zugeschickt wurde? Die Möglichkeiten, Rechner mit Schadsoftware zu infizieren, werden schließlich immer ausgeklügelter. Klassische Virenscanner oder Sicherheitsabfragen bei Downloads über den Browser lassen sich beispielsweise dadurch umgehen, dass bestimmte Sicherheitseinstellungen deaktiviert werden.

Zumindest für das Problem der Informationsweitergabe gelten für deutsche Anwender klare Regeln: Gemäß **Bundesdatenschutzgesetz (BDSG)**[3] ist es untersagt, personenbezogene Daten unbefugt zu verbreiten - kann ein Vorsatz nachgewiesen werden, drohen dem Mitarbeiter sogar als Privatperson strafrechtliche Konsequenzen. An dieser Stelle sollte aber bedacht werden, dass Datenschutzgesetze Ländersache sind und bereits von Bundesland zu Bundesland verschiedene Auslegungsmöglichkeiten bestehen, von internationalen Streitfällen einmal ganz abgesehen. Denn auch wenn der **europäische Datenschutz vereinheitlicht werden soll**[4], lässt sich feststellen: Da Social Media gerade dazu genutzt wird, länderübergreifend zu kommunizieren, stellen die geltenden Gesetze keine wirkliche Barriere zur Informationsabschöpfung dar. Oft verlaufen sich Gerichtsprozesse in Sackgassen, da klare Beweisführung schwierig ist. Zudem ändert sich das Medienrecht regelmäßig und erschwert dadurch die Rechtsfindung ungemein.

[Hinweis auf Bildergalerie:] gal1

Die nächste Stufe: Cyberspionage

Datenschutzverstöße und infizierte Links sind bekannte Phänomene, die fast so alt sind wie das Social Web selbst. Die nächste Eskalationsstufe hingegen rückt derzeit immer stärker in den Fokus von Security-Experten: Social Engineering und gezieltes Ausforschen bestimmter Personen und Unternehmen. Das Social Web ist ein Eldorado für Agenten und Profiler: Wenn jemand etwas über einen Menschen erfahren möchte, stellt heute zumeist die Internetrecherche die Suchmethode erster Wahl dar. Innerhalb weniger Stunden ist es für Privatpersonen möglich, durch gezielte Nachforschungen an Informationen zu gelangen, die vor dem Zeitalter des kommerziellen Internets wochenlange Arbeit in Anspruch genommen hätten. Nicht einmal staatliche Nachrichtendienste wären früher in der Lage gewesen, derart detaillierte Recherchen zu betreiben, wie es heutzutage für jedermann möglich ist. Und das Beste: Zumeist ist dieser Vorgang, auch "Competitive Intelligence" genannt, völlig legal - der Mitteilungsfreudigkeit und Unvorsichtigkeit vieler Anwender sei Dank.

"Wir leben heute in einer offenen Informationsgesellschaft. Das hat zufolge, dass rund 80 Prozent aller Informationen heutzutage aus frei zugänglichen Quellen erschlossen werden können", sagt Herbert Kurek, Mitarbeiter beim Bundesamt für den Verfassungsschutz in Köln. Im **7. Symposium des Bundeamtes für den Verfassungsschutz**[5] stellte er am Beispiel der Wirtschaftsspionage bereits 2007 die Bedrohungslage im Zeitalter der Globalisierung sowie Herausforderungen des Verfassungsschutzes dar. Damals noch eher abstrakt, ist aus dieser Erkenntnis heute ernste Realität geworden. Gerade soziale Netzwerke und Fachforen stellen mittlerweile einen reichhaltigen Datenfundus dar. "76 bis 80 Prozent der in sozialen Netzwerken Aktiven geben dort auch private Daten preis und ermöglichen dadurch eine gezielte Auswertung. Im Zuge dessen bildet sich bei Facebook für jeden einzelnen User der so genannte soziale Graph, der erst den Wert des Netzwerkes ausmacht", erklärt Frank Schönefeld, Mitglied der Geschäftsleitung von **T-Systems Multimedia Solutions (MMS)**[6]. Er fügt warnend an: "Während durch diesen zunächst nur definiert war, wer mit wem im Kontakt und Austausch steht, können heute viel weitreichendere Schlussfolgerungen gezogen werden."

EADS, Apple, Microsoft: Die Fälle häufen sich

Dass auch Unternehmen vor den Informationssammlern nicht gefeit sind, zeigen die sich häufenden Fälle von Industriespionage, Identitätsbetrug und -diebstahl. **Eine Studie der Unternehmensberatung Corporate Trust zur Industriespionage 2012**[7] kommt zu dem Ergebnis, dass in etwa jedem dritten Unternehmen ein Verdacht und in über 20 Prozent der befragten Unternehmen konkrete Fälle von Spionage vorlagen. Die bekannt gewordenen größeren Incidents der vergangenen Wochen bei Konzernen wie **Apple**[8], Microsoft, EADS oder ThyssenKrupp, in denen jeweils zumindest der Versuch einer größeren Hacking-Attacke gestartet worden ist, zeigen die aktuelle Brisanz des Themas ebenfalls.

Selbst wenn die aufgezählten Ziele Opfer von teils komplexen Cyberangriffen wurden, die nicht ausschließlich über das Social Web vorbereitet wurden, ist das Grundprinzip der digitalen Spionage heute doch ein sehr einfaches. Bei Facebook beispielsweise einen **"Fake-Account"**[9] einzurichten, ist eine leichte Übung. Damit lassen sich gezielt Kontakte und "Freundschaften" zu den Mitarbeitern interessanter Unternehmen aufbauen, um anschließend an sensitive Informationen zu gelangen. Besonders die "Fake-Accounts" weiblicher, attraktiver Personen oder vermeintliche Freundschaften mit Personen des öffentlichen Lebens können die zumeist männlichen Zielpersonen in höheren Hierarchieebenen eines Unternehmens locken, eine Kontaktanfrage schnell zu bestätigen und eigene Daten für den Gegenüber freizugeben. Bereits aus diesem scheinbar unkritischen Austausch von Informationen lässt sich für Angreifer Profit schlagen, indem sie verknüpfte Suchen und tiefer gehende Web-Recherchen anstellen. Durch die Vernetzungen mit anderen Freunden und Postings können ebenfalls sehr detaillierte Informationen in falsche Hände gelangen.

Infizierte Links verseuchen IT-Systeme

Es ist für Cyberkriminelle nun zudem ein Leichtes, infizierte Dateien oder Links zu Malware-verseuchten Websites weiterzugeben. Schicken sie ihrem neuen Kontakt beispielsweise eine PDF- oder Bilddatei, wird dieser sie mit ziemlicher Sicherheit ungeprüft öffnen - schließlich stammt sie aus einer vermeintlich bekannten, vertrauenswürdigen Quelle. Was das Opfer nicht weißt: Es handelt sich um ein Trojanisches Pferd, das beispielsweise Hintertüren im System oder Unternehmensnetz öffnet. Dem Versender stehen schnell umfangreiche Zugriffsrechte zu, ohne dass der Mitarbeiter etwas merkt. Einmal eingeschleust, lassen sich Passwörter, Kundendaten oder Geschäftsunterlagen ausspähen und abziehen. Die Corporate-Trust-Studie bestätigt, dass im vergangenen Jahr bereits über 42 Prozent der bekannt gewordenen Spionagehandlungen ein Hackerangriff zugrunde lag - 2007 waren es noch nur knapp 15 Prozent gewesen.

Für Unternehmen führt das in der Regel zu erheblichen juristischen, monetären oder Reputationsschäden - im schlimmsten Fall zu allem gleichzeitig. Natürlich sind diese Fälle bereits aus dem E-Mail-Zeitalter bekannt - viele Anwender sind jedoch mittlerweile dafür sensibilisiert, Anhänge vor dem Öffnen genauer unter die Lupe zu nehmen, sofern sie durch den E-Mail-Filter des Unternehmens überhaupt durchkommen. Eine Malware-Attacke über soziale Netze ist auch deshalb für Cyberkriminelle so attraktiv, weil der "Awareness-Faktor" hier noch längst nicht so hoch ist.

Neue Bedrohungen durch Social Apps

Doch es geht noch einfacher: Wer beispielsweise bei Facebook eine (Social-)App installiert, erklärt sich damit einverstanden, dass schlimmstenfalls sein gesamter Nachrichtenverkehr eingesehen werden kann. Das wird in aller Regel nicht offensichtlich erwähnt, sondern verschwindet im "Kleingedruckten" der AGBs. Wer also einen "Streu-Spionageangriff" starten möchte, schreibt eine App für mehrere mobile Betriebssysteme und stellt diese auf den gängigen Distributionsplattformen wie dem Apple App Store oder dem Google Play Store ein. Gerade Android-Apps sind wegen der nicht vorhandenen Kontrollmechanismen seitens Google für ein derartiges Vorgehen gut geeignet. Eine **Studie des Sicherheitsdienstleisters Bit9**[10] belegt, dass über 100.000 Android-Apps, die derzeit im Google Play Store verfügbar sind, Sicherheitsrisiken aufweisen. Das betrifft unter anderem den Zugriff auf persönliche Daten wie Telefonnummern oder GPS-Informationen.

Ist solch eine App erst einmal auf dem Gerät, kontrolliert nicht mehr der Besitzer sein Smartphone oder Tablet, sondern der App-Entwickler. Zu schade nur, dass der Anwender davon nichts ahnt. Richtig heftig wird es, wenn durch die App ein Zugriff auf die Mailbox des Telefons möglich ist und Sprachnachrichten abgehört und mitgeschnitten werden können. **Christian Solmecke**[11], Rechtsanwalt für IT- und Internetrecht in Köln, stellt zwar klar: "Wenn man das Auslesen der Mailbox technisch erlaubt, verstößt das gegen deutsches Datenschutzrecht und kann strafrechtlich relevant sein. Denn hier geht es nicht nur darum, dass der Nutzer selbst seine Daten Preis gibt, sondern es werden auch gleichzeitig die Daten der Freunde preisgegeben." App-Entwickler mit bösen Absichten sollten diese Risiken aber nicht weiter stören. Solche, die "nur Gutes" im Sinn haben, müssen hingegen durchaus aufpassen, dass sie nicht unabsichtlich Funktionen einbauen, die sie später bereuen.

Mögliche Lösungen für Unternehmen

Unternehmen, allen voran den Geschäftsführern und Vorständen, muss klar sein, dass der Einsatz von sozialen Netzen grundsätzliche Risiken mit sich bringt. Wird die Nutzung erlaubt, lassen sich diese durch technische, organisatorische und personelle Maßnahmen aber zumindest mindern. Durch Social-Media-Policies oder auch IT-Versicherungen kann das Restrisiko zudem auf andere übertragen und somit "ausgelagert" werden. Solche Internet-Richtlinien sollten unbedingt klarstellen, dass Mitarbeiter bei der Nutzung von Social Media beruflich und privat die Treuepflicht gegenüber Ihrem Arbeitgeber auch über Ihr Dienstverhältnis hinaus wahren müssen. Was das verbleibende Restrisiko angeht, ist es eine reine Abwägungsfrage, ob der Verzicht auf Social Media schwerer wiegt als mögliche Gefahren. Das muss jedes Unternehmen für sich entscheiden - es ist branchen-, zielgruppen-, abteilungs- und produktabhängig. Wer den Weg des geringsten Widerstands wählt - die Nutzung von Social Media also schlicht untersagt - ist zwar auf der rechtlich sicheren, unter Umständen aber auf der wirtschaftlich schlechteren Seite.

Private Internetnutzung in Unternehmen bleibt so oder so ein kritisches Thema, das die Unternehmerlandschaft besonders in Deutschland spaltet. Das **Bayerische Landesamt für Verfassungsschutz**[12] kommt in einer aktuellen Untersuchung zu dem Ergebnis,

dass 35 Prozent der befragten Unternehmen die private E-Mail-Nutzung am Arbeitsplatz verbieten - immerhin 19 Prozent untersagen das private Surfen im Netz explizit. Um den Wünschen der Mitarbeiter entgegen zu kommen, empfiehlt die Behörde dennoch **ausgewiesene Surfstationen für die private Internetnutzung**[13]. Das dort verwendete Netz sollte vom internen Unternehmensnetz abgekoppelt sein und mit Nutzungsrichtlinien, die von den Mitarbeitern zu akzeptieren sind, versehen sein.

Eine Abwägungsfrage

Denn nicht zuletzt ist es der "Dauerpatient" Mensch, der sich nur durch wiederkehrende Sensibilisierungsmaßnahmen wie firmeninterne Awareness-Kampagnen "behandeln" lässt. Angemessene Mitarbeiterschulungen erfordern ein durchdachtes Konzept, dass regelmäßig überarbeitet und den aktuellen Gefahren des Social Web angepasst werden muss. Die Unterstützung durch die Chefetage - und auch deren Schulung - ist dafür entscheidend. Damit fördern Unternehmen nicht nur ihre eigene Sicherheitskultur, sondern auch ihre Wettbewerbsfähigkeit.

Fünf goldene Regeln zur Nutzung von Social Media

1. Kontaktanfragen in sozialen Netzwerken hinterfragen;
2. Vorsicht bei der Weitergabe von personenbezogenen Daten (vor allem an Dritte);
3. Einverständniserklärungen bei der Installation und Nutzung von Apps beachten;
4. Kritische Unterlagen (Firmendokumente, persönliche Daten, Passwörter, Bankverbindungs- und Kreditkarteninformationen etc.) nicht über Social Media versenden;
5. Zur Anmeldung in sozialen Netzen nur Passwörter mit ausreichender Länge und Komplexität (Sonderzeichen, Zahlen etc.) verwenden. (sh)

[Hinweis auf Bildergalerie:] gal2

Links im Artikel:

[1] **http://www.computerwoche.de/k/social-media-fuer-unternehmen,3471**
[2] **http://www.computerwoche.de/a/atos-origin-will-e-mail-freie-zone-werden,2364066**
[3] **http://www.gesetze-im-internet.de/bdsg_1990/**
[4] **http://www.computerwoche.de/a/warum-europa-einen-neuen-datenschutz-braucht,2532272**
[5] **http://www.verfassungsschutz.de/download/SAVE/symp_2007.pdf**
[6] **http://www.t-systems-mms.com/**
[7] **http://corporate-trust.de/pdf/CT-Studie-2012_FINAL.pdf**
[8] **http://www.computerwoche.de/a/hacker-griffen-auch-apple-an,2533139**
[9] **http://www.computerwoche.de/a/fake-accounts-sind-ein-attraktives-lockmittel,2488118**
[10] **https://www.bit9.com/research/pausing-google-play-infographic/**
[11] **http://www.computerwoche.de/a/warum-europa-einen-neuen-datenschutz-braucht,2532272**
[12] **http://www.verfassungsschutz.bayern.de/**
[13] **http://www.wirtschaftsschutz-bayern.de/App.aspx?EditionViewID=3a5ebacf-5178-4f28-b47e-161d8d5d9fd5**
