IT-Sicherheitstipp: Soziale Netze für Unternehmer sicher nutzen

Um in einen Dialog mit der Öffentlichkeit zu treten, genügt das Betreiben einer Unternehmenswebseite heutzutage nicht mehr. Digitale Technologien und Medien, die Nutzern einen Austausch untereinander und inhaltliche Mitgestaltung ermöglichen, werden als *Social Media* bezeichnet. Mittlerweile ist nahezu jedes große Unternehmen auch im Bereich der Social Media aktiv. Kein Wunder: Das soziale Netzwerk *Facebook* verzeichnet laut *allfacebook.de* beispielsweise allein in Deutschland 21,5 Millionen Nutzer (Stand September 2011). Auch für kleine und mittelständische Unternehmen gewinnen soziale Netzwerke immer mehr an Bedeutung. Das Web 2.0 hat die Kommunikation zwischen Unternehmen und Konsumenten revolutioniert. Nie war es so einfach, direkt und schnell miteinander in Kontakt zu treten. Viele Unternehmer wissen aber auch um die Gefahren, die mit der Popularität der Social Media einhergehen: Laut der Studie *„2011 Global Information Security Survey“*, die die Wirtschaftsprüfungs- und Steuerberatungsgesellschaft *Ernst & Young* im September 2011 veröffentlicht hat, haben mehr als die Hälfte der weltweit befragten 1.700 Unternehmen den privaten Zugang zu sozialen Netzwerken für ihre Beschäftigten gesperrt oder stark eingeschränkt [3] – nicht ohne Grund. In diesem IT-Sicherheitstipp erfahren Sie, wie Sie als Unternehmer soziale Netzwerke sicher nutzen können, ohne große Risiken für Ihre IT-Sicherheit einzugehen.

Fangen Sie lieber klein an

Neben der Entscheidung, ob Ihr Unternehmen in einem sozialen Netzwerk auftreten sollte, steht die Wahl der geeigneten Kanäle. Versuchen Sie nicht, alle gängigen Netzwerke wie *XING*, *Facebook*, *Google+*, *Twitter* oder *LinkedIn* gleichzeitig zu bespielen, sofern Sie nicht ausreichend Ressourcen dafür zu Verfügung stellen können. In jedes Netzwerkprofil muss unterschiedlich viel Zeit investiert werden, damit Sie es aktiv moderieren können. **Sobald Sie ein zeitaufwändiges Netzwerk wie *Facebook* nicht täglich durch einen Beschäftigten betreuen lassen können, kann das nicht nur einen Imageverlust zur Folge haben, sondern auch Gefahren für Ihre IT-Sicherheit bedeuten.** Das Web 2.0 ist ein „Mitmach-Web“, das

jedem Akteur sozialer Netzwerke die Möglichkeit bietet, gleichberechtigt zu kommunizieren und Inhalte auszutauschen. Für Sie als Unternehmer bedeutet das, dass die Besucher Ihres Social Media-Auftritts in der Lage sind, Ihr Profil durch Kommentare, Bilder und Verlinkungen mitzugestalten, sofern dies beim jeweiligen Netzwerk, wie *Facebook*, durch Sie in den Profileinstellungen festgelegt wurde. Einige fragwürdige Inhalte der Nutzer sollten jedoch nicht mit Ihrem Unternehmen in Verbindung gebracht werden. Außerdem stellt die Möglichkeit, dass jeder zunächst ungeprüfte Inhalte auf Ihrem Unternehmensprofil online stellen kann, ein Sicherheitsrisiko für weitere Besucher Ihres Unternehmensprofils dar. Dazu gehört die Gefahr des so genannten „Clickjacking".

Schützen Sie sich und Ihre Besucher vor Clickjacking

Beim Clickjacking locken Kriminelle in sozialen Netzwerken mit Verlinkungen, die oftmals als herkömmliche Videoposts getarnt sind. Sobald ein Nutzer nun auf eine scheinbar reale Videomeldung in seinem Newsfeed klickt, gelangt er auf eine präparierte Internetseite, die mit betrügerischen Absichten erstellt wurde. Diese sieht häufig dem gängigen Videoportal *Youtube* zum Verwechseln ähnlich. In dem Glauben, das Video hier nun abspielen zu können, klickt der Nutzer auf das Video. Dadurch löst er automatisch und völlig unbemerkt die Weiterverbreitung des Links innerhalb der Kontaktliste des Netzwerkes aus. Dies geschieht durch eine unsichtbare Ebene, die über dem Abspiel-Button des Videos liegt. Auf dieser Ebene liegt unsichtbar der typische *„Gefällt mir"*-Button (bei *Facebook*) oder *„+1"*-Button (bei *Google+*). Ist der Rechner des Nutzers nicht durch einen ausreichenden Basis-Schutz geschützt, dient er den Betrügern nicht nur zur Weiterverbreitung des betrügerischen Links, sondern im schlimmsten Fall sogar als schutzlose Plattform für Schadsoftware, die sich schon beim Aufruf der präparierten Internetseite selbstständig installieren kann. Clickjacking in Social Networks kann für Besucher Ihres Unternehmensprofils und damit auch für Ihre Mitarbeiter bei unzureichenden Sicherheitsvorkehrungen ein zusätzliches Einfallstor für Schadprogramme darstellen, sofern kein Beschäftigter die Inhalte der Firmenprofilseite entsprechend moderiert und mehrmals pro Tag auf Inhalte mit betrügerischen Absichten überwacht. **Kann in der Belegschaft kein geschulter Mitarbeiter für diese Tätigkeit gefunden werden, ist die Einstellung eines Experten auf dem Gebiet der Social Media ratsam. Dieser sollte sowohl über Grundwissen im Bereich der IT-Sicherheit verfügen, als auch Erfahrungen in der Kommunikationsbranche gesammelt haben.**

Neben serverseitigen Schutzmaßnahmen kann den Nutzern das Browser-Plugin *NoScript* für den Browser *Mozilla Firefox* Sicherheit vor Clickjacking bieten. Die integrierte *„Clear-Click-Funktion"* sorgt dafür, dass verborgene Inhalte einer Website angezeigt werden. Zudem sollten Sie als Nutzer selbst überprüfen, ob es sich um seriöse Links innerhalb Ihres Newsfeeds handelt. Indizien für bösartige Links sind oft obszöne Titel oder fehlende Kommentare.

Legen Sie die Kommunikationsstrategie Ihres Unternehmens fest

In allen sozialen Netzwerken, in denen Ihr Unternehmen aktiv werden möchte, sollte jeweils nur ein offizielles Unternehmensprofil existieren. Dieses repräsentiert Ihr Unternehmen innerhalb des sozialen Netzes. So können Sie nicht nur kommunikative Fauxpas in Ihrer Öffentlichkeitsarbeit umgehen, die durch das gleichzeitige Vorhandensein mehrerer Unternehmensprofile innerhalb eines Netzwerkes entstehen können – ein Beispiel hierfür wären widersprüchliche Informationen innerhalb der verschiedenen Profile. **Durch den Betrieb eines Profils können Sie alle externen Anfragen an Ihr Unternehmen auf einer einzigen Kommunikationsplattform bündeln.**

Beim Anlegen des Profils sollten Sie darauf achten, für Ihren Benutzeraccount ein sicheres Passwort, bestehend aus mindestens zehn Zeichen inklusive Sonderzeichen, zu vergeben [2]. Schützen Sie das Passwort durch eine regelmäßige Neuvergabe. Beugen Sie Spam über den Betreiber des sozialen Netzwerkes vor, indem Sie eine E-Mail-Adresse speziell für jedes Netzwerk anlegen. Vermeiden Sie es, eine allgemeine Adresse wie „info@“ für diesen Zweck zu nutzen.
Laut dem Telemediengesetz sind alle gewerblichen Internetseiten impressumspflichtig. Da ein Unternehmensprofil innerhalb eines sozialen Netzes nach geltendem Recht Marketingzwecken dient, sind für Unternehmer auch hier die Angaben über das Impressum zwingend erforderlich. So sollten Name und Anschrift Ihres Unternehmens, Kontaktdaten, Umsatzsteuer-Identifikationsnummer, sowie in manchen Fällen auch der Name des Vertretungsberechtigten und die zuständige Aufsichtsbehörde auf Ihrer Unternehmensprofilseite vermerkt sein.

Beschränken Sie den Zugang zum Unternehmensprofil

Die Verantwortlichen sollten geschult sein im Umgang mit Social Media und sich durch besondere kommunikative Kompetenzen in Hinblick auf den Schutz sensibler Betriebsinterna auszeichnen. Indem sie das offizielle Unternehmensprofil betreuen, treten sie als Repräsentative des gesamten Unternehmens auf.

Ergänzend zu dem offiziellem Social Media-Auftritt Ihres Unternehmens können Sie Ihre Beschäftigten dazu ermutigen, eigene berufliche Benutzeraccounts zu erstellen, in denen Sie sich als Mitarbeitende Ihres Unternehmens vorstellen. Hier ist jedoch Vorsicht geboten: Dies macht nur Sinn, wenn die Interessenten über Erfahrungen im Bereich der Social Media verfügen. Es ist ratsam, hier vorhergehende Mitarbeiterschulungen durchzuführen.

Grundlage aller Aktivitäten in sozialen Netzwerken sollte für jeden Beschäftigten ein betriebliches Social Media-Regelwerk sein. Darin sollte genau festgehalten sein, wie im Web 2.0 kommuniziert werden sollte und welche Informationen preisgegeben werden dürfen.

Definieren Sie ein betriebliches Regelwerk für die Kommunikation

Sie und Ihre Beschäftigten sollten stets zwischen Privatem und Beruflichem trennen, wenn Sie sich in sozialen Netzwerken bewegen. **Dies gelingt Ihnen, indem Sie entweder Ihre bestehende Kontaktliste in zwei separate Listen unterteilen oder indem Sie zwei unterschiedliche Nutzeraccounts anlegen – einen für Geschäftskontakte und einen für Freunde und Bekannte.** So können Sie steuern, welches Publikum Ihre Informationen und Aktivitäten im jeweiligen Netz sehen kann. Möchten Ihre Beschäftigten auch auf der offiziellen Social Media-Plattform, sprich dem Unternehmensprofil, aktuelle Geschehnisse kommentieren, sollte stets erkennbar sein, dass es sich um eine persönliche Kommentierung des Einzelnen handelt. Name und Funktion des Mitarbeitenden sollten bei jedem Kommentar erkennbar sein. **Äußerungen von privaten Nutzeraccounts der Beschäftigten sind aus Datenschutzgründen tabu: Ein privater Account eines Beschäftigten ist ein beliebtes Ziel von Kriminellen, die sich mithilfe von Social Engineering-Attacken Zugang zum Unternehmensnetzwerk erschleichen wollen.** So kommt es vor, dass die Datendiebe gezielt einen privaten Account hacken, um sich dann mit diesem gehackten Account in einem Identitätsschwindel sensible Unternehmensinterna, zum Beispiel von Kollegen, zu erschleichen. In der Informationsbroschüre *„Gefahr durch Social Engineering“* finden Sie nützliche Tipps, um Ihr Unternehmen vor den Angriffen Krimineller zu schützen [1].

Weitere Hinweise zum Erstellen eines betrieblichen Social Media-Regelwerkes finden Sie im IT-Sicherheitstipp *„Social Networking – aber sicher!“* [2]

Schützen Sie vertrauliche Daten

In sozialen Netzwerken findet mittlerweile ein Großteil aller Phishing-Angriffe statt. Laut dem halbjährlichen *„Microsoft Security Intelligence Report“*, machen Phishing-Attacken, die über soziale Netzwerke ausgeübt werden, im Zeitraum Januar bis Juni 2011 rund 85 Prozent aller Phishing-Angriffe überhaupt aus. **Oft begünstigen Beschäftigte durch lockere Gepflogenheiten innerhalb eines sozialen Netzes Angriffe auf das Unternehmensnetzwerk.** Fotos von den Büroräumen oder detaillierte Auskünfte über die Arbeitsumgebung erleichtern Kriminellen beispielsweise den Zugang zu Ihrer Dienststelle oder Ihrem Betriebsnetzwerk. Eine große Gefahr für die Sicherheit Ihres Betriebsnetzwerkes stellt oft der allzu lockere Umgang der Beschäftigten mit Unbekannten dar. Dies gilt insbesondere für neue Bekanntschaften, die man innerhalb eines sozialen Netzwerkes schließt. Informationen über laufende Projekte der Beschäftigten sollten nur mit Einverständnis der Chefetage und in Absprache mit dem Verantwortlichen des Social Media-Unternehmensprofils über den offiziellen Firmenaccount oder über den beruflichen Account des jeweiligen Beschäftigten kommuniziert werden. Andernfalls besteht die Gefahr, Opfer von

Wirtschaftsspionage zu werden. **Hinterfragen Sie stets die Absichten von unbekannten Personen, die plötzlich mit Ihnen in Kontakt treten wollen. Wie immer gilt: Sicherheit kommt vor Höflichkeit. Anfragen an das Unternehmen sollten generell an die Verantwortlichen in der Kommunikationsabteilung weitergeleitet werden.**

Welche persönlichen und betriebsinternen Informationen keinesfalls Teil des Netzwerkprofils werden sollten, entnehmen Sie dem IT-Sicherheitstipp *„Richtiger Umgang mit vertraulichen Daten“* [2].

Autoren

Malte G. Schmidt, FH Gelsenkirchen, Institut für Internet-Sicherheit

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen

[1] http://www.kmu-sicherheit.de

http://www.ec-net.de

[2] https://ratgeber.it-sicherheit.de

[3] https://www.it-sicherheit.de

https://www.internet-sicherheit.de

http://www.bsi-fuer-buerger.de

http://www.sicher-im-netz.de

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.kmu-sicherheit.de

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de