„social networking“ – Leichtsinnige Mitarbeiter sind ein Risiko für Arbeitgeber

München, erstmals veröffentlicht im November 2008 – Mit wenigen Mausklicks global Kontakt zu neuen Kunden und Lieferanten aufnehmen und Personen mit gleichen Interessen finden, das ist in Zeiten der „social networks“ kein Problem mehr. Niemanden wundert es, dass bereits Millionen von Menschen Mitglieder in virtuellen Communities sind und es täglich mehr werden. Erstaunlich ist allerdings die Leichtsinnigkeit, mit der häufig persönliche und berufliche Informationen einem breiten Publikum zugänglich gemacht werden. Dass sie damit sich und ihre Arbeitgeber hohen Risiken aussetzen, scheint Vielen nicht bewusst.

Während sich die IT-Sicherheitsbranche auf die zunehmenden Bedrohungen aus dieser Ecke einstellt, scheint die Vertrauensseligkeit der Nutzer in das Medium ungebremst. Viele Arbeitgeber haben dabei offensichtlich gar keine Ahnung davon, was ihre Mitarbeiter so treiben. Der Unternehmensberater Peter Höfl hat das Nutzerverhalten auf Businessplattformen etwas unter die Lupe genommen und kommt zu erstaunlichen Ergebnissen: Durch die gezielte Auswertung und Recherche kann ein Angreifer ohne besonderen Aufwand und technisches Equipment einen Zugang zu sensibelsten Unternehmensinformationen erhalten.

Ein ganz einfaches Beispiel sind diejenigen Mitarbeiter, die unter ihrem Profil eingetragen haben, dass sie eine „neue Herausforderung“ suchen. „Ein solcher Eintrag unter dem groß und breit der Firmenname steht, ist ein gefundenes Fressen und eine Einladung für jeden, der etwas mehr über ein Unternehmen erfahren will“, meint Höfl. Abgesehen davon, dass dies eine Aufforderung zur Abwerbung qualifizierter Mitarbeiter darstellt, lassen sich mit ein wenig Geschick die sensibelsten Informationen über den derzeitigen Arbeitgeber in Erfahrung bringen. Bemerkenswert ist ebenso die Mitgliedschaft und Aktivität in Foren und Interessengruppen, die einen tiefen Einblick in die Persönlichkeit erlaubt und schon mal im Widerspruch zu der beruflichen Tätigkeit stehen kann. Da sehr viele Nutzer freimütig ihre persönlichen Vorlieben veröffentlichen, ist es tatsächlich oft ein Kinderspiel, sich als völlig Unbekannter das Vertrauen zu erschleichen.

Ein anderes typisches Beispiel ist die „Hilfe unter Kollegen“: Ein Mitarbeiter steht vor einer beruflichen Aufgabe und benötigt z.B. Hilfe beim Erstellen einer Excel-Formel und stellt seine Frage in einem Anwenderforum. Auf diesem Weg können interne Daten sehr schnell ihren Weg nach draußen finden können. Da reicht schon eine hilfsbereite einzeilige Nachricht in dem Stil „Schick mir das mal, ich werfe gerne einen Blick darauf“. Vor solcher Fahrlässigkeit kann oft keine noch so ausgereifte technische Lösung oder Firewall schützen. Es darf nicht übersehen werden, dass das social networking auch für die Nutzer selbst nicht völlig ohne Risiko ist: Mögliche Gefahren lauern in Form von Cybermobbing bis hin zum Diebstahl der Identität. Kaum mehr zu überbieten ist der Leichtsinn, wenn Nutzer ihre privaten Adressdaten jedem beliebigen Kontakt offen legen und sich dann in Foren vor Tausenden von Mitlesern freimütig darüber äußern, dass sie jetzt vier Wochen in Urlaub sind.

Damit auch künftig die Vorteile des „social networking“ die Risiken überwiegen, müssen die Arbeitgeber handeln. Dazu empfiehlt Höfl ein mehrstufiges Vorgehen:

Stufe 1: Wie so oft fängt es auch in diesem Bereich mit der Aufklärung an. Nur wer sich der Risiken bewusst ist, kann sievermeiden.

Stufe 2: Der nächste Schritt ist das Erstellen von Regeln oder Richtlinien, die den Sicherheitsansprüchen von Mitarbeitern und Unternehmen Rechnung tragen.

Stufe 3: Was für eine Geschwindigkeitsbeschränkung gilt, setzt sich hier fort: Regeln und ihre Einhaltung müssen überwacht werden. Für Unternehmen bedeutet dies, ein Auge darauf zu haben, was von den eigenen Mitarbeitern aber auch externen Stellen an Informationen (oder auch Desinformation) im Namen der Firma veröffentlicht und verbreitet wird.

Stufe 4: Die potenziellen Risiken, die durch die Beobachtung identifiziert werden, erfordern Abwehrmaßnahmen. Die können sehr individuell sein und sollen jetzt auch im Regelfall nicht übermäßig dramatisiert werden. Oft reicht sicher schon der dezente Hinweis: „Pass auf, was Du da schreibst!“.

Die Nutzung des „social networking“ betrieblich zu verbieten, hält Höfl für keine gute Lösung: „Da sich private und berufliche Interessen sehr stark vermischen, ist dies kaum realistisch und durchsetzbar. Zudem bieten die Communities mit ihren Möglichkeiten zur schnellen und unkomplizierten Kontaktaufnahme auch im geschäftlichen Bereich eine Vielzahl von Chancen und zählbaren Nutzen.“

Kontakt: Peter Höfl, Unternehmensberater
Zündterstrasse 12
80689 München
Tel. 089 255 491 88
Email: info@peter-hoefl.de
Web: www.peter-hoefl.de

Peter Höfl ist Unternehmensberater in München und widmet sich seit vielen Jahren hauptsächlich der Qualitätsoptimierung von Dienstleistungen. Dazu gehört z.B. die Überprüfung der Beratungsqualität durch Mystery-Aktivitäten, die bereits in einer Vielzahl von Branchen und bei namhaften Unternehmen dazu beigetragen haben, den Service zu verbessern.