

„social-networking“ – Weniger ist manchmal mehr

München, 11.04.2009 - Die Communities leben vom Austausch der Mitglieder untereinander. Trotzdem gilt der Grundsatz „weniger ist manchmal mehr“. Eine gewisse Zurückhaltung bei der Veröffentlichung von persönlichen Informationen, sei es im Profil, als Text, Ton, Bild oder Video kann vor unliebsamen Überraschungen schützen.

Zu den Klassikern gehören – gerade bei weiblichen Mitgliedern - der Ex und verschmähte Verehrer, die sich an die virtuellen Spuren der Angebeteten heften. Dies kann eine Form von Stalking darstellen. Nicht selten sind Versuche aus Rache den Ruf durch das Streuen gezielter Informationen zu schädigen.

Cyberkriminelle nutzen zunehmend die Möglichkeiten des social networking. Hierbei wird oft das Vertrauen der Mitglieder missbraucht. Die Gefahren reichen von Spam, der auf die Interessen des Mitglieds zugeschnitten ist, über das Einschleusen von Trojanern und Viren bis hin zum Diebstahl der kompletten Identität. Ziel ist hier immer in irgendeiner Form der Geldbeutel des Opfers.

Der beste Schutz sind der gesunde Menschenverstand und eine Portion Skepsis. Das ist wirksamer als der aktuelle Virenschutz und die Firewall, die natürlich trotzdem selbstverständlich sein sollten. Wer sich der Gefahren bewusst ist und entsprechend umsichtig handelt, kann das Risiko von Angriffen erheblich minimieren. Einige wichtige Regeln dazu:

1. Lesen Sie sich stets die Richtlinien des Anbieters zum Datenschutz und die AGB's durch, damit Sie wissen, wie mit Ihren persönlichen Informationen umgegangen wird.
2. Nutzen Sie die Einstellungsmöglichkeiten zur Privatsphäre bei den Anbietern, wenn Sie ihr Profil anlegen. Überlegen Sie sich gut, wie öffentlich Sie sein möchten.
3. Sofern die Plattform die Verwendung von Nicknames erlaubt, wählen Sie einen Namen, der nicht automatisch Rückschlüsse auf Ihre Person zulässt. Teile des Namens, Geburtsdatums, Wohnortes, Autonummer, Haustiernamen haben dabei nichts zu suchen.
4. Für Passwörter gilt dasselbe wie für Nicknames. Auch sie sollten stets ohne Zusammenhang zu Ihrer Persönlichkeit sein. Nutzen Sie keine Passwörter, die Sie bereits für andere Zwecke wie z.B. Onlinebanking verwenden.
5. Einige Plattformen verlangen die Eingabe des Geburtsdatums. Informieren Sie sich vor der Eingabe, wie sichtbar das Datum für die anderen Mitglieder ist. Im Zweifel schummeln Sie lieber etwas.
6. Mail-Adresse: Ohne Mailadresse geht bei den Online-Plattformen gar nichts. Verwenden Sie für Ihre Aktivitäten am besten eine eigens dafür angelegte Adresse bei einem der Freemail-Anbieter.
7. Telefonnummer: Egal, ob Sie jetzt die Telefonnummer in Ihrem Profil eintragen oder Sie später einem der Kontakte geben. Wenn Sie sich nicht zu 100% sicher sind, verwenden Sie eine gesonderte Telefonnummer. Bestücken Sie z.B. ein altes Handy mit einer Prepaid-Karte.
8. Profilfoto: Ein Foto macht ein Profil erst richtig spannend und wer zeigt sich nicht gerne von seiner besten Seite. Mit Ihrem Bild senden Sie aber auch Signale, die unter Umständen unerwünschte Personen geradezu magisch anziehen.
9. Ziel des social networking ist es, neue Kontakte zu knüpfen und deshalb werden Sie eine Menge Anfragen von anderen Mitgliedern erhalten, die in Ihre Freundes- oder Kontaktliste wollen. Bevor Sie einen Kontakt bestätigen, überlegen Sie sich, ob wirklich ein gemeinsames Interesse besteht. Lassen Sie sich den Kontaktwunsch ruhig begründen und scheuen Sie sich nicht, auch Kontakte abzulehnen. Prüfen Sie

Pressemitteilung von Peter Höfl, Unternehmensberater, München

im Zweifel die Echtheit eines Kontaktes über die Suchmaschine oder durch einen Anruf.

10. Beiträge in Gruppen und persönliche Nachrichten können mehr über Sie verraten, als Ihnen lieb ist. Das fängt schon bei einer Gruppenzugehörigkeit an, die Schlüsse auf Ihre religiösen, politischen oder sonstigen Einstellungen erlaubt. Wer dies kennt und nutzt, kann sich oft problemlos das Vertrauen von Mitgliedern erschleichen, die dann sehr offen Details der persönlichen Lebensumstände preis geben. Grundsätzlich nichts in der Öffentlichkeit verloren haben Informationen, die auf den täglichen Tagesablauf schließen lassen, wie „um 23:00 Uhr gehe ich immer mit dem Hund im Park Gassi“ oder die Abwesenheit von der Wohnung anzeigen „morgen geht mein Flieger und dann bin ich erst mal 14 Tage weg“.

Autor/Kontakt: Peter Höfl, Unternehmensberater
Zündterstr. 12 80689 München
Tel. 089-255 491 88 Fax 01803-551852371
Email: info@social-network-security.de
Web: www.social-network-security.de

Peter Höfl (48 und Unternehmensberater in München) ist selbst seit vielen Jahren in Communities aktiv und widmet sich neben den Sicherheitsthemen beim „social networking“ seit mehr als einem Jahrzehnt der Qualitätsoptimierung bei telefonischen Dienstleistungen. Dazu gehört z.B. die Überprüfung der Beratungsqualität der Mitarbeiter von Hotlines durch Mystery-Calls, die bereits in einer Vielzahl von Branchen und bei namhaften Unternehmen dazu beigetragen haben, den Service zu verbessern