

# Trau, schau, wem

## Gefährdungen durch Social Business Networks, Teil I

Markus Steinkamp, Information Security Consultant

Social Business Networks wie XING, LinkedIn und Co. erleben seit Jahren einen starken Mitgliederzuwachs. Der erste Teil des Artikels zeigt die, bisher weitgehend unbeachteten Gefährdungen auf, die sich für Firmen durch die berufliche und private Nutzung diese Social Business Networks ergeben.

Soziale Netze: umfangreich, nützlich, aber nicht ohne Risiko (Quelle: Stock.xchng)

Es ist wie so oft mit neuen Nutzungsformen der modernen Technik. Am Anfang wird die Entwicklung nicht wahrgenommen, da Sie den betrieblichen Alltag noch nicht erreicht hat. Dann werden die neuen Möglichkeiten nach und nach genutzt und schließlich wird vielleicht über die damit verbundenen Gefahren nachgedacht. Leider sind Angreifer selten so freundlich, diesen Prozess parallel zu vollziehen.

Social Business Networks, in denen sich Berufstätige in der Regel mit einem Steckbrief präsentieren, Kontakte knüpfen und weitere Dienste wie Foren nutzen, wurden zwar schon oft kritisch diskutiert. Deren Gefährdungen für die Informationssicherheit bleiben dabei jedoch außen vor.

Zuerst wurden die Netzwerke von Seiten der Arbeitgeber kritisch gesehen, da sich gute Mitarbeiter dort darstellen und somit für Headhunter leicht auffindbar und kontaktierbar sind. Doch auch wenn der Verlust guter Mitarbeiter für Unternehmen ärgerlich ist, wird die Informationssicherheit nur mittelbar durch den Verlust von Wissen und Erfahrung berührt.

In den letzten Monaten wurden Social Networks im Allgemeinen

aufgrund der Auswirkungen auf den Schutz personenbezogener Daten kritisch in den Medien diskutiert. Der Schutz personenbezogener Daten ist jedoch erst einmal abseits von der Informationssicherheit des Unternehmens zu sehen.

### Warum gefährlich?

Social Business Networks gehören aus verschiedenen Gründen direkt in den Fokus der Informationssicherheit eines Unternehmens. So haben die beiden schon angerissenen Themen indirekt Auswirkungen auf die Informationssicherheit.

Ausgeschiedene Mitarbeiter können unberechtigt Informationen weitergeben, unter Umständen geschieht das sogar ohne einen tatsächlichen Wechsel und mitunter unbewusst. Denkbar wäre, dass im Rahmen eines inszenierten Bewerbungsgesprächs augenscheinlich nach Produkterfahrungen gefragt, tatsächlich aber die IT-Landschaft des aktuellen Arbeitgebers erkundet wird.

Die durch Social Business Networks ermöglichte Aufdeckung von personenbezogenen Daten wiederum verletzt nicht nur die informationelle Selbstbestimmung des Betrof-

fenen – der aufgrund seiner tatkräftigen Mithilfe nur bedingt Mitleid verdient – darüber hinaus gefährdet sie die Informationssicherheit des Arbeitgebers. Erkenntnisse über einen Arbeitnehmer lassen sich hervorragend für personalisiertes Social Engineering gegen ihn selbst oder gegen seine Kollegen nutzen.



Markus Steinkamp, Information Security Consultant

In geringerem Maße treten bei der Nutzung solcher Netze technische Sicherheitsrisiken auf. So beispielsweise, wenn sich jemand aus dem Firmennetzwerk heraus über einen gesicherten Kanal mit einem anderen Netz verbindet. In der Regel laufen die Verbindungen mit Xing

und Konsorten über verschlüsseltes HTTP (HTTPS). Wenn das Firmenetzwerk eine solche Ende-zu-Ende verschlüsselte Verbindung akzeptiert, ohne diese am Übergang zum externen Netz aufzubrechen und die Kommunikation zu scannen, dann kann auf diesem Weg das interne Netz kompromittiert werden oder ein Kanal für Data Leakage entstehen. Die zuletzt zunehmenden Berichte über die Malware-Verteilung in Social Networks verstärken diese Befürchtungen.

## Warum besonders?

Für sich betrachtet stellt jede der bisher genannten Gefährdungen noch keine spezifische Gefährdung durch Social Business Networks dar: Mitarbeiter können auch auf anderen Wegen zu einem Bewerbungsgespräch gelockt werden, für personalisiertes Social Engineering eignen sich alle, auch offline zugängliche Informationen über Mitarbeiter und die Verbindung mit fremden Netzen kommt bei jedem Abruf privater E-Mails vor. Warum sollten Social Business Networks eine besondere Behandlung verdienen?

Zum einen bündeln Social Business Networks zahlreiche der vorgenannten Gefahren, zum anderen nehmen sie einem Angreifer Unmengen von Arbeit ab. Die Nutzer sorgen durch ihre oft umfangreiche Profilpflege bis hin zur Verlinkung anderer Online-Identitäten für eine Korrelation von Daten, an die bis vor wenigen Jahren noch nicht zu denken war. Darüber hinaus liegt in der Regel alles im Klartext vor, keine störenden Pseudonyme oder private Mailadressen müssen ergründet werden, dies alles hat der Betroffene schon für den Angreifer aufbereitet und unter Angabe von Arbeitgeber und Position online gestellt.

Ein Beispiel: Ein Administrator handelt seiner Ansicht nach bestem Wissen und Gewissen, als er im Forum eines Social Business Networks um

Hilfe bittet und denkt, dies ist im Sinn des Unternehmens. Dabei übersieht er, dass seine Anfrage zu einem Konfigurationsproblem der Firewall für einen Angreifer auch eine Einladung sein kann. Dieser bekommt frei Haus die Information geliefert, dass Firma ABC die Firewall XYZ einsetzt, diese aber ungenügend konfiguriert ist.

Ein Angreifer findet in Social Business Networks die benötigten Daten nicht nur sehr leicht, sondern auch in außergewöhnlich guter Qualität, wodurch die Bedrohungslage verstärkt wird. Wo früher das oben beschriebene fingierte Bewerbungsgespräch nötig war, kann heute die detaillierte Infrastruktur eines Unternehmens aus den Angaben zu Erfahrungen und Qualifikationen in den Profilen der Administratoren ermittelt werden.

Eine zusätzliche Dimension bekommen die Netzwerke außerdem durch die Abbildung von Kontaktbeziehungen zwischen den Mitgliedern. Eine ausgiebige XING-Session kann ausreichen, um komplette Abteilungsorganisationen zu rekonstruieren, was wiederum eine sehr gute Ausgangsbasis für Social Engineering Attacken darstellt.

Weiter gelten Profile in Social Business Networks als vertrauenswürdig, obwohl es keinerlei Grund dafür gibt, sicher zu sein, dass der Max Mustermann, der mich soeben über XING kontaktiert hat, der gleichnamige Arbeitskollege ist. Tatsächlich machen es die Daten aus einem Online-Profil leicht, ein identisches zu erstellen und so online die Identität eines anderen anzunehmen, was auf den ersten Blick nicht auffallen wird. Bei beruflichen Erstkontakten über ein Social Business Network ist also gesunde Zurückhaltung und unter Umständen ein Telefonat zur Verifizierung angebracht.

## Impressum

### Informationsdienst IT-Grundschutz

#### 4. Jahrgang – ISSN 1862-4375

#### Herausgeber

Nina Malchus

#### Redaktion

Elmar Török, Fachjournalist  
(verantwort. für den redaktionellen Teil)  
Auf dem Rain 2, 86150 Augsburg  
Tel.: +49 821 4981635  
E-Mail: redaktion@grundschutz.info

#### Verlag

SecuMedia Verlags-GmbH  
Lise-Meitner-Str. 4, 55435 Gau-Algesheim  
www.secu-media.de

Beteiligungsverhältnisse (Angabe gem. §9, Abs.4 Landesmediengesetz RLP) Gesellschafter zu je 1/6 sind Gerlinde Hohl, Klaus-Peter Hohl, Peter Hohl (GF), Veronika Laufersweiler (GF), Nina Malchus (GF), Stefanie Petersen.  
Registereintragung: Handelsregister Mainz B 22282  
Umsatzsteuer-Identifikationsnummer: DE148266233

#### Abo-Service

Veronika Leuschner  
Tel.: +49 6725 9304-25  
Fax: +49 6725 5994  
E-Mail: aboservice@secu-media.de  
www.grundschutz.info

#### Anzeigenleitung

Stefanie Cutuk  
(verantwort. für den Anzeigenteil)  
Tel.: +49 6725 9304-15  
E-Mail: anzeigenleitung@secu-media.de  
Mediadaten unter: www.grundschutz.info

#### Bezugspreise/Bestellungen/Kündigung

Erscheinungsweise 10 Mal jährlich  
(2 Doppelausgaben)

Jahresabopreis für die Printausgabe:

98,00 € inkl. MwSt. u. Vers.k. (Inland) /  
116,10 € inkl. MwSt. u. Vers.k. (Ausland).  
Einzelheft: 9,50 € inkl. MwSt. u. Vers.k. (Inland) /  
11,00 € inkl. MwSt. u. Vers.k. (Ausland).

Eine Kündigung ist jederzeit zur nächsten noch nicht gelieferten Ausgabe möglich. Überzahlte Beträge werden rückerstattet.

Preis Koppelabonnement mit <es> - Die Zeitschrift für Informations-Sicherheit:

198,00 € inkl. MwSt. und Versandkosten (Inland) /  
231,12 € inkl. MwSt. und Versandkosten (Ausland).

Vertriebskennzeichen: ZKZ 78871

#### Satz/Druckvorstufe

BLACKART Werbestudio Schnaas und Schweitzer,  
Stromberger Str. 47, 55413 Weiler

#### Druck

Silber Druck oHG,  
Am Waldstrauch 1, 34266 Niestetal

Urheber- und Verlagsrechte: Alle in diesem Informationsdienst veröffentlichten Beiträge sind urheberrechtlich geschützt. Jegliche Verwendung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und Einspeicherung in elektronische Systeme. Haftung/Gewährleistung Die in diesem Informationsdienst veröffentlichten Beiträge wurden nach bestem Wissen und Gewissen zusammengestellt. Eine Gewähr für die Richtigkeit und Vollständigkeit kann seitens der Herausgeber nicht übernommen werden. Die Herausgeber haften ebenfalls nicht für etwaige mittelbare und unmittelbare Folgeschäden und Ansprüche Dritter.

Titelbild: © plumbe/PIXELIO