

# Trau, schau, wem

## Gefährdungen durch Social Business Networks, Teil II

Markus Steinkamp, Information Security Consultant

**Social Business Networks wie XING, LinkedIn und Co. erleben seit Jahren einen starken Mitgliederzuwachs. Bisher weitgehend unbeachtet blieben aber die Gefährdungen, die sich für Firmen durch die berufliche und private Nutzung dieser Plattformen ergeben.**

**Der zweite Teil des Artikels geht auf Schutzmaßnahmen ein, die Unternehmen ergreifen können.**

Wer ein Social-Business Network nutzt, bewegt sich meist zwischen den beiden Polen private und berufliche Nutzung. Selbstständige und Freiberufler verwenden Plattformen wie Xing oder LinkedIn oft für die Akquise und Projektabwicklung. Für die meisten fest Angestellten überwiegt bei Social Business Networks dem beruflichen Kontext zugeordnet. Dies ist nicht unproblematisch, da IT-Sicherheitsabteilungen Gefährdungen unterschätzen können. Oft nimmt der CIO an, dass die Nutzung von LinkedIn oder ähnlichen Diensten als privat deklariert und damit wirksam untersagt wurde. In Einzelfällen kommt es sogar zur teilweisen Verlagerung von geschäftlicher Kommunikation oder der Pflege von Kunden-/Auftragnehmerbeziehungen aus dem eigenen Netzwerk heraus, womit Kontakte und Nachrichten den dafür konzipierten Prozessen wie einer rechtssicheren Archivierung entzogen werden. Entsprechend greifen auch die für diese Prozesse implementierten Sicherheitsmaßnahmen nicht mehr.

### Was tun?

Die umfangreichste Maßnahme „gegen“ Social Business Networks wäre das Verbot der Nutzung oder mindestens das Verbot der Arbeitgebennennung. Noch vor Kurzem wurde diese Idee von Juristen abge-



Gemeinsam stark: Social Business Networks können beim Finden von Fähigkeiten und Ressourcen helfen. (Quelle: Stock.xchng)

lehnt, da ein solcher Eingriff in die Privatsphäre des Arbeitnehmers nicht zu rechtfertigen sei. Allerdings fand die Diskussion vor dem Hintergrund der eingangs beschriebenen Abwerbproblematik statt. Das Verbot wurde deswegen abgelehnt, da man einem Arbeitnehmer nicht verbieten könne, einen Lebenslauf mit der Angabe des aktuellen Arbeitgebers zu erstellen.

Unter Arbeitsrechtlern mehren sich nun in Anbetracht der vorgenannten Gefährdungen die Stimmen, die ein, zumindest teilweises, Verbot als zulässig bewerten. Wenn schon die Information über die Betriebs-

zugehörigkeit sensibel ist, erscheint dies in jedem Fall angemessen. So ist es sicher kein Zufall, dass man bei XING vergeblich nach einem der geschätzten 6.000 Mitarbeiter des Bundesnachrichtendienstes sucht. Dies bleibt jedoch aufgrund der konfliktreichen Umsetzung und schwierigen Kontrolle eine akademische Diskussion, konkrete Streitfälle oder gar arbeitsgerichtliche Urteile sind nicht bekannt.

Weil der Nutzen von Social Business Networks unbestritten ist, wäre ein allgemeines Verbot meist nicht sinnvoll. Wichtig ist aber, dass sich jedes Unternehmen der grundsätzlichen

Gefährdungen bewusst ist und für sich im eigenen Information Security Management System (ISMS) eine angemessene Entscheidung trifft. Diese Entscheidung muss anschließend in die entsprechenden Richtlinien und Prozesse integriert und kommuniziert werden. Eine eigene Richtlinie dürfte nur in seltenen Fällen angemessen sein. Meist sind Internet-Richtlinien und Awareness-Programme betroffen.

### Nutzung klar trennen

Die Internet-Richtlinie sollte festlegen, ob und wo es im Unternehmen eine sinnvolle berufliche Nutzung

von Social Business Networks, beispielsweise im Personalbereich, gibt. Jede weitere Nutzung muss unmissverständlich der Privatsphäre zugeordnet und mit allen Konsequenzen wie gegebenenfalls dem Verbot der Nutzung über den vom Arbeitgeber zur Verfügung gestellten Internet-Zugang behandelt werden.

In den Awareness-Programmen sind die Gefährdungen durch Social Networks zu vermitteln. Dies kann und sollte im Rahmen der Fürsorgepflicht mit einer Sensibilisierung für den Datenschutz einher gehen: Gesundes Misstrauen und die oft vorhandenen, aber standardmäßig

nicht aktivierten Privacy-Optionen der Netzwerke wie die Unterdrückung der Anzeige eigener Kontakte nutzen schließlich auch dem Unternehmen.

Ob dazu noch konkretere Regelungen getroffen werden und beispielsweise die Nennung aktuell im Unternehmen eingesetzter Produkte verboten ist, muss jedes Unternehmen für sich entscheiden. Vor dem Hintergrund der schwierigen Kontrolle und der Überwachung eines Bereichs, der vorher ausdrücklich der privaten Sphäre zugeordnet wurde, sollte es bei Hinweisen und Bitten belassen werden.

# Veranstaltungen

## Messen Kongresse

### Integralis Security World 2009

Integralis Deutschland GmbH  
23. - 24.6.2009, Stuttgart Airport  
www.integralis.de

### Corporate Compliance 2009

IQPC  
30.6. - 2.7.2009, Berlin  
www.iqpc.de

### IT-Security Update

IIR Technology  
1.7.2009, Frankfurt a.M.  
www.iir.de

## Seminare

### Roadshow: SECURE ON TOUR

Management Circle AG  
26.6.2009, Frankfurt a.M.  
www.managementcircle.de

### SOA-Security

CAST e.V.  
18.6.2009, Darmstadt  
www.castforum.de

### BSI IT-Grundschutz

BSP. SECURITY  
22.6. - 24.6.2009, Regensburg  
www.bsp-security.de

### T.I.S.P. TeleTrusT Information Security Professional

Fraunhofer-Institut für Sichere Informationstechnik (SIT)  
22. - 27.6.2009, Darmstadt  
www.sit.fraunhofer.de

### Aufbau einer Windows PKI

Secardeo GmbH  
23. - 25.6.2009, Ismaning  
www.secardeo.de

### Datenschutzprüfungen durch die Aufsichtsbehörde

datakontext GmbH  
24.6.2009, Hamburg  
www.datakontext.com

### Die IT-Security Policy

TÜV Rheinland Akademie GmbH  
25. - 26.6.2009, Hamburg  
www.tuev-akademie.com

### Recht und Haftung für IT-Leitung und Management

PROKODA GmbH  
26.6.2009, Berlin  
www.prokoda.de

### Datenschutz aktuell

FFD Forum für Datenschutz  
29. - 30.6.2009, München  
www.ffd-seminare.de.

### Schulung: IT-Forensik - Praxiserprobte Vorgehensweisen

isits International School of IT Security  
29. - 30.6.2009, Bochum  
www.is-its.org

### Sicherheit in IP-Netzen

SMLAN - SoftwareTraining  
29.6. - 1.7.2009, Berlin  
www.smlan.de

### Security Certification Seminar (SCS)

Lanworks AG  
29.6. - 3.7.2009, Neuss  
www.lanworks.de

### ISO 27001: 2005 - Lead Auditor Kurs (IRCA)

qSkills GmbH & Co. KG  
29.6. - 3.7.2009, Nürnberg  
www.qskills.de

### Spionagerisiko Computer

VSW Vereinigung f.d. Sicherheit d. Wirtschaft  
Hessen, Rhl.-Pfalz, Saarl.  
30.6.2009, Mainz  
www.vsw-service.com

### Information Security Management auf Basis ISO 2700x

CBT Training & Consulting GmbH  
1. - 2.7.2009, Hamburg  
www.cbt-training.de

### Praxisgerechte Anwendung von ISO 27001 und ISO 27002

ITACS Training AG  
1. - 3.7.2009, Zürich  
www.itacs.ch

### ISSECO Certified Professional for Secure Software Engineering

Virtual Forge GmbH  
1. - 7.2009, FH Brandenburg  
www.virtualforge.de

### Sicherheit und Zuverlässigkeit eingebetteter Systeme

Deutsche Informatik-Akademie GmbH  
2. - 3.7.2009, Mannheim  
www.dia-bonn.de

### Ausbildung zum geprüften, betrieblichen Datenschutzbeauftragten

Filges IT Beratung  
6. - 10.7.2009, Oberhausen (Ruhrgebiet)  
www.filges.de

### Forensik - Verfahren, Tools, Praxiserfahrung

Secorvo Security Consulting GmbH  
7. - 10.7.2009, Karlsruhe  
www.secorvo.de.college

### Prüfung des Notfall- & Krisenmanagements

Haub + Partner GmbH  
9. - 10.7.2009, München  
www.haub-seminare.de

### EC-Council: Certified Ethical Hacker (CEH)

ROMAN - Consulting & Engineering AG  
13. - 17.7.2009, Zürich  
www.roman.ch