

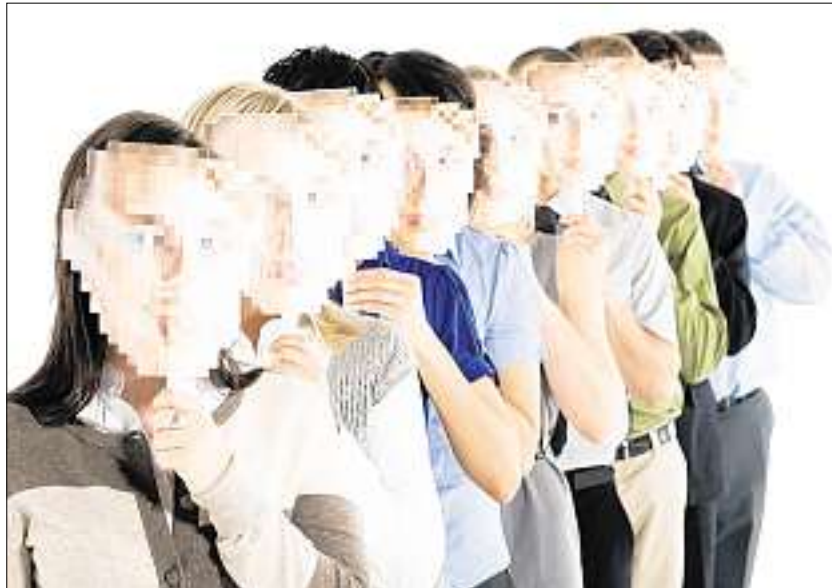
(Unfreiwillige) Spione im eigenen Haus

SOCIAL MEDIA: Soziale Netzwerke stehen hoch im Kurs. Doch es kann zu Schwierigkeiten führen, wenn Mitarbeiter – bewusst oder unbewusst – sensible Infos aus Unternehmen ausplaudern.

VDI nachrichten, Bonn, 25. 3. 11, cha

Einfach sympathisch sieht die junge Frau aus, die sich auf Facebook als Reut Zukerman vorstellt: schwarze Haare, braune Augen, ein unwiderstehliches Lächeln. Unwiderstehlich finden die Frau auch 200 Soldaten der israelischen Armee. Sie offenbaren sich der vermeintlichen Freundin, plaudern Details über Stützpunkte aus und verraten Codes. Im Mai 2010 gehen die Freundschaften dann plötzlich in die Brüche. Journalisten finden nämlich heraus, dass Reut Zukerman gar nicht existiert, sondern eine Erfindung libanesischer Agenten ist, die so den Feind aushorchen wollen.

Der Fall Zukerman sorgte und sorgt für Wirbel – und auch in Unternehmenskreisen. Denn was Angestellte in sozialen Netzwerken treiben, bringt immer mehr Sicherheitschefs um den Schlaf: Da plaudern Unzufriedene die Namen von Kunden aus oder bandeln ohne es zu wissen mit Industriespionen und Geheimagenten an, die Know-how abschöpfen wollen. „All das passiert – nur wollen es die meisten Unternehmen nicht wahrhaben“, meint Thorsten zur Jacobsmühlen, Experte für soziale Medien. Öffentlich würden solche Face-



Ist das auch wirklich die Person, für die sie sich ausgibt? Social Media sind Fluch und Segen zugleich, auch für Firmen. Sie können erheblich zum Imagegewinn beitragen, aber auch gefährlich werden. Foto: fionline

book-Lecks nicht gemacht, so zur Jacobsmühlen, nur Indizien deuteten auf den Infokrieg hinter den Kulissen hin. Ein Beispiel: Im Oktober letzten Jahres sperrte Porsche für seine Mitarbeiter den Zugang zu Facebook – aus Sicherheitsgründen, wie Zuffenhausen verkündete.

Fest steht: Die Freundschaftsplattformen haben den Traum aller Schlapphüte wahr gemacht. „Der virtuelle Agent muss das Operationsgebiet nicht betreten“, erklärt Reinhard Vesper aus der Abteilung Verfassungsschutz beim Innenministerium Nordrhein-Westfalen. Was Spione früher in einem gefährlichen Einsatz vor Ort recherchieren mussten,

könnten sie heute – dank Facebook, Xing und LinkedIn – mit wenigen Klicks herausfinden: Positionen von Wissensträgern, Kontaktdaten, private Interessen, warnt Vesper.

Die typische Facebook-Attacke läuft so ab: Der Angreifer gibt sich als Branchenkollege aus und nimmt Kontakt zu einem deutschen Angestellten auf, z. B. über Xing oder Facebook. „Diese Person wird dann mithilfe von Social Engineering ausgeforscht“, schildert Abwehrexperte Vesper. Social Engineering bedeutet zwischenmenschliches Hacking: Zunächst verrät der neue „Freund“ ein paar vermeintliche Geheimnisse von seinem eigenen Arbeitgeber und

baut so Vertrauen auf. Schritt für Schritt wird Nähe aufgebaut, man redet über Hobbys oder die privaten Finanzen. Wenn die Zielperson ihrem neuen Bekannten vollends vertraut, schlägt der Agent zu. Er bietet Geld für Informationen an oder startet einen Hackerangriff. Auch dafür bereiten soziale Netzwerke den Boden: Statistiken aus den USA zeigen, dass ein Facebook-Nutzer auf einen Link, den ein vermeintlicher Freund vorschlägt, 20-mal häufiger klickt als wenn der Link aus einer unbekannten Quelle stammt.

Mitarbeiter, die in eine solche Falle tappen, haben juristisch gesehen schlechte Karten – selbst wenn der Betrieb das Surfen während der Arbeitszeit hinnimmt. „Aus einer Duldung entspringt nicht automatisch ein Recht zur Privatnutzung“, betont Nina Diercks, Rechtsanwältin bei der Kanzlei Rasch in Hamburg. Sprich: Wer trotzdem in eigener Sache surft, riskiert eine Abmahnung oder sogar die Kündigung.

Selbst in der Freizeit gelten Geheimhaltungspflichten. Ob im Büro oder am privaten PC Interna ausgeplaudert werden, spielt keine Rolle. Anwältin Diercks zieht den Vergleich zur Offline-Welt: „Auf einer Party mit 50 Gästen über geheime Vertragsverhandlungen zu reden, ist ja auch tabu.“

Dennoch raten die meisten Experten von einem strikten Facebook-Verbot ab. Anwältin Diercks empfiehlt Firmen, so genannte Social-Media-Guidelines aufzustellen (siehe Kasten), damit Mitarbeiter und Vorgesetzte erkennen können, was erlaubt ist und was nicht. „Wichtig

ist, dass die Regeln verbindlich sind und auch mögliche Sanktionen klar genannt werden.“ Verfassungsschützer Vesper fügt hinzu, dass die Unternehmen ihren „Exhibitionismus“ im Netz beenden sollten. Es sei z. B. schlichtweg fahrlässig, auf einer Homepage interne Fachleute namentlich zu präsentieren. Darüber hinaus sollten Mitarbeiter im Web 2.0 nicht ihren Arbeitgeber nennen und insgesamt vorsichtiger agieren.

Internetexperte zur Jacobsmühlen plädiert ebenfalls dafür, die Mitarbeiter stärker aufzuklären. Doch er gibt auch zu bedenken, dass es letztendlich ein schlechter Führungsstil sei, der Mitarbeiter zu Maulwürfen mache: „Wo die Angestellten Wertschätzung erfahren, gibt es weniger Unzufriedene – und damit auch weniger Lecks.“ CONSTANTIN GILLIES

Regeln für Facebook & Co.

- Die IBM Social Computing Guidelines sehen Folgendes vor (gekürzt):
- Machen Sie klar, dass Sie nur für sich selbst und nicht das Unternehmen sprechen (nutzen Sie einen passenden Disclaimer).
- Publizieren Sie keine vertraulichen und proprietären Informationen.
- Nennen Sie keine Kunden ohne vorherige Erlaubnis. C.G.