COMPUTERWOCHE

Gefährliche Freundschaften

Facebook, Twitter & Co. schaffen einen fruchtbaren Boden für Industriespionage. Durch Social Engineering ist der Aufwand, den Angreifer auf der Suche nach Geheimnissen treiben müssen, so gering wie noch nie.

Von **Constantin Gillies***

Früher war die Arbeit von Jim McDowell** anstrengend. Er musste sich vor den Toren einer Firma auf die Lauer legen und Autos zählen oder stundenlang telefonieren, um Namen von Mitarbeitern herauszufinden. Der gebürtige Amerikaner forscht im Auftrag von Firmen die Konkurrenz aus. Dafür muss er in letzter Zeit aber kaum noch ausrücken, dem Web 2.0 sei Dank. Denn auf Facebook, Xing und LinkedIn verraten ihm die Mitarbeiter mittlerweile ganz von selbst, was er wissen will: Spezialgebiete, Funktion, private Hobbys. McDowell sichtet nur noch die Profile,

Thorsten zur Jacobsmühlen, Experte für soziale Medien:

„Viele Firmen wollen nicht wahrhaben, was ihre Mitarbeiter ausplaudern."

und schon weiß er, wie stark welche Abteilung ist und wo die Wissensträger sitzen – Informationen, die für die Konkurrenz bares Geld wert sind. Deutsche Angestellte seien in Bezug auf Know-how-Schutz viel zu blauäugig, folgert McDowell, „die denken, weil kein Chinese mit dem Fotoapparat auf dem Hof steht, seien sie in Sicherheit".

Nur ein paar Klicks auf Facebook – und schon wird man zum ungewollten Maulwurf? Dieses Risiko ist real. Soziale Netzwerke avancieren zunehmend zum Sicherheitsrisiko für Firmen: Da plaudern unzufriedene Angestellte die Namen von Kunden aus oder bandeln, ohne es zu wissen, mit Industriespionen und Geheimagenten an. „All das passiert – nur wollen es die meisten Unternehmen nicht wahrhaben", meint Thorsten zur Jacobsmühlen, Experte für soziale Medien aus Lohmar bei Bonn. Öffentlich würden solche Facebook-Lecks nicht gemacht, nur Indizien deuteten auf reges Spionagetreiben hinter den Kulissen hin. Ein Beispiel: Im Oktober letzten Jahres sperrte Porsche für seine Mitarbeiter den Zugang zu Facebook – aus Sicherheitsgründen, wie aus Zuffenhausen verkündet wurde.

Was Schlapphüte nicht schafften

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 herausfinde, warnt Vesper.

Die typische Facebook-Attacke läuft so ab: Der Angreifer gibt sich als Branchenkollege aus und nimmt Kontakt zu einem deutschen Beschäftigten auf, zum Beispiel über Xing oder Facebook. „Diese Person wird dann mit Hilfe von Social Engineering

Foto: Fotolia/Tomasz Trojanowski

ausgeforscht", beobachtet 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 erzeugt, man redet über Hobbys oder die privaten Finanzen. Wenn die Zielperson ihrem neuen Bekannten vollends vertraut, schlägt dieser zu. Er erschleicht oder erkauft sich Informationen oder startet einen Hacker-Angriff.

Geheimhaltung gilt überall

Soziale Netzwerke bereiten dafür den Boden: Statistiken aus den USA zeigen, dass ein Facebook-Nutzer auf einen Link, den ein vermeintlicher Freund vorschlägt, mit 20-mal so großer Wahrscheinlichkeit klickt, als wenn der Link aus einer unbekannten Quelle stammt. Und dieser Klick ist besonders gefährlich: Die Sicherheitsfirma Symantec hat eine Million Posts auf Facebook untersucht – und fand in 15 Prozent von ihnen einen Verweis auf Seiten, die mit Malware gespickt waren.

Juristisch gesehen haben Mitarbeiter, die sich im Web 2.0 tummeln, schlechte Karten – selbst, wenn der Chef beim privaten Surfen bislang ein Auge zugedrückt hat. „Aus einer Duldung entspringt nicht automatisch ein Recht zur Privatnutzung", warnt Nina Diercks, Rechtsanwältin bei der Kanzlei Rasch, Hamburg. Angestellte, die ohne ausdrückliche Genehmigung im Büro ihre privaten Kontakte pflegten, riskierten eine Abmahnung oder sogar die Kündigung.

Nina Diercks, Rechtsanwältin bei der Kanzlei Rasch:

„Aus einer Duldung entspringt nicht gleich das Recht zum Privatsurfen."

So verhindern Sie, ungewollt zum Maulwurf zu werden

- Befolgen Sie die Social-Media-Guidelines ihres Arbeitgebers – sofern vorhanden. Sie stehen üblicherweise im Arbeitsvertrag.
- Besuchen Sie soziale Netzwerke während der Arbeitszeit nur dann, wenn der Arbeitgeber das ausdrücklich erlaubt. Wichtig: Stillschweigende Duldung ist keine Erlaubnis!
- Nennen Sie in Online-Profilen nicht Ihren aktuellen Arbeitgeber.
- Publizieren Sie keine vertraulichen oder proprietären Informationen. Nennen Sie keine Kunden ohne vorherige Erlaubnis.
- Wenn Sie Fotos von Ihrem Smartphone aus posten, sollten Sie sicherstellen, dass Ihre Position nicht in den Metadaten auftaucht (ist bei vielen Smartphones voreingestellt!).
- Vorsicht bei vermeintlichen Branchenkollegen, die sich über Facebook bei Ihnen melden. Hinter dem Kontakt kann sich ein Experte für Wettbewerbsausforschung verbergen (Fachwort: Competitive Intelligence).
- Verwenden Sie im Job keine Lokalisierungsdienste wie Foursquare oder Facebook Places. Die Positionsdaten können Dritten wertvolle Hinweise geben. Beispiel: Halten sich viele Manager einer Firma im Hauptquartier des Konkurrenten auf, kann das auf eine bevorstehende Fusion hindeuten.

Was viele Angestellte nicht wissen: Selbst, wenn sie abends am heimischen PC ins Netz gehen, müssen sie die Geheimhaltungspflichten einhalten, die sie mit ihrem Arbeitsvertrag unterschrieben haben. Ob im Büro oder am Privatrechner Interna ausgeplaudert werden, spielt vor dem Arbeitsrichter 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."

Selbst vermeintlich harmlose Statusmeldungen können Angestellten zum Verhängnis werden. „Soziale Netzwerke sind eine Goldmine für Angreifer", betont Candid Wüest von der IT-Sicherheitsfirma Symantec. Er gibt folgendes Beispiel: Der Systemadministrator setzt über Twitter folgende Meldung ab: „Heute Schulung zum neuen Firewall-Programm des Herstellers ...". „Wenn ein potenzieller Angreifer diesen Tweet liest, weiß er, mit welchem System er es in Zukunft zu tun hat", warnt Wüest.

Zuerst Vorgesetzten informieren

Aber was ist, wenn Angestellte soziale Medien nutzen, um auf Missstände im Betrieb oder sogar Gefahren für die Öffentlichkeit hinzuweisen? Rechtfertigt dieses höhere Ziel nicht die Mittel, so wie es etwa Wikileaks für sich in Anspruch nimmt? Nicht unbedingt, sagt die deutsche Justiz. Solche Hinweisgeber – im englischen Sprachraum Whistleblower genannt – haben hierzulande einen schweren Stand. Wer öffentlich Alarm schlägt, sei es über Facebook oder die Presse, riskiert unter Umständen die Kündigung – selbst wenn sich die Vorwürfe später als berechtigt erweisen sollten.

Mitarbeiter müssen sich mit Beschwerden zunächst an ihren Vorgesetzten wenden, also den Dienstweg und die Geheimhaltungsverpflichtungen einhalten. Zwar versuchen Interessengruppen wie das Whistleblower-Netzwerk *(www.whistleblower-net.de)*, mehr Schutz für Tippgeber zu erkämpfen, doch derzeit gilt auch für Facebook-Nutzer im Zweifel: Wer plaudert, fliegt.

Dennoch raten die meisten Experten davon ab, nach Porsche-Vorbild die Schotten komplett dicht zu machen. Damit würde sich das Unternehmen die Chancen nehmen, die das Social Web bietet. Anwältin Diercks empfiehlt stattdessen, Social-Media-Guidelines aufzustellen, damit Mitarbeiter und Vorgesetzte erkennen können, was erlaubt ist und was nicht. Internet-Experte zur Jacobsmühlen plädiert außerdem dafür, die Mitarbeiter rundum 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." *(hk)*

Candid Wüest, Symantec:

„Soziale Netzwerke können eine Goldmine für Angreifer werden."

***Constantin Gillies** ist freier Journalist in Bonn.
**Name geändert