

George Clooney möchte Ihr Freund sein

Richtiger Umgang mit sozialen Online-Netzwerken

Facebook, StudiVZ, Myspace – das Profil im Online-Netzwerk hat längst die frühere Rolle der E-Mail Adresse eingenommen. Selbst Liebeserklärungen werden per Statusmeldung an den elektronischen Freundeskreis gepostet. Was für die einen nichts weiter als die Fortsetzung der SMS mit anderen Mitteln ist, nutzen andere für weit weniger harmlose Zwecke.

Meine Güte, man wird doch noch einmal einen Scherz machen dürfen. Dachte sich ein Brite, als er das Facebook-Profil seines ehemaligen Schulfreunds aus Jux und Tollerei nachahmte. Da standen dann mehr oder weniger originelle Sprüchlein über das Paarungsverhalten des Ex-Kumpels drin, sowie der eine oder andere Hinweis über dessen (angebliche) finanzielle Gegebenheiten. Leider konnte der Banknachbar aus Jugendtagen gar nicht darüber lachen und zeigte den Verursacher an. Resultat: etwa 28.000 Euro Strafe, so entschied der Londoner High Court. Identitätsdiebstahl ist nun mal strafbar, online genauso wie auf dem Papier.

Soziale Netzwerke können eine bequeme und praktische Art sein, wenn Sie mit Ihrem verteilten Freundeskreis in Kontakt bleiben wollen. Doch ein digitaler Freund entspricht per se nicht unbedingt seiner realen Repräsentation. Bei MySpace, StudiVZ, SchülerVZ, Facebook, LinkedIn, Xing, wer-kennt-wen und was es noch an entsprechenden Seiten gibt, ist die Kontrolle, ob eine angemeldete Person tatsächlich die ist, die sie vorgibt zu sein, fast bis nicht vorhanden. Das kann selbst bei relativ irrelevanten Fälschungen gefährlich werden. Eigentlich interessiert es nur die Stars selbst, ob die Profile von Victoria Beckham, Beyoncé Knowles und Kate Hudson tatsächlich zur echten Person gehören oder ob sich ein paar Halbwüchsige in Wuppertal den langweiligen Nachmittag aufhübschen. Doch immer öfter werden solche Fakes als Sprungbrett für Cybercrime genutzt. Links, die Sie angeblich zu Fotogalerien der Musik- und Filmgrößen führen sollen, enden in einem Trojaner und infizieren Ihren Computer. Zurzeit macht der Wurm Mickey Schlagzeilen – er gilt als einer der ersten Crimeware für den extrem trendigen Micro-Blogging-Dienst Twitter. Wurde ein infiziertes Profil angesurft, forderte der Wurm den Usernamen und das Twitter-Cookie an. Damit konnte der Schädling unter dem Namen des Opfers Kurznachrichten verschicken und sich im Profil des Betroffenen einnisten, um weitere User zu infizieren.

Antivirus-Spezialist Kaspersky Lab geht davon aus, dass Crimeware, die soziale Netzwerke ausnutzt, zu den am stärksten zunehmenden Bedrohungen 2009 gehören wird. Übrigens hat Kate Winslet im Februar 2009 die bisherige Spitzenreiterin Britney Spears in puncto Anzahl der Fake-Profil abgelöst. Zwölf falsche Seiten sollen trotz Bemühungen von Facebook nach wie vor online sein.

Elvis lebt!

Wer heute in den Netzwerken auf gut Glück herumsucht, wird praktisch alles und jeden finden, dessen Name irgendeine Bekanntheit erlangt hat. Friedrich Nietzsche ist genauso mit von der Partie wie Karl Marx oder Old Shatterhand. Kein Wunder bei etwa 200 Millionen aktiven Benutzern, allein auf Facebook (2) Bereits bei Jugendlichen gilt: wer keinen Account bei einem der Online-Netzwerke hat, ist irgendwie nicht mit dabei. Aber auch die älteren Semester fühlen sich offensichtlich mit den digitalen Lebensblicken sehr wohl. Laut Facebook ist die demographische Gruppe der über 35-jährigen das am schnellsten wachsende Segment. Auch hier werden fleißig Bilder vom letzten Strandurlaub oder der Geburtstagsparty online gestellt und für Freunde frei geschaltet. Das kann böse ins Auge gehen, wie schon so mancher Bewerber beim Einstellungsgespräch feststellen musste. Für viele Personalchefs gehört die Online-Recherche zur Vorauswahl von Stellenkandidaten. Finden sich im Internet zahlreiche Fotos von klassischen Party-Fehlleistungen, landen Bewerbungsmappen oft im Papierkorb, bevor es überhaupt zu einem ersten Gespräch kommt.

Natürlich sollten Personalchefs in der Lage sein, harmlose Ausfälle im jugendlichen Leichtsinn oder in fortgeschrittener Partylaune als das zu sehen, was sie sind: Privatsache und nur all zu menschlich. Verlassen sollten Sie sich allerdings besser nicht darauf. Das gilt auch für Textäußerungen in Foren, Chats, auf der eigenen Webseite oder eben bei MySpace und Co. Das Internet hat ein langes Gedächtnis. Die Cache-Speicher der Suchmaschinen, in denen einmal erfasste Webseiten auf Jahre hinaus in ihren verschiedenen Versionen

gespeichert werden, sorgen noch nach langer Zeit für unerwünschte Sucheinträge. Solange es um Ihre eigene Website geht, haben Sie die Chance, eine Löschung der Einträge durchzuführen. Bei Einträgen auf Webseiten von Dritten bleibt nur die freundliche Bitte; ein Rechtsmittel besteht in der Regel nicht. Es gibt schon eine ganze Reihe von Dienstleistern, die sich im Kundenauftrag um die Löschung von unerwünschten Informationen im Internet bemühen. Nehmen Sie als Erziehungsberechtigter auch Ihre Verantwortung ernst und achten Sie darauf, welche Web-Inhalte Ihr Kind von sich ins Netz stellt.

Loose Lips sink ships

Reden ist Silber, Schweigen ist Gold – auch für das Internet ist das ein gutes Motto. Entweder halten Sie sich von den diversen digitalen sozialen Netzwerken fern, riskieren dann aber, dass ein anderer ein Profil unter Ihrem Namen anlegt. So gibt es die Variante des Identitäts-Hijacking. Dabei wird ein Profil für das Opfer angelegt und dessen echter Freundeskreis online infiltriert. Das Netzwerk wächst schnell, Verbindungen werden aufgebaut und intensiviert, ohne dass diese Personen Verdacht schöpfen. Später konfrontiert die reale Person mit dem gekaperten Netzwerk und verlangt Geld, wenn über das Profil keine „unangenehmen Dinge“ verbreitet werden sollen.

Es kann also sinnvoll sein, ein Profil anzulegen, bevor es ein Anderer tut. Dann sollten Sie aber auch Gebrauch von den möglichen Datenschutzeinstellungen machen, die solche sozialen Netzwerke bieten. Facebook erlaubt seinen Benutzern sehr detailliert einzustellen, wer welche Informationen sehen darf. Die meisten machen nur keinen Gebrauch davon. Überlegen Sie doch einfach zuerst, welchen Zweck Sie mit Ihrer Mitgliedschaft in diesem Netzwerk verfolgen. Geht es nur um eine Art virtuelle Gedächtnisstütze für Wohnorte und Beschäftigungen Ihrer Freunde? Dann beschränken Sie den Zugriff auf die wesentlichen Daten, das genügt. Lassen Sie die zahlreichen Optionen zunächst ausgeschaltet. Wenn Sie später feststellen, dass eine Funktion wirklich sinnvoll ist, können Sie sie immer noch freigeben.

Im Übrigen ist gesundes Misstrauen immer dann angesagt, wenn Sie sich nicht absolut sicher sein können, dass eine Person wirklich die ist, die sie vorgibt zu sein. Gehen Sie sparsam mit der Akzeptanz von Einladungen um, nutzen Sie für neue Kontakte die Möglichkeit „Limited Friends“, die nur einen Teilbereich Ihrer Infos sehen können. Wenn Sie einer großen Gruppe beitreten – Facebook nimmt neue Mitglieder bei der Registrierung automatisch in bestimmte Gruppen auf – dann geben Sie nicht allen Mitgliedern volle Zugangsrechte. Auch das können Sie in den Datenschutzoptionen einstellen. Absolut Tabu sollten sehr persönliche Daten wie Steuernummern und Geburtsdatum sein. Mit diesen Daten nehmen zahlreiche Unternehmen wie Versicherungen oder Internet-Provider die Verifizierung ihrer Kunden vor. Und ein absoluter Klassiker ist der Passwort-Hinweis. Wenn der Geburtsname der Mutter, die Lieblingsfarbe oder das Haustier entscheidende Hinweise zum Passwort geben, dann haben diese Infos nichts im Profil verloren.

Steigbügel für Social Engineering

Je mehr Infos über eine Person bekannt sind, desto einfacher hat es der Angreifer, sich für ihn auszugeben oder von ihm Informationen zu erhalten. Was früher Talent, Chuzpe und viel Risikobereitschaft erforderte, ist heute per Internet ganz ohne Aufwand möglich. Wer sich mit kreativer Suchmaschinennutzung auskennt, sammelt im Handumdrehen Informationen über eine Person, die früher schlichtweg nicht zur Verfügung standen. Sie haben einen Wunschzettel bei Amazon? Die Titel sagen vermutlich viel über Ihre Hobbys aus. In einer Newsgroup baten Sie um Hilfe bei einem Firewall-Problem? Der Angreifer weiß nun, welche Firewall Ihre Firma benutzt und was damit nicht stimmt. Das Internet erleichtert vor allem die Korrelation verschiedener Quellen, so dass eigentlich zusammenhanglose Bruchstücke ein aussagekräftiges Profil ergeben.

Cyberkriminelle nutzen soziale Netzwerke aber auch ganz traditionell als Verbreitungsmedium für Crimeware. Nach einer Harris Interactive Studie vom Juni 2008 steigen die Spam-Angriffe auf soziale Netzwerke rapide an. In zwölf Monaten haben nach den Ergebnissen 83 Prozent der User unerwünschte Spam-Mails in Form von vermeintlichen Einladungen von Freunden, Postings oder Nachrichten bekommen. Mit dabei waren auch Versuche, die Nutzer auf eine Phishing-Seite oder eine Webseite mit Crimeware zu locken.

Aber Sie sind Phishing-Angriffen nicht hilflos ausgeliefert. Die Angreifer können nur versuchen, Schwachstellen und Nachlässigkeiten auszunutzen. Wenn Sie auf Ihrem Computer ein aktuelles Antiviren-Programm wie Kaspersky Internet Security installieren, ist ein großes Einfallstor bereits geschlossen. Die Software bewahrt Sie nicht nur vor Viren und Trojanern, sondern filtert unerwünschte Spam-Nachrichten aus und schützt vor Bedrohungen während des Online-Chats mit ICQ und Instant-Messenger. Sollten Sie mit Ihrem Web-Browser zu einer Phishing-Website unterwegs sein, werden gute Sicherheitsprogramme ebenfalls Alarm schlagen.

Schwachstellen schnell flicken

Aktualität ist wichtig. So fordert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Bürger dazu auf, ihre Virenschutzsoftware immer auf dem neusten Stand zu halten. Damit nicht genug: Ob Betriebssystem oder Web-Browser, ständig werden Schwachstellen entdeckt, die Hacker mit speziell entwickelten Programmen ausnutzen, um Schadsoftware einzuschleusen. Eigentlich sollten solche Schwachstellen kein großes Problem darstellen: Die Softwarehersteller entwickeln kostenlose Reparaturprogramme, sobald die Fehler bekannt werden. Wenn der Computer richtig eingestellt ist, lädt er sich diese „Patches“ sogar automatisch aus dem Internet herunter. Aber viele Privatanutzer und sogar Firmen warten zu lange, bis sie die Patches einspielen. So konnte sich vor kurzem der so genannte „Conficker“-Wurm (aka Kido) über eine längst bekannte Schwachstelle in Windows auf geschätzte zehn Millionen PCs einschleichen. Heute warnen gute Sicherheitsprogramme auch, wenn sie Schwachstellen finden, für die bereits ein Reparaturprogramm vorliegt.

(1) <http://diepresse.com/home/techscience/internet/454939/index.do?from=simarchiv>

(2) <http://www.facebook.com/press/info.php?statistics>