Facebook als Angriffstool für Cybercrime

„Bezahlen“ mit dem guten Namen

Die Webseite von Facebook ist einladend: Unter der Registrierung steht „Facebook ist und bleibt kostenlos”. Das weltgrößte soziale Netzwerk suggeriert eine kostenlose Erfahrung, die ein umfangreiches Angebot an Informationen und Kontakten mit einschließt. Auch wenn kein Geld fließt – bezahlt wird dennoch: mit persönlichen Daten der Nutzer, für die sich Facebook weitreichende Rechte in den AGBs als Gegenleistung einräumen lässt. Über individualisierte Werbung kommt schließlich doch Bares in die Kasse. Die persönlichen Daten aber bilden auch ein attraktives Ziel für Kriminelle, die sich damit entweder direkt bereichern oder die bei weiteren Usern Missbrauch treiben wollen. Damit es am Ende nicht doch teuer wird – hier ein paar Infos und Tipps für den adäquaten Umgang mit dem beliebten sozialen Netzwerk.

Facebook ist zwar ein soziales Netzwerk, aber alles andere als ein sozialer Verein. Selbstverständlich handelt sich um ein profitorientiertes Unternehmen, das Verantwortung gegenüber Mitarbeitern, Werbekunden und Investoren hat – und die erwarten auf Dauer nichts anderes als steigendes Wachstum und am Ende schwarze Zahlen und einen satten Profit. Im Unternehmen selbst sind zurzeit rund 3.200 Menschen tätig. Mittelfristig sollen circa 1.000 weitere hinzukommen – und sie alle wollen entlohnt werden. Die soziale Medien-Plattform Facebook gibt es in 70 Sprachen mit Servern und Niederlassungen in 20 verschiedenen Ländern. Facebook ist Marktführer in allen Ländern außer Russland (dort ist „VKontakte“ Spitzenreiter) und China – hier ist der Zugriff auf die Plattform komplett gesperrt. Das Wachstum der angemeldeten Nutzer, die das Fundament des Konzepts sind, ist enorm und scheint weiterhin ungebremst. Mittlerweile sind über eine Milliarde Menschen bei Facebook angemeldet.

Wäre Facebook ein Land, wäre es mit seinen 1,01 Milliarden „Bürgern“ das drittbevölkerungsreichste der Welt. Lediglich China und Indien haben (noch) mehr „Einwohner“ (Abbildung 1). In Deutschland nutzen circa 22,6 Millionen (in den letzten sechs Monaten + 2,5 Millionen) Menschen soziale Netzwerke, was 25,1 Prozent der Bevölkerung entspricht. Davon sind 52 Prozent männlich und 48 Prozent weiblich (Abbildung 2). Bei rund 1,01 Milliarden angemeldeten aktiven Nutzern (circa 552 Millionen besuchen Facebook täglich) und einem erzielten Umsatz von 924,4 Millionen Euro lässt sich grob über den Daumen rechnen: ein Euro Umsatz pro angemeldetem Nutzer.

Abbildung 1

Abbildung 2

Im direkten Vergleich mit anderen sozialen Netzwerken ist der Facebook-Nutzer am aktivsten: 52 Prozent sind täglich auf Facebook unterwegs – bei Twitter sind es immerhin noch 36 Prozent und bei LinkedIn „nur“ 6 Prozent. Die hohe Aktivität spiegelt sich auch in den Uploads: Die Facebook-Nutzer laden schätzungsweise 300 Millionen Fotos pro Tag auf die Server von Facebook und teilen 2,5 Milliarden Inhalte. Das macht insgesamt etwa 500 TByte an neuen persönlichen Daten täglich – auf ein ganzes Jahr bezogen also 182,5 PetaByte an neuen Daten, die gespeichert und wieder mehrfach ausgeliefert werden.

Der durchschnittliche Nutzer pflegt circa 229 Freundschaftsbeziehungen, von denen er jedoch im Durchschnitt 6,9 Menschen (drei Prozent) noch nie persönlich begegnet ist. Dies bietet insgesamt ein hohes Maß an Potenzial für die Veröffentlichung von Informationen an Menschen, die diese eigentlich nicht sehen sollten. So wäre beispielsweise die Einstellung „sichtbar für Freunde von Freunden“ sehr ungünstig, da genau diese 6,9 „Freunde“ als Multiplikator dienen würden, um private Inhalte in Profile zu streuen, die dort nicht gesehen werden sollten. Weiterhin sind davon 22 Prozent von der Universität, 12 Prozent Arbeitskollegen und 9 Prozent von der Schule her bekannt. Während der durchschnittliche Nutzer 2008 circa 33 Jahre alt war, ist er heute schon 38 Jahre alt.

Der Erfolg eines sozialen Netzwerks, dem viele persönliche Daten anvertraut werden, hängt aber auch stark von der realen und empfundenen Vertrauenswürdigkeit ab. Es sollte gewährleistet werden, dass die eigenen privaten hochgeladenen Daten sicher aufbewahrt und nur bestimmten ausgewählten Personen und Kreisen zugänglich gemacht werden. Zur Vertrauenswürdigkeit gehört aber auch die Verlässlichkeit der genutzten Funktionen. Rufen wir uns nochmal in Erinnerung, wie Vertrauen definiert ist und was es genau bedeutet. Wikipedia lehrt uns: „Vertrauen ist die subjektive Überzeugung von der Richtigkeit, Wahrheit von Handlungen, Einsichten und Aussagen eines anderen oder von sich selbst (Selbstvertrauen). Zum Vertrauen gehört auch die Überzeugung der Möglichkeit von Handlungen und der Fähigkeit zu Handlungen.“ Übertragen auf Facebook muss also sichergestellt sein, dass vor allem beim Punkt Aussagen und Wahrheit die suggerierten Informationen, die wir als Nutzer in Form von Nachrichten, Apps und Links respektive E-Mails erhalten, diesem Schema folgen. Genau hier lauern die Gefahren, die nachfolgend in den gängigsten Szenarien genauer erklärt werden sollen.

Missbrauchs-Szenarien mit Facebook

Der vor einiger Zeit eingeführte Like-Button wird im Durchschnitt von jedem Facebook-Nutzer täglich 2,8-mal benutzt und jeder Nutzer teilt circa 2,6 Inhalte täglich mit seinen „Freunden". Das „liken" von Inhalten hat aber weitreichendere Folgen, als manchem zunächst bewusst ist. Klickt einer der Freunde aus dem eigenen Netzwerk auf einen Inhalt seiner Freunde/Fan-Seite, mit denen er nicht direkt befreundet ist oder ohne diese abonniert zu haben, wird diese Information trotzdem für den Nutzer sichtbar und praktisch in dessen eigene „Timeline" gestreamt.

An normalen Tagen „liken" 26 Prozent der durchschnittlichen Facebook-Nutzer das Status-Update ihrer „Freunde", wobei Unternehmensseiten hierbei mit eingerechnet werden. Insgesamt 22 Prozent kommentieren die Updates ihres Netzwerks und 15 Prozent bringen ihre eigenen Status-Updates auf den neuesten Stand. Unter diesen Rahmenbedingungen haben beispielsweise „schädliche Links", getarnt als Statusnachrichten, die Möglichkeit, ein hohes Maß an Reichweite zu gewinnen.

Angriffsmethode: Angreifer erstellen eine scheinbar echte Fan-Seite

Zu den bekanntesten Features der Facebook-Plattform gehören sicherlich die „Fan-Seiten". Hier kann jeder Nutzer zu jeder Zeit nach Belieben eine eigene Facebook-Seite gründen oder schließen und dieser ein gewünschtes Thema mit Layout verpassen. Der eigentliche Zweck, das Motiv und die Echtheit solcher Facebook-Seiten wie auch der Besitzer sind für die Facebook-Nutzer nur schwer überprüfbar. Dies ist in jedem Fall ein Verstoß gegen die Vertrauenswürdigkeit, die eine Grundlage für den offenen Umgang mit Informationen in sozialen Netzwerken ist. Im Umkehrschluss ist es leicht, die „nicht echte" Vertrauenswürdigkeit der Fan-Seite zu „kaufen", beispielsweise durch Lockangebote wie „20-Euro-Gutscheine für's Liken" oder die Verlosung hochwertiger Geräte wie Smartphones. Die Angriffsmethodik ist dabei denkbar einfach: Die Täter erstellt eine gefakte Fan-Seite als Ausgangspunkt, um die Besucher auf Webseiten zu locken, die in der Lage sind, den Computer mit Malware zu verseuchen. Zu den gängigsten Schad-/Missbrauchsszenarien gehören unter anderem die Installation von Key-Loggern („Tasten-Rekorder"), die Nutzung des Computers als Spam-PC, DDoS (Distributed Denial of Service: Verteilte Dienstblockade)-Angriffe, Click Fraud (Klickbetrug) und zunehmend auch Erpressung des Nutzers mit Lösegeldforderungen für seine eigenen Daten, die zuvor durch den Schädling verschlüsselt worden sind (Abbildung 3).

Abbildung 3

Es gibt auch Profile von Kneipen, Lieblingsfirmen oder Vereinen, die statt einer Fan-Seite ein personenorientiertes Facebook-Profil verwenden und „Freundschaften" mit ihren Kunden pflegen, um auf sich aufmerksam zu machen und Informationen zu publizieren. Es ist generell absolut davon abzuraten, solche Profile blindlings als „Freund" zu akzeptieren. Der Grund liegt auf der Hand: Niemand kann mit Sicherheit sagen, wer hinter diesem Facebook-Profil steckt, wie viele Personen Zugriff zur „Accountpflege" haben und welche Informationen meines Profils wie verwendet werden. Denn durch das Annehmen der „Freundschaft" öffnet der Facebook-Nutzer seine gesamte Privatsphäre diesen Unbekannten – inklusive Fotos, Videos, Orte, Statusnachrichten und aller gemachten Angaben, die eigentlich nur für den eigenen engen Freundeskreis bestimmt waren. In dem Fall hilft auch die höchste und penibelste Sicherheitseinstellung nichts.

Es ist empfehlenswert, zu hinterfragen, ob die vorgegebenen Firmen wirklich hinter den Offerten der abonnierten Facebook-Seiten stehen: Fehlerhafte Rechtschreibung und nicht authentisches Auftreten sollten in dem Fall sofort Misstrauen erwecken. Die erwähnten „Freundschaftsanfragen" von Vereinen, Gastronomen und anderen Institutionen sollten in jedem Fall aufgrund der oben genannten Gründe generell abgelehnt werden.

Angriffsmethode: Gefälschte Facebook-E-Mail-Benachrichtigungen versenden

Bei neuen Ereignissen wie Freundschaftsanfragen oder Anfragen zur Markierung der eigenen Person auf Fotos versendet Facebook E-Mails, um den Nutzer über diese Aktivitäten zu informieren. Der Nutzer kann dann entweder den eigentlichen Inhalt in der E-Mail sehen oder er wird gebeten, die Facebook-Seite über einen eingebetteten Link in der E-Mail aufzurufen, um sich zur notwendigen Unterseite zu begeben. Solche E-Mails bieten ein hohes Maß an Möglichkeiten der Vortäuschung, denn E-Mail-Absenderadressen können allgemein leicht gefälscht werden, auch die von Facebook. Die Links in der falschen Facebook-E-Mail zeigen dann auf manipulierte Webseiten der Angreifer. Diese Angriffsmethode dient wiederum in erster Linie der Infektion des Computers mit Malware (Schadensszenarien siehe oben) oder dem Diebstahl der eigenen Zugangsdaten.

Es wird empfohlen, bei dieser Art der Benachrichtigung niemals die Links aus den E-Mails zu verwenden, sondern sich immer direkt auf Facebook mithilfe der Favoriten im Browser (stets per https) dorthin zu begeben. Alternativ auch über die gegebenenfalls installierte Smartphone-App. Ist tatsächlich eine Benachrichtigung aktiv, wird sie hier entdeckt, aber sollte dies nicht der Fall sein, wird dies spätestens nach dem Aufruf des Facebook-Portals ersichtlich. Zusätzlich empfiehlt es sich, dass voreingestellte Optionen in den eigenen Kontoeinstellungen unter „Benachrichtigungseinstellungen" überarbeitet werden, um die Benachrichtigungsintensität auf ein Minimum zu reduzieren (Abbildung 4).

Abbildung 4

Generell gilt: In E-Mails enthaltene Links, die auf reine IP-Adressen verlinken oder kryptische Domainnamen nutzen, die keinerlei Bezug zur erwarteten Webseite enthalten, sollten keinesfalls benutzt werden. In diesem Fall sind die Webseiten meist gefälscht oder manipuliert. Auch sollten der eingesetzte Browser immer auf dem neuesten Stand gehalten werden und ein aktuelles Antiviren-Programm mit einem aktiven Hintergrundscanner sollte installiert sein. Letzteres sollte in der Lage sein, Daten und Webseiten in Echtzeit zu analysieren und Schädlinge herauszufiltern. Ein achtsames Handeln ist ebenfalls ein probates Mittel, um tückischen E-Mails auf den Leib zu rücken.

Angriffsmethode: Manipulierte Anwendungen (Apps) anbieten

Zu einer interaktiven und komplexen sozialen Plattform, die sich dem Thema Personalisierung verschrieben hat, gehören auch Erweiterungen, die Dienste/Anwendungen und Funktionalitäten nachrüsten (Apps) oder, an die Daten von Facebook gekoppelt (Freunde, Interessen), für zusätzliche Unterhaltung sorgen (Spiele). So ist es möglich, „Anwendungen" direkt im Profil zu „installieren", um den normalen Funktionsumfang zu erweitern. Ein einfaches Beispiel wäre eine tägliche Meldung des eigenen Horoskops oder Ähnliches (Abbildung 5).

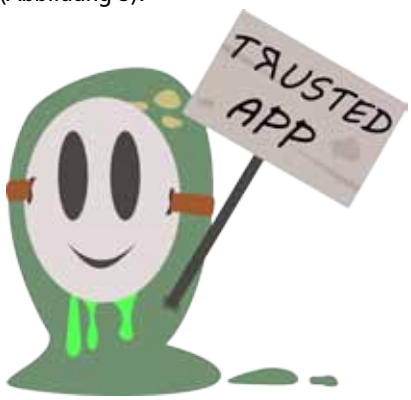

Abbildung 5

Jede Anwendung, die ins Profil integriert wird, verlangt eine Datenfreigabe mit einer Auswahl an verschiedenen Daten und den Zugriff auf verschiedene persönliche Informationen aus dem eigenen Profil. Die Freigabe dieser persönlichen Daten wird bei der Installation der App angefordert und wird, einmal erteilt, dauerhaft „scharf" geschaltet. Viele Anwendungen verlangen den Zugriff auf die privaten Fotos, Freundeslisten, persönliche Informationen wie E-Mail-Adresse, Telefonnummern und eindeutige IDs, die dem Nutzer auf Facebook gegeben werden und ihn so universell identifizierbar machen. Dies ist sehr problematisch, da nicht sichergestellt werden kann, wo diese ausgelesenen persönlichen Daten versinken und was genau mit ihnen geschieht.

Ein Beispiel: Vor einiger Zeit gab es eine Anwendung mit dem Namen „Wer besuchte meine Facebook-Seite am häufigsten", die einen hohen Grad der Verbreitung erreichte. Die versprochene Funktionalität ist bei Facebook nicht realisierbar, da es hierzu keinerlei Daten gibt, auf deren Basis sich solch eine Anwendung in der Realität mit korrekter Funktionalität würde entwickeln lassen. Als Ergebnis hat diese Anwendung willkürliche Angaben geliefert. Ihre wahre Funktion jedoch war es, mit den erteilten Rechten im Hintergrund Spam auf der eigenen und den Pinnwänden der Freunde zu verteilen.

Auch wurde kürzlich die unter Smartphone-Nutzern sehr bekannte und beliebte Chat-App „WhatsApp" auf Facebook als Anwendung angeboten mit der Verlockung, endlich auch außerhalb des Smartphones mit seinen Freunden chatten zu können – nämlich als Browser-App integriert in das eigene Facebook-Profil. Klingt auf den ersten Blick als WhatsApp-Benutzer sehr praktisch und verlockend, denn diese Funktionalität wird von den Nutzern seit längerem gewünscht und von den Entwicklern scheinbar ignoriert. Wie schade nur, dass es weder Schnittstellen seitens des offiziellen Anbieters für solch eine Funktionalität gibt noch solch einen Dienst oder solch eine Anwendung auf Facebook! WhatsApp ist bis dato eine rein mobile App, und die Installation dieser „schädlichen App" hat zur Folge gehabt, dass Facebook-Nutzer den Zugriff auf eine Menge persönlicher Informationen (dauerhaft) zulassen, ohne irgendeinen Gegenwert dafür zu erhalten (Abbildung 6).

Abbildung 6

Durch solche erteilten Freigaben ist es für die Anbieter möglich, neben den ausgelesenen Daten des Opfers, unwissentlich Statusnachrichten in seinem Namen zu veröffentlichen und so sein Netzwerk mit beispielsweise erschreckenden Fotos und gekürzten Links auf externe Webseiten zu locken, über die Schädlinge auf die genutzten Computer verbreitet werden können. Eine Analogie hierzu wäre auch die Bezeichnung Facebook-Wurm oder Click-Jacking.

Angriffsmethode: Horror-, Sex- oder Promi-Video anbieten

Spektakuläre Videos oder angedeutete sexuelle Inhalte mit Prominenten, aber auch schreckliche Videos mit dem scheinbar realen Unglück von Menschen oder ähnliches Material wecken oft die Neugier der User und verleiten diese dazu, „kurz reinzuschauen". Diese Inhalte sprechen in erster Linie Instinkte wie Neugier, Sexualtrieb und Voyeurismus an. Facebook-Nutzer werden motiviert, gefälschte Fan-Seiten zu „liken" oder (gefährliche externe) Links aufzurufen, um die „spektakulären" Inhalte sehen zu können. Ausgangspunkt sind oft Statusnachrichten von Freunden, die in ihren Postings darauf hinweisen, von denen sie oft allerdings selbst nicht wissen, dass sie diese verfasst haben sollen (Abbildung 7).

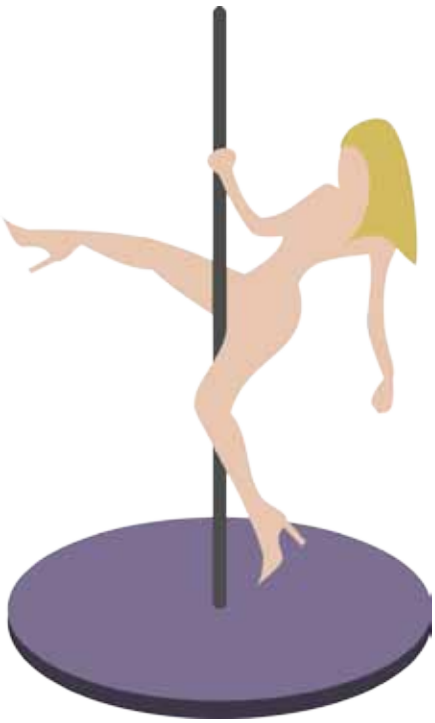

Abbildung 7

Diese gefälschten Nachrichten finden dank „Click-Jacking" den Weg von einer beliebigen Webseite direkt ins Profil eines Opfers. Für das Click-Jacking wird ein bestimmter „interessanter" Inhalt gezeigt, den man „liken" soll und der jedoch durch einen weiteren völlig anderen „unsichtbaren" überlagert wird. Klickt man nun auf einer Webseite eine „Gefällt mir"-Fläche an, zeigt man seinen Freunden in seinem persönlichen Netzwerk nicht das scheinbar interessante Video oder Ähnliches, sondern Inhalte, die der Angreifer beliebig bestimmen kann: verkürzte Links auf Webseiten mit schädlichem Inhalt oder Werbung etwa für Diät- oder Potenzmittel.

Die Verbreitung von schädlichen und ungewollten Inhalten lässt sich durch Wachsamkeit bei der Abfrage persönlicher Daten und durch die Ablehnung unrealistischer Videos und Inhalte verhindern.

Angriffsmethode: Hoaxes und falsche Warnungen verbreiten

Häufig werden von Angreifern Nachrichten mit Inhalten versendet, die schockieren oder verblüffen sollen. Nachrichten mit Inhalten wie „Hilf uns, dass Facebook kostenlos bleibt" oder „Kind vermisst" werden häufig als Träger verwendet, um Spam mit schädlichen Links zu versenden oder einfach nur Unruhe zu stiften und den Empfänger emotional zu belasten. Diese Falschmeldungen, Scherze oder Schwindeleien werden als „Hoax" bezeichnet.

Bei Vermissten- oder Verbrecheranzeigen ist generell Vorsicht geboten, denn solche Themen sind polizeiliche Angelegenheit und sollten nicht in privatem Umfeld weitergeschickt werden, sofern nicht ein direkter Bezug und ein guter Grund vorliegen. Falschmeldungen sollen Aufmerksamkeit erregen und dafür sorgen, dass sich Warnungen und unwahre Behauptungen schnell möglichst weit verbreiten. Das kann sogar so weit gehen, dass Börsenkurse größerer Konzerne in Mitleidenschaft gezogen werden. Die Absicht dahinter ist klar, denn ein fallender Kurs hat nicht nur Verlierer, sondern auch Gewinner. Sollte auch die Polizei aufgrund solcher Falschmeldungen tätig werden (müssen), bindet das wiederum beispielsweise wertvolle Ressourcen.

Grundsätzlich sollten solche Inhalte immer hinterfragt werden. Mit Hilfe der Google-, oder Microsoft-Suche kann schnell Klarheit erzielt werden, bevor die Nachricht einfach an alle Bekannten weitergeleitet wird.

Angriffsmethode: Identitätsdiebstahl und Gutgläubigkeit oder „Bitte sende mir schnell Geld"

Kreative Menschen mit krimineller Energie scheuen nicht davor zurück, „Notsituationen" darzustellen, in denen ein vermeintlicher Freund zu stecken scheint, um an Geld zu kommen. In einem denkbaren Szenario übernimmt hierzu der Täter ein echtes Facebook-Konto. Über einen gefälschten Hot-Spot mit einem Namen wie zum Beispiel „Free-Net" lässt sich das relativ schnell und unproblematisch erledigen: Ein Facebook-Nutzer sitzt in einem Café und möchte kurz überprüfen, ob es etwas Neues gibt. Leider wählt er den kostenfreien Hot-Spot-Zugang eines Angreifers, der in der Nähe sitzt. Schon kann der Angreifer die ID und das Passwort mitlesen und der Facebook-Account ist weg.

Ist der Angriff erfolgreich verlaufen, besteht der Zugriff auf das Facebook-Konto inklusive aller Informationen und Freunde des Opfers: ein vollständiger Identitätsdiebstahl. Der Angreifer versucht dann, „schnelle finanzielle Hilfe" bei Freunden zu erbitten: „Hallo, ich wurde bestohlen und stecke in Prag am Bahnhof fest. Könntest Du mir etwas Geld senden, damit ich mir kurzfristig ein Ticket kaufen kann? Bin total am Ende … 250 Euro sollten ausreichen. Hier die Bankverbindung einer Western-Union-Filiale hier in Prag: … Grüß [Name der Freundin/Ehefrau] – lade euch dann zum Dank zum Essen ein, wenn ich wieder zu Haus bin!!" – So oder so ähnlich könnte die erhaltene Nachricht lauten. Bei solch „eigenartigen" Anfragen sollten wir stets den Wahrheitsgehalt hinterfragen und den persönlichen Kontakt zum Hilfesuchenden aufnehmen. Ist er in einer Notlage, wird der Hilfesuchende das sicher kurz telefonisch oder per E-Mail erläutern können. Falls das Opfer selbst ahnungslos ist, ist sofort klar, dass es sich um einen Angriff handelt. Um solche Angriffe auf die eigene Identität zu vermeiden, sollte der Nutzer unbedingt sichere Passwörter verwenden und nicht einschätzbare Hot-Spots vermeiden. Lieber etwas Geld für Hot-Spots ausgeben, weil damit die Vertrauenswürdigkeit erhöht werden kann. Telekommunikationsanbieter unterliegen dem Fernmeldegeheimnis. Der Verstoß gegen dieses wird sehr hoch bestraft (Abbildung 8).

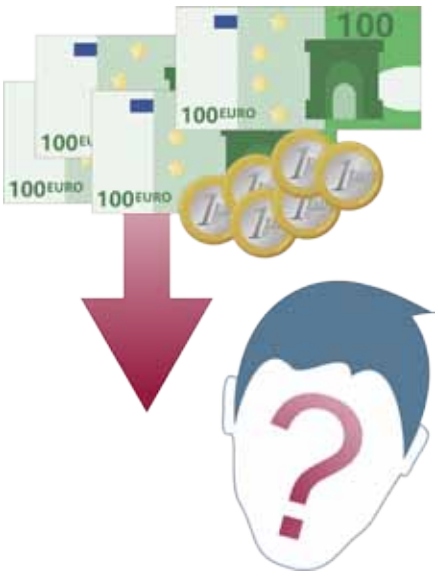

Abbildung 8

Fazit

Viele dieser Angriffsmethoden, bei denen Facebook als Angriffstool genutzt oder missbraucht wird, lassen sich, wie so oft im realen Leben, bereits durch achtsames Handeln eliminieren. Facebook ist die Basis und der Ausgangspunkt der Angriffe auf unsere Privatsphäre und die persönlichen Daten, ist jedoch auch selbst oft der Leidtragende. Komplexe soziale Medien mit sehr vielen Nutzern – wie Facebook – müssen sich durch Sicherheitsbemühungen und konzeptionelle Veränderungen in puncto Vertrauenswürdigkeit und IT-Sicherheit verbessern. Hier besteht ein sehr großer Nachholbedarf.

Der einfachste Weg für den Facebook-Nutzer ist, das Prinzip des Minimalismus anzuwenden: möglichst wenig über das eigene Privatleben online stellen. Damit sind schon viele Probleme gelöst. Zudem gilt es genau zu überlegen, mit wem wir „Freundschaften" schließen und welche Mindestanforderungen wir an uns selbst stellen, um eine eingegangene Anfrage zu bestätigen. Das Ablehnen von Anfragen und das Beenden von „Freundschaften" sind ebenfalls ein probates Mittel und sollten als sol-

che auch Anwendung finden. Das tun wir in der realen Welt auch!

Soziale Netze haben eine enorme gesellschaftliche Bedeutung. Sich diesen interessanten, modernen Technologien generell mit einem großen Maß an Misstrauen zu verschließen, ist nicht immer der richtige Weg und bringt oftmals mehr Nach- als Vorteile mit sich. Die eigentliche Herausforderung ist es, eine Balance zu finden zwischen einem gesunden Maß an Misstrauen und der engen Begrenzung der Onlinestellung privater Daten. Nutzer müssen lernen, die Vertrauenswürdigkeit der vielen Funktionen, Dienste und Informationen von Facebook richtig einzuschätzen. Dazu gehören der richtige Umgang mit dem Browser, die richtige Sicherheitskonfiguration des Computers (Anti-Malware, Personal Firewall, automatisches Update usw.) sowie der Verzicht auf Möglichkeiten, die nicht solide einzuschätzen sind. ■

Sebastian Barchnicki,
studentischer Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen und dort im Forschungsbereich soziale Netze und Mobile Security tätig.

Norbert Pohlmann,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen.