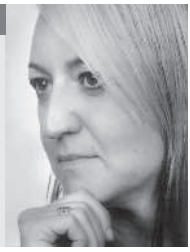
Aleksandra Sowa

Warum Sherlock Holmes heute Facebook nutzen würde

»Private information is practically the source of every large modern fortune« schrieb Oscar Wilde – und eine Reihe von Cyberkriminellen würde ihm heute vermutlich beipflichten. Noch nie ist es so einfach gewesen, an sensible und vertrauliche Informationen zu gelangen, wie in der Facebook-Ära. Der legendäre Hacker Kevin Mitnick wühlte noch in Mülltonnen nach sicherheitsrelevanten Informationen – seine Nachahmer »wühlen« heute eher in den sozialen Netzwerken.

Aleksandra Sowa

leitete zusammen mit dem deutschen Kryptologen Hans Dobbertin das Horst Görtz Institut für Sicherheit in der Informationstechnik. Sie ist Autorin zahlreicher Fachpublikationen und aktuell in einem großen Telekommunikationskonzern tätig.



»Koobface« ist der Name eines Computerwurms, der sich seine Opfer in sozialen Netzwerken wie Facebook, MySpace, Friendster oder Twitter sucht, ihre Rechner infiziert und sie anschließend nutzt, um ein sogenanntes Peer-to-Peer Botnetz (ein Rechnernetz) aufzubauen. Bei der Auswahl des Namens Koobface bewiesen die Schöpfer des Wurms viel Humor: Es ist ausgerechnet ein Anagramm des aktuell größten Betreibers sozialer Netzwerke – Facebook.

Der Wurm verbreitet sich, indem aus dem infizierten Facebook-Konto Nachrichten verschickt werden, die die »Freunde« des Opfers zum Aufruf einer Webseite Dritter (oft als YouTube-Video getarnt) auffordert. Beim Aufrufen der Internetseite wird auf dem Computer eine Schadsoftware installiert. Der auf diesem Wege durch den Koobface-Wurm befallene Rechner leitet beispielsweise die Suchanfragen bei Suchmaschinen auf kontaminierte Server um, schaltet Links zu Webseiten Dritter auf der Facebook-Pinwand oder sperrt den Zugang zu den Webseiten von Sicherheitsdienstleistern (mit dessen Hilfe die »Machenschaften« des Wurms aufgedeckt werden könnten).

Koobface wurde erstmalig im Jahr 2008 eingesetzt. 2010 wurde die Anzahl der mit dem Wurm infizierten Rechner auf etwa 400.000 bis 800.000 geschätzt. Der Koobface-Wurm späht keine sensiblen oder finanziellen Informationen auf den infizierten Rechnern aus. Vielmehr leitet er »lediglich« den Internetverkehr geschickt um. Mit dem so erzeugten »Traffic« auf bestimmten Webseiten und zusätzlich erzeugten Werbeklicks im Internet konnten die Koobface-Schöpfer laut Experten zwischen 2009 und 2010 einen »Umsatz« von etwa zwei Millionen Dollar erzielen.

So weit die Erfolgsgeschichte der »bösen« Koobface-Gang.

Im Jahr 2012 wurde die berüchtigte Gruppe, die hinter dem Computerwurm steht, von den SophosLabs-Experten enttarnt – der Beginn einer anderen Erfolgsgeschichte.

Während sie die Schwächen der sozialen Netzwerke – und ihrer Nutzer – für ihre Machenschaften nutzten, haben die Mitglieder der Koobface-Gang unbehelligt gelebt und nutzten selbst rege die sozialen

Netzwerke, um ihre Reisen, Standorte, Besitztümer und Freundschaften zu dokumentieren. Genau diese Informationen haben es den SophosLabs-Experten ermöglicht, die wahren Identitäten der Gangmitglieder zu ermitteln und diese anschließend der Polizei und dem FBI zu übergeben.

Die Gang-Jäger entdeckten auf einem vom Koobface-Wurm genutzten Server Telefonnummern, den Nickname des Programmierers »Krotreal« und ein Foto. Die Analyse ergab, dass das Foto an Koordinaten aufgenommen wurde, die dem Standort von St. Petersburg entsprechen. Mit diesen Hinweisen ausgestattet, begaben sich die Jäger auf die Suche im Netz: Sie fanden zwei Internet-Anzeigen, bei denen eine der Telefonnummern sowie der Nickname »Krotreal« in den Kontaktdaten aufgeführt waren. Außerdem tauchte ein neuer Name auf: »Anton«.

Die Jäger durchsuchten die sozialen Netzwerke nach passenden Profilen und wurden bei Flickr fündig. Dort gab es einen Anton, auch die anderen Hinweise aus den Anzeigen stimmten überein. Doch Krotreal ging mit seinem Profil äußerst umsichtig um und beschränkte den Zugang ausschließlich auf seine Freunde. Zumindest bis zu dem Zeitpunkt, an dem er die Links zu seinen Fotos »twitterte« und sie damit auf einen Schlag öffentlich machte.

Nicht nur durch Fotos gelang den Ermittlern ein Coup. Vielmehr steckten die Kommentare zu den Abbildungen voller nützlicher Informationen und so gelang es den Experten Schritt für Schritt, die Namen, die Telefonnummer und schließlich die Identitäten aller fünf Koobface-Gang-Mitglieder zu entlarven.

Glanz und Schatten der Sozialkonstruktion

Die Methode, mit der es den SophosLabs-Experten gelungen ist, die Cybergang aufzuspüren, ist in der Informatik als »Sozialkonstruktion« bekannt. Die Sozialkonstruktion, auch *Social Engineering* oder *Social Hacking* genannt, kann mit gleichem Erfolg von den »Guten« zum Aufspüren von »Bösen« verwendet werden und umgekehrt.

Popularisiert wurde diese Methode im Hacker-Milieu von dem »meistgesuchten Hacker der Welt« (wie er sich selbst bezeichnet): Kevin Mitnick. Seine Methode, mittels geschickter Fragestellungen an die Insider-Informationen zu gelangen, beschrieb er in dem Bestseller *Die Kunst der Täuschung. Phishing* und *Pharming* waren die ersten massenhaft eingesetzten – und sehr erfolgreichen – Arten des *Social Engineering*. Diese modernen Angriffsarten auf Online-Banking, Online-Shops und Internet-Auktionen, zielen vorrangig auf das schwächste Glied der Sicherheitskette ab – den Menschen. Und tatsächlich hat der Erfolg der *Phishing*- und *Pharming*-Angriffe oft herzlich wenig mit der Angreifbarkeit der IT-Systeme zu tun. Vielmehr ist er allein von dem Grad der Naivität abhängig, mit der die Nutzer mit ihren sensiblen Kontoinformationen umgehen. Mit *Social Engineering* ist die Gesamtheit der Angriffsarten gemeint, die auf das Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels gesellschaftlicher oder gespielter Kontakte abzielt.

Social Engineering wird aber nicht nur eingesetzt, um Konten der Privatpersonen oder Institutionen zu plündern. Unternehmensgeheimnisse, Patentinformationen, personenbezogene Interna, Informationen über bevorstehende Fusionen, Käufe, Strategien und neue Technologien und Produkte sind andere, nicht weniger attraktive »Waren« für die externen Angreifer. Das Thema *Social Engineering* wurde deshalb als ernstes, wachsendes Problem der Unternehmen erkannt, wie die aktuelle Security-Studie von Check Point bestätigt.

Demnach sollen in den vergangenen zwei Jahren knapp zwei Drittel der deutschen Unternehmen bereits Opfer von *Social Engineering*-Attacken geworden sein.

Nach Einschätzung der Unternehmen hatten sie pro Vorfall mit Folgekosten von über 25.000 Dollar zu rechnen. Eine andere Erhebung des Unternehmens KPMG bezüglich Internetdelikte in den deutschen Unternehmen bestätigt, dass die Unternehmen Angriffe, die von Mitarbeitern, ehemaligen Mitarbeitern oder sonstigen Insidern ausgeführt werden, als Hauptgefahr einschätzen.

Mit der Verbreitung von Facebook und anderen sozialen Netzwerken ist es heute nicht mehr notwendig, wie ehemals Kevin Mitnick die Mülltonen nach sicherheitsrelevanten Informationen zu durchsuchen oder falsche Identitäten vorzugaukeln, um Passwörter zur erschleichen und sich somit Zugang zu den IT-Systemen zu verschaffen. Den »Stoff«, aus dem potenziell die Ideen für Passwörter geschöpft werden, findet man häufig in den privaten Profilen der Mitarbeiter, deren Familien, Kunden, Partner und Freunde bei Facebook, MySpace etc. Die Namen der Hunde, Katzen, Hamster, Kosenamen der Kinder, Ehefrauen und Freunde, Geburtstage und Jubiläen, Lieblingsfarben und -musik – das alles ist mit wenigen Klicks in sozialen Netzwerken zu finden. So ist auch das Erraten eines Zugangspassworts (Lieblingsmarke für Krawatten kombiniert mit Datum der Golf-Platzreife), der Diebstahl einer Zugangskarte (während eines zweiwöchigen Urlaubs auf dem Bauernhof, über den sich die Kinder in einem Schulforum mit Ihren Schulkameraden bereits Wochen im Voraus ausgetauscht haben), eine simple Aufgabe geworden.

Wird man in den Online-Communities nicht fündig, so ist es immer noch möglich, einfach nur aufmerksam den Gesprächen in der Bahn, auf dem Flughafen, im Flugzeug, im Restaurant oder bei einer Grillparty zu lauschen.

Wie konnte es passieren, dass in der heutigen Gesellschaft eloquente Marktschreierei und neurotische Selbstvermarktung als Tugend angesehen werden, fragt Susan Cain in dem Buch *Still: Die Bedeutung von Introvertierten in einer lauten Welt.*

Das trifft heute nicht allein auf die Geschäftsführer, Vorstände und Aufsichtsräte namhafter Unternehmen zu, die per se zu öffentlichen Persönlichkeiten werden, ähnlich wie die Politiker, Schauspieler und andere Prominente. Auch das »Hänschen« aus dem Vorzimmer, dem der Aufstieg in die Eckbüros der Macht (vorerst) vorenthalten bleibt, möchte an dieser Glitzerwelt teilhaben.

Im Kreis der Bekannten – aber auch der Unbekannten – wird oftmals nach der Bestätigung für den gewählten Lebensstil gesucht. Mit dem »Wissen« kann die Zugehörigkeit zu »bestimmten Kreisen«, oberen Unternehmensetagen oder politischen Machtzentren signalisiert werden. Es gehört zur Selbstvermarktung, darüber zu sprechen, wen man kennt, wohin man reist, mit wem man speist oder welchen herausragenden Persönlichkeiten man bei der Ausübung beruflicher Pflichten begegnet.

Denn ein nicht unbeachtlicher Kreis an Personen rund um die Zentren der Macht in Unternehmen, Behörden und Regierungsinstitutionen hat heute Zugriff auf sensible Dokumente und Informationen. Darin inbegriffen ist häufig der Zugriff auf die Korrespondenz und Termine der Kollegen und Vorgesetzten. Man weiß, wann wer mit wem telefoniert hat, warum und nicht selten auch worüber. Man weiß, welches Transportmittel wann benutzt und wann wer durch welche Tür bei welcher Veranstaltung erscheint. Man kennt den Tagesablauf, die Krawattenmarke, die Krankheitsgeschichte – und eben auch die sicherheitstechnischen Details. Und man erzählt möglicherweise, leicht beschwipst auf einer Grillparty, was man Interessantes oder Unterhaltsames in den Chef-Mails gesehen hat – und das nicht selten mit verheerenden Konsequenzen.

Der Mitarbeiter als Risiko? In den 90er Jahren forderten die Regulierer und Gesetzgeber von den Unternehmen, wirksa-

me interne Kontrollen einzurichten, damit die den Fortbestand des Unternehmens gefährdende Risiken früh erkannt werden. Seitdem wurden in den Unternehmen derartige Kontrollen etabliert, die u.a. auch das Risiko »Mensch« beherrschbar machen sollen. Doch das ist nicht genug. Neben den Kontrollen sind auch Maßnahmen und Kampagnen notwendig, die das Bewusstsein der Mitarbeiter wecken und sie für die Methoden des *Social Engineering* sensibilisieren. Denn die bereits früher erwähnte Security-Studie von Check Point bescheinigte den deutschen Unternehmen »deutlich zu wenig Sicherheitsbewusstsein«.

In einer Sache dürften die »Bösen« den »Guten« voraus sein. Finanzielle Vorteile, Erlangen von Wettbewerbsvorteilen und Rachemotive sind nicht mehr allein die Hauptmotivationen für die Angriffe. Der Wunsch nach Bestätigung der gewählten Lebensweise, nach Selbstbestätigung und Selbstvermarktung dürften heute zu den ebenbürtigen Motiven gehören, auch wenn der wissenschaftliche Beleg noch aussteht.

Neben dem von Sascha Lobo kürzlich abgestaubten und modernisierten neu-alten Typus' des »digitalen Spießers«, der das Internet primär zur Selbstvermarktung und asozialen Selbstbestätigung nutzt, gibt es ihn immer noch: den Spießer alter Prägung, den Horvath in seinem Buch *Der ewige Spießer* als »hypochondrischen Egoisten« beschrieben hat. Mit seiner Hilfe verlassen unbeobachtet sensible und vertrauliche Informationen die Organisationen – ohne dass es jemand bemerkt oder verfolgen kann – und ohne, dass die mit enormem finanziellen Aufwand installierten Überwachungssysteme es aufspüren und protokollieren würden. ■

Rainer Hillrichs

YouTube als politisches Medium – Eine Zwischenbilanz

Neben Justin Bieber und lachenden Babys spielen auch politische Inhalte auf YouTube eine Rolle. Inwiefern ist die Videoplattform aber ein politisches Medium? Was zeichnet die politischen Nutzungen von YouTube aus? Und: Wie macht man dort erfolgreich Politik? Eine Zwischenbilanz nach sieben Jahren YouTube.

YouTube wurde Anfang 2005 als kommerzielles Projekt von drei Internet-Profis – einem Designer und zwei Programmierern – geplant und umgesetzt. Die Geschichte von drei Freunden, die auf einer Party eine interessante Idee hatten und dann einfach »probierten«, ist Teil des Selbstmarketings von YouTube und wird leider oft für bare Münze genommen – zuletzt in der Titelstory des *Stern* (5/2012). Ein Grund für das rasante Wachstum der Seite war, dass die Gründer in der Gestaltung keine eindeutige Antwort auf die Frage lieferten, für wen YouTube überhaupt gemacht wurde. YouTube verkörperte die Idee der Plattform, auf der vieles, wenn nicht gar alles, möglich war. Als *fastest growing website of all time* gefeiert, verkauften die Gründer ihre Firma 2006 für 1,3 Milliarden

Ranier Hillrichs

(* 1980) promoviert an der Universität Bonn in Medienwissenschaft über die Videokultur von YouTube. Er ist Koordinator der Arbeitsgruppe »New Media« des European Network for Cinema and Media Studies (NECS) und absolvierte 2011 einen sechsmonatigen Forschungsaufenthalt an der University of California, Santa Barbara.

hillrichs@uni-bonn.de