G DATA Presseinformation 2008

Cybercrime 2.0: Kriminelle lieben Social Networks

Facebook & Co bei Onlinekriminellen hoch im Kurs

Bochum (Deutschland), 20. November 2008 – Soziale Netzwerke bieten Menschen weltweit vielfältige Möglichkeiten, neue Kontakte zu knüpfen oder bestehende Verbindungen zu pflegen. Nicht von ungefähr sind daher eingefleischte Networker von Plattformen, wie Facebook, My Space, XING, StudiVZ oder Linkedin begeistert. Das Networking sich auszahlt, hat aber auch die Schattenwirtschaft für sich entdeckt. Nach Analysen des G DATA Security Labs setzen Kriminelle die Idee des Mitmachnetzes längst für ihre Zwecke ein. Die Infiltration der Communities, die Verbreitung von Spam oder Schadcode sind in Social-Netzworks mittlerweile an der Tagesordnung. Tendenz steigend!

Das Missbrauchspotenzial ist für die Täter vielfältig und reicht vom gezielten Ausspähen persönlicher Daten, über die Verteilung von Spam- und Phishingmails bis hin zum Ausnutzen von Sicherheitslücken der jeweiligen Social-Networking-Plattform.

Ralf Benzmüller, Leiter G DATA Security Lab, schlägt Alarm: „Der Community-Gedanke ist längst bei den Online-Kriminellen angekommen. Im Laufe der vergangenen Monate beobachteten wir eine bedrohliche Zunahme von kriminellen Aktivitäten in Social-Networks. Kaum eine Community ist dabei verschont geblieben. Die Spielarten der Täter sind ausgeklügelt und umfassen das gesamte eCrime-Repertoire. Neben der direkten Einspeisung von Schadcode oder deren Verbreitung durch Massenmails, nutzen die Täter soziale Netzwerke, um Nutzer auf präparierte Webseiten zu locken. Das Ziel: Computer per Drive-by-Infektion oder Datei-Downloads zu infizieren oder potenzielle Käufer auf die Bestellseiten zwielichtiger Angebote zu leiten."

Die große Akzeptanz der Mitmachnetze und deren Spezialisierung auf einzelne Themengruppen beschert den Tätern reiche Beute: „Im Vergleich zur realen Welt, stehen Kosten, Aufwand und möglicher Gewinn in einem für Kriminelle besonders günstigen Verhältnis. Allein Facebook hat mehr als 130 Millionen Nutzer weltweit.", resümiert Ralf Benzmüller. „Die Aufteilung in Subcommunities, ermöglicht Spammern ihren Werbemüll noch gezielter auf die jeweilige Zielgruppe auszurichten."

Die größten Social Networks

Social Network	Nutzer (in Mio.)
Facebook	132
My Space	117
Hi5	56
Friendster	37
Orkut	34
Bebo	24
Skyrock	21
XING	6,5
StudiVZ	5,7

(Quellen: comScource, XING & AOGF)

Gezielte Angriffe auf Unternehmen
Die Informationen, die Mitglieder von Social Networks über sich und ihr Umfeld preisgeben, erlauben es Cyber-Kriminellen aber auch gezielte Angriffe auf Unternehmen durchzuführen. „Mit den Informationen, die man in Xing über eine Firma zusammentragen kann, lassen sich gezielte Phishing-Mails an Geschäftsführung, Vertrieb oder Buchhaltung verfassen. Diese können Bezug nehmen auf die Position im Unternehmen, Kollegen und Hobbies. Die so eingeschleusten maßgeschneiderten Spyware-Trojaner können Firmen ruinieren.", warnt Ralf Benzmüller.

Persönliche Daten im Visier

Neben der direkten Einspeisung von Schadcode oder deren Verbreitung via Massenmails, nutzen die Täter soziale Netzwerke, um persönliche Daten zu stehlen und gewinnbringend weiter zu verkaufen. Im Visier der Täter stehen neben Login-Daten unter anderem klassische Kontodaten, Telefonnummern, E-Mail-Adressen und Geburtsdaten. Aktuell ermittelte das G DATA Securty Lab einen Schwarzmarktpreis von 40,- Euro für 500 MByte unbereinigte Daten. Datenhehler veräußern diese Daten oftmals an unseriöse Call-Center im Ausland, die so leichter auf Kundenfang gehen.

Der gläserne Networker
Nutzer von Plattformen legen oftmals persönliche Daten oder Firmendaten leichtfertig einer breiten Öffentlichkeit offen. Informationen, die z. B. bei Xing oder Linkedin ungeschützt publiziert werden, stehen so nicht nur Freunden zur Verfügung. Durch Dienste wie 123people oder Yasni, ist es ein Leichtes Anwenderprofile, Wohnort oder Hobbies zusammenzutragen und für gezielte Angriffe einzusetzen. „Grundsätzlich sollte man in Social Networks nur das veröffentlichen, was man nicht auch am Hauptbahnhof auf eine Plakatwand schreiben würde. Unternehmen sollten entsprechende Richtlinien erlassen, um den Missbrauch einzugrenzen.“, so Security-Experte Ralf Benzmüller.

Grundlegende Sicherheitsmaßnahmen
Wer soziale Netzwerke nutzen und dabei sein persönliches Sicherheitsrisiko minimieren möchte, sollte einige grundlegende Sicherheitshinweise beachten:

- Die Infektion eines Rechners mit Schadsoftware kann wie im Vorbeigehen erfolgen (sog. Drive-by-Download), ohne dass dabei ein Festplattenzugriff erfolgt. Klassische Virenscanner, die nur das Dateisystem überwachen, können daher wirkungslos sein. Zusätzlichen Schutz bietet ein http-Scanner, der die Webinhalte bereits prüft, bevor sie den Internet-Browser erreichen und dort möglicherweise Schaden anrichten können.

- Der Virenschutz , das Betriebssystem und der Browser sollten immer auf dem aktuellsten Stand gehalten werden. So werden Sicherheitslücken geschlossen und ihre Virenabwehr befindet sich immer auf dem neuesten Stand.

- Skepsis bei Freundschaftsanfragen von Unbekannten – hier könnte es sich um Datenhehler handeln, die auf der Jagd nach persönlichen Daten sind und diese weiterverkaufen.

- Nutzer von Xing und Co. sollten nur ausgewählten Personen Zugang zu ihren persönliche Daten gestatten. Andernfalls können Personensuchmaschinen, wie 123people oder Yasni, diese personenbezogenen Daten indizieren, abspeichern und jedermann zur Verfügung stellen.

- Reagieren Sie nicht auf Anfragen, in denen man von Ihnen die Herausgabe von Passwörtern, Kontonummern, PIN-Codes oder anderer persönlicher Informationen etc. fordert. Insbesondere, wenn dabei die Schließung des Accounts angedroht wird.

- Benutzen Sie komplexe Passwörter. Vermeiden Sie gängige Begriffe, Namen oder Geburtsdaten. Sie laufen sonst Gefahr, dass Ihr Passwort erraten werden könnte. Wählen Sie stattdessen als Kennwort Kombinationen aus Buchstaben, Zahlen und Sonderzeichen, die in keinem Wörterbuch vorkommen.

- Benutzen Sie für jede Community ein eigenes Passwort!!

Informationen zum Unternehmen
G DATA ist Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz. Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen.

Bereits vor mehr als 20 Jahren entwickelte G DATA das erste Anti-Viren-Programm.

Kein anderer europäischer Security-Hersteller hat in den letzten fünf Jahren mehr nationale und internationale Testsiege und Auszeichnungen gewonnen als G DATA.
G DATA InternetSecurity ist bereits zweimal in Folge Testsieger der Stiftung Warentest. Als Qualitätsführer vereint G DATA in seinen Produkten die besten Sicherheitstechnologien der Welt. Beispiele hierfür sind die DoubleScan-Technologie mit zwei unabhängigen Virenscannern oder der Sofortschutz OutbreakShield. Das Produktportfolio von G DATA Security umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen.

G DATA Security-Lösungen sind in den USA, Japan, Deutschland, England, Frankreich, Italien, Spanien, Kanada, Polen, Korea, den Niederlanden, Belgien, Österreich, der Schweiz, Ungarn und Luxemburg erhältlich. Der Sitz des Unternehmens ist Bochum (Deutschland).

Weitere Informationen zum Unternehmen und zu G DATA Security-Lösungen finden Sie unter www.gdata.de.

Ihr Redaktionskontakt

Presseservice G DATA Software AG
Thorsten Urbanski
Königsallee 178 b
44799 Bochum

Tel. +49 (0) 234 / 9762-239
Fax +49 (0) 234 / 9762-299
thorsten.urbanski@gdata.de
www.gdata.de