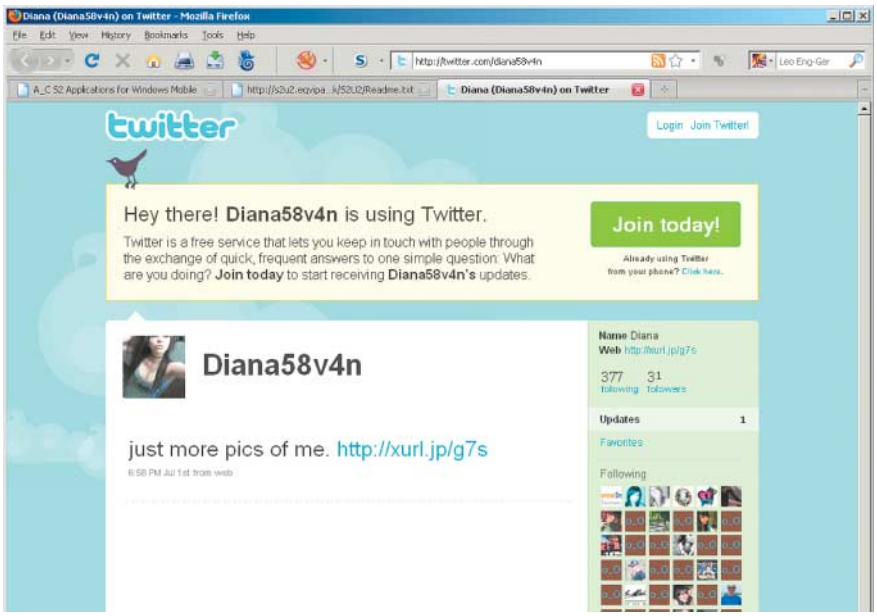
Die Gefahren des Microblogging-Dienstes Twitter

Zu Risiken und Nebenwirkungen

Sabine Pfautsch, Christian Dietrich, Sebastian Spooren, Norbert Pohlmann



Kaum entstehen neue Dienste im Internet, dauert es nicht lange, bis die gesamte Bandbreite der Angriffe auf sie angewendet werden kann und wird. Twitter bildet hier keine Ausnahme.

Da ist ein Flugzeug im Hudson River. Ich bin in einer Fähre, die die Leute aufsammelt. Verrückt.“ Diese Meldung von Janis Krumis brachte Twitter im Januar 2009 den Durchbruch. Seitdem ist der Microblogging-Dienst in aller Munde.

Immer mehr Menschen lassen die Welt in 140 Zeichen daran teilhaben, was sie gerade tun, denken oder zu tun gedenken. Auch Prominente aus allen Bereichen, Medien oder Unternehmen bedienen sich zunehmend des Dienstes. Noch wenig im öffentlichen Fokus stehen derzeit allerdings seine Gefahren und Schwachstellen.

Bereits die Passwortwahl bei der Registrierung ist aus Sicherheitsperspektive problematisch. Registrierte Anwender werden zwar auf die Passwortstärke hingewiesen (zum Beispiel schwach oder sehr stark). Ein schwaches Passwort wie „111111“ oder „123456“ akzeptiert das System allerdings trotzdem. Von Twitter kommt nur der Hinweis, dass es mindestens sechs Zeichen lang sein und der Benutzer es bei Gelegenheit ändern sollte. Vermutlich haben viele, insbesondere die für IT-Risiken wenig sensibilisierten Twitterer, schwache Passwörter in Gebrauch. Die Folge: Accounts zu knacken wird für Hacker zum Kinderspiel.

In der Vergangenheit wurden etwa der US-Präsident Barack Obama und die Pop-Sängerin Britney Spears Opfer solcher Angriffe. Das Problem: Unbekannte legten den Prominenten recht geschickt Unwahrheiten in den Mund und rückten sie somit in ein schlechtes Licht. Um diese Sicherheitslücke zu vermeiden, sollte es Hinweise mit Beispielen geben, wie ein sicheres Passwort zu wählen ist. Idealerweise dürfte das System primitive Passwörter und Beispielpasswörter gar nicht erst akzeptieren. Ein sicheres Passwort sollte aus einer Kombination von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.

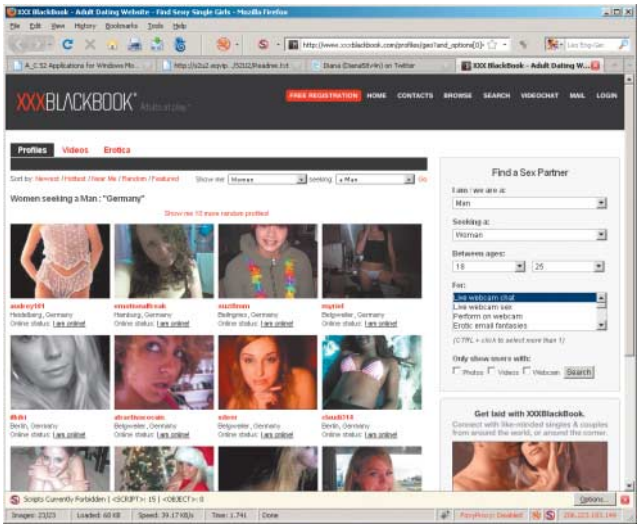
Ein weiterer Nachteil von Twitter: Die „Zwitscherer“ werden quasi daran gewöhnt, ihr Passwort aus der Hand zu geben, wenn sie Third-Party-Dienste wie twitpic nutzen. Sie müssen ihren Benutzernamen und ihr Passwort auf einer fremden Webseite eingeben. Aus Sicherheitsgründen und zur Sensibilisierung der Benutzer sollten die Betreiber das technisch anders lösen. Immerhin weist Twitter darauf hin, dass man seine Zugangsdaten nicht an einen dubiosen Third-Party-Service weitergeben soll.

Wer Twitter nutzt, kennt es: Bereits zwei Minuten nach der Anmeldung hat der Benutzer Spam-Follower in seinem Tweed. Spammer machen auf sich aufmerksam, indem sie einem Tweed wahllos folgen. Besucht man das Profil des Followers (Beispiel siehe Aufmacher), findet man Links auf Spam-Webseiten (s. Abb. auf S. 107), die möglicherweise Schadcode enthalten und per Drive-by Download das eigene System infizieren.

Auch von Phishing bleibt der Kurznachrichtendienst nicht verschont. Phisher versuchen mithilfe von Nachrichten, Twitter-Benutzer auf eine gefälschte Twitter-Seite zu locken, um dort die Zugangsdaten abzugreifen. Allerdings ist das Ziel der Phisher noch nicht bekannt. Möglicherweise benutzen sie die gestohlenen Zugangsdaten für Spam-Follower oder den Identitätsdiebstahl.

Nur wenige gesicherte Identitäten

Ferner gibt es ein weiteres Risiko: Benutzer können sich bei Twitter ganz einfach unter einem anderen Namen anmelden – eine Authentifizierung der registrierenden Person ist nicht zwingend erforderlich. Das vermutlich bekannteste Beispiel zu diesem Fall ist Rob Vegas, der einige Monate lang im Glauben vieler Follower als Harald Schmidt twitterte. Eine erste Gegenmaßnahme haben die Betreiber mittler-



Klickt man einen Link in einem Spam-Follower-Profil an, landet man auf dubiosen Webseiten, von denen man sich unter Umständen unbemerkt Malware auf den Rechner lädt.

weile ergriffen. Der Identitätsdiebstahl wird nun teilweise durch sogenannte Verified Accounts verhindert. Dazu erfolgt eine Authentifizierung. Ein blaues Siegel kennzeichnet, dass es sich bei der twitternden tatsächlich um die genannte Person handelt. Da der manuelle Aufwand dafür sehr hoch ist, wird das Siegel jedoch derzeit nur bei wenigen Accounts vergeben.

Kurze URLs gehören bei Twitter zum guten Ton. Sie erlauben jedoch keine Transparenz. Es ist nicht ersichtlich, auf welche Seite ein gekürzter Link führt – eventuell zeigt er auf eine Seite mit gefährlichem Inhalt. Ruft der Anwender sie auf, kann sie seinen Rechner mit Malware infizieren.

API als Einfallstor

Vor Kurzem entdeckte Mikko Hypponnen von F-Secure, dass Twitter ohne Vorankündigung begonnen hat, Tweets mit URLs von verseuchten Webseiten zu filtern. Wer einen solchen Link einstellt, erhält eine Warnung: „Oops your tweet contained a URL to a known malware site!“. Sicherheitsexperten bemängelten nach ersten Tests jedoch die Filterwirksamkeit, berichtet die Computerworld Security.

Der Sicherheitsspezialist Aviv Raff schrieb, dass und wie sich die Twitter-API zur Verbreitung von Würmern mittels einer Cross-Site-Scripting-Schwachstelle (XSS) missbrauchen lässt. Die API ermöglicht Konfiguration, Verwaltung und Statusabfrage des eigenen Kontos mit HTTP-Requests. Während Benutzer von Twitter innerhalb ihres Profils keine beliebigen HTML-Tags verwenden können, liefert der Twitter-Bilderdienst „Twitpic“ HTML-Tags und damit auch Javascript-Code ungefiltert aus – dieser wird dann im Browser eines anderen Besuchers ausgeführt.

Auf diese Weise können andere Anwender – wie bei einem XSS-Angriff üblich – unbefugt Daten auslesen und überdies Interaktionen wie das Veröffentlichen eines Kommentars ausführen. Raff lieferte sogar einen Proof-of-Concept dieses Exploits. Mittlerweile ist die Lücke zwar auf Twitpic geschlossen, allerdings könnte es weitere Anwendungen geben, die ähnliche Schwachstellen aufweisen und die Twitter-API auf diese Art missbrauchen könnten.

Nicht zu unterschätzen ist neben allen technischen Sicherheitslücken die ungewollte Informationsverbreitung über Twitter. Bestes Beispiel: Bei der Wahl zum Bundespräsidenten im Mai 2009 hatten Abgeordnete bereits vor der offiziellen Bekanntgabe den Sieg Horst Köhlers bei Twitter bekannt gegeben.

Wünschenswert wäre bei allen existierenden und noch kommenden Web-2.0-Anwendungen eine ausreichende Sensibilisierung der Anwender. Mindestens sollten sie ein ausreichend starkes Passwort verwenden und keine vertraulichen Inhalte veröffentlichen, die ihnen zu einem späteren Zeitpunkt in irgendeiner Weise schaden können. Entsprechende Hinweise seitens der Diensteanbieter wären ein erster Schritt. (ur)

SABINE PFAUTSCH,
CHRISTIAN J. DIETRICH,
SEBASTIAN SPOOREN UND
PROF. DR. NORBERT POHLMANN

sind Mitarbeiter des Instituts für Internet-Sicherheit if(is) an der Fachhochschule Gelsenkirchen.