Missbrauch und Betrug auf Twitter

Eva Zangerle

Zusammenfassung

Soziale Netzwerke wie Facebook, Twitter oder auch LinkedIn und XING haben im letzten Jahrzehnt explosives Wachstum erfahren. Die Popularität dieser Netzwerke hat allerdings nicht nur positive Aspekte, es treten zunehmend auch negative Aspekte auf. Dazu gehören unter anderem die gezielte Verbreitung von Falschinformationen, das Hacken von Accounts und die Verteilung von Spam über gehackte Accounts.

Dieser Aufsatz hat zum Ziel, derartige negative Aspekte am Beispiel der Microblogging-Plattform Twitter einerseits aus einem technischen Standpunkt zu analysieren, andererseits aber auch die persönlichen Auswirkungen auf die Benutzerinnen und Benutzer selbst zu beleuchten.

Einleitung

Soziale Netzwerke wie Facebook oder Twitter haben in den letzten Jahren enormes Wachstum erfahren. So hat sich beispielsweise die Anzahl der weltweit aktiven Benutzerinnen und Benutzer des Kurznachrichtendienstes Twitter zwischen März 2010 und März 2013 von 30 auf 204 Millionen gesteigert (Washington Post, 2013). Speziell die sogenannte „Generation Y“, die Frauen und Männer zwischen 19 und 34 Jahren umfasst, stellt jene Benutzerschicht dar, die Soziale Netzwerke am stärksten nutzt (Bergh, 2013). So zeigt eine aktuelle Studie in 19 Ländern aus dem Jahre 2013, dass sich 80% der Generation Y täglich in mindestens ein Soziales Netzwerk einloggen, wobei 66% der Generation Y Facebook und 29% Twitter benützen (Bergh, 2013).

Eine derartig große Anzahl von erreichbaren Nutzerinnen bzw. Nutzern und verfügbaren Informationen führt zu Missbrauch, der sich primär darin äußert, dass personalisierte Informationen über Benutzerinnen und Benutzer gesammelt und verkauft werden und auch gezielt versucht wird, das Meinungsbild der Benutzerinnen und Benutzer zu verändern und Produkte zu promoten. Das Propagieren von Produkten und Meinungsbildern führt dazu, dass eine ständig steigende Anzahl an Spam-Nachrichten über Soziale Netzwerke verbreitet wird. Aktuelle Studien zeigen, dass der Anteil von Spam-Nachrichten in Sozialen Netzwerken bei 5% liegt (Nexgate, 2013). Diese Zahl mutet im Vergleich zu E-Mail-Spam, der derzeit für 70% des gesamten E-Mail-Verkehrs weltweit verantwortlich ist (Wagner, 2013), gering an. Allerdings lag die Wachstumsrate für Spam auf Social-Media-Plattformen im ersten Halbjahr 2013 bei 355% (Nexgate, 2013). Dieses Wachstum lässt sich auch darauf zurückführen, dass das Bewusstsein für Spam in Sozialen Netzwerken noch weniger vorhanden ist und Benutzerinnen und Benutzer teils unbedarft auf Links in Spam-Nachrichten in Sozialen Netzwerken klicken, wohingegen sich bei E-Mail-Spam bereits eine gewisse Routine seitens der Benutzerinnen und Benutzer eingestellt hat. Derartige Verhaltensmuster führen dazu, dass 0,13% aller Spam-Links auf

Twitter angeklickt werden, aber nur 0,003% aller Spam-Links in E-Mails angeklickt werden – die Click-Through-Rate ist bei Twitter-Spam also wesentlich höher. Diese Zahlen versprechen höhere Erfolgschancen für Kriminelle auf Twitter, was dazu führt, dass mittlerweile 8% aller URLs in Tweets zu Schadsoftware, betrügerischen Webseiten oder Phishing-Webseiten führen (Grier, et al., 2010).

Der vorliegende Aufsatz soll im Weiteren am Beispiel der Twitter-Plattform Missbrauch und Betrug in Sozialen Netzwerken exemplarisch aufzeigen und auch darlegen, wie Benutzerinnen und Benutzer auf derartige Fälle reagieren und damit umgehen.

Der Aufsatz ist wie folgt aufgebaut: Zunächst wird der Kurznachrichtendienst Twitter näher beschrieben, um dann auf die verschiedenen Ausprägungen von Kriminalität in Zusammenhang mit dieser Plattform einzugehen. Darauffolgend wird auf eine Art des Missbrauchs, auf das Kompromittieren von bestehenden Benutzer-Accounts, näher eingegangen und eine Analyse des Benutzerverhaltens im Falle eines kompromittierten Accounts vorgestellt. Der Aufsatz wird mit einer Zusammenfassung abgeschlossen.

Der Kurznachrichtendienst Twitter

Twitter ist ein Kurznachrichtendienst, der es seinen Benutzerinnen und Benutzern erlaubt, 140 Zeichen lange Nachrichten auf der Plattform zu posten. Diese sogenannten *Tweets* sind öffentlich auf der Plattform abrufbar. Ein Beispiel für einen Tweet lautet wie folgt: „Jetzt in der Aula: Vergabe der Mittel aus dem Tiroler Wissenschaftsfonds. #Förderungen http://instagram.com/p/j0-BomO052/“, in dem über den Twitter-Account der Universität Innsbruck (@uniinnsbruck) über die Vergabe der Fördermittel aus dem Tiroler Wissenschaftsfonds berichtet wird. Zudem ist ein Link zu einem Foto enthalten, das über die Foto-Sharing-Plattform Instagram verfügbar ist. Die Plattform Twitter basiert einerseits auf den beschriebenen Kurznachrichten und andererseits auf mehreren damit verknüpften Konzepten, die maßgeblich zum Erfolg der Plattform beitragen. Diese sollen nachfolgend vorgestellt werden.

- *Follower*: Ein Follower ist ein User A, der sich für die Nachrichten eines anderen Users B interessiert und diese abonniert und somit automatisch angezeigt bekommt. A folgt (engl. *follows*) damit B. Dabei ist wichtig anzumerken, dass diese Beziehung nicht reziprok ist, d.h. wenn User A einem anderen User folgt, bedeutet das nicht automatisch, dass auch B dem User A folgt.
- *Retweet*: Ein weiteres wichtiges Features, das großen Anteil an der Verbreitung von Tweets hat, sind die sogenannten Retweets. Diese ermöglichen es einem User A, einen Tweet eines anderen Users an alle Follower von A zu tweeten und diesen Tweet damit weiter zu verbreiten.
- *Direct Message*: User können Kurznachrichten auch direkt untereinander austauschen. Dazu wird der Nachricht der Benutzername des Empfängers hinzugefügt (beispielsweise ist der Tweet „@eva_zangerle was denkst du über das neue Twitter-Design?“

an die Benutzerin @eva_zangerle gerichtet). Diese spezielle Art von Tweets ist auch öffentlich einsehbar.

– *Hashtag*: Zu Zwecken der Übersichtlichkeit wurden von Userinnen und Usern sogenannte Hashtags eingeführt, die Schlagwörter (versehen mit einem #-Zeichen) darstellen und zur Kategorisierung von Tweets herangezogen werden. Im obigen Beispiel wird der Hashtag *#Förderungen* verwendet, um festzuhalten, dass dieser Tweet sich mit dem Thema Förderungen befasst.

Kriminalität auf Twitter

Kriminalität auf Twitter konzentriert sich hauptsächlich auf die Verbreitung von Spam-Tweets. Dazu zählt einerseits das Sammeln von Informationen über Benutzerinnen und Benutzer, um diese Informationen verkaufen zu können und in weiterer Folge Spam personalisiert und gezielt an bestimmte Benutzergruppen schicken zu können. Andererseits wird dies auch über das massenhafte Versenden von großen Mengen an Tweets mit dem Ziel, möglichst viele Benutzerinnen und Benutzer damit erreichen zu können, realisiert.

Prinzipiell lassen sich drei Ausprägungen von Kriminalität auf Twitter unterscheiden, die im Folgenden näher beschrieben werden (Chu, et al., 2010), (Egele, et al., 2013):

1. Anlegen von künstlichen Accounts (sogenannte Fake Accounts), die ausschließlich dazu dienen, Spam-Nachrichten zu verbreiten.
2. Erzeugen eines Bots bzw. eines Cyborgs.
3. Kompromittieren von bereits bestehenden Benutzer-Accounts.

Das *Anlegen von Fake Accounts* hat zum Ziel, Tausende von neuen Twitter-Accounts zu erstellen, um diese in weiterer Folge dazu zu verwenden, Spam zu verbreiten. Aktuelle Studien zeigen, dass 5 von 7 neu angelegten Benutzer-Accounts auf Twitter Spam-Accounts sind (Nexgate, 2013). Die Twitter-Plattform verfügt über Erkennungsmechanismen für Spam-Accounts, die sich auf ein ständig erweitertes Set von Regeln stützen (Thomas, et al., 2011). Ein Verletzen dieser Regeln führt zur Sperre von Accounts, deren Verhalten sich vom durchschnittlichen Verhalten menschlicher Userinnen und User unterscheidet. So werden beispielsweise Accounts, die überdurchschnittlich viele Tweets innerhalb eines festgelegten Zeitfensters absenden, als Spam-Accounts eingestuft. Ein weiteres Erkennungsmerkmal ist die Anzahl der Follower bzw. die Anzahl jener Accounts, denen gefolgt wird. Bei normalen Usern hat sich gezeigt, dass die Anzahl der Follower in etwa der Anzahl von Accounts, denen gefolgt wird, entspricht. Bei Spam-Accounts ist dieses Gleichgewicht verschoben (Thomas, et al., 2011). Dies ist darauf zurückzuführen, dass Spammer das Ziel haben, die Reichweite der ausgesendeten Tweets zu maximieren. Eine solche Maximierung der Reichweite kann unter anderem durch eine große Anzahl von Followern erreicht werden, die diese Spam-Tweets erhalten. Dies führt dazu, dass Spam-Accounts meist innerhalb kurzer Zeit einer großen Anzahl von anderen Accounts followen – mit dem Ziel, dass einige dieser Accounts dem Spam-Account „zurück“-

followen. Damit lässt sich die Diskrepanz zwischen der Anzahl an Followern und der Anzahl an gefolgten Accounts erklären und für die Erkennung von Spam-Accounts nützen.

Weitere Einflussfaktoren für den Erkennungsmechanismus sind beispielsweise die Anzahl an Links, die in den Tweets enthalten sind oder etwa wie viele unterschiedliche Tweets gesendet werden, da Tweet-Accounts meist versuchen, denselben Tweet tausendfach auszusenden. Der Twitter-Erkennungsmechanismus für Spam-Accounts ermöglicht es, 77% aller Spam-Accounts innerhalb eines Tages zu erkennen und zu sperren. 92% aller Spam-Accounts werden innerhalb von drei Tagen gesperrt (Thomas, et al., 2011). Dieses Sperren von Accounts ist auch mit ein Grund, warum lediglich etwa 200 Millionen von insgesamt 750 Millionen erzeugten Twitter-Accounts aktiv sind (Koetsier, 2013). Nichtsdestotrotz ist der Verkauf von Fake Accounts zu einem Geschäftsmodell geworden. So kann man online 1.000 Twitter-Accounts für 10-200$ kaufen (Perlroth, 2013).

Das *Erzeugen eines Bots oder Cyborgs* ist eng verwandt mit dem Anlegen von Fake Accounts, da Bots und Cyborgs oftmals auf einem Fake Account basieren. Ein Bot ist ein Programm, das automatisiert Aufgaben von Menschen übernimmt und ausführt. Ein Cyborg ist hingegen eine Mischung aus Mensch und Bot, bei der ein Mensch von einem Bot unterstützt wird (oder umgekehrt). Beispielsweise kann die Registrierung eines Accounts durch einen Menschen durchgeführt werden, um sogenannte Captchas (engl. *Completely Automatic Public Turing test to tell Computers and Humans Apart*, Von Ahn, et al., 2003) überwinden zu können. Captchas sind kleine Problemstellungen, die nur von Menschen gelöst werden können – beispielsweise verzerrte Bilder, die einen Text oder eine Rechenaufgabe enthalten, die für Menschen sehr leicht zu lesen bzw. zu lösen sind. Ein Computer hingegen muss komplexe Bilderkennungs-Algorithmen anwenden, um diese Problemstellungen lösen zu können, und daher können Captchas dazu verwendet werden, zu verhindern, dass Bots große Mengen von Benutzer-Accounts automatisch erstellen.

Nach der Registrierung durch den Menschen übernimmt dann der Bot den Account, um zu tweeten. Im Speziellen nützen Bots und Cyborgs die von der Twitter-Plattform zur Verfügung gestellten Schnittstellen, um automatisiert Spam-Tweets auszusenden. Aktuelle Studien zeigen, dass auf der Twitter-Plattform lediglich 35% aller Accounts von Menschen verwendet werden. Die verbleibenden 65% werden von Bots und Cyborgs zur automatischen Verbreitung von Tweets genützt (Urbina, 2013). Dazu muss allerdings angemerkt werden, dass in diesen 65% der Accounts nicht nur Spam-Bots enthalten sind. So verfügen beispielsweise viele Nachrichten-Plattformen über Bots, die automatisch einen Tweet aussenden, sobald ein neuer Artikel auf der Plattform publiziert wurde.

Die dritte Ausprägung von Kriminalität auf Twitter – das *Kompromittieren von bestehenden Benutzer-Accounts* – ist die populärste und in Bezug auf die Click-Through-Rate erfolgreichste Methode, um Spam auf Twitter zu verbreiten. Aus diesem Grund soll im folgenden Abschnitt detaillierter darauf eingegangen werden.

Analyse gehackter Twitter-Accounts

Im Weiteren soll eine Analyse des Verhaltens von Twitter-Usern, deren Account kompromittiert wurde, vorgestellt werden (Zangerle & Specht, 2014). Ein kompromittierter Account lässt sich dadurch definieren, dass der Account gehackt wurde und in einem nächsten Schritt dazu verwendet wird, über Tweets und Direct Messages Spam zu verbreiten. Ein wichtiger Faktor diesbezüglich ist, dass bei einem solchen Vorgehen das Vertrauensverhältnis zwischen einem User und seinen Followern ausgenützt wird, da ein Link, der vermeintlich von einem für den User vertrauenswürdig erscheinenden Account auf Twitter gesendet wurde, mit höherer Wahrscheinlichkeit angeklickt wird.

Das Ziel dieser Studie war, zu untersuchen, wie Benutzerinnen und Benutzer auf das Kompromittieren reagieren und welche Maßnahmen sie daraufhin setzen. Dazu wurden Tweets untersucht, mithilfe derer Twitter-Benutzerinnen und -Benutzer ihren Followern mitteilen, dass ihr Account gehackt wurde. Ein Beispiel für einen derartigen Tweet lautet wie folgt: „My account was hacked. Sorry for any tweets that may have been inappropriate. Back to normal now." (gesendet von Twitter User @dennishambright am 19.05.2014). Um ein repräsentatives und ausreichend großes Datenset für die Analyse zur Verfügung zu haben, wurden über einen Zeitraum von acht Monaten Tweets gesammelt. Dazu wurde die Twitter Filter API, eine öffentliche Schnittstelle, verwendet, die es erlaubt, alle Twitter-Nachrichten, die bestimmte Suchwörter enthalten, abzufragen (Twitter, 2014). Gesamt wurden während dieses Zeitraumes 1.231.468 Tweets abgefragt, die die Suchwörter „hacked account" oder „compromised account" enthalten. Twitter limitiert jene Datenmenge, die über die Twitter Filter-Schnittstelle abgefragt werden kann, auf etwa 1% aller Nachrichten, die pro Tag auf Twitter gepostet werden. Da die Anzahl jener Tweets, die den angeführten Suchkritierien entsprechen, stets unter dieser 1%-Marke lagen und damit die Limits nicht erreicht wurden, kann sichergestellt werden, dass alle relevanten Tweets abgefragt und gespeichert wurden. Tabelle 1 enthält die wichtigsten Eckdaten der abgefragten Daten. Durchschnittlich wurden pro Tag 5.331 Tweets gesammelt, wobei der große Unterschied zwischen der minimalen und der maximalen Anzahl an gesammelten Tweets durch sehr populäre Tweets, die tausendfach retweeted wurden, zu erklären ist. So wurde während des Crawling-Zeitraumes der Account der Firma Burger King gehackt, was tausendfach retweeted wurde.

Charakteristik	**Anzahl**
Tweets gesamt	1.231.468
Benutzer-Accounts gesamt	839.013
Durchschnitt Tweets pro Tag	5.331
Minimum Tweets pro Tag	262
Maximum Tweets pro Tag	42.670
Retweets	339.824
Hashtags	179.994
URLs	125.603

Tabelle 1: *Datenset-Charakteristika*

Nach einer qualitativen Analyse der Tweets wurden folgende Klassen für die Kategorisierung verwendet:

1. Der User schreibt, dass der Account gehackt wurde (z.B. „ooh looks like I've been hacked! That explains the inability to get into my account! Will be putting that right“).
2. Der User entschuldigt sich für Tweets, die in ihrem/seinem Namen gesendet wurden (z.B. „My Account was hacked pls ignore all the tweets I sent today. I apologize for the inconvenience”).
3. Der User entschuldigt sich für Direct Messages, die in ihrem bzw. seinem Namen gesendet wurden (z.B. „If I sent you spams via DM, I'm really sorry – my account got hacked”).
4. Der User schreibt, dass sie bzw. er einen neuen Account eröffnet hat (z.B. „Hey guys, go follow my new account because this one is hacked and is sending out spam“).
5. Der User schreibt, dass sie bzw. er sein Passwort geändert hat (z.B. „Very sorry everyone. My account was hacked. password changed, hopefully that does the trick.”).
6. Der User schreibt, dass er von Freunden oder Verwandten gehackt wurde (z.B. „my brother hacked my account – sorry“).
7. Sonstige Tweets, die keiner der oben angeführten Kategorien entsprechen.

Die Klassifikation wurde mittels betreuten Lernens durchgeführt. Im Speziellen wurden Support Vector Machines (SVM) verwendet (Joachims, 1998), bei denen Texte als Feature-Vektoren kodiert werden. Das Ziel einer SVM ist es, im Vektorraum Hyperebenen zu finden, die den Raum in Vektoren-Klassen unterteilen. Dazu ist es notwendig, ein ausreichend großes Test- und Trainingsdatenset zu erstellen. Aus diesem Grund wurden 2.500 Tweets händisch in die oben angeführten Klassen eingeordnet. In einem ersten Schritt wurden in einem ersten Klassifizierungsvorgang all jene Tweets herausgefiltert, in denen eine Benutzerin oder ein Benutzer davon berichtet, dass sein/ihr eigener Account gehackt wurde, da oftmals auch über andere gehackte Accounts berichtet wird. Die so ermittelten 358.639 Tweets, die sich mit dem Hacken des eigenen Accounts beschäftigen, dienten in weiterer Folge als Eingabe für die eigentliche Klassifizierung des Benutzerverhaltens bei kompromittierten Accounts. Diese Klassifikation konnte mit einer Genauigkeit (engl. *accurracy*) von 78,25% durchgeführt werden. Nähere Details zur Klassifizierung können dem Originalpaper (Zangerle & Specht, 2014) entnommen werden.

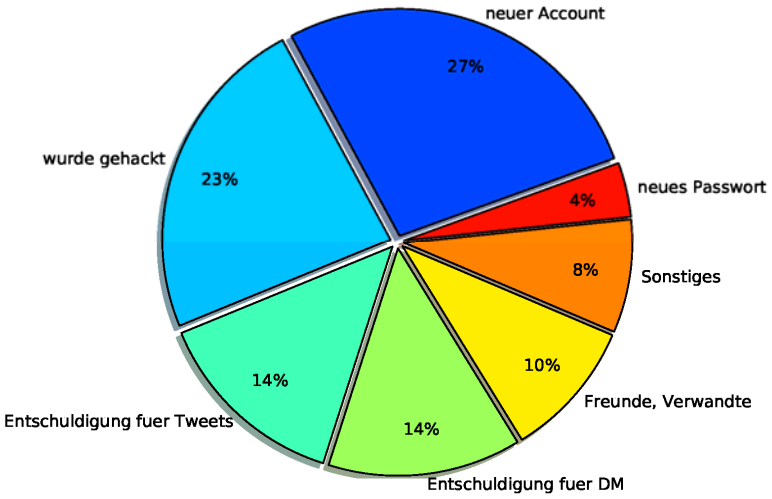

Abbildung 1: *Resultat der Klassifikation*

Abbildung 1 zeigt das Ergebnis der durchgeführten Klassifikation. Auffallend dabei ist, dass 27% aller User einen neuen Account anlegen und dies ihren Followern über einen Tweet mitteilen. 23% der analysierten User teilen ihren Followern lediglich mit, dass sie gehackt wurden. Insgesamt 28% aller User entschuldigen sich für Tweets oder Direct Messages, die in ihrem Namen versendet wurden. 10% aller User wurden durch Freunde oder Verwandte „gehackt", wobei sich dies bei genauerer Untersuchung der entsprechenden Tweets darauf zurückführen lässt, dass beispielsweise ein Smartphone ungesperrt liegen gelassen wurde und damit nicht als ein Kompromittieren zum Zweck des professionellen Spam-Versands zu bewerten ist.

In einem weiteren Schritt wurden die klassifizierten Tweets nochmals inhaltlich untersucht, um eine genauere Analyse der Ergebnisse zu ermöglichen. In Klasse 1 – jenen Tweets, die festhalten, dass der Besitzer oder die Besitzerin des Accounts gehackt wurde – ist auffällig, dass viele gehackte Accounts während der Zeitspanne, während der der Account kompromittiert und missbraucht wurde, Follower verlieren. Daher haben 25% der Tweets dieser Klasse zum Ziel, Benutzerinnen und Benutzer, die dem Account bereits einmal gefolgt sind, zu fragen, ob sie dem Account wieder folgen möchten. Die bemerkenswerteste Erkenntnis der durchgeführten Analyse ist, dass 27,3% der Benutzerinnen und Benutzer einen neuen Account anlegen, insbesondere in Hinblick darauf, dass Twitter Hilfe-Seiten für dieses Szenario zur Verfügung stellt (vgl. Twitter Support, 2014). Darin werden Benutzerinnen und Benutzer für den Fall eines gehackten Accounts angehalten, (i) ihr Passwort zu ändern, (ii) Verbindungen zu Drittapplika-

tionen zu widerrufen, (iii) das Passwort in vertrauenswürdigen Applikationen von Drittanbietern zu aktualisieren und (iv) sich zu vergewissern, dass die E-Mail Adresse sicher ist.

Auch bietet Twitter einen Hilfe-Account an (@support), der direkt über einen Tweet kontaktiert werden kann. Im vorliegenden Datenset wurde dieser Account lediglich von 1.105 Benutzerinnen und Benutzern kontaktiert. Auffallend ist, dass viele Benutzerinnen und Benutzer viel Zeit dafür investieren, ihre bestehenden Follower auf ihren neuen Account aufmerksam zu machen, wobei der alte Account mit den zuvor genannten Schritten wieder hergestellt und abgesichert werden könnte. Dies lässt darauf schließen, dass sich Nutzerinnen und Nutzer dieser Möglichkeit der Wiederherstellung nicht bewusst sind, da sie darüber nicht ausreichend informiert sind. Dazu zählt auch die Verwendung eines ausreichend sicheren Passwortes, um ein Kompromittieren des Accounts zu verhindern. Auch dazu stellt Twitter entsprechende Hilfe-Seiten zur Verfügung (vgl. Twitter Support, 2014).

Zusammenfassung

Im vorliegenden Paper wurden Missbrauch und Betrug in Sozialen Netzwerken am Beispiel des Kurznachrichtendienstes Twitter aufgezeigt. Dazu wurden die drei Ausprägungen von Kriminalität auf Twitter erklärt, wobei auf das Kompromittieren von bestehenden Benutzer-Accounts näher eingegangen wurde. Im Speziellen wurde eine Studie vorgestellt, die das Benutzerverhalten im Falle von kompromittierten Accounts untersucht. Dabei wurde festgestellt, dass 23% der Benutzerinnen und Benutzer Tweets aussenden, in denen sie festhalten, dass ihr Account gehackt wurde. 27,3% der Benutzerinnen und Benutzer schreiben hingegen, dass sie nach dem Kompromittieren des Accounts einen neuen Account angelegt haben. Diese Erkenntnis legt den Schluss nahe, dass die Benutzerinnen und Benutzer sich aufgrund von mangelnder Informationen nicht bewusst sind, dass kompromittierte Accounts wieder zurückerlangt und gesichert werden können.

Literatur

Bergh, J. V. d. (2013): *InSites Consulting.* [Online] Available at: http://www.insites-consulting.com/infographic-millennials-social-media/ [Stand vom 17-02-2014].

Chu, Z., Gianvecchio, H. & Jajodia, S. (2010): Who is Tweeting on Twitter: Human, Bot, or. In: *Proceedings of the 26th Annual Computer.* s.l.:s.n., S. 21–30.

Egele, M., Stringhini, G., Kruegel, C. & Vigna, G. (2013): COMPA: Detecting Compromised Accounts on Social Networks. In: *ISOC Network and Distributed System.* s.l.:s.n.

Grier, C., Thomas, K., Paxson, V. & Zhang, M. (2010): @spam: the underground on 140 characters or less. In: ACM (Hrsg.): *Proceedings of the 17th ACM conference on Computer and communications security 2010 (CCS '10).* New York: s.n., S. 27–37.

Joachims, T. (1998): Text Categorization with Support Vector Machines: Learning with Many Relevant Features. *Machine Learning: ECML-98,* S. 137–142.

Koetsier, J., 2013. *How Twitter plans to make its 750M 'users' like its 250M real users.* [Online] Available at: http://venturebeat.com/2013/09/16/how-twitter-plans-to-make-its-750m-users-like-its-250m-real-users/ [Stand vom 21-02-2014].

Nexgate (2013): *Research Report: 2013 State of Social Media Spam.* [Online] Available at: http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf [Stand vom 17-02-2014].

Perlroth, N. (2013): *Bits Blog New York Times.* [Online] Available at: http://bits.blogs.nytimes.com/2013/04/05/fake-twitter-followers-becomes-multimillion-dollar-busines [Stand vom 18-02-2014].

Thomas, K., Grier, C., Song, D. & Paxson, V. (2011): Suspended Accounts in Retrospect: an Analysis of Twitter Spam. In: ACM (Hrsg.): *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement.* s.l.:s.n., S. 243–258.

Twitter Support (2014): *Keeping your account secure.* [Online] Available at: https://support.twitter.com/articles/76036-safety-keeping-your-account-secure# [Stand vom 19-02-2014].

Twitter Support (2014): *My account has been compromised.* [Online] Available at: https://support.twitter.com/articles/31796-my-account-has-been-compromised# [Stand vom 19-02-2014].

Twitter (2014): *Filter API Documentation.* [Online] Available at: https://dev.twitter.com/docs/api/1.1/post/statuses/filter [Stand vom 17-02-2014].

Urbina, I. (2013): *New York Times SundayReview: I Flirt and Tweet. Follow Me at #Socialbot.* [Online]. Available at: http://www.nytimes.com/2013/08/11/sunday-review/i-flirt-and-tweet-follow-me-at-socialbot.html [Stand vom 18-02-2014].

Von Ahn, L., Blum, M., Hopper, N. & Langford, J. (2003): CAPTCHA: Using hard AI problems for security. *Advances in Cryptology-EUROCRYPT 2003.* s.l.: Springer, S. 294–311.

Wagner, K. (2013): *More Than 70% of Email Is Spam.* [Online] Available at: http://mashable.com/2013/08/09/70-percent-email-is-spam/ [Stand vom 19-02-2014].

Washington Post (2013): *Twitter turns 7: Users send over 400 million tweets per day.* [Online] Available at: http://articles.washingtonpost.com/2013-03-21/business/37889387_1_tweets-jack-dorsey-twitter [Stand vom 17-02-2014].

Zangerle, E. & Specht, G. (2014): "Sorry, I was hacked" – A Classification of Compromised Twitter Accounts. In: ACM (Hrsg.): *Proceedings of the 29th ACM Symposium on Applied Computing.* Gyeongju, Korea: s.n.

Geocaching – das Spiel mit Geodaten

Andreas Aschaber und Michaela Rizzolli

Zusammenfassung

Geocaching, eine moderne Art der Schnitzeljagd, erfreut sich zunehmender Beliebtheit. Der Beitrag thematisiert Geocaching als Spiel mit Geodaten. Im Vordergrund stehen dabei die steigende Produktion von Daten und ihre materielle Einbindung in Form von Caches im physischen Raum. In der Auseinandersetzung mit Geocaching wird deutlich, dass nicht die Datenflut selbst, sondern der Umgang mit ihr und die Reaktion darauf zu Problem- und Konfliktfeldern führt.

Einleitung

Es raschelt am Waldboden. Eine Gestalt huscht durch das Unterholz, ein Ast wird vorsichtig zur Seite geschoben. Verstohlene Blicke ins Blättergewirr – ist da etwas? Nichts zu entdecken. Kurz darauf an einer anderen Stelle ganz in der Nähe: Ein Stein wird umgedreht, plötzlich Aufregung, ein Aufschrei – Fund! Der Cache ist gehoben.

In den Medien wird Geocaching gerne als „moderne Schatzsuche mit GPS" (Scheller 2011) oder „Hightech-Schnitzeljagd" (Arnu 2006) betitelt. Sein elementarer Baustein ist der „Geocache", der sowohl das von der Erde (Geo) offenbarte Versteck, als auch den darin verborgenen Schatz benennt (vgl. Schreiber 2012, S. 133). Ein solcher Schatz besteht in der Regel aus einer Box, einem Logbuch, in das sich die Geocacherinnen und Geocacher eintragen können, sowie diversen kleinen Tauschgegenständen.

Beim Geocaching verstecken Mitglieder der Geocaching-Community kleine Schätze, sogenannte „Caches", an möglichst unauffälligen Orten. Der „Owner" – die Person, die den Cache platziert – veröffentlicht die genauen GPS-Koordinaten des Verstecks zusammen mit einer kurzen Beschreibung auf Geocachingplattformen im Internet. Die „Cacher" machen sich mit den veröffentlichten Koordinaten, einem Empfänger für globale Navigationssatellitensysteme und einer Beschreibung des Caches auf die Suche. Kann der Schatz „gehoben" werden, tragen sich die Cacherinnen und Cacher in das Logbuch ein und legen den Schatz wieder an dieselbe Stelle zurück (vgl. Breuer 2013, S. 12).

Die Schatzsuche soll möglichst von „Muggles" (die Bezeichnung ist J.K. Rowlings Harry-Potter-Büchern entlehnt) unbeobachtet erfolgen. Außenstehende, die Geocaching nicht kennen, werden von der Geocaching-Community als „Muggles" bezeichnet. Ein gemuggelter Cache meint einen Schatz, der von Nicht-Geocacherinnen und Nicht-Geocachern gefunden und entfernt wurde (vgl. Gram-Hansen 2009).

In erster Linie geht es beim Geocaching um die Suche und das Auffinden der Caches (vgl. Louis, Meléndez & Steg 2011, S. 533). Mittlerweile gibt es eine Reihe von verschiedenen Geocache-Typen. Der *traditionelle Cache* ist der einfachste und auch der am weitesten verbrei-