



Gemeinde Lindlar – Der Bürgermeister – Borromäusstraße 1, 51789 Lindlar

An die Mitglieder des Haupt- und Finanzausschusses der Gemeinde Lindlar

Nachrichtlich
an alle Ratsmitglieder

Auskunft erteilt:
Geschäftszeichen:
Zimmer Nr.: 400
Telefondurchwahl: (02266) 96 410
Telefax: (02266) 96 7 410
E-Mail: diana.froitzheim@gemeinde-lindlar.de
Homepage: <http://www.lindlar.de>

Lindlar, den 11. September 2009

15. Sitzung des Haupt- und Finanzausschusses am 23. September 2009

Sehr geehrte Damen und Herren,
wir beabsichtigen, die Tagesordnung um

**TOP 4a: Information der Bürgerinnen und Bürger über www.twitter.com
Antrag der Fraktion Bündnis 90/Die Grünen vom 18.08.2009**

zu erweitern. Die Sitzungsvorlage hierzu reichen wir hiermit nach.

Mit freundlichen Grüßen

Dr. Hermann-Josef Tebroke
Bürgermeister

Anlage

zentrale und techn. Dienste

Sitzungsvorlage
für die Sitzung des
Haupt- und Finanzausschusses
am 23.09.2009

- öffentliche Sitzung -

TOP 4a: Information der Bürgerinnen und Bürger über www.twitter.com Antrag der Fraktion Bündnis 90/Die Grünen vom 18.08.2009
--

Sachverhalt:

Mit fristgerecht eingereichtem Schreiben vom 18.08.2009 (Anlage I) stellt die Ratsfraktion Bündnis 90/Die Grünen folgenden Antrag:

„Der Rat der Gemeinde Lindlar beauftragt die Verwaltung, zur Information der Bürgerinnen und Bürger über Bekanntmachung, Termine und Inhalte von Sitzungen des Rates und seiner Ausschüsse u.ä. den Internet-Informationsdienst twitter (www.twitter.com) zu nutzen.“

Zur Begründung des Antrags wird auf Anlage I dieser Sitzungsvorlage verwiesen.

Auf der Website <http://www.wikipedia.de> ist folgende Information unter dem Suchbegriff „twitter“ zu finden, welche nachfolgend auszugsweise zitiert wird:

„**Twitter** ist ein soziales Netzwerk und ein meist öffentlich einsehbares Tagebuch im Internet (Mikro-Blog), welches weltweit per Website, Mobiltelefon, Desktopanwendung, Widget oder Webbrowser-Plug-in geführt und aktualisiert werden kann. Twitter wurde im März 2006 der Öffentlichkeit vorgestellt und gewann 2007 den ‚South by Southwest Web Award‘ in der Kategorie ‚Blogs‘.

Angemeldete Benutzer können eigene Textnachrichten mit maximal 140 Zeichen eingeben und anderen Benutzern senden. ... Die Beiträge auf Twitter werden als ‚Tweets‘ (engl. to tweet = zwitschern) oder ‚Updates‘ bezeichnet. ...

Mittels Erweiterungen lassen sich zusätzliche Informationen über den Absender und die Empfängergruppe anzeigen, wie etwa den jeweiligen Standort auf dem Kartendienst [Google Maps](http://www.google.com/maps). ...

Twitter sammelt personenbezogene Daten seiner Benutzer und teilt sie Dritten mit. Twitter sieht diese Informationen als einen Aktivposten und behält sich das Recht vor, sie zu verkaufen, wenn die Firma den Besitzer wechselt.“

Die Möglichkeit der v.g. Sammlung von personenbezogenen Daten und der Standortlokalisierung sind datenschutzrechtlich relevant, deswegen unterbreitet die Verwaltung dem Haupt- und Finanzausschuss folgenden

Beschlussvorschlag:

Vor der weiteren Beratung im Gemeinderat soll die Verwaltung die Stellungnahme des Datenschutzbeauftragten einholen und von der civitec (vormals GKD) prüfen lassen, ob die Verwendung von Twitter die Sicherheit des gemeindlichen Datennetzwerks gefährden könnte.

Herbert Schibelka
Fachleiter

Dr. Hermann-Josef Tebroke
Bürgermeister

Ratsfraktion Lindlar

www.gruene-lindlar.de



c/o Fraktionsprecher Patrick Heuwes Alsbacher Str. 41a 51789 Lindlar
Tel.: 0160-3519834, E-Mail: patrick.heuwes@gruene-lindlar.de

Herrn
Bürgermeister Dr. Tebroke

→ H. Tebroke
→ Herr Schibeltner

18.08.2009

B.T.
nach der Wahl
25.8.09

Antrag zur Sitzung des Haupt- und Finanzausschuss am 23.09.2009

Sehr geehrter Herr Dr. Tebroke,

die Ratsfraktion B'90/Die GRÜNEN beantragt:

Der Rat der Gemeinde Lindlar beauftragt die Verwaltung, zur Information der Bürgerinnen und Bürger über Bekanntmachungen, Termine und Inhalte von Sitzungen des Rates und seiner Ausschüsse u.ä. den Internet-Informationsdienst twitter (www.twitter.com) zu nutzen.

Eine solche twitter-Nachricht könnte z.B. lauten: „Ratssitzung am 29.09.09. Unterlagen finden Sie unter: <http://www.lindlar.de/buergerinfo/politik/einladungen-und-niederschriften.html>“.

Begründung:

In vielen Gesprächen mit Bürgerinnen und Bürgern insbesondere im Rahmen des Wahlkampfes und unserer Veranstaltungsreihe „GRÜN (be-) trifft ...“ äußerten diese, dass sie seit Abschaffung der Veröffentlichung der Termine und TOPS der Sitzungen des Rates und seiner Ausschüsse im Mitteilungsblatt absolut unzureichend über die Geschehnisse in Lindlar und die Lindlarer Politik informiert sind.

Insbesondere Menschen ohne Internetanschluss sind faktisch, von dem Informationsfluss über die Politik in der Gemeinde abgeschlossen, da die Presse, wenn überhaupt, erst berichtet, wenn die Entscheidungen bereits getroffen worden sind. Aber auch Menschen mit Internetanschluss haben noch viele andere Sachen zu tun, als täglich auf der Internetseite der Gemeinde nach aktuellen Informationen zu suchen. Da bietet sich die Nutzung des Internetinformationsdienstes twitter geradezu an. Interessierte BürgerINNEN könnten der Gemeinde Lindlar bei twitter „folgen“ und wären

so immer aktuell über neue Aktualisierungen auf der Seite www.lindlar.de informiert und könnten die Informationen bei Interesse online abrufen.

Dieser neue Bürgerservice würde zwar den BürgerINNEN ohne Internetanschluss nicht helfen, wäre aber für Interessierte, die „online“ sind, ein komfortable Möglichkeit auf dem Laufenden zu sein.

Mit freundlichen Grüßen,



Patrick Heurtes (Fraktionsprecher)

Anlage II

12.09.2009 16:12

Twitter ändert Nutzungsbedingungen

Nachdem Twitter[1] rund zwei Jahre absolut werbefrei lief, erklärte Mitbegründer Biz Stone jetzt im offiziellen Firmen-Blog[2] "die Tür für Anzeigen offen zu lassen." Dafür änderte der Microblogging-Dienst seine Nutzungsbedingungen[3].

Die Änderung beinhaltet den Umgang mit Tweets, die der Dienst unter anderem nutzen, kopieren, reproduzieren, modifizieren und veröffentlichen darf ("Twitter is allowed to 'use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute' your tweets because that's what we do. However, they are your tweets and they belong to you."). Dass das Vorhaben, mit Werbeeinblendungen Geld zu verdienen, von Erfolg gekrönt wird, bezweifeln einige Internetexperten, da die potenziell werbenden Unternehmen und Twitter selbst keinen Einfluss auf die vom User erstellten Inhalte haben.

(rst[4]/c't)

URL dieses Artikels:

<http://www.heise.de/newsticker/meldung/145230>

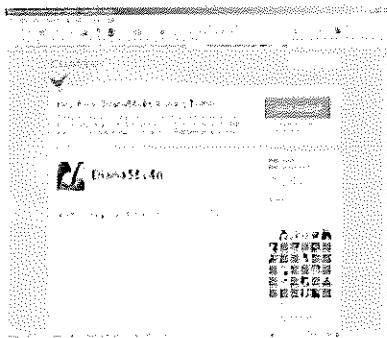
Links in diesem Artikel:

- [1] <http://twitter.com/>
- [2] <http://blog.twitter.com/>
- [3] <http://twitter.com/tos>
- [4] <mailto:rst@ct.heise.de>

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.

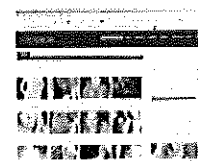
Immer mehr Menschen lassen die Welt in 140 Zeichen daran teilhaben, was sie gerade tun, denken oder zu tun gedenken. Auch Prominente aus allen Bereichen, Medien oder Unternehmen bedienen sich zunehmend des Dienstes. Noch wenig im öffentlichen Fokus stehen derzeit allerdings seine Gefahren und Schwachstellen.

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.



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.

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, 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 mittlerweile 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 Hypponen 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.

Quelle: <http://www.heise.de/ix/artikel/2009/09/106/>