

Link: <https://www.computerwoche.de/a/handy-eroeffnet-einblick-in-die-privatsphaere,2350579>

Soziale Netzwerke

Handy eröffnet Einblick in die Privatsphäre

Datum: 12.08.2010

Autor(en): Werner Kurzlechner

Social Networking von unterwegs ist ein Sicherheitsrisiko: Handy-Nutzer laufen Gefahr, ungewollt Informationen etwa über den eigenen Standort weiterzugeben, wie eine akute Studie aus den USA belegt.



Netzwerke über
Smartphone? Geht easy.
Hat aber auch seine
Sicherheitslücken.

Über GoogleStreetview und verletzte Privatsphäre redet sich streckenweise die ganze Republik die Köpfe heiß. Leider ist das nicht das einzige **Datenschutzproblem**¹ in der in alle Richtungen vernetzten und überall kommunizierenden Welt. Wer twittert und flickrt und facebookt und auch über **Handy**² in Social Networks unterwegs ist, gibt möglicherweise mehr persönliche Daten an Dritte preis, als ihm lieb und bewusst ist. Zu diesem Ergebnis kommt eine Studie des in Massachusetts ansässigen Worcester Polytechnic Institute (**WPI**)³ und der Research-Abteilung von **AT&T-Labs**⁴.

Wer weiß zum Beispiel Bescheid über den aktuellen **Aufenthaltort**⁵ eines Nutzers, der sich mobil in ein Netzwerk einwählt? Diese und ähnliche Fragen sind brisanter als angenommen, haben die Forscher herausgefunden. Sie stießen auf diverse **Lecks**⁶, durch die gegenüber Anbietern von Social Networking-Seiten freigegebene Daten in weitere Hände gelangen.

Insgesamt 20 Websites untersuchten die Wissenschaftler aus den USA: 13 **Mobile**⁷ Online Social Networks wie Brightkite, Flickr, Foursquare, Gowalla und Urbanspoon und sieben Netzwerke wie Facebook, LinkedIn, MySpace und Twitter, die ihren Usern auch Zugang über mobile Endgeräte gestatten. Ernüchterndes Resultat: Sämtliche 20 Seiten weisen in irgendeiner Form **Sicherheitslücken**⁸ auf.

Es geht beispielsweise darum, dass von Usern gewählte **Schutzeinstellungen**⁹ zwar auf Rechnern funktionieren - aber nicht mehr beim Zugriff über **Handy**¹⁰. Wer zum Beispiel seinen **Aufenthaltort**¹¹ über mobilen "Check In" nur seinen Freunden im Netzwerk anzeigen lassen will, läuft Gefahr, dass unerwartet jeder angemeldete User diese Information bekommen kann.

Derartige Ärgernisse geschehen zum Teil als punktuelle Anwendungsfehler, zum Teil sind sie sogar die Regel. Die Palette an Lücken ist bunt und vielfältig - leider. Besonders häufig gelangt die individuelle Geräte-Identifizierung von Social Networking-Nutzern an Dritte. Diese könnten damit die Profile im Netzwerk mit eigenen Daten über das Browsing-Verhalten der User abgleichen.

Standortinfos und Geräte-Identifizierung werden zur Gefahr

Eine andere undichte Stelle ist die Verknüpfung von Standortinformationen, die **User**¹² den Networking-Anbietern gewähren, mit Map-Tools, die diese sichtbar machen. Dabei kommt es vor, dass die Informationen über den Aufenthaltsort an die Betreiber der Landkarten- und Stadtplananwendungen gelangen. Bei zwei der untersuchten Dienste stellten die Forscher diese Lecks fest.

"Die Kombination von Standortinformationen, individueller Geräte-Identifizierung und klassischen Schlupflöchern für andere persönliche Daten fügt sich zu einem Problem für die Privatsphäre der User zusammen", heißt es in der Studie.

"Der erste Blick auf Mobile Online Social Networks gibt Anlass für ernste **Sorgen**¹³", meint Mitautor Craig Wills, Professor für Computerwissenschaften am WPI. Insbesondere seien die Anwender häufig überfordert durch die komplizierten und verstreuten Kontrolloptionen, über die sie den Schutz ihrer Daten regulieren können. Wissenschaftler Wills fordert einen einheitlichen, leicht verständlichen und handhabbaren Rahmen, über den User den von ihnen gewünschten Schutz der **Privatsphäre**¹⁴ einstellen können.

Ob die genannten Probleme eher bei Twitter oder Facebook auftauchen, verrät die Studie übrigens nicht. Es wird nicht öffentlich gemacht, auf welchen Seiten sich welche konkreten Lecks verbergen. Die Studie kann kostenlos auf der Homepage des WPI heruntergeladen werden.

Links im Artikel:

¹ <https://www.computerwoche.de/filesserver/idgwpcw/files/1769.pdf>

² <https://www.computerwoche.de/netzwerke/mobile-wireless/2350214/>

³ <http://www.wpi.edu/>

⁴ http://www.research.att.com/editions/201005_home.html

⁵ <https://www.computerwoche.de/subnet/telekom/1938469/>

⁶ <http://geschaeftskunden-center.telekom.de/>

⁷ https://www.cio.de/knowledgecenter/mobile_it/875923/

- 8 <https://www.computerwoche.de/netzwerke/mobile-wireless/2350104/>**
 - 9 <https://www.computerwoche.de/filesserver/idgwpcw/files/1778.pdf>**
 - 10 <https://www.computerwoche.de/filesserver/idgwpcw/files/1780.pdf>**
 - 11 <https://www.computerwoche.de/netzwerke/mobile-wireless/1938586/>**
 - 12 https://www.cio.de/knowledgecenter/desktop_trends/872029/**
 - 13 <https://www.cio.de/knowledgecenter/security/870605/index2.html>**
 - 14 <https://www.cio.de/knowledgecenter/security/2237880/>**
-

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.