idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Friedrich-Alexander-Universität Erlangen-Nürnberg
Blandina Mangelkramer

19.07.2013
http://idw-online.de/de/news544382

Buntes aus der Wissenschaft
Gesellschaft, Informationstechnik
überregional

Menschen sind mit Datenschutz überfordert

Das Thema Datenspionage beherrscht derzeit die öffentliche Diskussion: Erst sorgten die Ausspähungsprogramme Prism und Tempora für Aufregung. Nun heizt Facebooks Graph Search, das Nutzern die Suche nach Interessen von anderen Personen ermöglicht, die Debatte um Datensicherheit und Privatsphäre im Internet weiter an. Warum Internetnutzer ihre Daten nur begrenzt schützen können, erklärt Dr. Zinaida Benenson, Lehrstuhl für Informatik 1 – IT-Sicherheitsinfrastrukturen der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), im Gespräch mit „FAU aktuell".

> Wie gut schützen deutsche Bürger ihre Daten und ihre Privatsphäre im Internet?

Deutsche Bürger sind genauso wie alle anderen Menschen mit dem Schutz ihrer Daten und ihrer Privatsphäre restlos überfordert. Allein in Facebook muss man seine Einstellungen an mindestens fünf Stellen anpassen, um seine Daten nur für die Facebook-Freunde verfügbar zu machen. Einige Umfragen und Experimente, die wir in der letzten Zeit durchgeführt haben, zeigen, dass die meisten sich weder mit der Sichtbarkeit ihrer eigenen Daten auf Facebook noch mit dem Zugriff der Smartphone-Apps auf ihre Daten auskennen.

Daran sind meiner Meinung nach nicht die Benutzer schuld, sondern die unübersichtlichen Einstellungen und schwer verständlichen Informationen der Anbieter. Zum Beispiel wird bei der Installation jeder Android-App angezeigt, auf welche Daten diese zugreift. Diese „Android Permissions" sind allerdings so technisch formuliert, dass selbst Informatiker Schwierigkeiten haben, sie zu verstehen.

Ein anderes Beispiel sind die Datenschutzrichtlinien von Facebook, die sehr kompliziert formuliert sind. Da ist es nicht verwunderlich, dass laut einer Umfrage die meisten Benutzer glauben, dass ihre Daten vollständig Facebook gehören. Tatsächlich geben sie Facebook jedoch nur die Erlaubnis die Daten zu nutzen, auch wenn diese Nutzung sehr umfangreich ausfällt.

> Warum gehen viele Menschen mit dem Datenschutz im Internet sehr locker um, obwohl sie die Gefahren kennen?

In der Forschung wird diese Lage „Privacy Paradox" genannt. Dafür gibt es mehrere Gründe. Auf der einen Seite wissen Firmen wie Facebook oder Payback, wie sie Kundendaten nutzen können und was diese wert sind. Andererseits haben die Benutzer kaum Kenntnisse darüber und können die langfristigen Folgen der Datenweitergabe nicht abschätzen – das fällt selbst Experten schwer: Dort, wo große Mengen an personenbezogenen Daten gesammelt werden, entstehen immer neue Ideen, wofür diese Daten nützlich sein könnten. Das sieht man am Beispiel von Facebook Graph Search. Auch wenn Gesetze uns eigentlich gegen diese nicht zweckgebundene Nutzung schützen, ist es für Firmen immer noch viel zu einfach, die Datenschutzbestimmungen entsprechend zu ändern und die Benutzer erneut zustimmen zu lassen ¬– die meisten lesen vermutlich solche neuen Richtlinien ohnehin nicht. Facebook, Google oder PayPal haben diesen Trick schon mehrmals eingesetzt.

Außerdem werden viele Menschen durch die kurzfristigen und greifbaren Ziele – ein Rabatt zu bekommen oder eine App zu nutzen – von den langfristigen und abstrakten Zielen – Datenschutz – abgelenkt. Das ist eine ganz normale menschliche Eigenschaft, derer sich Marketing und Werbung schon lange bedienen.

> Welche Vorsichtsmaßnahmen sollte jeder Internetnutzer ergreifen?

Wer seine Daten schützen möchte, sollte kein Konto bei Facebook oder Google Mail haben, kein Smartphone benutzen – und niemals mittels Google nach Informationen suchen. Sicher werden die meisten Menschen über solche Vorsichtsmaßnahmen nur den Kopf schütteln. Jedoch gibt es momentan leider keine technischen Maßnahmen für den Durchschnittsnutzer. Die Verfahren und Programme sind viel zu kompliziert.
Meines Erachtens gibt es nur eins: den gesunden Menschenverstand einsetzen. Zum Beispiel sollte man immer überlegen, ob eine Aussage oder ein Foto einem langfristig peinlich werden könnte, bevor man diese veröffentlicht, und zwar nicht nur auf Facebook oder Twitter, sondern auch dann, wenn man sich „anonym" fühlt, zum Beispiel in einem Forum unter einem Nicknamen postet oder chattet.

> Ist es möglich, sich vor Ausspähprogrammen wie Prism und Tempora zu schützen?

Wenn Nachrichtendienste auf Informationen zugreifen, auf die sie nicht zugreifen dürften, ist ein Schutz kaum möglich. Zum Beispiel übermitteln wir unsere Verbindungsdaten an die Mobilfunkanbieter und Internetprovider, um deren Service nutzen zu können. Wer auf diese Daten zugreifen kann, hat schon sehr viel gewonnen. Genauso ist es technisch extrem schwierig, sich gegen einen Gegner zu schützen, der den kompletten Datenfluss in einem Netzwerk protokolliert. Man kann zwar E-Mails verschlüsseln, aber selbst dann wäre bekannt, mit wem, wann, und wie oft man kommuniziert. Und das sind an sich schon sehr wertvolle Informationen.
Ich glaube, dass man sich als Internetnutzer nicht gegen diese mächtigen Ausspähprogramme schützen kann. Die technischen Möglichkeiten der Ausspähung und der Datenanalyse können nur durch Gesetze und transparente Kontrollmaßnahmen begrenzt werden.

Ansprechpartner für die Presse:
Dr. Zinaida Benenson
Tel.: 09131/85- 69908
zinaida.benenson@cs.fau.de

Dr. Zinaida Benenson
Foto: FAU