Soziale Netzwerke

Ökotest: Datenschutz bei Facebook, Google, Twitter & YouTube „ungenügend“

03.05.2010 – 19:34 – Robert A. Gehring

Die Zeitschrift Ökotest hat den Datenschutz ausgewählter sozialer Netzwerke und Internetdienste untersucht. Das Ergebnis ist eindeutig: Nur die untersuchten deutschen Anbieter schneiden „sehr gut“ ab. US-amerikanische Anbieter nehmen es hingegen mit dem Datenschutz oft nicht so genau.

Facebook ist ohne Zweifel der Platzhirsch unter den sozialen Netzwerken. Rund 400 Millionen Erdenbürger haben sich bereits bei Facebook registriert. Aus Deutschland sollen rund neun Millionen Mitglieder kommen. Aber auch andere soziale Netzwerke haben Millionen Teilnehmer und täglich werden es mehr. Wer sich bei einem sozialen Netzwerk anmeldet, gibt nicht selten persönliche Daten von sich preis. Doch wie gehen die Betreiber der Netzwerke damit um? Wie halten sie es mit dem Datenschutz? Das wollte die Zeitschrift Ökotest genauer wissen und hat für ihre Mai-Ausgabe die Datenschutzbestimmungen mehrerer großer Anbieter unter die Lupe nehmen lassen.

Das Ergebnis ist zwiespältig ausgefallen. Auf der einen Seite gibt es eine ganze Reihe von Anbietern, denen Ökotest die Note „sehr gut“ für den Datenschutz gibt. Denen stehen jedoch ebenso viele Anbieter gegenüber, die beim Datenschutz durchgefallen sind. Zu den mit „sehr gut“ bewerteten sozialen Netzwerken gehören die deutschen Anbieter SchülerVZ, StudiVZ und Xing. Ein „ungenügend“ bekam hingegen Facebook, das seinen Sitz in den USA hat.

Neben sozialen Netzwerken hat Ökotest auch den Datenschutz bei anderem Internet-Diensteanbieter untersucht. Mit „gut“ wurden Amazon und Ebay bewertet, mit „ungenügend“ Google, Twitter und die Google-Tochter YouTube.

Ökotest bewertet die ungenügenden Testergebnisse amerikanischer Anbieter so: „Besonders bedenklich ist, dass die Unternehmen mit Ausnahme von Twitter das Safe-Harbor-Abkommen unterzeichnet haben. Damit verpflichten sie sich eigentlich, das deutsche Datenschutzrecht zu beachten. Doch ganz offenbar sind solche Verträge das Papier nicht wert, auf dem sie unterschreiben sind bzw. die E-Mail nicht, mit der sie versandt wurden.“

Wer sich also bei Facebook, Twitter oder einem der anderen Dienste mit mangelhaftem Datenschutz anmeldet, sollte sich genau überlegen, welche persönlichen Daten er dort speichert. Im Zweifel sollten Sie lieber dem Grundsatz der Datensparsamkeit folgen und

möglichst wenig von sich preisgeben. Oder aber, Sie suchen sich einen Anbieter, der den Datenschutz ernst nimmt.

Datenschutz: Warum Twitter gefährlicher ist als Facebook

Es wird viel darüber berichtet, dass Twitter Drittanbietern im großen Stil Zugriff auf seine Datenbank erlauben will. Damit ist nicht nur der Zugriff auf Tweets verbunden, die für "normale" User nicht mehr verfügbar sind, weil sie zu alt sind. Käufer dieser Daten können auch auf 40 weitere Variablen wie den Zeitpunkt, den Ort, die Zeitzone und den Benutzernamen, unter denen der Tweet veröffentlich wurde, zugreifen. Eine Vereinbarung mit einem Drittanbieter besteht bereits seit November 2010, eine weitere soll jetzt folgen.

Dieses Vorgehen stößt im Netz auf Kritik, die völlig richtig ist, aber einen wesentlichen Aspekt gar nicht berücksichtigt: Twitter tut dies alles, ohne dem User die Möglichkeit zu geben, Dritten den Zugriff auf die eigenen Daten zu verwehren. Vergleicht man das mit Facebook, dessen Datenschutzgebaren oft kritisiert und nicht selten als das Böse schlechthin dargestellt wird, wo aber User die Datenweitergabe an Dritte durch Facebook über entsprechende Privatsphäre Einstellungen in der Regel verhindern können, bleibt einem nur das Fazit: Facebooks Datenschutzgebaren ist durch die oft deaktivierten, gut versteckten, aber immerhin vorhandenen Privatsphäre Einstellungen, mit denen man die Datenweitergabe durch Facebook an Dritte verhindern kann - wie etwa bei der umgehenden Personalisierung - deutlich besser. Twitter ist spätestens jetzt viel gefährlicher.

Twitter erlaubt nun Drittanbietern nicht nur den Zugriff auf Daten der letzten 30 Tage, wie es bisher der Fall war, sondern auf alle Daten seit Januar 2010. Dieser erweiterte Zeitraum verschärft das Problem noch.

So gelten datenschutzrechtlliche Bedenken in gleichem Maße für alle Arten von sozialen Netzwerken:
Die Erhebung, die Speicherung und die Weitergabe personenbezogener Daten bedürfen nach § 4 BDSG immer einer Rechtsgrundlage oder einer Einwilligung nach § 4a BDSG, die nur dann wirksam erteilt werden kann, wenn sie auf einer freien Entscheidung des Nutzers beruht.
Rein formal betrachtet stimmt ein Facebook-Nutzer den Nutzungsbedingungen zwar zu und gibt damit seine Einwilligung in freier Entscheidung, ist sich aber oft der Gefahren und Risiken im Regelfall überhaupt nicht bewusst. Eine verbindliche datenschutzrechtliche Bewertung sozialer Netzwerke ist allerdings weder allgemein noch im Einzelfall erfolgt.