

"recht.extrajournal.net" gefunden am 30.05.2018 09:06 Uhr

WU Studie sieht die User als größte Datenschleudern

Datenschutz. 9 von 10 Apps geben Kontaktdaten von Familie und Freunden an Unternehmen weiter, so eine WU-Studie: Besonders bedenklich sei, wie die User damit umgehen.



Die Datenschutzgrundverordnung (DSGVO) ist seit Ende letzter Woche in Kraft und soll einen Meilenstein in puncto Datenschutz darstellen. Auch die Weitergabe von personenbezogenen Daten an Dritte wird darin geregelt. **Bernadette Kamleitner vom Institute for Marketing and Consumer Research der WU Wien** macht in ihrer aktuell erschienenen Studie deutlich, welche zentrale Rolle unsere Mitmenschen im Datenschutz spielen.

Die WU-Professorin zeige gemeinsam mit einem internationalen Forscherteam eine potentiell große Lücke im Datenschutz auf: App-Nutzer gestatten vielen Unternehmen Zugriff auf ihre gesamten Kontaktdaten am Handy – ohne Zustimmung der betroffenen Familienmitglieder, FreundInnen und Bekannten.

Die Untersuchung

Wie leicht Unternehmen in der Vergangenheit an eine Vielzahl an Daten gelangten und immer noch gelangen können, zeige die aktuelle Studie von Kamleitner gemeinsam mit Vincent W. Mitchell, Andrew Stephen und Ardi Kolah. Das internationale Team untersuchte, ob Konsumenten bereit sind die Daten ihrer Familie und Freunde zu schützen, wenn Dienste und Services darauf zugreifen wollen und diese nutzen wollen.

Die Ergebnisse seien ernüchternd: Via App gewährten rund 80 Prozent der 792 Untersuchungsteilnehmer den Unternehmen leichtfertig Zugriff auf sämtliche Files (inklusive Kontaktdaten) am Endgerät und gaben binnen Sekunden die explizite Zustimmung, dass sämtliche Daten, die auf ihrem Endgerät gespeichert waren, verwendet werden durften.

Die Crux: Dies passierte vorwiegend ohne dass es den Nutzern bewusst wurde. Im Rahmen der Studie wurde versucht, das Bewusstsein und die Aktivität der NutzerInnen in puncto Datenschutz zu messen und zu sehen, ob sich dieses ankurbeln lässt.

Hierfür wurden zwei Untersuchungsgruppen – eine Gruppe bestehend aus digital-versierten Business-Studierenden in London ebenso wie eine gemischte Untersuchungsgruppe aus der Europäischen Union sowie den USA – auf deren Verhalten im Datenweitergabeprozess analysiert.

Konkret, so die AutorInnen, braucht es drei Schritte, damit Konsumenten die Daten anderer schützen. 9 von 10 TeilnehmerInnen stolperten über mindestens einen dieser Schritte.

Schritt 1: Wenig Aufmerksamkeit trotz Information

Im ersten Schritt wurde untersucht, ob eine genaue Darstellung aller Berechtigungen seitens der NutzerInnen überhaupt korrekt wahrgenommen wird. „Die Ergebnisse geben massiv zu denken: 95 Prozent der Studierenden sowie 71 Prozent der Befragten der breiten Öffentlichkeit unterschätzten bereits Sekunden danach das Ausmaß an Berechtigungen, die sie gerade eben noch ausdrücklich, mit Rückfrage, erteilt haben“, so die Studienautorin Bernadette Kamleitner.

Schritt 2: Wenig Bewusstsein, wenig Einsicht

Im Schritt 2 wurden alle Teilnehmer explizit noch einmal an alle Berechtigungen erinnert. Dabei stellte sich heraus: Selbst wenn die Personen wussten, dass sie Zugriff auf die Kontaktdaten gegeben hatten, realisierten viele nicht, dass sie damit auch Daten freigegeben hatten, die anderen – Familie und Freunden – „gehören“.

„Viele Konsumenten sind sich ihrer Verantwortung in puncto Schutz von Daten anderer offenbar nicht bewusst. 42 Prozent der Studierenden und 49 Prozent der breiten Öffentlichkeit realisierten nicht, dass es auch andere betrifft, wenn man am Handy gespeicherte Daten über andere, insbesondere personenbezogenen Daten im Telefonbuch oder der Kontaktliste, freigibt“, erklärt Kamleitner.

Schritt 3: Nutzen vor Datenschutz

Im dritten Schritt wurden die Probanden explizit darauf hingewiesen, dass eine Zugriffsberechtigung auf das Telefonbuch und die Kontaktliste bedeutet, dass man Daten anderer weitergibt. Auch hier überraschten die Ergebnisse: 70 Prozent der Studierenden und 65 Prozent der breiten Öffentlichkeit zogen es vor, die Rechte ihrer persönlichen Kontakte zu ignorieren und die Handy-Applikationen weiter zu nutzen.

Die Implikationen

Insgesamt legen die Ergebnisse nahe, dass die DSGVO einen wichtigen Aspekt des Schutzes der Privatsphäre noch nicht ausreichend abdeckt, heißt es: „Menschen haben und geben nicht nur Zugriff auf ihre eigenen Daten, sondern auch auf Daten anderer. Je mehr Informationen wir selbst über andere sammeln, desto mehr sind unsere Mitmenschen auch eine potentielle Quelle von Datenverlust“, so Kamleitner.

Die DSGVO fokussiert primär auf den Datentransfer zwischen tatsächlichen KundInnen und Unternehmen. Wie die Rechtsprechung mit der Tatsache umgeht, dass Kunden auch leichtfertig Daten ihrer Mitmenschen weitergeben, bleibe abzuwarten – Firmen wie Endkunden könnten belangt werden.

Kamleitner: „Die Tatsache, dass wir mit unseren Mitmenschen verbunden sind und viel über diese wissen, ist aus sozialer Sicht sinnvoll. Wenn dieses Wissen aber auch auf unseren Geräten gespeichert ist, dann – so zeigen unsere Ergebnisse – kann es schnell passieren, dass wir dieses Wissen unvorsichtig und in großem Stil teilen. Es ist an der Zeit zu realisieren, dass die Privatsphäre des Einzelnen von vielen abhängt. Das Bewusstsein für die soziale Abhängigkeit der Privatsphäre muss dringend gestärkt und in Taten umgesetzt werden.“

Über die Autoren

Bernadette Kamleitner ist Professorin für Marketing an der WU und leitet dort das Institute for Marketing and Consumer Research.

Vincent Mitchell ist Professor für Marketing und Leiter des gleichnamigen Institutes an der Sydney Business School.

Andrew Stephen ist L'Oréal Professor of Marketing und Dekan für Forschung an der University of Oxford.

Ardi Kolah ist Direktor des GDPR Programms an der Henley Business School.

Link: WU Wien

Weitere Meldungen:

Neues zu TPA und Immos, KPMG und Cyber-Security

Drei Tage bis zur DSGVO: Post bringt Notfall-Kit

FMA nimmt Banken-IT stärker unter die Lupe

Neues von E&H, D.A.S., Hogan Lovells und Donau Uni