Service

Datenkrake: Viele Betreiber von Internetseiten platzieren auf Webprogrammen von Surfern Cookies für gezielte Werbung

In den Fängen der Datenkraken

Datenklau » Internetgiganten wie Apple, Google oder Facebook wissen mehr über Interessen und Vorlieben von Nutzern, als denen lieb ist. Wie sich Surfer vor Missbrauch schützen, erklärt IT-Experte Markus Morgenroth

66 Mrd. US-Dollar

setzte Internetgigant Google 2014 um. 90 Prozent davon stammen aus dem Geschäft mit platzierter Werbung.

VON **REGULA HEINZELMANN** UND **MICHAEL H. SCHULZ**

Jeder Klick hinterlässt Spuren im Internet. Und keiner hat die Auswertung dieser Spuren so optimiert wie Google. Dazu gehören auch personenbezogene Daten, die der Konzern oft gegen den Willen von Nutzern absaugt. Der Internetgigant umgeht schon mal die Standard-Datenschutzeinstellungen von Browsern, wie etwa Apples Safari. Als sich englische iPhone-Besitzer dagegen wehrten, spielte das mächtige Internetunternehmen den Vorfall überheblich herunter. Den Apple-Nutzern sei kein Schaden entstanden. Ohnehin könne Google mit Sitz in den USA gar nicht in England verklagt werden.

Das sah das englische Berufungsgericht anders. „Es geht um eine angeblich heimliche und verdeckte Verfolgung und Zusammentragung von Informationen von häufig sehr privater Art“, rügten die Richter. Google habe somit unzulässig in die Privatsphäre eingegriffen. Unabhängig davon, ob dadurch den Internetnutzern ein finanzieller Schaden entstanden sei, handle es sich um eine Verletzung des Rechts auf informationelle Selbstbestimmung.

Das Urteil bezieht sich zwar in erster Linie auf englische Verbraucher, die zwischen 2011 und 2012 über den Internetbrowser Safari auf Apple-PCs, iPhones und iPads surften, kann aber laut Rechtsexperten auch als Vorlage für mögliche Klagen von deutschen Safari-Surfern dienen.

Ausgespäht mit „Keksen“

Cookies ist die englische Bezeichnung für Kekse oder Plätzchen. Im übertragenen Sinn handelt es sich um Textformen, die auf der Software des Internetbrowsers eines Nutzers platziert werden. Diese Datenkekse knabbern sozusagen besuchte Websites an und übermitteln das Nutzungsverhalten der Surfer. Der Zweck der Aktion: Mit diesem Ausspähen lässt sich gezielt personalisierte Werbung auf besuchten Internetseiten platzieren – eben dies ist das Geschäftsmodell von Google, inzwischen ein höchst lukratives Milliardengeschäft.

Google ist kein Einzelfall. Ob Surfen am PC, Datenspeichern in der Cloud oder eine App auf dem Smartphone, die sensible personenbezogene Daten enthält: Viele Händler spionieren Kunden aus, indem sie private Daten gezielt auswerten und zu Geld machen. Manchem Internetsurfer wird auch sein nachlässiger Umgang mit den Daten zum Verhängnis.

Es ist zwar im Prinzip erlaubt, Personendaten für Marktforschung und Kundenprofile zu verwenden, einige sensible Daten gelten aber als schutzwürdig und unterliegen der Geheimhaltung (siehe Kasten unten). Dazu gehören: die gesellschaftliche Schicht, Rasse, Volkszugehörigkeit, sexuelle Vorlieben, Mitgliedschaft in Gewerkschaften, religiöse und politische Überzeugungen, geistige und körperliche Gesundheit und die finanzielle Situation. Diese besonders schutzwürdigen Daten werden aber missbraucht, wenn sie für die Vergabe eines Jobs oder einer Mietwohnung entscheidend waren.

Fatale Folgen kann für Selbstständige und Firmen auch ein falscher Eintrag in Bewertungsportalen haben. Zwar können sie vom Betreiber eines Internetportals verlangen, die Einträge zu löschen. Allerdings darf der Betreiber keine Auskünfte über den Urheber der falschen Behauptungen preisgeben. So steht es im Telemediengesetz. Betroffene können sich nur über eine Strafanzeige gegen die Verbreitung von ruf- oder geschäftsschädigenden Behauptungen wehren.

Doch wie können Internetnutzer, abgesehen von technisch aufwendigen Zusatzprogrammen, überhaupt vorbeugen? Und ist dieser Schutz vor Missbrauch der preisgegebenen Daten überhaupt ausreichend?

Einer, der es wissen muss, ist Markus Morgenroth. Der Informatiker und Autor des Buches „Sie kennen Dich! Sie haben Dich! Sie steuern Dich! Die wahre Macht der Datensammler“ war lange in den USA als Informatiker tätig. Morgenroth ist jetzt selbstständiger IT-Berater im Datenschutzbereich.

€URO AM SONNTAG: In Europa gibt es strenge Datenschutzvorschriften. Warum kommen trotzdem so ein massive Datenmissbrauch vor?

MARKUS MORGENROTH: Das Problem ist, dass die Einhaltung der Vorschriften kaum kontrolliert wird. Wird ein Verstoß gemeldet, sind häufig personalintensive Untersuchungen notwendig. Erst recht fehlt das Personal für flächendeckende Untersuchungen. Außerdem sind die Strafen derzeit leider meistens gering. Die Unternehmen kalkulieren oft, dass der Nutzen der Datenschutzverletzung höher ist als die zu erwartende Strafe. Man bräuchte Strafen, die den Unternehmen wehtun. Dies ist einer der Punkte, die in der neuen EU-Datenschutz-Grundverordnung vorgesehen sind.

IT-Berater Markus Morgenroth: „Jeder sollte wissen, wer Daten sammelt“

Können Sie einige dieser Punkte nennen?

Das wären Geldbußen bis zu 100 Millionen Euro oder bis zu fünf Prozent des weltweiten Jahresumsatzes.

Die EU-Verordnung würde nur in Europa gelten. Datenschutzprobleme sind aber ein internationales Phänomen. Wir könnte man dieses lösen?

Es ist richtig, dass es für effizienten Datenschutz nur globale Lösungen gibt. Internationale Bestrebungen bestehen, aber es ist schwierig, etwas durchzusetzen. Welche Auswirkungen hätten etwa Freihandelsabkommen wie TTIP, über das derzeit die EU und die USA verhandeln? Diesen stehe ich äußerst kritisch gegenüber. Denn Unternehmen würden offensichtlich mehr Rechte gegenüber den Konsumenten bekommen.

Von offizieller Seite ist also nicht viel zu erwarten. Wie können sich Privatpersonen dann vor Datenmissbrauch schützen?

Der beste Schutz ist, so wenige Daten wie möglich preiszugeben, was vor allem für private Daten und ganz besonders für Gesundheitsdaten und finanzielle Informationen gilt. Auch ist mehr Aufklärung nötig. Das sollte schon in den Schulen mit Informatik als Pflichtfach beginnen. Jeder sollte wissen, wer die eigenen Daten sammelt, was mit ihnen passiert und vor allem auch, wie man sich vor Missbrauch dieser Daten schützen kann.

Sie erwähnen in Ihrem Buch Produkte, die Konsumenten ausspionieren, beispielsweise Fernseher, die das Verhalten der Nutzer beobachten. Müssen diese Produkte klar gekennzeichnet werden? Wie kann man solche Funktionen überhaupt erkennen?

Beim Fernsehen sind das sehr moderne Modelle mit eingebauter Webcam. Auch normale Smart-TVs, also Geräte, die mit dem Internet verbunden sind, haben das Potenzial, das Fernsehverhalten der Nutzer auszuspähen. Aber es gibt viele andere Möglichkeiten, Personendaten auszuwerten, die ebenso gefährlich sind. So werden zum Beispiel in den sozialen Netzwerken die meisten Bilder automatisch analysiert. Dabei registriert man die Emotionen der Personen, indem man die Gesichtsausdrücke auswertet, es werden Logos von Produkten erkannt. Man versucht zu erfahren, was die Menschen tun, die auf einem Foto zu sehen sind. Mittels Gesichtserkennung werden auch zunehmend die einzelnen Personen auf den Bildern identifiziert. All das geschieht, weil man mit den gewonnenen Daten Geld verdienen möchte.

Wie ist es mit Smartphones?

Auch hier fallen Unmengen an sensiblen Daten an. Nicht nur die Telefondaten – wer spricht wann mit wem –, sondern auch die Bewegungsprofile können ausgewertet werden. Auch viele Apps saugen Daten ab. Das ist besonders deshalb problematisch, weil man als Kunde kaum noch einen Überblick hat, welchen Weg die Daten gehen und was mit ihnen geschieht. All das kann man nur mit technisch schwierigen Einstellungen und Zusatzprogrammen eindämmen. Ich empfehle, Apps, die sensible Daten, etwa zur Gesundheit, sammeln, nicht oder nur sehr eingeschränkt und vorsichtig zu benutzen.

KLEINGEDRUCKTES

Augen auf beim Surfen

Das Recht auf **informationelle Selbstbestimmung** ist ein Grundrecht. Das hat das Bundesverfassungsgericht im sogenannten Volkszählungsurteil von 1983 bestätigt (Az. 1 BvR 209 u. a.). Grundsätzlich kann also jeder für sich entscheiden, welche persönlichen Daten er preisgeben will oder nicht. Wer sicher im Netz surfen will, sollte so wenig wie möglich angeben. Beim **Online-Einkauf** sollte man die Nutzungsbedingungen und Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen Händlers lesen. Wichtig: Manche Datenverarbeitungsklauseln von Internetseitenbetreibern sind laut deutschen Gerichten unzureichend. Generell gilt für Onlinehändler: Daten, an deren Geheimhaltung eine Person ein besonderes schutzwürdiges Interesse hat, dürfen nicht Unbefugten bekannt gegeben werden. Hierzu zählen Angaben etwa zu ihrer rassischen und ethnischen Herkunft, politische Meinung und Gewerkschaftszugehörigkeit. Darüber hinaus haben Nutzer ein Recht zu erfahren, welche Daten Unternehmen über sie gespeichert haben.

Bild: iStockphoto (M.), w 8615 c/Droemer Knaur GmbH & Co. KG