Angela Meindl

Internet-Profiling

Umfang, Risiken und Schutzmaßnahmen am Beispiel von Google

Internet-Profiling nennt man den Vorgang, über Menschen, die sich im Internet bewegen, möglichst differenzierte Informationen zu sammeln und diese in einem möglichst genauen Persönlichkeitsprofil zusammenzuführen. Für diesen Zweck werden nicht nur die Daten gesammelt und gespeichert, die jemand, z. B. beim Ausfüllen von Formularen, selbst preisgibt. Es kann mithilfe diverser Techniken, die beim Besuch einer Webseite nicht zu bemerken sind, das Nutzungsverhalten während des Surfens in Erfahrung gebracht werden. Überspitzt könnte man sagen, alles, was man im Internet tut, wird mitgelesen.

Begründet wird dieses Verfahren in der Regel zum einen damit, besseren personenbezogenen Inhalt bieten zu können und die Usability zu verbessern. Zum anderen geht es darum, die Effektivität von Webseiten zu erhöhen und Werbekampagnen analysieren zu können.

In diesem Papier soll auf das in puncto Profiling technisch Machbare und das datenschutzrechtlich Erlaubte eingegangen werden. Es werden die gängige Praxis, die damit verbundenen Interessen und die Frage nach der Notwendigkeit thematisiert. Stellvertretend für viele andere wird dies am Beispiel von Google geschehen.

Wie werden Daten gesammelt?

Die wichtigsten Techniken, die zum Datensammeln eingesetzt werden, sind Zählpixel, Cookies und Logdateien.

Beim Zählpixel wird die Technik genutzt, mit der HTML-Bilder in eine Webseite eingebunden werden. Da das Bild nicht direkt in der HTML-Datei liegt, sondern dort nur ein Hinweis für den Browser steht, der ihm sagt, wo das Bild liegt, muss der Browser eine Verbindung zum Bilder-Server aufbauen, um das Bild zu laden. Da das Bild auf jedem Internetserver liegen kann, wird diese Vorgehensweise genutzt, um mit dem Zählpixel Daten zu sammeln. Dabei wird dem Browser mitgeteilt, dass er ein Bild laden soll. Es wird aber keine Verbindung zum Bilder-Server hergestellt, sondern zu einem Tracking-Server. Diesem Verbindungsaufbau können diverse Parameter mitgegeben werden, die dem Tracking-Server mitteilen, ob z. B. Skripte übertragen oder Cookies gesetzt werden sollen. Ein so gesetztes Cookie ist zwar ein Drittanbieter-Cookie, wird vom Browser aber nicht als solches betrachtet. So gesetzte Cookies enthalten in der Regel eindeutige Nutzer-IDs, die es ermöglichen, jemanden immer wiederzuerkennen und alle gesammelten Daten eindeutig zuordnen zu können.

Mit den Skripten können diverse Informationen über die Webseitennutzer und ihr Verhalten auf der Webseite eingesammelt und an den Tracking-Server gesendet werden, um sie dort im entsprechenden Profil zu speichern.

Die dritte Technik im Bunde ist die Auswertung der Logdateien. Ursprünglich zum Debuggen gedacht, werden in ihnen alle Aktivitäten von Server, Router oder Firewall gespeichert. Aber sie enthalten nicht nur Aktivitäten wie die aufzurufende Webseite, den Referrer oder die benutzte Suchmaschine inkl. Suchbegriff, sondern können auch diverse Informationen über das benutzte Computersystem enthalten. Dazu gehören die IP-Adresse, der Browsertyp und die Version, die eingestellte Sprache, die Bookmarks, installierte Plug-ins, die eingestellte Zeitzone, das Betriebssystem, die Bildschirmauflösung oder installierte Schriftarten.

Aus diesen Informationen lässt sich ein Browser-Fingerprint erstellen, der besonders dann dazu beitragen kann, jemanden wiederzuerkennen, wenn die Cookies und mit ihnen die Nutzer-ID gelöscht wurden. Nach einer Studie von Henning Tillmann [1] sind Browser-Fingerprints mit bis zu 92,57 % eindeutig.

Maus-, Geo- und Behavioural-Targeting

Beim Targeting geht es darum, möglichst viele Einzelheiten über das Nutzerverhalten im Internet in Erfahrung zu bringen und auswerten zu können. Dafür kommt die Möglichkeit, per Zählpixel Skripte einsetzen zu können, zum Einsatz.

Man unterscheidet hauptsächlich zwischen Maus-, Geo- und Behavioural-Targeting. Maus-Targeting wird eingesetzt, um das Leseverhalten auf der Webseite in Erfahrung zu bringen. Dabei wird die Position der Maus ausgewertet, weil man davon ausgeht, dass bei sehr vielen Menschen die Maus genau dort ist, wo gelesen wird. Aber auch wenn dies nicht bei allen Menschen der Fall ist, kann immer noch das Navigationsverhalten ermittelt werden.

Angela Meindl

Angela Meindl, B. Sc., ist Medien-Informatikerin aus Bremen, *a.meindl@artinfakt.de*

Das Geo-Targeting kommt zum Einsatz, um den Standort des Nutzers definieren zu können. Dabei werden die IP-Adresse und die Browser-Einstellungen wie Sprache und Zeitzone ausgewertet. Bemerken kann man das Ergebnis von Geo-Targeting, wenn man Google-Maps oder ähnliche Seiten aufruft. Es wird die Region angezeigt, in der der Rechner des Nutzers steht.

Die größte Rolle spielt jedoch das *Behavioral-Targeting*. Zum Einsatz kommt es in zwei verschiedenen Varianten. Entweder ausschließlich innerhalb einer Webseite oder webseitenübergreifend. Technisch wird Behavioral-Targeting, genauso wie Maus-Targeting, mit einer Kombination aus Zählpixel und Cookie umgesetzt.

Daten, die in Cookies gespeichert werden, können gelöscht werden. Daten, die mit Skripten über das Zählpixel erhoben werden, landen, ohne dass der Nutzer überhaupt etwas von deren Erhebung ahnt, direkt in der Datenbank des Tracking-Servers.

Wie und wo sammelt Google unsere Daten?

Google sammelt mit seinen Diensten wie der Suchfunktion, Google+, Google Analytics, Picasa, YouTube usw. Unmengen von Daten, weltweit und in 156 Sprachen, die beim Nutzen der Dienste entweder freiwillig eingegeben werden oder einfach anfallen. Dabei nutzt Google alle drei zuvor beschriebenen Techniken. Es werden Cookies mit eindeutiger ID auf dem Clientrechner gesetzt, die Logfiles ausgewertet und Scripting z. B. mit Zählpixeln betrieben [2]. Auch wenn sich das lange niemand klar gemacht hat, macht Google kein Geheimnis daraus. Wenn man vor allem die Google-Hilfe-Seiten und die Datenschutzrichtlinien der einzelnen Dienste aufmerksam liest und erkennen kann, wo Google seine Sammelwut schönredet, kann man dort sehr wohl ziemlich viel darüber erfahren, wann, wie und wo Daten gespeichert werden.

Wenn man vom Anfallen von Daten spricht, sind die Daten gemeint, die durch Protokolle entstehen und in den Logfiles gespeichert werden. Aus den Logfiles kann Google folgende Informationen über jede Nutzerin entnehmen:

IP-Adresse, Referrer, benutzte Suchmaschine, Suchbegriffe (d. h. alle Interessen oder Probleme, nach denen man über die Google-Suche recherchiert hat), Zeitstempel, benutzter Browser, Betriebssystem, Bildschirmauflösung, installierte Browser-Plug-ins, Lesezeichen, eingestellte Sprache, installierte Schriftarten, eingestellte Zeitzone.

Es ist wohl nur wenigen Menschen bewusst, wie viel sie über sich preisgeben, wenn sie einfach ihre Suchbegriffe bei Google eingeben und anschließend die Suchergebnisse durchstöbern und dass diese Informationen alle und für lange Zeit gespeichert und einem Profil zugeordnet werden.

Googles Wissen über uns

Wie umfassend schon die Informationen sind, die Google und andere Suchmaschinenbetreiber nur durch die Suchbegriffe über uns erhalten, zeigt das Beispiel von Thelma Arnolds. Der Fall hat 2006 in den USA für Schlagzeilen gesorgt. Damals hatte AOL eine Datei mit ihren Logfiles der AOL-Suche ins Internet gestellt. Sie wollten Informatikern diese Datei zur Verfügung stellen, damit sie verfeinerte Suchalgorithmen damit entwickeln könnten. Es wurde schnell klar, wie brisant die Daten sind, und AOL hat die Datei schnell wieder zurückgezogen. Aber es war schon zu spät. Viele Informatiker hatten die Datei schon heruntergeladen und mit der Analyse begonnen.

Auch die *New York Times* hatte einen Informatiker damit beauftragt, die Daten zu analysieren. Sie wollten sehen, ob sie eine Person nur über ihre Suchbegriffe identifizieren könnten. Sie werteten alle Suchanfragen der Nutzerin mit der Benutzerinnennummer 4417749 aus. Sie suchte unter anderem nach „taube Finger, alleinstehende Männer ab 60, Hund uriniert auf alles, Landschaftsgärtner in Lilburn GA (GA = Georgia – *Anmerkung der Autorin*), den Namen Arnolds in Kombination mit verschiedenen Vornamen".

Allein durch diese Informationen ist es der New York Times gelungen, die betreffende Person zu finden. Es handelte sich um besagte Thelma Arnolds. Eines schönen Nachmittags standen die Reporter der New York Times bei Thelma Arnolds in der Tür und lasen ihr ihre Suchbegriffe vor. Man kann sich vorstellen, wie überrascht Ms. Arnolds war.

Es werden aber nicht nur mit der Suche Daten über uns gesammelt. Auch mit allen anderen Diensten sammelt Google Daten über uns. Wobei man für alle Dienste, mit wenigen Ausnahmen, ein Google-Konto braucht, für das man persönliche Daten wie Name, Adresse, Geburtsdatum usw. angeben muss. Mit diesen Angaben können dann alle von Google gesammelten Daten eindeutig einer Person zugeordnet werden. Was Google von jemandem weiß, hängt natürlich davon ab, welche Dienste man nutzt oder auf wie vielen Webseiten man war, die von Google Analytics etc. getrackt werden. Aber zu dem, was Google über uns wissen kann, gehören die folgenden Informationen: IP-Adresse, Referrer, benutzte Suchmaschine, Suchbegriffe (d. h. alle Interessen oder Probleme, nach denen man über die Google-Suche recherchiert hat), Zeitstempel, benutzter Browser, Betriebssystem, Bildschirmauflösung, installierte Browser-Plug-ins, Lesezeichen, eingestellte Sprache, installierte Schriftarten, eingestellte Zeitzone, Name, E-Mail-Adresse, Geburtsdatum, Geschlecht, Mobiltelefon-Nr., Standort, welche Digitalkamera man benutzt, wo die Bilder aufgenommen wurden, wie wir aussehen, über welche Themen man sich mit wem in seinen Mails austauscht, mit wem man befreundet ist, mit wem man welche Interessen teilt, Vorlieben, Hobbys, Bankkonto-Daten etc.

Man kann sicher sein, dass, egal wie man mit Google in Berührung gekommen ist, ein ziemlich umfassendes Persönlichkeitsbild dabei herauskommt.

Sind wir durch Datensammlungen über uns gefährdet?

Das Beispiel von Thelma Arnolds mag für den einen oder anderen vielleicht noch nicht wirklich nach Gefahr aussehen, weil ja weder Unglück noch Schaden daraus entstanden sind. Aber es weckt schon ein wenig eine Vorstellung davon, dass so viel Wissen über eine Person Begehrlichkeiten wecken kann, die nicht zwangsläufig freundlicher Natur sein müssen.

Wenig erfreulich fanden es sicher auch WhatsApp-Nutzer, als Facebook WhatsApp gekauft hat und damit auch alle Daten, die WhatsApp über ihre Nutzerinnen gesammelt hatte, in den Besitz von Facebook übergingen. Das zeigt, dass alle Daten, die über uns gesammelt werden, in das Eigentum der sammelnden Firma übergehen und Teil ihres Wertes sind. Sie können verkauft werden und gehen bei Insolvenz in die Konkursmasse ein.

Beide Beispiele zeigen, dass wir keinerlei Kontrolle mehr darüber haben, wer was über uns erfährt oder zu welchem Zweck unsere Daten verwendet werden. Noch viel weniger können wir wissen, welche Konsequenzen der Umgang mit unseren Daten für uns oder andere haben kann.

Gefährdungen können daraus sowohl auf politischer und wirtschaftlicher als auch auf privater Ebene entstehen. Betrachtet man die politische Ebene, denken die meisten Leute vermutlich an Vorratsdatenspeicherung. Nach deutschem Recht darf nur durch richterlichen Beschluss gezielt auf einzelne Datensätze zugegriffen werden. Jetzt könnte man denken, dass man sich sicher fühlen kann, wenn man nichts zu verbergen hat. Aber abgesehen davon, dass man nie sicher sein kann, dass man nichts zu verbergen hat, gilt deutsches Recht nur für einen kleinen Bruchteil des Internets. Nämlich nur für Webseiten, die auf deutschen Servern liegen. Der Großteil der Webseiten, die auch in Deutschland viel genutzt werden, liegt aber nicht auf deutschen, sondern auf amerikanischen Servern. Dazu gehören Google, Facebook, eBay und Skype, um nur die Spitze des Eisberges zu nennen. Liegen die Seiten auf amerikanischen Servern, gilt amerikanisches Recht. Die amerikanische Regierung hat schon mehr als einmal große Internetunternehmen dazu verpflichtet, große Mengen an Daten zum Zweck der Verbrechensbekämpfung den Behörden zu überlassen.

Aber ganz unabhängig davon, wie die Gesetze formuliert sind, gibt es keine Garantie, dass sich Regierungen an ihre eigenen Gesetze halten, wie der aktuelle NSA-Skandal zeigt. Und Gesetze sind nicht in Stein gemeißelt. Sie können jederzeit geändert werden.

Wenn wir nur die möglichen Folgen für Privatpersonen betrachten, finden wir schon ein breites Spektrum an Gefährdungen. Denn überall, wo wir digitale Spuren hinterlassen, können andere diese nutzen.

Da wäre zunächst das Image-Problem. Denn alles, was die Google-Suche oder soziale Netzwerke über eine Person finden, kann jeder lesen. Was liegt also näher, als sich vor einer Begegnung mit einer Person, die man noch nicht kennt, im Internet zu informieren. Das heißt aber, dass die Informationen, die über uns im Internet zu finden sind, das Bild, das andere von uns haben, prägen. Im privaten Bereich mag das noch nicht so schwerwiegend sein. Schwieriger wird es da schon, wenn zukünftige Arbeitgeber sich im Internet über Bewerberinnen informieren. Zu den möglichen K.o.-Kriterien gehören nicht nur Partybilder. Auch das Betreiben von Leistungssport mit regelmäßigen Wettkämpfen am Wochenende, politisches oder soziales Engagement usw. können Negativpunkte bringen, weil das ein Hinweis auf mangelnde Bereitschaft sein kann, am Wochenende Überstunden zu machen.

Auch Banken und Versicherungen bedienen sich der Möglichkeiten des Internets, wenn es um den Leumund von jemandem geht, der einen Kredit haben möchte oder eine Versicherung abschließen möchte. Die Benachteiligungen, die entstehen können, sind also nicht unerheblich.

Ein weiteres Problem besteht darin, dass diese Informationen auch für Mobber, Stalker und Kriminelle viele Anhaltspunkte bieten, wenn es darum geht, jemandem zu schaden. Es können ganze Identitäten gestohlen werden.

Ist Profiling wirklich nötig?

Diese Frage muss man unter verschiedenen Aspekten beleuchten. So ist es natürlich ein Unterschied, ob jemand seine Daten selbst zur Verfügung stellt oder ob sie ohne sein Wissen erhoben und gespeichert werden.

Selbst stellt man seine Daten beispielsweise bei einem Einkauf in einem Online-Shop zu Verfügung. Ohne Informationen wie Name, Adresse, E-Mail-Adresse, Geburtsdatum, Inhalt des Warenkorbes und gewünschte Zahlungsweise ließe sich eine Online-Bestellung gar nicht abwickeln. In der Regel speichern Online-Shops zwar auch die IP-Adresse des Kunden, das ist aber unbedenklich, solange kein weiteres Tracking betrieben wird.

Ganz anders sieht es mit den Daten aus, die ohne unser Wissen erhoben und gespeichert werden. Oft wird dieses Vorgehen mit der Verbesserung der angebotenen Dienste begründet. Des Weiteren geht es um Werbeeinblendungen, die auf die einzelne Person zugeschnitten sind. Natürlich sind Informationen darüber, mit welcher technischen Ausstattung jemand auf die Webseite geht, für die Seitenbetreiber interessant. Genauso wie Informationen über die Aufenthaltsdauer auf einzelnen Seiten und die Uhrzeit des Besuches.

Wird eine Seite schnell wieder verlassen, ist das ein Hinweis auf schlechten Inhalt oder technische Probleme. Zu diesem Zweck werden oft Analysetools wie Google Analytics eingesetzt. Google Analytics legt aber eben auch sehr differenzierte Profile von jedem einzelnen Nutzer an, bei dem die Nutzer nicht selten über viele verschiedene Webseiten geradezu verfolgt werden, um wirklich jede digitale Lebensäußerung abspeichern zu können. Bei Datensammlungen in diesem Umfang geht es nicht mehr darum, Dienste zu verbessern.

Der zweite Grund für das Sammeln von Daten sind Werbeeinblendungen. Auch hier werden über Partnerprogramme sehr viele Daten erhoben, um die Werbekampagnen auszuwerten. Das wohl bekannteste Programm ist Google AdWords, dessen Werbeeinblendungen in den Suchergebnisseiten von Google eingeblendet werden.

Um eine Werbekampagne abrechnen zu können, braucht man aber lediglich Informationen darüber, wie oft die Werbebanner angeklickt wurden und wie oft es tatsächlich zum Verkauf gekommen ist. Sowohl bei Google Analytics als auch bei AdWords sind die erhobenen Daten nicht im Besitz der Seitenbetreiber, sondern sie sind im Besitz von Google. Die Seitenbetreiber erhalten lediglich eine Auswertung zur Verfügung gestellt.

Dass Seitenbetreiber ihre Webseite für ihre Nutzer optimieren möchten, ist legitim. Dafür sind aber nur Informationen darüber notwendig, mit welcher technischen Ausstattung wie viele Nutzer wie lange auf den einzelnen Seiten gewesen sind. Man muss nicht wissen, wer diese Personen sind oder was sie sonst noch so im Internet machen. Und man muss schon gar nicht die Daten an Dritte weitergeben, wie es bei den Google-Tools der Fall ist.

In einem Test habe ich geprüft, ob es möglich ist, diese grundlegenden Daten personenunabhängig zu bekommen, ohne sie an Dritte weitergeben zu müssen. Zu diesem Zweck habe ich nach Open-Source-Tools gesucht, die man im eigenen Webspace installieren kann. Fündig geworden bin ich bei Piwik [3] als Alternative zu Google Analytics und den AdServer Revive [4] als Alternative zu Google AdWords. Beide Programme habe ich auf einem lokalen Webserver ohne Internetzugang installiert, um zu testen, ob sie auch nicht heimlich die Daten an den Softwarehersteller übertragen.

Das Ergebnis war überzeugend. Beide Programme haben in Anzahl und Menge zusammengefasste Ergebnisse geliefert, ohne auf einzelne Besucher einzugehen. Beide Programme haben gut funktioniert, ohne eine Verbindung zum Hersteller aufbauen zu können. Daraus kann man den Schluss ziehen, dass Webseitenbetreiber gut auf die differenzierten Datensammlungen verzichten können und trotzdem in der Lage sind, ihre Webseiten zu optimieren und Werbekampagnen korrekt abzurechnen.

Wenn man bedenkt, welche Risiken, von denen hier ja nur eine kleine Spitze des Eisberges beschrieben wurde, Nutzer durch das Profiling tragen müssen, ist Profiling nicht akzeptabel.

Profiling und Datenschutz?

Profiling aus der Sicht des Datenschutzes ist ein durchaus komplexes Thema. Da das Internet international ist, gilt es als erstes festzustellen, welches Recht eigentlich gilt. Obwohl im Internet grundsätzlich das Recht des Landes gilt, in dem die Server stehen, auf denen die Webseiten liegen, möchte ich einen Blick auf deutsches (bzw. EU-)Recht, amerikanisches Recht und die Datenschutzrichtlinien von Google werfen.

Das deutsche Datenschutzrecht gilt als das strengste der Welt. Genau genommen besteht es aber aus einer Vielzahl von Gesetzen und Regelungen. Die wichtigsten sind wohl das Telemediengesetz, das Grundrecht auf informationelle Selbstbestimmung und das Gesetz zur Vorratsdatenspeicherung.

Das Telemediengesetz besagt, dass personenbezogene Daten nur genutzt werden dürfen, wenn die betroffene Person vor dem Nutzungsvorgang über Art, Umfang und Zweck der Erhebung und Verwendung in verständlicher Form unterrichtet wurde, auch wenn die Daten außerhalb der EU verarbeitet werden. Die Nutzerin muss ihre Einwilligung bewusst und eindeutig erteilt haben.

Das Grundrecht auf informationelle Selbstbestimmung erweitert das Ganze noch, indem es besagt, dass jede Bundesbürgerin das Recht hat, selbst zu bestimmen, wem sie Informationen über sich preisgibt und wem nicht. Eingeschränkt werden diese beiden Rechte allerdings durch die Vorratsdatenspeicherung, die alle Medienanbieter dazu verpflichtet, alle Daten, die über ihre Infrastruktur laufen, für einen vorgegebenen Zeitraum zu speichern.

Das europäische Datenschutzrecht hat eher die Funktion, für alle Mitgliedstaaten einen gemeinsamen Mindeststandard zu schaffen.

Ganz anders sieht es da im amerikanischen Datenschutz aus. In Amerika setzt man auf Selbstverpflichtung. Das heißt im ersten Schritt, dass man machen kann, was man will. Es muss nur korrekt und zugänglich beschrieben werden, wie mit den erhobenen Daten umgegangen wird. Sollten sich falsche Angaben herausstellen, gibt es eine Verwarnung und die Auflage, ein Pflichtenheft zum Umgang mit den Daten zu entwickeln, an das man dann auch gebunden ist. Erst nach einem Verstoß gegen das selbst entwickelte Pflichtenheft kann die Justiz tätig werden. Sollte eine Firma bei einem solchen Verstoß ertappt werden, kommt es meistens nur zu einer Geldstrafe.

Sieht man sich nun die Datenschutzerklärung von Google an, so weist Google eindeutig darauf hin, dass sie alle Daten sammeln, die sie bei der Nutzung ihrer Dienste von ihren Nutzerinnen bekommen können. Sie verharmlosen zwar, indem sie immer davon reden, dass die Daten möglicherweise erhoben werden. Es wird darauf hingewiesen, dass Browser-Fingerprint-Daten erhoben werden und, wenn vorhanden, mit dem Google-Konto verknüpft werden. Es wird gesagt, dass Cookies und Zählpixel zum Einsatz kommen. Es wird darauf hingewiesen, dass die Server, auf denen die Daten gespeichert werden, überall auf der Welt stehen können.

Google gesteht seinen Nutzerinnen zwar das Recht auf Änderung fehlerhafter personenbezogener Daten zu, schränkt die Umsetzung aber ein. Es darf nicht zu aufwändig werden und nicht zu offensiv eingefordert werden. Und Daten in den Google-Sicherungssystemen werden nie gelöscht. Google verschweigt auch nicht, dass personenbezogene Daten an für Google vertrauenswürdige Dritte zwecks Verarbeitung weitergegeben werden.

Vergleichen lassen sich der deutsche und der amerikanische Datenschutz kaum. Dafür sind die Herangehensweisen zu unterschiedlich. Google hält sich an das amerikanische Recht, auch wenn sie schon einmal zur bisher höchsten verhängten Geldstrafe von 22,5 Millionen Dollar verurteilt wurden [5], weil sie falsche Angaben zu Tracking-Cookies im Safari-Browser gemacht hatten.

Die Art und Weise, wie Google Daten sammelt, ist mit dem deutschen Datenschutz schon schlechter zu vereinbaren. Das Problem mit der geforderten Zustimmung der Nutzer löst Google in einem Spagat. Wie viele andere große Internetfirmen sagt Google in seiner Datenschutzerklärung, dass eine Nutzung der Dienste gleichbedeutend mit einer Zustimmung ist.

Resümee

Die Art und Weise, wie vom Nutzer unbemerkt Daten über ihn erhoben und gespeichert werden, ist nicht akzeptabel, mit welcher Begründung auch immer sie gerechtfertigt wird. Ohne Notwendigkeit muss jeder, der an den Optionen der Informations-

technik teilhaben will, auf seine Privatsphäre verzichten, und er trägt ein nicht zu unterschätzendes Gefährdungsrisiko, während diejenigen, die für diesen Zustand verantwortlich sind, Unmengen Geld mit unserer Privatsphäre verdienen.

Um dem Gedanken der Selbstbestimmung und der geforderten Zustimmung Rechnung zu tragen, sollte es für das Tracking und Profiling eine Double-Opt-in-Lösung geben. Ähnlich wie es bei Newslettern ja schon Gesetz ist. Webseiten, die getrackt werden, sollten ein vorgeschaltetes Pop-up öffnen, in dem über Art und Zweck der Datenerhebung informiert wird. Dieses natürlich noch nicht getrackte Pop-up sollte zwei Buttons enthalten. Einer, mit dem man zustimmt, und einer, mit dem man das Tracking ablehnen kann. Lehnt man das Tracking ab, müsste eine ungetrackte Version der Website geöffnet werden. Zusätzlich sollte in dem Pop-up gleich ein Link vorhanden sein, der auf eine Seite führt, auf der sich jeder anzeigen lassen kann, was über ihn gespeichert ist. Wo er die Möglichkeit hat, Korrekturen bei fehlerhaften Angaben vorzunehmen, und wo er auch das Löschen aller gespeicherter Daten inklusive derer, die an Dritte weitergegeben wurden, beauftragen kann.

Auch sollte über ein internationales Datenschutzrecht für das Internet nachgedacht werden, an das sich alle Internetseitenanbieter verbindlich halten müssten. Um dieses Recht durchsetzen zu können, wäre natürlich eine entsprechend umfangreiche Kontrollinstanz und ein wirkungsvoller Maßnahmenkatalog für Verstöße notwendig.

Referenzen

[1] Tillman, Henning: http://bfp.henning-tillmann.de

[2] Google: Google-Nutzungsbedingungen. https://www.google.com/intl/de/policies/terms/index.html

[3] Piwik: Liberating Analytics. http://piwik.org/ – Version 16.6.2014

[4] Revive Software and Services: Introducing Revive Adserver. http://www.revive-adserver.com/

[5] SPIEGEL ONLINE: Datenschutz-Verstoß: Google zahlt Rekordbußgeld. 9.8.2012. http://www.spiegel.de/netzwelt/netzpolitik/ftc-google-muss-wegen-safari-verstoss-22-5-millionen-dollar-zahlen-a-849210.html

Carsten Seeger

Android? Aber sicher!?

Die Pleiten-, Pech- und Pannenserien unserer mobilen Welt

Unser Handy ist mittlerweile ein Standard-Accessoire, so wie Schlüssel und Portemonnaie. Es ist nutzbringend, einfach zu bedienen, und man ist immer erreichbar. Früher im Wesentlichen zum Telefonieren und SMS-Schreiben gebraucht, ist es heute ein multimediales Erfolgskonzept. Facebook, Twitter, YouTube, und das alles auch noch drahtlos mit Breitband-Internet. Doch welchen Preis zahlen Nutzerinnen und Nutzer für diesen Komfort?

Google gilt als einer der Monopolisten der modernen Internetgesellschaft, unter anderem durch sein mobiles Betriebssystem Android. Mit durchschnittlich mehr als 70 % aller verwendeten mobilen Systeme ist es das weitverbreitetste Betriebssystem für Handys und Tablets.[1]

Wie sicher ist aber unser gelie
Google hat sich ja schließlich
Während anfangs lediglich einz
kraften waren[2], wird es heute sel
schwieriger zu überprüfen, ob ihre Apps auch wirklich das tun, was sie sollen.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Überprüfen der Berechtigungen von Apps

Was eine App darf und was nicht, wird über deren Berechtigungen abgebildet. Dass man vor der Installation schauen sollte, welche Berechtigungen verwendet werden, ist keine Neuheit und wurde schon öfter diskutiert[3]. Denn es kommt häufiger vor, als man denkt, dass Apps gerne von Datenkraken verwendet werden.

Mit Einführung der neuen Berechtigungsgruppen im letzten Jahr wurde der Aufschrei wieder einmal größer und das zu Recht[4]. Denn Googles neues Gruppenkonzept ist zwar einfacher geworden, dafür aber auch unübersichtlicher. Es wurden 13 neue Gruppen eingeführt[5]. Die zunächst wichtigste Änderung beschreibt Google aber wie folgt: „*These days, apps typically access the Internet, so network communication permissions including the full Internet access permission have been moved out of the primary permissions screen.*" Internet-Zugriff wird also künftig jeder App gewährt, denn es ist ja jetzt Standard und der Benutzer muss sich nicht darum kümmern.

oid-User? Jede App, egal ob nun
erhält Zugang zum Internet und
llation einen Hinweis dafür gibt.
Für Social-Media-Apps wie Facebook, Twitter etc. oder Chat-Apps wie das weitverbreitete WhatsApp kommt der Nutzer ja durchaus noch selbst dahinter, dass Internet-Zugang ein notwendiges Übel ist. Was ist aber mit unserer Taschenlampen-, Batterie- oder Wecker-App? Dem Nutzer wird die Information für diese Apps nur noch über Umwege angezeigt: Dies geht nur noch über die Berechtigungsansicht der App unter den Einstellungen des Systems.

Die nächste Pleite des neuen Konzeptes folgt auf dem Fuße, denn bereits installierte Apps bekommen über die automatische Updatefunktion auch neue Berechtigungen ohne die Erlaubnis des Nutzers. Sofern also die automatische Updatefunktion aktiviert ist, darf jede App, die bereits auf dem System läuft, mit dem Update ihre Berechtigungen innerhalb der vorhandenen Berechtigungsgruppen beliebig erweitern. Das erschwert dem Benutzer ein feingranulares Steuern der Berechtigungen. Besser