verbraucherzentrale Bundesverband

04. Oktober 2011

Hintergrundpapier

AUF DIE VOREINSTELLUNG KOMMT ES AN

MEHR DATENSCHUTZ – WENIGER STRESS

Verbraucherzentrale Bundesverband e.V. – vzbv
Markgrafenstr. 66
10969 Berlin
www.vzbv.de

Kontakt
Florian Glatzner
Referent Datenschutz und Netzpolitik
datenschutzkampagne@vzbv.de

Einleitung

Viele kennen das Problem: Man hat sich neu bei einem sozialen Netzwerk angemeldet oder ein neues Smartphone gekauft und möchte eigentlich direkt los legen. Doch es gibt so viel einzustellen und zu personalisieren. Und dann sind da noch diese lästigen Datenschutzeinstellungen, um die man sich im Moment am liebsten gar nicht kümmern möchte. Aber Datenschutz ist wichtig. Also quält man sich durch die langen Menüs, von denen man die Hälfte nicht versteht.

Technische Systeme werden immer komplexer, die mit ihnen verbundenen Datenverarbeitungen immer schwerer zu überblicken. Verbraucher, die die neuen Produkte und Dienstleistungen nutzen, aber gleichzeitig die Kontrolle über ihre Daten behalten wollen, stehen vor einem Problem. Sie müssten Fachmann für die Einstellungsmöglichkeiten der verschiedenen sozialen Netzwerke oder die Tracking-Technologien der Internetwerbewirtschaft werden. Und sie müssen sich stets über neue rechtliche und technische Entwicklungen und Funktionen auf dem Laufenden halten.

Vielen Menschen macht das Spaß, andere haben nicht die Fähigkeiten oder die (zeitlichen) Ressourcen, sich intensiv mit diesen Fragen auseinander zu setzen. Sie wollen die neuen Technologien nutzen, die viele Möglichkeiten bieten und an ihren Vorzügen Teil haben. Sie wollen es jedoch entspannt tun, ohne die Kontrolle über ihre Daten zu verlieren oder erst langwierig nach den richtigen Einstellungen in Sozialen Netzwerken, Browsern oder Smartphones suchen zu müssen.

Eine Lösungsmöglichkeit für dieses Problem bietet das Prinzip **„Privacy-by-Default“**. Demnach müssen alle Produkte und Dienstleistungen bei ihrer Auslieferung oder ihrer ersten Inanspruchnahme datenschutzfreundlich voreingestellt sein. Standardmäßig dürfen nur so viele Daten erfasst, verarbeitet und weiter gegeben werden, wie für die Bereitstellung des Dienstes unbedingt erforderlich ist.

Es handelt sich bei diesem Prinzip nicht um eine Bevormundung der Nutzer, sondern schafft erst echte Wahlfreiheit. Eine bewusste Wahl kann nur treffen, wer über die nötigen Informationen verfügt. Nicht umsonst „fängt jeder mal klein an“, nicht umsonst lernen wir erst zu krabbeln und dann zu laufen. Es ist ein Grundprinzip des Lernens nicht direkt mit der Fülle aller Informationen und Möglichkeiten überschüttet zu werden, sondern sich mit den Grundlagen vertraut zu machen und sein Wissen und seine Fähigkeiten langsam zu erweitern.

Durch das Prinzip Privacy-by-Default werden nicht nur unerfahrene Anwender geschützt. Auch erfahrene Verbraucher können so neue Produkte und Dienste entspannter nutzen und müssen nicht immer die Sorge im Hinterkopf haben, dass sie eine Entwicklung oder ein neues Feature verpassen und plötzlich Daten gegen ihren Willen verwendet und verbreitet werden. Des Weiteren beinhaltet das Prinzip die automatisierte Löschung von nicht mehr verwendeten User-Accounts. Dadurch hat Privacy-by-Default auch im Hinblick auf die Datensicherheit viele Vorteile, da keine Daten gestohlen werden können, die nicht erfasst oder bereits gelöscht wurden.

Nur die Konzerne, deren Geschäftsmodelle auf der intransparenten Verwendung von Nutzerdaten basieren, laufen Sturm gegen diese Regelung. Sie profitieren davon, dass

viele Nutzer die Möglichkeiten der modernen Datenverarbeitung und ihre Risiken nicht überblicken können und die Voreinstellungen daher nie ändern.

Eine erste Gelegenheit, verbraucherfreundliche Voreinstellungen gesetzlich zu verankern, bietet die laufende Novelle des Telemediengesetzes. Da dieses jedoch nur Telemediendienste (wie Soziale Netzwerke) regelt, sollte das Prinzip „Privacy-by-Default“ auch im Bundesdatenschutzgesetz geregelt werden.

Privacy-by-Default muss als Grundprinzip des Datenschutzes gesetzlich verankert werden. Was dies im Einzelnen heißt, wird im Folgenden anhand von vier Beispielen erläutert.

Beispiel 1: Soziale Netzwerke / Facebook

Nahezu alle Funktionen und Dienste, die Facebook anbietet, sind standardmäßig aktiviert. Für den Nutzer ist es sehr mühsam, sich durch die vielen verschiedenen Privatsphäreneinstellungen zu arbeiten, um bestimmte Dienste und Funktionen zu deaktivieren. Auf diese Weise wird Facebooks gigantische Datensammlung immer größer. Sie reicht von persönlichen Interessen über Standortdaten bis hin zu biometrischen Daten. Facebook trägt die von den Nutzern eingestellten Daten und solche, die aus der Nutzung der verschiedenen Dienste und Anwendungen stammen, zusammen. Auf dieser Grundlage werden umfassende Profile der einzelnen Nutzer erstellt, um zielgerichtete Werbung zu schalten. Worum geht es im Einzelnen?

1. Viele Informationen, wie die Freundesliste, Statusmitteilungen, Fotos, Beiträge, Biografie, Familie und Beziehungen, sind **standardmäßig auf „alle“ voreingestellt**. Das bedeutet, dass diese Informationen für alle Internetnutzer, also auch außerhalb von Facebook sichtbar sind und genutzt werden können. Nicht zu vergessen: Der Name und das Profilbild gelten stets als öffentliche Informationen und können gar nicht anders eingestellt werden.

2. Nicht nur Facebook kann auf die Nutzerdaten zugreift und diese verwenden, sondern auch Dritte, die auf Facebook Anwendungen, wie Spiele und Umfragen zur Verfügung stellen. Genau das ist vielen Nutzern überhaupt nicht bewusst. Die Anwendungen haben immer Zugriff auf die „öffentlichen“ Daten. Dazu gehören der Name, das Profilbild, das Geschlecht, die Verbindungen und die Nutzerkennnummer. Darüber hinaus **können die Drittanbieter auf alle Daten zugreifen**, die für „alle“ eingestellt sind. Besonders problematisch ist, dass Anwendungen auch stets auf die Freundeslisten zugreifen können und sich häufig das Recht einräumen, auch auf die Informationen von Freunden zugreifen zu dürfen. So gibt der Nutzer Daten über seine Freunde mit heraus, ohne dass diese dem zustimmen. Selbst wenn ein Nutzer keine eigenen Anwendungen verwendet, werden Daten an Dritte weitergeben, sobald er mit einem aktiven App-Nutzer befreundet ist.

3. Mit dem **„Gefällt-mir-Button“** kann der Nutzer nicht nur auf Facebook selbst, sondern auch **auf vielen Webseiten außerhalb des Netzwerkes** seine Vorlieben und Geschmäcker zum Ausdruck bringen. Außerdem wird angezeigt, welchen Freunden das auch noch gefällt. Datenschutzrechtlich ist die Einbindung des Buttons in Webseiten außerhalb von Facebook höchst bedenklich. Allein durch das Aufrufen einer Webseite, auf der der Gefällt-mir-Button eingebunden ist, erhält Facebook standardmäßig Angaben zu Datum, Uhrzeit, Webseite, Browser, Betriebssystem und IP-Adresse. Anhand dieser Daten besteht die Möglichkeit, dass Facebook die Daten zusammenführt, um Nutzerprofile zu erstellen. Ist der Nutzer bei einem Webseitenbesuch bei Facebook eingeloggt oder betätigt er den Gefällt-mir-Button, kann Facebook die vorgenannten Daten mit dem Facebookprofil des Nutzers umfassend verknüpfen.

4. Hat der Nutzer die **Facebook-App und die Funktion Places** auf seinem Handy installiert, kann er auf Facebook mitteilen, wo er sich gerade befindet. Auch seine Freunde können das für ihn tun. Diese Funktion ist bei Facebook standartmäßig voreingestellt. Die Meldung wird auf Facebook als Statusnachricht

und in der Rubrik „Personen, die jetzt hier sind“ in einer Karte angezeigt. Die besuchten Orte können Aufschluss über die mutmaßlichen Gewohnheiten und Interessen geben – interessant nicht nur für die Werbebranche.

5. Laden Nutzer auf Facebook Fotos hoch, erkennt eine **Gesichtserkennungs-software** die auf den Fotos abgebildeten Freunde und schlägt vor, diese zu markieren, das heißt mit einem Namen zu versehen. Die Erkennung basiert auf der Auswertung biometrischer Daten für Gesichter. Die Funktion ist standard-mäßig für alle Nutzer aktiviert. Das „Tagging“ durch andere Nutzer kann zwar deaktiviert werden, die Gesichter auf den Bildern werden jedoch trotzdem bio-metrisch erfasst und ausgewertet.

6. So einfach es ist, ein Profil zu erstellen, so schwer ist es, aus Facebook auszu-treten. Facebook bietet hierfür zwei Möglichkeiten: Einerseits kann ein Account deaktiviert werden. Der Useraccount wird auf „inaktiv“ geschaltet – die Daten verbleiben jedoch auf den Rechnern der Firma und werden bei einer erneuten Anmeldung im System sofort wieder genutzt. Unter einem zweiten, schlecht zu findenden Link kann man sich komplett von **Facebook abmelden**. Offenbar werden jedoch auch dann die Daten nicht gelöscht. Ein weiteres Problem be-steht darin, dass Drittanbieter die Daten häufig ohne Wissen des Verbrauchers nutzen. Hat man es endlich geschafft, seine Daten in einem Sozialen Netzwerk zu löschen, bleiben die Daten bei dem Drittanbieter jedoch weiterhin bestehen.

Beispiel 2: Smartphones / Geodaten

Unternehmen wie Apple, Google und Microsoft sammeln Standortdaten von Smartphones ihrer Kunden, um „standortbezogene Produkte und Dienste anzubieten und diese zu verbessern“[1]. Hierzu speichern die Unternehmen neben GPS-Koordinaten (bis auf 5 Meter genau) die Standorte von WLANs und Mobilfunkzellen, die sich in der Nähe des Nutzers befinden.

In den Datenschutzbestimmungen von Google heißt es dazu beispielsweise: „Google bietet standortbezogene Services wie Google Maps oder Latitude an. Wenn Sie diese Services nutzen, erhält Google möglicherweise Informationen zu Ihrem tatsächlichen Standort (beispielsweise von einem Mobilgerät übermittelte GPS-Signale) oder Informationen, über die Ihr ungefährer Standort ermittelt werden kann (zum Beispiel die Zellen-ID).“ Was im Einzelnen mit diesen Informationen geschieht, ist nicht ersichtlich. Der Kunde erfährt nur folgendes: „Darüber hinaus verwenden wir die gesammelten Daten zu folgenden Zwecken: Bereitstellung, Aufrechterhaltung, Schutz und Verbesserung unserer Services, einschließlich der Werbeprogramme und der Entwicklung neuer Services und Schutz der Rechte oder des Eigentums von Google und unseren Nutzern.“

Die Artikel 29-Gruppe, ein unabhängiges Beratungsgremium der Europäischen Union in Datenschutzfragen, hat in einer Stellungnahme befunden, dass es sich bei Geodaten von Smartphonenutzern in der Regel um personenbezogene Daten handelt. Ein Telefon ist meist an eine Person gebunden, das diese normalerweise dicht bei sich trägt. Aus den gewonnenen Lokalisierungsdaten können daher umfassende Bewegungsprofile erstellt werden, aus denen sich Rückschlüsse auf die Lebensgewohnheiten des Nutzers ziehen lassen. Beispielsweise können die Unternehmen an den Daten erkennen, wo eine Person wohnt (Inaktivität in der Nacht), wo sie arbeitet (Aktivität am Tag), welche Interessen und Hobbys sie hat (zum Beispiel Besuch von Sportstudios) und, in Verbindung mit den Geodaten anderer Personen, mit wem sie befreundet ist. Sogar Krankheiten (Besuch von Fachärzten), Religionszugehörigkeit (Besuch von Gotteshäusern), politische Ansichten (Teilnahme an Demonstrationen) und Sexualleben (Besuch einschlägiger Lokalitäten) können erschlossen werden.

Aus diesen Informationen werden durch die Unternehmen – die keiner nennenswerten Datenschutzkontrolle unterliegen - umfassende Persönlichkeitsprofile gebildet. Diese Profile werden beispielweise für die Erstellung und Zusendung von interessens-, verhaltens- und standortbezogener Werbung verwendet. Problematisch dabei ist, dass viele Nutzer nicht wissen und erkennen können, dass ihr Standort übermittelt wird und wer die Daten erhält.

Die Erhebung und Übermittlung von Standortdaten muss nach Auffassung des vzbv an eine vorherige, ausdrückliche und bewusste Einwilligung des Nutzers gebunden sein. Hersteller müssen die Voreinstellungen von Geräten zudem so konfigurieren, dass die Übertragung von Standortdaten bei der Inbetriebnahme zunächst ausgeschaltet ist.

[1] Aus der Apple-Datenschutzrichtlinie

Beispiel 3: Browser / Cookies

Cookies sind kleine Textdateien, die über eine Webseite auf dem Computer des Besuchers abgelegt werden können. Genauer: der Webserver speichert das Cookie im Browser des Nutzers und kann es wieder abrufen, wenn er später dieselbe Webseite oder eine andere des gleichen Anbieters aufruft.

Es gibt verschiedene Arten von Cookies. Beispielsweise kann mit ihnen der Webserver auf dem Rechner des Nutzers dessen Oberflächeneinstellungen abspeichern, etwa Schriftgröße, Farbe und Sprache. So genannte „Session Cookies“ ermöglichen dem Nutzer außerdem das reibungslose Surfen auf einer Webseite, zum Beispiel beim Onlineshopping oder Online-Banking. Diese Sorte Cookies wird gelöscht, wenn der Nutzer den Browser schließt.

Mit dauerhaften Cookies hingegen, die sich über einen Zeitraum von mehreren Monaten oder gar Jahren auf der Festplatte befinden, kann das Surfverhalten des Nutzers analysiert werden. Oft werden diese „Tracking-Cookies“ nicht durch die Webseitenbetreiber selber, sondern durch Dritte (meist Werbefirmen) platziert, weshalb sie gelegentlich auch als „Drittanbieter-Cookies“ bezeichnet werden. Sie dienen dazu, alle Webseitenbesuche aufzuzeichnen und einem Nutzer zuzuordnen.

Mit Hilfe der Tracking-Cookies lässt sich das Surfverhalten eines Nutzers über lange Zeit und über viele Webseiten hinweg aufzeichnen. Anhand der gesammelten Informationen können Unternehmen umfassende Nutzerprofile erstellen, um Werbung zielgenauer zu platzieren. Während der eine Nutzer eine Autowerbung präsentiert bekommt, erscheint bei einem anderen auf genau derselben Werbefläche zur selben Zeit eine Reklame für Kinderbekleidung. Man spricht von digitaler Profilbildung. Problematisch ist dabei, dass viele Nutzer gar nicht erkennen können, dass Informationen über sie gesammelt, ausgewertet und an Dritte weiter gegeben werden. Daher können sie auch ihre Rechte nicht wahrnehmen, zum Beispiel eine Auskunft über die gespeicherten Daten einzuholen oder deren Löschung zu veranlassen.

Zwar gibt es bei allen gängigen Webbrowser die Möglichkeit, gespeicherte Cookies zu löschen, gar nicht erst zu speichern oder direkt nach dem Schließen des Browsers automatisch zu löschen. Die Voreinstellungen sind jedoch meist so konfiguriert, dass Cookies akzeptiert werden – auch jene von Drittanbietern, bei denen es sich so gut wie immer um Tracking-Cookies handelt, die für die Verbraucher keinen direkten Nutzen bringen.

Beispiel 4: (Handy-)Betriebssystem / IPv6

Im Internet werden Daten mit Hilfe des Internet-Protokolls (IP) übertragen. Wie Postleitzahlen in der realen Welt, sind die so genannten IP-Adressen notwendig, um die Daten dem richtigen Empfänger zuzustellen. Bei dem derzeit verwendeten Standard („Internet Protocol Version 4“ – IPv4) besteht eine IP-Adresse aus vier Zahlen, die Werte von 0 bis 255 annehmen (z.B. 213.71.163.94). Damit ergeben sich jedoch nur knapp 4,3 Milliarden Zahlenkombinationen, die im Frühjahr 2012 alle vergeben sein werden.

Es herrscht also Knappheit im Netz. Mit diesem Problem gehen Internetanbieter derzeit um, indem sie aus einem gewissen Portfolio den Nutzern dynamisch IP-Adressen zuweisen. Das bedeutet, dass diese jedes Mal eine neue IP-Adresse erhalten, wenn sie sich in das Internet einwählen und diese wieder verlieren, wenn sie sich abmelden. Aus Datenschutzsicht hat das enorme Vorteile: Nur der Internetanbieter weiß, wer sich zu welchem Zeitpunkt mit welcher IP-Adresse im Internet bewegt. Außerdem erhält nicht jedes Endgerät eine eigene IP-Adresse, sondern nur der jeweilige Internetanschluss, unabhängig davon, wie viele Computer darüber am Netz hängen.

Doch Knappheit soll es im Internet künftig nicht mehr geben. Mit dem Format IPv6 wird ein neuer Standard eingeführt, der mehr Stellen und eine veränderte Schreibweise mit sich bringt, zum Beispiel 2001:db8:1234:0001:00aa:00ff:fe3f:2a1c. Damit stehen nun über 340 Sextillionen IP-Adressen zur Verfügung.

Die neue IP-Adresse besteht aus zwei Teilen. Der erste wird vom Internetanbieter vergeben (wie bisher die IPv4-Adresse auch). Allerdings besteht zumindest technisch keine Notwendigkeit mehr, dies dynamisch zu tun. Jeder Anschluss kann also eine feste Adresse erhalten. Der zweite Teil wird aus einer festen, einmaligen Hardware-Adresse (MAC-Adresse) des Endgeräts berechnet. Der Nutzer surft somit mit einem eindeutigen „Nummernschild“ durchs Internet. Datenschutz ist so nicht mehr vorhanden. Dies ist insbesondere bei Smartphones ein Problem, die normalerweise nur von einer Person genutzt werden. Die Erstellung von umfassenden Nutzungs-, Interessens- und Bewegungsprofilen und damit die Beobachtung und Manipulation der Verbraucher durch Unternehmen würde um ein vielfaches leichter als bisher. Auch anonyme Meinungsbekundungen oder die anonyme Teilnahme an sensiblen Diskussionen oder Beratungen im Internet wären kaum mehr möglich.

Die Problematik ist bekannt. Deshalb wurde die so genannte „Privacy Extension“ entwickelt, ein Verfahren, durch das der zweite Teil der Adresse zufällig berechnet wird. An diesem Punkt wird erneut die Voreinstellung relevant. Die Anonymisierung ist bisher nur bei Windows, Mac OS X ab Version 10.7 und bei iOS ab Version 4.3 standardmäßig aktiviert. Bei älteren Mac-Rechnern und bei Computern mit Linux-Betriebssystem müssen die Nutzer dies selbst einstellen. Besonders problematisch: Bei vielen Smartphones ist die Funktion gar nicht erst vorgesehen.

Für den Datenschutz im Internet ist es nach Auffassung des vzbv unerlässlich, feste Regelungen für die Vergabe von IPv6-Adressen zu formulieren. Jeder Internetanbieter muss verpflichtet werden, ohne Aufpreis auch weiterhin dynamische Adressen an seine Kunden zu vergeben. Zudem dürfen internetfähige Geräte nur mit aktivierter Privacy Extension ausgeliefert werden.