Aktive informationelle Selbstbestimmung in der Online-Welt

Privacy Service macht das Internet vertrauenswürdiger

Eine klare Übersicht über die bei den Internet-Dienstanbietern gespeicherten eigenen persönlichen Daten ist Grundvoraussetzung, um sich selbstbestimmt im Internet zu bewegen. In der aktuellen Praxis findet aktive informationelle Selbstbestimmung im Internet somit so gut wie nicht statt. Mit dem Online Privacy Service oder auch mit dem „Elektronischen Datenbrief" stellt das Institut für Internet-Sicherheit – if(is) einen zukunftsweisenden und pragmatischen Lösungsvorschlag für die Anbieter von Internet-Diensten vor, wie eine aktive informationelle Selbstbestimmung und das Recht auf Vergessen-Werden im Internet umgesetzt werden können. Dieses Recht ist in der neuen EU-Verordnung für Datenschutz im Internet explizit formu-

Die Betreiber von sozialen Netzwerken wie beispielsweise Facebook und Google+ verdienen ihr Geld vor allem mit Werbung. Die Nutzer dieser Netzwerke zahlen zunächst nichts für den jeweiligen Internet-Dienst, geben jedoch im Gegenzug unzählige personenbezogene Daten über sich preis. Die Erhebung, Speicherung und Weiterverarbeitung dieser Nutzerdaten sichern die Betreiber mithilfe ihrer AGB. Diesen müssen die Nutzer während der Anmeldung zustimmen. Aus den erhobenen persönlichen Daten der Nutzer erstellen Betreiber sozialer Netze Nutzerprofile, die für den Verkauf von Waren und Dienstleistungen genutzt werden, weil sie passgenaue, individualisierte Werbung ermöglichen. Zielgenaue Werbung lassen sich die Betreiber vieler sozialer Netzwerke durch das Schalten von individualisierten Anzeigen gut bezahlen. Dieses Prinzip „Bezahlen mit persönlichen Daten" wird auch bei anderen Diensten wie Suchmaschinen, E-Mail-Diensten und Nachrichten-Diensten angewendet. Aber auch im Bereich von E-Commerce wie beispielsweise beim Online-Versandhaus Amazon werden personenbezogene Daten erhoben, gespeichert und ausgewertet, um den Kunden individuelle Angebote machen zu können.

In Deutschland gibt es das Recht auf informationelle Selbstbestimmung. Dieses Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Bislang sind Nutzer allerdings kaum bis gar nicht Herr ihrer persönlichen Daten im Internet.

Der Datenbrief als Forderung des Chaos Computer Clubs

Als Forderung des Chaos Computer Clubs sollen Firmen, Behörden und Institutionen, die personenbezogene Daten erheben, verpflichtet werden, in regelmäßigen Abständen den kostenlose Information über die gespeicherten Daten in Form eines Datenbriefs an die Betroffenen zu versenden. Dies beinhaltet auch „angereicherte Daten", wie zum Beispiel Profile und Scoring-Werte. Scoring-Werte sind die Ergebnisse eines analytisch statistischen Verfahrens, welche Prognosen über mögliche Verhaltensweisen von Nutzern repräsentiert. Sie sind für eine gezielte Werbung von hoher Bedeutung. Ein Datenbrief würde die informationelle Selbstbestimmung maßgeblich stärken. Im Moment hat ein Internet-Nutzer nach dem Bundesdatenschutzgesetz bereits ein Recht auf Auskunft (vgl. §§ 19, 34 BDSG). Ihm muss jedoch dazu bekannt sein, an welchen Stellen seine personenbezogenen Informationen gespeichert sind. Anschließend muss der Bürger als Bittsteller gegenüber der speichernden Stelle, also der Firma, Behörde oder Institution, auftreten. Diese Vorgehensweise wird oft durch eine aufwendige Identifikation mittels einer Kopie des Personalausweises oder des Post-Ident-Verfahrens erschwert.

Meinung der Politik zum Datenbrief

Der Datenbrief wurde Anfang 2010 auch in der Politik diskutiert. So zeigten sich zum Beispiel der damalige Bundesinnenminister Thomas de Maizière und die Bundesjustizministerin Sabine Leutheusser-Schnarrenberger Anfang März 2010 aufgeschlossen gegenüber der Idee. Auch der Bundesdatenschutzbeauftragte Peter Schaar bezeichnete den Datenbrief bereits im Januar 2010 als „sinnvoll". Im Mai 2010 relativierten die Bundesjustizministerin Sabine Leutheusser-Schnarrenberger und der Bundesdatenschutzbeauftragte Peter Schaar jedoch ihre Meinung, da es unter praktischen Gesichtspunkten „riesige Probleme" gebe. Das Anliegen sei „absolut unterstützenswert", aber „noch nicht ganz zu Ende gedacht" (siehe auch [HePo2012]).

Die Idee des Online Privacy Service

Der Großteil der Kritik am Konzept des Datenbriefs konzentriert sich auf die Art der Zustellung, speziell auf das Problem der Fehladressierung und das damit verbundene Missbrauchspotenzial. Der vom if(is) entwickelte Online Privacy Service verpflichtet daher Firmen, Behörden und Institutionen, die personenbezogene Daten erheben und Anbieter eines Internet-Dienstes sind, den Betroffenen die Informationen über die gespeicherten Daten regelmäßig kostenlos über einen standardisierten Dienst zur Verfügung zu stellen. Der Service sollte in den bestehenden Internet-Dienst integriert sein, damit der Zugriff mit den gleichen Zugangsdaten möglich ist. Jeder Internet-Dienst sollte analog zum Datenbrief-Konzept alle über den Betroffenen gespeicherten personenbezogenen Daten sowie deren Ursprung enthalten und auch zeigen, ob und, wenn ja, welche Daten an eine dritte Stelle übermittelt wurden. Zudem müssen der Zweck und die Rechtsgrundlage für die Speicherung und Übermittlung sowie eine Widerspruchs- und Korrekturmöglichkeit enthalten sein. Die Widerspruchs- und Korrekturmöglichkeit impliziert ebenfalls, auch alle nicht für den ordnungsgemäßen Betrieb des Internet-Dienstes erforderlichen Daten, wie zum Beispiel für Werbezwecke angereicherte Informationen, komplett löschen zu können.

Lösung der Probleme des ursprünglichen Datenbrief-Konzepts

Der Online Privacy Service löst damit die Probleme des älteren Datenbrief-Konzepts. Durch die Nutzung der gleichen Zugangsdaten wie für den Internet-Dienst und die erforderliche Identifizierung nach dem Erhalt einer Benachrichtigung über die Erfassung besteht bei einer Fehladressierung kein Missbrauchspotenzial. Da die Datenbriefe nicht etwa elektronisch mittels E-Post zugestellt, sondern nur dort aufbereitet werden, wo sie sowieso liegen, schafft der dezentrale Abruf des Online Privacy Service über einen standardisierten Online-Privacy-Service-Dienst (OPS-Dienst) zudem keine weiteren potenziellen Angriffsziele. Auch ist der Aufwand für die Internet-Dienstanbieter überschaubar, da durch die Integration des Online-Privacy-Service-Datenbrief-Dienstes in den bestehenden Internet-Dienst lediglich einmalige Kosten anfallen. Da der Online-Privacy-Service-Datenbrief-Dienst standardisiert sein soll, bietet er eine sehr hohe Vertrauenswürdigkeit und Sicherheit für die Nutzer.

Service-Umsetzung

Eine mögliche Umsetzung des OPS lässt sich wie folgt veranschaulichen:

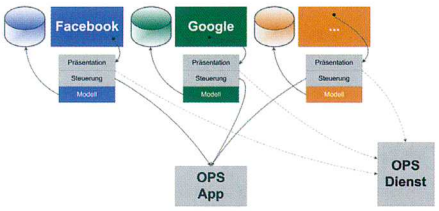

Bild 1: Überblick einer möglichen OPS-Umsetzung

Bei der Abbildung wird exemplarisch angenommen, dass Facebook (blau), Google (grün) und ein weiterer Dienst (orange) den Online Privacy Service (grau) implementieren.

Schichtenarchitektur

Die verwendete Schichtenarchitektur erlaubt eine konzeptionelle Trennung des Modells, der Steuerung sowie der Präsentation. Diese Strukturierung ist notwendig, da der Zugriff auf die Daten (Modell) von jedem Dienstanbieter verschieden implementiert werden muss und eine Darstellung der Daten (Präsentation) nicht nur im Browser, sondern auch in weiteren Anwendungen ermöglicht werden soll (OPS-App).

Implementierung

Da die standardisierte Steuerungs- sowie Präsentationsschicht durch den OPS zur Verfügung gestellt wird, ist auf Seiten der Dienstanbieter nur der Zugriff auf die Datenbank gegen die einheitliche Schnittstelle der Steuerungsschicht sowie ein Verweis auf die Präsentationsschicht zu implementieren. Die Steuerungs- sowie die Präsentationsschicht sind physikalisch ebenfalls bei dem Dienstanbieter ausgeführt, so benötigen sie Zugriffe auf den OPS-Dienst, um Aktualisierungen zu empfangen.

OPS-Dienst

Der OPS-Dienst stellt Aktualisierungen der Steuerungs- und Präsentationsschicht zur Verfügung. Außerdem verwaltet er die Kategorisierung der Daten, indem er kategorisierte Merkmale für allgemeine Daten anbietet und diese nach Anfragen der Dienstanbieter einheitlich ergänzt. Über den OPS-Dienst kann der Nutzer seine gespeicherten Daten ansehen und verwalten.

OPS-App

Die OPS-App stellt die offizielle ebenfalls vom OPS zur Verfügung gestellte Anwendung dar. Über die einheitliche Schnittstelle der Steuerungsschicht ist die Anwendung (OPS-App) in der Lage, die Daten der verschiedensten Dienstanbieter abzurufen. Dies erlaubt für den jeweiligen Nutzer eine globale Sicht und damit Vergleichbarkeit der Datensammlungen.

Vorgehensweise zur Umsetzung

Standardisierung des Online Privacy Service

Für die Standardisierung des OPS empfiehlt sich die Einrichtung eines Arbeitskreises. Dieser sollte Rahmenbedingungen und eine Kategorisierung entwerfen. Beim Entwurf der Kategorisierung muss beachtet werden, dass sich viele Daten der verschiedenen Dienste überschneiden. Somit besteht die Herausforderung darin, eine Kategorisierung zu entwerfen, welche die Daten der verschiedenen Dienste genau einem Merkmal in der Kategorisierung zuordnet. In einem weiteren Schritt müssen die wichtigen Akteure die standardisierte Steuerungs- und Präsentationsschicht sowie die OPS-App entsprechend den erarbeiteten Rahmenbedingungen entwickeln. Aufgrund der Sensibilität der Daten ist bei der Entwicklung insbesondere auf höchste Sicherheitsvorkehrungen zu achten. Die entwickelte Software muss zudem entsprechend den Sicherheitsanforderungen zertifiziert werden.

Integration der Dienstanbieter

Die Integration von Diensten verläuft typischerweise in den folgenden Schritten:

- Entwicklung der Modellschicht
- Beantragung neuer Merkmale
- Einbindung in die vorhandene Onlineplattform

Für die Entwicklung der Modellschicht müssen den Dienstanbietern eine Dokumentation zu den Schnittstellen der Steuerungsschicht sowie Merkmale der Kategorisierung zur Verfügung gestellt werden. Um Redundanzen zu vermeiden, muss außerdem die Zuordnung der Daten zu den Merkmalen der einheitlichen Kategorisierung während der Integration überprüft werden. Für diesen Prozess muss es für den Dienstanbieter außerdem möglich sein, neue Merkmale in der Kategorisierung zu beantragen. Die Einbindung in die vorhandene Onlineplattform muss vorgegebenen Rahmenbedingungen entsprechen, damit der Verweis zu dem Online Privacy Service von den Nutzern schnell und intuitiv gefunden wird.

Wartung des Online Privacy Service

Die Wartung des Online Privacy Service muss die mindestens monatliche Aktualisierung der Kategorien und Merkmale umfassen. Außerdem muss die standardisierte Steuerungs- und Präsentationsschicht kontinuierlich weiterentwickelt und im Zuge dessen der aktuellen Sicherheitslage angepasst werden.

Betreuung durch die Dienstanbieter

Die Dienstanbieter müssen nach der Integration verpflichtet werden, Anfragen, die über den Online Privacy Service eingehen, in einem vorgeschriebenen Zeitraum individuell zu bearbeiten.

Exkurs: Datendownload bei Facebook

Max Schrems hatte im Juni 2011 seine persönlichen Daten bei Facebook angefordert und daraufhin ein 1222 Seiten umfassendes Dokument von Facebook erhalten. Da Facebook einen Sitz im irischen Dublin hat, haben alle Europäer nach Art. 12 der EU-Datenschutzrichtlinie (95/46/EG) ein Anrecht auf die Zusendung der über sie gespeicherten Daten. Die in dem Dokument enthaltenen 57 Datensätze gliedern sich in 22 Datensätze mit Profilinformationen sowie 35 Datensätze mit generierten Daten. Schrems vermutet jedoch, dass Facebook über 100 verschiedene Datensätze über jeden Nutzer speichert. Viele Datensätze fehlen, zum Beispiel diejenigen, die Daten der automatischen Gesichtserkennung, der Handysynchronisation und von Friend Finders enthalten.

Aufgrund des hohen Zuwachs an Anfragen, die Facebook Irland durch die Initiative Schrems erhielt, bietet Facebook seit November 2011 jedem Nutzer in den Kontoeinstellungen die Möglichkeit an, die über ihn gespeicherten Informationen in einem Archiv herunterzuladen (Bild 2). Dieser Download enthält jedoch lediglich die Profilinformationen; die im Hintergrund generierten Daten fehlen komplett. Nach Rückfrage bei Facebook handele es sich bei den weiteren Daten um ein Geschäftsgeheimnis und geistiges Eigentum des Unternehmens. Außerdem gestalte sich der Transfer der angeforderten Daten „überproportional schwierig".

Bild 2: Daten-Download bei Facebook

Bild 2 zeigt eine anonymisierte Ansicht der herunterladbaren Profilinformationen auf Facebook. Bereits hier ist zu erkennen, dass nicht alle über den Betroffenen gespeicherten Daten sowie deren Ursprung enthalten sind. Viele Datenschutzexperten sind der Meinung, dass die Möglichkeit des Datendownloads lediglich der Irritation des Nutzers dient, da keine volle Dateneinsicht erfolgt.

Kategorisierung des Prototyps

Mit der Erstellung des Prototyps war gleichzeitig der Entwurf einer Kategorisierung notwendig. Die entwickelte Kategorisierung kann alle Daten des anonymisieren Facebook-Datensatzes von Schrems aufnehmen. Sie stellt durch die Wahl von allgemeingültigen Kategorisierungen und Merkmalen jedoch ein generisches Modell dar, sodass dieses auch für weitere Dienste verwendet werden kann. Die Google-Dienste lassen sich beispielsweise wie folgt in das generische Modell einordnen:

- +1 in Vorlieben und Gefühle
- Circles in Kontakte
- Google Buzz in Kommunikation
- Kontakte in Kontakte
- Picasa-Webalben in Multimedia

Auch die Daten eines weniger verwandten Anbieters wie einer Krankenkasse lassen sich in das generische Modell einordnen. Dabei würden die spezifischeren Daten in einer beim Online-Privacy-Dienst zu beantragenden neuen Kategorie „Gesundheit" Platz finden.

Integration in die vorhandene Onlineplattform

Die Einbindung in die vorhandene Onlineplattform am Beispiel von Facebook könnte wie folgt aussehen (Bild 3):

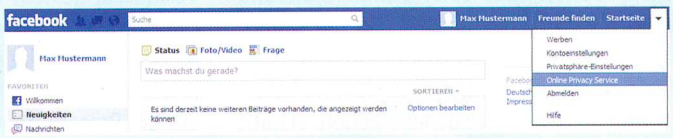

Bild 3: Integration in die vorhandene Onlineplattform – hier am Beispiel Facebook

Dabei wäre gewährleistet, dass der Verweis zum OPS schnell und intuitiv zu finden ist. Der Verweis könnte beispielsweise wie folgt realisiert werden (Bild 4):

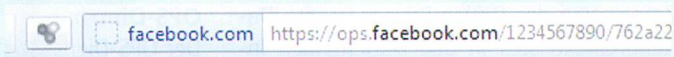

Bild 4: Verweis zum OPS

An dieser Stelle realisiert SSL/TLS eine sichere Verbindung zum OPS. Durch die Verwendung eines Access-Tokens kann nur die zum Access-Token passende Profil-ID aufgerufen werden. Zusätzlich könnte durch ein IP-Binding die Versendung einer Mobile-TAN (Medienwechsel) ermöglicht werden. Die Verifikation durch den neuen Personalausweis gewährleistet zudem eine noch stärkere Sicherheit.

Einheitliche Ansicht ermöglicht Vergleichbarkeit

Eine einheitliche Ansicht, die sowohl eine Vergleichbarkeit als auch eine vertraute, leicht zu bedienende Umgebung für den Nutzer schafft, wurde in dem Prototyp wie folgt realisiert (Bild 5):

Bild 5: Einheitliche Ansicht ermöglicht Vergleichbarkeit

Hierbei ist zu beachten, dass es sich bei dem Entwurf des Prototyps lediglich um eine Veranschaulichung einer möglichen Umsetzung handelt und kein Wert auf ein ansprechendes Design gelegt wurde.

Interaktionsmöglichkeiten des Prototyps

Um dem Nutzer die Möglichkeit zu geben, sich weitere Informationen zu den Merkmalen anzeigen zu lassen oder Rückfragen zu Merkmalen zu stellen, wurden die folgenden Interaktionsmöglichkeiten integriert:

- Informationen
- Korrektur beantragen
- Löschung beantragen

Diese Interaktionsmöglichkeiten lassen sich in einem Pop-up-Fenster realisieren.

Informationen
Das Fenster „Informationen" liefert die folgenden ergänzenden Informationen zu einem Merkmal (Bild 6):

- Zeitpunkt der Speicherung
- Ursprung der Daten
- Zweck der Speicherung
- Übermittlung der Daten
- Rechtsgrundlage der Übermittlungen

Bild 6: Interaktionsmöglichkeiten des Prototyps

Korrektur beantragen
Das Fenster „Korrektur beantragen" bietet die Möglichkeit, die verschiedenen Informationen des Merkmals zu korrigieren. Nach dem Absenden der Korrektur geht diese bei dem entsprechenden Dienstanbieter ein, um anschließend zeitnah in einem vorgeschriebenen Bearbeitungszeitraum überprüft zu werden.

Löschung beantragen
Das Fenster „Löschung" beantragen bietet die Möglichkeit, die Inhalte eines kompletten Merkmals zu löschen. Auch hier wird mit dem Absenden der Löschung eine entsprechende Nachricht an den Dienstanbieter erstellt, der anschließend in dem vorgeschriebenen Bearbeitungszeitraum auf die Anfrage reagieren muss.

Online Privacy Service in der Praxis

Um den Umfang des Online Privacy Service an einem Beispiel der Praxis zu verdeutlichen, wurde ein Prototyp entwickelt, der eine fiktive Integration in Facebook darstellt (s. Kasten). Dabei wurde Facebook als Datenquelle gewählt, da für diesen Dienst weitgehende bereits anonymisierte Datensätze der Initiative europe-v-facebook.org von Max Schrems zur freien Verfügung stehen.

Fazit

Der Exkurs zum Datendownload bei Facebook zeigt, dass die Internet-Dienstanbieter den Bedarf eines Online Privacy Service erkennen. Jedoch wird dieser größtenteils so umgesetzt, dass der speichernden Stelle keine Nachteile entstehen und der betroffene Nutzer des Internet-Dienstes „getäuscht" wird. Es ist deshalb wichtig, dass der vom Institut für Internet-Sicherheit entwickelte Lösungsvorschlag als verpflichtende Richtlinie etabliert wird, damit in Zukunft für alle Betroffenen jederzeit und bei jedem Internet-Dienst die standardisierte Möglichkeit besteht, die gespeicherten personenbezogenen Daten vollständig, einheitlich, einfach und sicher abrufen, korrigieren und löschen zu können. Nur dies kann der richtige Weg für eine modere Gesellschaft sein, bei der die Wahrung der Grundrechte der Bürger gewährleistet wird. ■

Literatur/Info:

- *M. Heidisch, N. Pohlmann: „Elektronischer Datenbrief – eine aktive informationelle Selbstbestimmung im Internet", Website Boosting, Nürnberg, 03-04.2012*
- *http://www.internet-sicherheit.de/institut/forschung/publikationen-vortraege/dokumente-als-pdfs/dokumente-2012/?no_cache=1&tx_damfrontend_pi1%5Bpointer%5D=1*
- *Link zum Prototyp: http://www.internet-sicherheit.de/temp/ops/*

Maik Heidisch,
studentischer Mitarbeiter am Institut für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen

Norbert Pohlmann,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen