Googles Cloud-Angebot – Wie wertvoll ist uns der Datenschutz? (Teil 2)

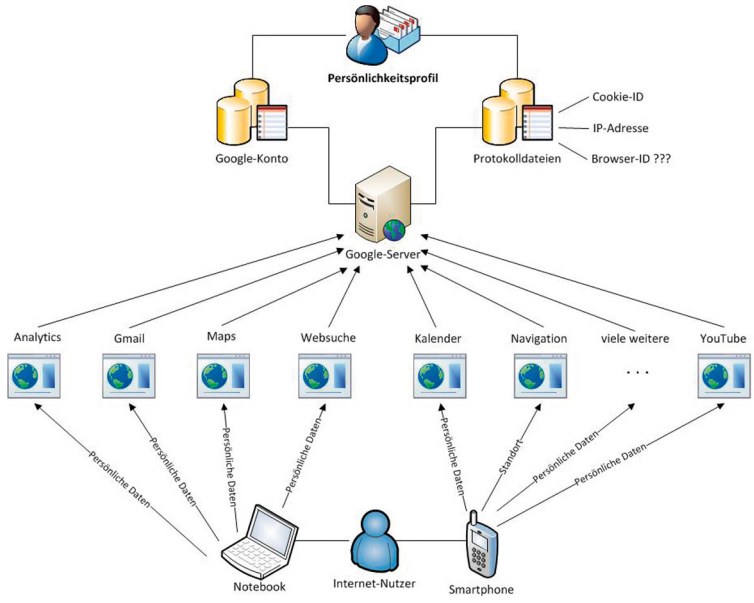
In der Cloud, aber nicht anonym!

Bekannt wurde das US-amerikanische Unternehmen Google durch seine gleichnamige Suchmaschine – doch mittlerweile bietet Google viel mehr als das. Google ist ein Internet-Konzern, der in vielen Geschäftsfeldern aktiv ist und immer wieder innovative Produkte und Dienste auf den Markt bringt. Google ist in fast allen Sparten tätig und macht sich mit über einhundert verschiedenen Diensten im Internet breit. Dazu zählen Betriebssysteme, Office-Tools, ein Web-Browser und diverse Plattformen für Kommunikation, Kollaboration, Multimedia, Organisation und Softwareentwicklung sowie Technologien für das Einstellen und Finden von Inhalten. Auch beim Cloud Computing setzt Google Akzente und wirkt beispielsweise mit Google Chrome OS als Cloud-Client wie ein Innovationsmotor. Im SaaS-Bereich spielt Google mit seinen vielen Diensten eine wichtige Rolle. Außerdem mischt Google mit der App Engine beim PaaS-Angebot mit. Nachdem wir uns im ersten Teil mit dem Geschäftsmodell von Google, den Google-Applikationen (Apps) und Datenschutzrisiken aus Nutzer- und Unternehmensperspektive beschäftigt haben, dreht sich im zweiten Teil alles um die Frage, wie das Sammeln und Verknüpfen von persönlichen Daten von Internet-Nutzern bei Google reglementiert werden kann.

Um trotz der Risiken dennoch in den Genuss der Google-Dienste zu kommen, gibt es im Google-Umfeld verschiedene Maßnahmen, um seine Privatsphäre zu schützen und sein Recht auf informationelle Selbstbestimmung zumindest teilweise auszuüben. Da persönliche Daten im Google-Konto zusammenlaufen, sollte man nur dann mit seinem Google-Konto angemeldet sein, wenn dies auch zwingend erforderlich ist. Viele Funktionalitäten rund um Suchen und Zugriffe auf Content (Blogger.com, Knol, Books, YouTube etc.) oder Kartendienste (Maps, Street View etc.) setzen kein Google-Konto voraus. Diese Strategie impliziert auch, dass teils alternative Dienste genutzt werden, denn nicht alle Google-Dienste sind in ihren jeweiligen Anwendungsfeldern die besten. Soziale Netzwerke wie Orkut und Bezahldienste à la Checkout beispielsweise verarbeiten sehr sensible Daten. Diese sollten nicht (auch noch) mit dem Google-Konto verknüpft werden. Auch bei Content gilt: Alles wird im Google-Konto gespeichert. Dessen sollte man sich stets bewusst sein und gegebenenfalls Ausschau nach alternativen Content-Providern halten.

Außerdem sollten allgemein nur Angaben über persönliche Sachverhalte gemacht werden, die für die Nutzung eines Google-Kontos beziehungsweise eines -Dienstes zwingend erforderlich sind. Dazu zählt vor allem, seine verschiedenen Profile nicht mit persönlichen Daten anzureichern. Vielmehr sollte man versuchen, sein Google-Konto anonym zu halten. Das gelingt jedoch nur, solange keine Bezahldienste wie AdWords, AdSense, DoubleClick oder Checkout in Anspruch genommen werden. Möchte man solche Dienste dennoch verwenden oder zum Beispiel sehr wohl unter seinem richtigen Namen auf Blogger.com bloggen, empfiehlt sich die Verwendung eines separaten Google-Kontos. Infolgedessen kann ein professionelles Google-Konto verwendet werden, das den Internet-Nutzer identifiziert und ein privates, das idealerweise anonym ist. Generell ist mit mehreren Google-Konten dafür gesorgt, dass nicht alle persönlichen Daten dienstübergreifend in einem einzigen Google-Konto zusammenlaufen. So können ausführliche Persönlichkeitsprofile auf Google-Servern verhindert werden. Das funktioniert allerdings nur dann, wenn Google die verschiedenen Konten nicht per Zusatzinformationen wie der IP-Adresse des Nutzers verknüpft – technisch möglich wäre das.

Für persönliche Daten, die sich nicht im Google-Konto, sondern in den Protokolldateien anhäufen, empfiehlt sich die Verwendung von Browser-Plugins. Diese verhindern beispielsweise, dass Daten im Internet auf der Basis von Cookies und IP-Adressen zu Persönlichkeitsprofilen verknüpft werden können. Auch Google selbst bietet im Rahmen seiner Opt-out-Strategie zwei solcher Plugins an: Das eine verhindert, dass persönliche Daten an Google Analytics gesendet werden, und das andere sorgt dafür, dass das DoubleClick-Cookie dauerhaft deaktiviert wird. Mit beiden Plugins kann verhindert werden, dass Verhaltensweisen des Internet-Nutzers aufgezeichnet und zu Profilen verknüpft werden, um beispielsweise Interessen für interessensbasierte Werbung abzuleiten. Darüber hinaus gibt es viele weitere Plugins wie zum Beispiel Google-Sharing, ein unabhängiges Projekt, bei dem Anfragen an Google-Server über einen Proxy umgeleitet werden. Dieser verschleiert die Identifikation des Nutzers (sowohl IP-Adresse als auch Cookie-ID), indem er sie



Bildung von Persönlichkeitsprofilen auf Google-Servern

durch eigene, interne Identifikationsmerkmale ersetzt. Diese eigenen Identifikationsmerkmale werden bei einer weiteren Anfrage dem nächsten GoogleSharing-Nutzer zugewiesen. Nutzer und deren Identifikationsmerkmale werden so verwürfelt. Infolgedessen kann Google nicht mehr unterscheiden, welcher Nutzer mit welcher IP-Adresse und welcher Cookie-ID mit Google-Servern kommuniziert. Insbesondere in der Firefox-Community gibt es zahlreiche weiterer Datenschutz-Plugins.

Googles Opt-out-Strategie bietet außerdem weitere Maßnahmen, um seine persönlichen Daten im Google-Umfeld zu schützen. Doch was ist die Opt-out-Strategie? Google hat sich überlegt, seinen Nutzern Wahlmöglichkeiten bezüglich des Datenschutzes anzubieten um auf diesem Wege sowohl Kritiker als auch Internet-Nutzer zu besänftigen. Da Google jedoch weiterhin auf die persönlichen Daten seiner Nutzer angewiesen ist, sind diese Wahlmöglichkeiten standardmäßig deaktiviert. Das heißt, sie sind auf „datenschutzfeindlich" voreingestellt und müssen erst aktiv konfiguriert werden.

Diese Wahlmöglichkeiten, auf die in den Google-Datenschutzbestimmungen explizit hingewiesen wird, sind meist Teil der Dienstkonfiguration: In den Einstellungen der Dienste kann man diese Optionen aktivieren. Im Grunde genommen deaktiviert man Optionen, die persönliche Daten an Google übertragen beziehungsweise speichern und verknüpfen, daher auch die Bezeichnung „Opt-out". Beispiele für solche Optionen sind, dass bei Google Talk eingestellt werden kann, dass Konversationen nicht im Google-Konto abgespeichert werden. Auch kann verhindert werden, dass Kommunikationspartner die Konversation ihrerseits mit dem Google-Konto verknüpfen. Das Web-Protokoll, das beim Anlegen eines Google-Kontos standardmäßig aktiviert ist, kann ebenfalls deaktiviert werden. Danach werden Suchanfragen nicht mehr im Google-Konto gespeichert. Bei Chrome und der Toolbar können Funktionen, die beispielsweise automatisch die Eingaben in das Adressfeld des Browsers an Google senden, deaktiviert werden.

Fazit und Ausblick

Die genannten Maßnahmen zum Schutz der persönlichen Daten sollten von jedem Internet-Nutzer gewählt werden. Würde

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

man beispielsweise Chrome OS mit den Google Apps und weiteren Google-Diensten ohne entsprechende Schutzmaßnahmen nutzen, dann würde sich ein umfangreiches Persönlichkeits- beziehungsweise Unternehmensprofil auf den Servern von Google bilden und man selbst wäre nicht mehr Herr über dieses eigene Profil:

- Name und Adresse bei Checkout, Gmail, Orkut etc.
- Soziale Kontakte bei Gmail, Orkut, Talk, Voice etc.
- Aufenthaltsort bei Android und mobilen Diensten sowie per Geolocation API
- Reiseziele bei Earth, Maps, Navigation etc.
- Termine bei Kalender, Sync etc.
- Bankverbindungen bei AdWords, AdSense, Checkout, DoubleClick etc.
- Finanzielle Transaktionen bei Checkout
- Wertpapiere und Depots bei Finance
- Gesundheitsdaten bei Health
- Lichtbild beziehungsweise Passfoto bei Gmail, Orkut, Picasa, YouTube etc.
- Interessen bei Analytics, Chrome, DoubleClick, Gmail, Groups, Orkut, Toolbar, YouTube, Websuche etc.
- Besuchte Webseiten bei AdSense, Analytics, Chrome, DoubleClick, Toolbar etc.
- Bilder, Dokumente, Videos und weiterer Content bei Docs, Picasa, YouTube etc.
- …

Der Datenschutzproblematik entzogen hat sich Google mit seiner Opt-out-Strategie allerdings nicht, denn sie ist nicht mit dem europäischen Datenschutz-Prinzip „Verbot mit Erlaubnisvorbehalt" in Einklang zu bringen. Bei Google-Diensten ist die Einwilligung des Nutzers unzureichend realisiert: In den Nutzungs- und Datenschutzbestimmungen wird zwar grob beschrieben, welche persönlichen Daten von Google erhoben und verarbeitet werden. Diese Formulierungen lassen jedoch viel Interpretationsfreiraum. Bei Google Analytics oder DoubleClick fehlt eine Einwilligung sogar vollständig. Hier werden persönliche Daten im Internet gesammelt, ohne dass der Nutzer irgendwelchen Nutzungs- beziehungsweise Datenschutzbestimmungen zustimmen muss. Ihm werden seine Wahlmöglichkeiten also nicht gewahr und zwar ebenso wenig, wie er bemerkt, dass überhaupt „jemand" seine persönlichen Daten aufzeichnet. Bei den meisten anderen Diensten erklärt man sich mit der Nutzung eines Dienstes mit den jeweiligen Bestimmungen sowie mit Googles allgemeinen Bestimmungen und Richtlinien einverstanden. Dass bei vielen Diensten datenschutzrechtliche Grundprinzipien wie Zweckbindung, Erforderlichkeit, Datenvermeidung und -sparsamkeit sowie das Transparenzgebot nicht eingehalten werden, verschärft die Problematik. Es wird nämlich nicht ausführlich definiert, welche Daten genau für welche Zwecke erhoben werden. Daher ist nur schwer ersichtlich, ob erhobene Daten wirklich erforderlich sind. Persönliche Daten zu erheben, um einen Dienst erbringen zu können oder die Systemsicherheit zu gewährleisten ist viel zu allgemein gehalten. Das alles sind Gründe, warum Google trotz der Opt-out-Strategie wohl auch weiterhin der Kritik von Datenschützern ausgesetzt sein wird. Solange sich diesbezüglich nichts ändert, muss der Internet-Nutzer selbst für seinen Datenschutz aktiv werden.

Die Datenschutzproblematik im Google-Umfeld beruht auch auf der Tatsache, dass in den USA, wo Google ansässig ist, kulturell bedingt eine andere Einstellung zum Datenschutz herrscht als in Europa und insbesondere Deutschland (siehe auch: http://www.teletrust.de/uploads/media/RSA2011-Pr%C3%A4sentation_TeleTrusT-VIP_Meeting_ifis_Cloud_Security.pdf). Eine weitere Forderung an Google ist, dass sowohl Privatanwender als auch Unternehmen eine vernünftige Wahl haben sollten, ob Cloud-Angebote mit persönlichen beziehungsweise unternehmensinternen Daten oder mit barem Geld bezahlt werden. Beim Cloud Computing geht es um Vertrauen, weil wir unsere Daten – unsere Werte – einem Provider anvertrauen. ■

Nikolai Spogahn

Norbert Pohlmann