Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info

14. Jahrgang, Heft 4, Dezember 2014

Schwerpunkt:

Tracking

fokus: Der «betreute» Mensch

fokus: Tracking im Internet und Selbstdatenschutz

report: Recht auf Vergessen bei Suchmaschinen

Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

fokus

Schwerpunkt:
Tracking

auftakt
Niemand entkommt dem totalen Blick
von Aurel Schmidt Seite 133

Tracking – und was man dagegen tun kann
von Beat Rudin Seite 136

Der betreute Mensch
von Günter Karjoth Seite 138

Tracking im Internet und Selbstdatenschutz
von Norbert Pohlmann Seite 144

Notwehr oder notwendiger Ungehorsam?
von Dominik Herrmann Seite 150

Tracking – rechtliche Standortbestimmung
von Roland Mathys/ Christian Meier Seite 156

Tracking im Internet und Selbstdatenschutz

Tracking im Internet – durch Geheimdienste, aber auch durch die IT-Marktführer aus den USA, die es mit dem Datenschutz und unserer Privatsphäre nicht so genau nehmen. Die Politik scheint mit dieser globalen Herausforderung überfordert zu sein. Mit welchen IT-Sicherheitsstrategien und IT-Sicherheitsmassnahmen können die Nutzer selber das Risiko eines Schadens reduzieren?

Notwehr oder notwendiger Ungehorsam?

Durch Techniken zum Selbstdatenschutz können sich Nutzer vor der Überwachung durch übermächtige Staaten und Konzerne schützen. Darüber hinaus eignen sie sich jedoch auch als Werkzeug zur Ausübung zivilen Ungehorsams, also als Mittel zum Protest gegen die allgegenwärtige Überwachung im Internet.

Tracking – rechtliche Standortbestimmung

Mittels Tracking werden Personendaten in grosser Zahl gesammelt und bearbeitet, wobei Bearbeitungszwecke und Datenempfänger oft unklar bleiben. Was ist beim Einsatz von Tracking zu beachten und wie kann sich der Einzelne gegen unerwünschtes Tracking wehren?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktorin: Dr. iur. Sandra Husi-Stämpfli

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo: CHF 158.00, Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com

Recht auf Vergessen bei Suchmaschinen

Im Urteil des Europäischen Gerichtshofes vom 13. Mai 2014 zu Google Search wird die Anwendbarkeit des EU-Datenschutzrechts auf Google Spain festgehalten und ein Recht auf Vergessen anerkannt. Allerdings wäre eine sorgfältigere Abwägung zwischen Meinungsfreiheit und Datenschutz äusserst wünschenswert gewesen.

Auftragsdatenbearbeitung – zum Vierten

Auftragsdatenbearbeitung – zum Vierten
Der vierte und abschliessende Teil widmet sich der Ausgestaltung und dem Inhalt der datenschutzrechtlichen Regelungen, die unmittelbar von der konkreten Risikolage des Einzelfalls abhängen. Die Autorin stellt die risikotreibenden Faktoren zusammen, zeigt Lösungsansätze auf und stellt eine Checkliste zur Verfügung.

«Micropayment»: IT-Security & IT-Risk

Bei Micropayment geht es um die Möglichkeit, im Internet kleinste Beträge bezahlen zu können. Solche Systeme müssen einfach und angemessen sicher sein. Der Beitrag stellt die Weiterentwicklung eines solchen Bezahldienstes in einer Kooperation zwischen Fachhochschule und einem Industriepartner dar.

Big Mother im Kinderzimmer

Nicht nur Geheimdienste und Werbewirtschaft «bemuttern» uns. Auch mit der Angst der Mütter und Väter lassen sich gute Geschäfte machen – die Datensammelwut beginnt im Kinderzimmer …

Potentes Tracking

Wozu Tracking im Alltag führen kann, zeigt unser Cartoonist Reto Fontana anschaulich.

report

Rechtsprechung
Recht auf Vergessen bei Suchmaschinen
von Kurt Pärli Seite 162

agenda Seite 167

Recht
Auftragsdatenbearbeitung – zum Vierten
von Barbara Widmer Seite 168

Forschung
«Micropayment»: IT-Security & IT-Risk
von Ralf Mock/ Tomas Hruz Seite 180

forum

privatim
Aus den Datenschutzbehörden
von Sandra Husi-Stämpfli Seite 184

Der Blick nach Europa und darüber hinaus
Was tun, wenn Rechtsunsicherheit droht?
von Barbara Widmer Seite 186

schlusstakt
Big Mother im Kinderzimmer
von Beat Rudin Seite 188

cartoon
von Reto Fontana

Tracking im Internet und Selbstdatenschutz

Die Sicherheitsprobleme werden grösser, unsere Privatsphäre ist in Gefahr! Kann der Selbstdatenschutz helfen?

Norbert Pohlmann, Prof. Dr., Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen, Gelsenkirchen, Deutschland pohlmann@internet-sicherheit.de

Das Prinzip «Bezahlen mit persönlichen Daten» ist eine besondere Herausforderung bezüglich des Datenschutzes. Mit dem Selbstdatenschutz können wir eigenständig etwas dagegen tun.

Das Internet mit seinen vielfältigen innovativen Möglichkeiten hat eine hohe Relevanz in unserer modernen Gesellschaft erreicht, die noch weiter steigen wird.

Seit dem Beginn des Internets beobachten wir, dass die IT-Sicherheitsprobleme immer grösser und grösser werden, nicht kleiner. Die Probleme sind mit der NSA-Affäre nochmals grösser geworden. Das heisst, wir haben ein starkes Ungleichgewicht zwischen Angreifern und Verteidigern. Bei der kritischen Beurteilung der aktuellen IT-Sicherheitssituation fallen einige Sicherheitsprobleme besonders deutlich auf, die berücksichtigt werden sollten, um mehr IT-Sicherheit und Vertrauenswürdigkeit aufzubauen. Diese zurzeit besonderen Sicherheitsprobleme sind:

- Zu viele Schwachstellen in Software;
- ungenügender Schutz vor Malware;
- immer noch werden Passwörter für die Authentifikation im Internet verwendet;
- zu viele unsichere Webseiten im Internet;
- neue Gefahren durch die Nutzung mobiler Geräte;
- zu wenige E-Mails werden verschlüsselt übertragen;
- zu wenig Internet-Kompetenz der Internet-Nutzer, um sich angemessen und sicher im Internet zu bewegen;
- Manipulation der IT und IT-Sicherheitstechnologien durch die NSA usw.

Das Geschäftsmodell «Bezahlen mit persönlichen Daten» ist eine besondere Herausforderung bezüglich des Datenschutzes. Soziale Netzwerke wie Facebook, Partnerbörsen, YouTube, XING, LinkedIn, Twitter und Co. bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen und ermöglichen den Nutzern, sich darzustellen und sich real zu begegnen. Soziale Netzwerke schaffen auch neue Wege, Demokratie und Bürgerbeteiligungen zu gestalten, was eine neue und ungewohnte Herausforderung für alle Beteiligten darstellt. Ausserdem bringen soziale Netzwerke die Diskussion über die informationelle Selbstbestimmung und den Datenschutz auf. Eine Frage dazu ist, inwieweit Internet-Angebote zu tolerieren sind, bei denen wir nicht mit Geld, sondern mit unseren persönlichen Daten bezahlen. Wir lassen es mit dem Akzeptieren der AGB zu, dass die Anbieter über Profilbildungen indirekt Geld verdienen können. Aus dem Tracking von 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[1]. Hier werden unsere wichtigen und notwendigen Persönlichkeitsrechte sehr stark berührt. Die Herausforderung in diesem Bereich ist, die Aufklärung der Nutzer über die Risiken und eine gemeinsame angemessene Lösung mit den Anbietern von sozialen Netzwerken zu finden und umzusetzen.

Nur eine klare Übersicht über die eigenen persönlichen Daten, die bei den Internet-Dienstanbietern gespeichert sind, hilft, sich selbstbestimmt im Internet zu bewegen.

Eine Möglichkeit, die wir selbst in der Hand haben, ist der Selbstdatenschutz. Als Erstes

werden in diesem Artikel die IT-Sicherheitsstrategien aufgezeigt, die prinzipiell möglich sind; dann wird das Thema Tracking am Beispiel von Google behandelt, und abschliessend werden einige Vorschläge zum Selbstdatenschutz gemacht.

IT-Sicherheitsstrategien, um uns gegen Angriffe zu schützen

Im Folgenden werden drei prinzipielle IT-Sicherheitsstrategien beschrieben, die uns helfen können, uns zu schützen.

Angriffe vermeiden

Die einfachste IT-Sicherheitsstrategie ist die, dass Angriffe erfolgreich vermieden werden. Beispiele von Vermeidungsstrategien sind:

- Nicht alle IT-Systeme ans Internet anschliessen;
- so wenig wie möglich Daten generieren, die angegriffen werden können;
- keine Technologie mit bekannten Schwachstellen verwenden usw.

Bewertung: Das Vermeiden von Angriffen ist die beste IT-Sicherheitsstrategie, aber praktisch nur begrenzt umsetzbar, da wir mit unseren IT-Systemen ans Internet angeschlossen sein wollen, um die Vorteile nutzen zu können.

Der Punkt «Keine Technologie mit bekannten Schwachstellen verwenden» wäre im Prinzip einfach umzusetzen, wenn alternative Technologien zur Verfügung stehen würden. Ein Beispiel ist die potenzielle Nutzung von mehreren Browsern. Wenn der gerade genutzte Browser eine bekannte Schwachstelle hat, wird einfach ein alternativer Browser verwendet, um nicht angreifbar zu sein.

Angriffen entgegenwirken

Angriffen entgegenzuwirken ist die meist verwendete IT-Sicherheitsstrategie, um Schäden durch Angriffe zu vermeiden. Hier werden IT-Sicherheitsmechanismen verwendet, die eine hohe Wirkung gegen bekannte Angriffe zur Verfügung stellen und damit die Werte angemessen schützen.

Beispiele für IT-Sicherheitstechnologien sind Verschlüsselungssicherheitssysteme (Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, SSL, …), Authentifikationsverfahren (Passwörter, Biometrie, Challenge-Response, …), Firewall-Systeme, Rechteverwaltung usw.

Bewertung: Angriffen entgegenzuwirken ist eine naheliegende IT-Sicherheitsstrategie, aber leider stehen zurzeit nicht genug wirkungsvolle IT-Sicherheitstechnologien, -Lösungen und -Produkte zur Verfügung oder werden nicht angemessen eingesetzt, was die erfolgreichen professionellen Hacker und diverse Geheimdienste uns jeden Tag vor Augen halten.

Angriffe, denen nicht erfolgreich entgegengewirkt werden kann, erkennen

Wenn Angriffen mithilfe von IT-Sicherheitsmechanismen nicht angemessen entgegengewirkt werden kann, dann bleibt nur noch die Strategie, diese zu erkennen und zu versuchen, den Schaden so schnell wie möglich zu minimieren.

Bei der Nutzung von Google-Diensten besteht ein Risiko, das im schlimmsten Fall mit der Aufgabe der Privatsphäre bzw. des Rechts auf informationelle Selbstbestimmung endet.

Bewertung: Die IT-Sicherheitsstrategie, Angriffe, denen nicht erfolgreich entgegengewirkt werden kann (wenigstens) zu erkennen, ist sehr hilfreich, hat aber definierte Grenzen. Advanced Evasion Techniques (AET) ist z.B. eine Technologie, die dafür sorgt, dass Angriffe unentdeckt an Sensoren vorbei gehen können. Dies kann z.B. durch die Provozierung von IP-Fragmentierung erreicht werden, bei der IP-Pakete in kleine Teile aufgeteilt und damit Signaturen verschleiert werden.

Tracking

Tracking oder Spurbildung umfasst im Kontext dieses Artikels alle Bearbeitungsschritte, die der Verfolgung von Aktivitäten im Internet dienen.

Kurz&bündig

Das Internet wird für uns und unsere Gesellschaft immer wichtiger. Seit dem Beginn des Internets beobachten wir leider, dass die IT-Sicherheitsprobleme immer grösser und grösser werden, nicht kleiner. Die IT-Kriminalität erfährt eine zunehmende Industrialisierung und damit eine nicht zu unterschätzende und nie dagewesene professionalisierte Nachhaltigkeit. Die IT-Marktführer aus den USA wie Google, Microsoft, Facebook, Amazon usw. nehmen es mit dem Datenschutz und unserer Privatsphäre nicht so genau, und die Politik scheint mit dieser globalen Herausforderung überfordert zu sein. Wir sollten uns der grundsätzlichen IT-Sicherheitsstrategien bewusst sein und die Möglichkeiten der IT-Sicherheitsmassnahmen, die wir eigenständig nutzen können, kennen und aktiv einsetzen. Damit haben wir es in der Hand, das Risiko eines Schadens deutlich zu reduzieren.

Im Folgenden wird am Beispiel von Google aufgezeigt, was Tracking im Internet bedeutet. Bei der Nutzung von Google-Diensten besteht ein Risiko, das im schlimmsten Fall mit der Aufgabe der Privatsphäre bzw. des Rechts auf informationelle Selbstbestimmung gipfelt. «Bezahlen mit persönlichen Daten» ist die Kehrseite der kostenlosen Dienste.

Zum Verständnis von Tracking soll zuerst erläutert werden, wo Google welche Art von persönlichen Daten erhebt und speichert. Auf der einen Seite laufen persönliche Informationen im Google-Konto zusammen. Dieses Google-Konto wird für viele Dienste, manchmal aber auch nur für bestimmte Funktionalitäten innerhalb der jeweiligen Dienste benötigt. Diese stehen dem Nutzer erst nach einem erfolgreichen Login zur Verfügung. Bei den persönlichen Daten, die im Google-Konto gespeichert werden, kann zwischen direkt und indirekt erfassten Daten unterschieden werden. Direkt werden persönliche Daten dann erfasst, wenn der Internet-Nutzer sie bewusst angibt, indem er selbst aktiv wird und diese z.B. in entsprechende Formularfelder einträgt oder Dateien hochlädt. Somit wird das Nutzerprofil (hier das Google-Konto) freiwillig mit persönlichen Daten angereichert:

- der Name, die Anschrift und die Karriere (bei diversen Profilen verschiedener Dienste);
- die Kontoverbindung (z.B. bei *Adwords* oder *Google Checkout*);
- Posts in Blogs und Foren (z.B. bei *Blogger.com* oder *Google Groups*);
- Dokumente (z.B. bei *Google Docs*);
- Bilder (z.B. beim sozialen Netzwerk *Google Buzz* oder in den *Picasa Webalben*);
- Videos (z.B. bei *YouTube*) usw.

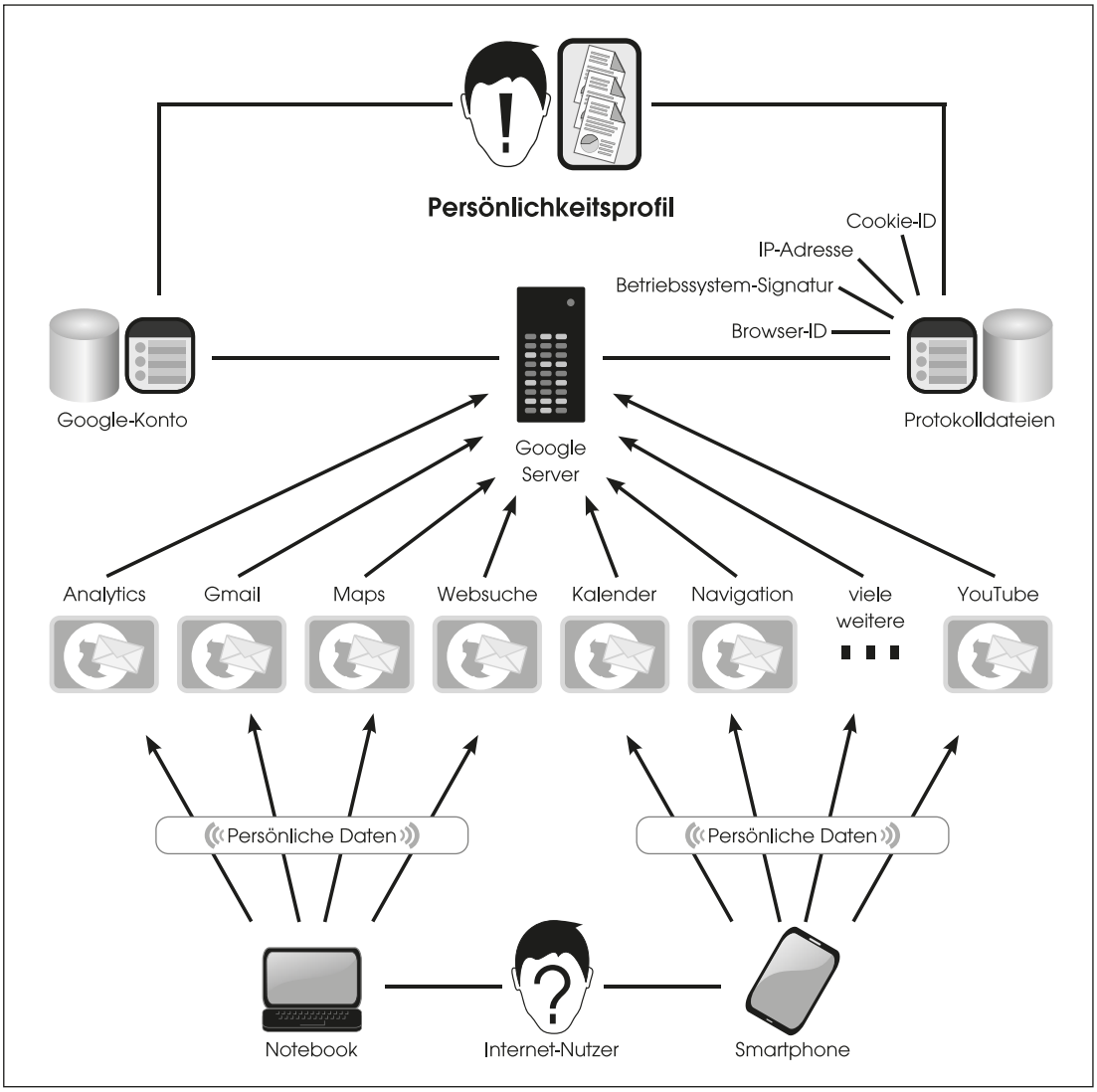
Dazu kommen die indirekt und (vermutlich) für den Nutzer eher ungewollt erfassten persönlichen Daten. Diese werden erfasst, indem das Verhalten des Internet-Nutzers aufgezeichnet wird:

- Berechnete Routen in *Google Maps;*
- Kontakte in *Google Buzz* oder *Gmail;*
- Kommunikationsinhalte in *Gmail, Google Talk* oder *Google Voice;*
- Suchanfragen in der Webhistorie usw.

In Protokolldateien wird das Verhalten des Internet-Nutzers aufgezeichnet, indem Webanfragen und -antworten zwischen dem Internet-Nutzer und Google aufgezeichnet werden.

Weitere Informationen wie Anfragen und abgerufene Inhalte werden ebenfalls dienstübergreifend erfasst und unabhängig von der Nutzung eines Google-Kontos in sogenannten Protokolldateien gespeichert. In diesen Dateien wird also das Verhalten des Internet-Nutzers aufgezeichnet, indem Webanfragen (HTTP-Request) und -antworten (HTTP-Response) zwischen dem Internet-Nutzer und Google aufgezeichnet werden. Dazu zählen Suchanfragen, angeklickte Suchergebnisse, abgerufene Webseiten usw. Um diese einem bestimmten Internet-Nutzer zuordnen zu können, werden die persönlichen Daten unter entsprechenden Identifikations- bzw. Wiedererkennungsmerkmalen erhoben und abgespeichert. Dazu gehören insbesondere Cookies und IP-Adressen. Cookies erlauben es Google und anderen Firmen, ein Wiedererkennungsmerkmal lokal im Webbrowser des Internet-Nutzers abzulegen. Die IP-Adresse ist die technische Identifikation des Internetzugangs und identifiziert nicht den Webbrowser, sondern den Computer im Netz. Ausserdem ist die Zuordnung vom Internet-Nutzer zur IP-Adresse nicht so konsistent wie bei einem Cookie, denn IP-Adressen werden vom Internet-Provider in der Regel dynamisch zugewiesen. Daher sind IP-Adressen als Nutzeridentitäten aus Sicht von Google ungenauer als Cookies, aber dennoch eine willkommene Zusatzinformation. Auch als «Ausweich-Identifikation» können IP-Adressen dienen, falls der Browser des Nutzers keine Cookies akzeptiert. Neben Cookies und IP-Adressen bietet sich auch eine Browser-ID zur Identifikation von Internet-Nutzern an; *Google Chrome* z.B. verfügt über eine solche eindeutige Installationskennung. Wie der Name schon sagt, identifiziert sie eine spezielle Installation des *Chrome*-Browsers auf dem Computer des Internet-Nutzers. Sie ist daher deutlich konsistenter als Cookies, da solche schnell gelöscht werden können, die Browser-ID hingegen nicht. Alle betrachteten technischen Identifikationsmerkmale ermöglichen Google eine Verknüpfung bzw. Korrelation von persönlichen Daten zu entsprechenden Profilen.

Durch Google-Kontos und Protokolldateien entstehen ausführliche Nutzer- bzw. Persönlichkeitsprofile. Diese lagern auf Google-Servern und sind dort prinzipiell nicht einhundertprozentig vor Datenmissbrauch und eigens von Google verursachten Datenschutzpannen geschützt. Auch vor gerichtlichen Zugriffen sind diese Profile mit persönlichen Daten nicht gesichert. Die Möglichkeit der dienstübergreifenden Verknüpfung und Korrelation von persönlichen Daten verschärft das Problem erheblich.



Diesbezüglich nimmt Google eine besondere Stellung ein, denn Google hat über einhundert Dienste, die (fast) sämtliche Bereiche abdecken und bei denen gemäss Single Sign-on ein einziges Google-Konto verwendet werden kann. Es gibt kein Internet-Unternehmen, das sich diesbezüglich im Internet so breit macht und zugleich von personenbezogenen Daten lebt. Daher ist Google auf diese Daten seiner Nutzer angewiesen wie kein anderer. Zu den allgemeinen Risiken, die mit Persönlichkeitsprofilen im Internet verbunden sind, gehören zusätzlich Identitätsdiebstähle (vor allem, um Kriminaltaten unter vorgetäuschter Identität auszuüben), Belästigungen (z.B. durch Werbetreibende oder Personalvermittler), Verfolgungen (z.B. Rasterfahndungen oder Stalking), Demütigungen (Stichwort «Cyber-Mobbing») und verzerrte Persönlichkeitsbilder (Google und andere, die elektronisch Daten erfassen und verknüpfen, unterscheiden nicht zwischen richtigen und falschen Informationen). Das Google-Konto ist also ein lukrativer Angriffspunkt für Hacker, da hier viele relevante Informationen zusammenlaufen.

Selbstdatenschutz

Unter dem Begriff Selbstdatenschutz wird in diesem Artikel verstanden, dass die Internet-Nutzer sich über grundsätzliche und aktuelle Gefahren, die beim Datenschutz und der Datensicherheit vorhanden sind, ausreichend informieren und in der Lage sind, eigenständig Gegenmassnahmen aktiv zu nutzen.

Zu den Risiken, die mit Persönlichkeitsprofilen im Internet verbunden sind, gehören Identitätsdiebstähle, Belästigungen, Verfolgungen, Demütigungen und verzerrte Persönlichkeitsbilder.

Im Folgenden werden Beispiele von Selbstdatenschutz aufgezeigt.

Basisschutz

Der Basisschutz gehört zu den Verbraucherpflichten und genügt, um viele Angriffe aus dem Internet erfolgreich abzuwehren.

Der Basisschutz ist leicht herzustellen. Zu ihm gehören der aktive Einsatz von einem Anti-Malware-Programm und einer Personal Firewall sowie die Nutzung der automatischen Updates von den Betriebssystemen und den Anwendungsprogrammen. Ausserdem sind die Verwendung von Anti-Spyware-Programmen, die Durchführung von regelmässigen Backups und der gesunde Menschenverstand Sicherheitsmassnahmen des Basisschutzes[2].

Eine Gesellschaft, die wirtschaftlich und politisch auf die Eigenverantwortlichkeit des Einzelnen setzt, muss auch schützen, was diesen als Sozialwesen und als Wirtschaftsfaktor ausmacht: seine persönliche Integrität und seinen materiellen Besitz.

Internetbrowser sinnvoll einstellen und richtig nutzen

Der Internetbrowser ist das Tor zur Internet und das wichtigste Hilfsmittel für die Internet-Nutzer, um Informationen zu sammeln, Bankgeschäfte zu erledigen, einzukaufen, mit Freunden zu chatten, Zeitung zu lesen oder zu spielen. Daher ist es im Sinne des Selbstdatenschutzes wichtig, dass die Internet-Nutzer einerseits einen sicheren Browser verwenden, anderseits aber auch wissen, wie dieser funktioniert und wie er sicher und vertrauenswürdig zu bedienen ist.

Ein Beispiel ist die Statusleiste im Browser, welche die Internet-Nutzer unbedingt verstehen und nutzen sollten. Hier wird die Zieladresse eines Links angezeigt. Wenn der Internet-Nutzer den Mauszeiger auf einen Link bewegt, ohne ihn anzuklicken, wird automatisch die Zieladresse angezeigt. Zeigt die Statuszeile nicht das gewünschte Ziel, sollte der Link nicht geklickt werden. Durch dieses Wissen und Überprüfen lässt sich beim täglichen Surfen so mancher Angriff vermeiden.

Eine weitere einfache Möglichkeit des Selbstdatenschutzes ist die Möglichkeit, Werbung und aktive Inhalte aktiv zu blocken. Sperren Sie bei aktuellen Gefahren «Aktive Inhalte» so lange, bis die Sicherheitslücken wieder geschlossen sind. AdBlocker, wie AdBlock, NoScript, Flash Control usw. sind empfehlenswert, weil sie die Sicherheit erhöhen.

Besondere Schutzmassnahmen gegen das Tracking

In diesem Abschnitt werden ein paar Beispiele aufgezeigt, wie sich ein Internet-Nutzer vor dem Tracking, im Sinne des Selbstdatenschutzes, schützen kann.

- *Browser:* Im Browser werden standardmässig temporäre Dateien angelegt: Cookies, Cache, Logins. Diese temporären Dateien sollten regelmässig gelöscht und deaktiviert werden. Funktionen wie «Passwörter speichern» oder «Auto-Vervollständigung» sollten nicht genutzt werden. Cookies und History/Chronik sollten regemässig gelöscht werden. Auch die Datenschutzeinstellungen, wie z.B. der Private-Mode helfen, sich selbst zu schützen.
- *Proxy-Server (Web-Server):* Ein Proxy-Server ist ein spezieller Server im Internet, der als Vermittler arbeitet. Der Proxy-Server kann auf einer Netzwerkseite Anfragen entgegennehmen, um dann über seine andere Netzwerkseite mit der Adresse des Proxy-Servers eine Verbindung zur anderen Webseite herzustellen. Surft ein Internet-Nutzer über einen Proxy-Server, bleibt die tatsächliche IP-Adresse des eigenen Endsystems (PC, Notebook, Smartphone, …) dem Webserver verborgen, was eine gewisse Anonymität schafft. Über Signaturen, wie das verwendete Betriebssystem, Browser, installierte Plugins, Zeitzone usw. kann diese Anonymität in vielen Fällen ausgehebelt werden.

Weitere Mechanismen für die Anonymität im Internet: Es gibt noch weitere Mechanismen für die Anonymität im Internet, wie z.B.:

- *VPN-Proxy-Server,* der eine verschlüsselte Kommunikation zum Proxy-Server anbietet;
- *Tor-Projekt (Onion Routing Projekt):* Tor ist ein Netzwerk zur Anonymisierung von Verbindungsdaten. Es wird für TCP-Verbindungen eingesetzt und kann beispielsweise zum Surfen und für weitere Dienste verwendet werden. Das Tor-Netzwerk schützt vor der Analyse des Datenverkehrs und basiert auf der originalen Idee des Onion-Routings. Ein enormer Nachteil des

Literatur

- Linnemann Markus/Pohlmann Norbert, «Sicherheit im Internet – Tipps und Tricks für das digitale Leben. Orell Füssli Verlag, 2010.
- Pohlmann Norbert, Daten gegen Diebstahl sichern, Wirtschaftsspiegel, IHK Münster, 2/2013.
- Pohlmann Norbert/Spogahn Nikolai, Bauchladen – Wie man Googles Dienste umsichtig nutzt, iX – Magazin für professionelle Informationstechnik, Heise-Verlag, 07/2011.
- <http://www.sicher-im-internet.de>.

Fussnoten

1 Pohlmann/Spogahn (2011).
2 Linnemann/Pohlmann (2010).

Tor-Netzwerkes sind die Geschwindigkeitseinbussen, die die aktive Verwendung für Realzeitanwendungen unmöglich macht. Im Rahmen der NSA-Affäre ist klar geworden, dass auch das Tor-Netzwerk keine hundertprozentige Anonymisierung bieten kann.

Zusammenfassung

Die Internet-Nutzer müssen den Wert der Privatsphäre aktiv und gründlich diskutieren, weil er eine sehr wichtige Rolle spielt. Eine Gesellschaft, die wirtschaftlich und politisch auf die Eigenverantwortlichkeit des Einzelnen setzt, muss umgekehrt auch das schützen, was den Einzelnen als Sozialwesen und als Wirtschaftsfaktor ausmacht: einerseits seine persönliche Integrität und andererseits seinen materiellen Besitz. Wenn wir als Gesellschaft nicht mehr in der Lage sind, diese Anforderung zu erfüllen, dann verlieren wir einen Teil der Demokratie, unsere Freiheit. Unsere Reaktionen sind bezogen auf die Schwere des Angriffes auf unsere Privatsphäre, die durch US-Internet-Marktführer und die NSA durchgeführt wird, lächerlich. Hier müssen wir den politischen Druck erhöhen und unsere wirtschaftliche Macht als Internet-Nutzer ausspielen.

Wenn wir die positiven Möglichkeiten der modernen IT und des Internets strategisch nutzen wollen, dann müssen wir in der Zwischenzeit lernen, einen aktiven Selbstdatenschutz umzusetzen. ■

Neuerscheinung aus dem Schulthess Verlag

September 2014
ISBN 978-3-7255-7088-1
330 Seiten, broschiert
CHF 79.00

Staatsschutz oder Datenschutz?

Die Vereinbarkeit präventiver Datenbearbeitung zur Wahrung der inneren Sicherheit mit dem Grundrecht auf informationelle Selbstbestimmung

Zürcher Studien zum öffentlichen Recht, Band 219

Martin Sigrist

In der heutigen Zeit der Terrorismusbekämpfung wird dem Schutz der inneren Sicherheit vermehrt Priorität eingeräumt, selbst unter Einschränkung der Freiheit und der Grundrechte. Dabei manifestiert sich das Spannungsfeld aktueller denn je in der Gegenüberstellung von Datenschutz und Staatsschutz.
Die vorliegende Arbeit zeigt auf, inwiefern präventiv Daten durch den Staat bearbeitet werden können, ohne die Verfügungsmacht des Einzelnen über die persönlichen Daten zu verletzen. Sie folgt dabei der klassischen Grundrechtsprüfung, wobei der Grundrechtsschutz gemäss Bundesverfassung und der Europäischen Menschenrechtskonvention im Zentrum steht. Die Untersuchung umfasst Geschichte, Judikatur und aktuelle Rechtsentwicklung.
Das Werk richtet sich dabei an alle Interessierten in Wissenschaft, Rechtsprechung und Praxis.

Schulthess Juristische Medien AG
Zwingliplatz 2, Postfach, CH-8022 Zürich
Telefon +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28
buch@schulthess.com, www.schulthess.com

Schulthess §
Der Verlag zu Recht

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (inkl. Versandkosten)

Name _____ Vorname _____

Firma _____

Strasse _____

PLZ _____ Ort _____ Land _____

Datum _____ Unterschrift _____

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §