02/2007

datum

Newsletter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

Inhalt

datum ist eine Publikation des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und erscheint zweimal jährlich.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Editorial

Liebe Datenschutzinteressierte

Willkommen zur Lektüre des zweiten *datums* im laufenden Jahr. Der erste Artikel befasst sich mit Facetten des Überwachungsstaats, die teilweise schon so alltäglich sind, dass wir sie gar nicht mehr als Überwachung empfinden. Dabei werden kleine und Kleinstgeräte eingesetzt, die oft unbemerkt bleiben. Der Artikel legt den Fokus auf private Datenbearbeiter, die „Little Brothers" – dies soll aber keine Verharmlosung der staatlichen Überwachung sein, die sich übrigens derselben Mittel und Geräte bedient, sondern Ihre Wachsamkeit gegenüber nicht-staatlichen Datenbearbeitungen, so nötig, erweitern. Der zweite Artikel greift das Thema WLAN auf und dringt noch einmal darauf, die nötigen Sicherheitsmassnahmen zu ergreifen, wenn Sie sich in Ihrem Haushalt, Ihrer Firma oder an öffentlichen Orten dieser Technologie bedienen. In den Kurzrubriken finden Sie wiederum Hinweise auf datenschutzfreundliche technische Neuerungen, Interessantes aus der Presse und Tipps, wie Sie Ihre Rechte in Bezug auf Ihre Krankengeschichte geltend machen können.Eine gute Lektüre wünscht

Eliane Schmid
Redaktionsverantwortliche ◄

Themen

Vom Big Brother zum Little Brother

In Sachen Überwachung der Bürgerinnen und Bürger wird immer wieder der Staat an den Pranger gestellt. Dies geschieht nicht immer zu Unrecht, greift aber zunehmend zu kurz. Denn im Hinblick auf die technischen Entwicklungen der letzten Jahre lohnt es sich, den Schutz der Privatsphäre breiter zu denken.

Überwachung ist keine Erfindung der letzten Jahrzehnte; in Gemeinschaften gab es schon immer Formen von sozialer Kontrolle. Eine neue Dimension aber eröffnete George Orwell mit seinem nach dem 2. Weltkrieg publizierten Science-Fiction-Roman „1984". Mit „Big Brother is watching you" beschrieb er die totale Überwachung des Individuums durch den Staat, der durch versteckte Mikrofone und den Telescreen, eine Art Kombination von Fernsehgerät und Kamera, buchstäblich bis in die hintersten Winkel der privaten Wohnung blicken konnte. Bestandteil dieses umfassenden Überwachungsstaats war aber auch die Bespitzelung und Denunziation durch Nachbarn, Arbeitskolleginnen und sogar die eigenen Kinder. Was sollen Unternehmen, was soll der Staat dürfen?

Über 20 Jahre nach 1984 sind wir heute glücklicherweise noch von dieser Dystopie entfernt. Aber auch in unserem Alltag nimmt die Überwachung, nehmen die Datensammlungen zu. Dabei lohnt es sich, unter dem Stichwort Little Brother einmal genauer zu beleuchten, wo Gefahren für unsere Privatsphäre lauern, die weniger offensichtlich sein mögen als die Kamera auf dem Dorfplatz.

Über die Miniaturisierung der Technik …

Aus heutiger Sicht betrachtet blieben Orwells Vorstellungen der Überwachungsmassnahmen der Zukunft reichlich rudimentär. Real hat die technische Entwicklung des Informationszeitalters ganz andere und viel subtilere Möglichkeiten zur Überwachung von Individuen hervorgebracht. Wo vor 20 Jahren im Zuge der Fichensammlung Informationen auf Papier- oder Kartonkarten festgehalten und diese in Regalen verstaut wurden, können

heute mit den modernen Informationsverarbeitungssystemen in Sekundenschnelle Personendaten verknüpft und detaillierte Persönlichkeitsprofile erstellt werden.

Immer handlichere und billigere Technologien geben nicht nur dem Staat, sondern eben auch Privaten die Mittel in die Hände, andere zu überwachen und unbemerkt oder sogar unsichtbar tief in ihre Privatsphäre einzudringen. Videoüberwachung wird nicht erst seit den Handykameras auch von Privaten betrieben, und dies nicht selten in Unkenntnis der datenschützerischen Vorgaben. Mittels GPS kann man die Bewegungen von Fahrzeugen oder Menschen live verfolgen; für Private erschwingliche Empfänger können auf 10 Meter genau geortet werden. RFID-Chips, meist unbemerkt in Kleidern oder Waren befestigt und bald vielleicht auch in jedem Pass, haben eindeutige Informationen gespeichert, die ohne physischen Kontakt mit entsprechenden Geräten ausgelesen und unter Umständen mit einer bestimmten Person verbunden werden können (s. unten, „Aus der Presse“). Seit kurzem sind Minidrohnen auf dem Markt – mit 18'000 Franken wohl immer noch teuer für einzelne Privatpersonen, für Firmen aber durchaus erschwinglich. Und offenbar kann man mittlerweile gar mit dem eigenen Arm bezahlen – indem man sich einen RFID-Chip unter die Haut einpflanzen lässt, der gewissermassen Kreditkartenfunktionen übernehmen kann.

Alle die geschilderten Überwachungsmöglichkeiten haben wichtige positive Seiten – die Wirtschaft profitiert von vereinfachten Abläufen durch die Computerisierung, die Kundschaft von zielgerichteten Informationen und Angeboten, die Strafverfolgung von Videoaufnahmen und DNA-Datenbanken. Die Kehrseite ist, dass unsere Bewegungen und Aktivitäten täglich in zahlreichen Datenbanken festgehalten und dort sortiert, gesiebt und kategorisiert werden.

… hin zum Pervasive Computing

„Pervasive“ oder „Ubiquitous Computing“ ist der Fachbegriff für die Durchdringung des Alltags mit Informationsverarbeitung. Über Videokameras, RFID-Chips, Kunden- und Kreditkarten, Mobiltelefonie, Bewegungen im Internet etc. werden grosse Datenmengen gesammelt. Das mag auf den ersten Blick harmlos erscheinen, solange diese Daten nicht verknüpft werden; dieser Eindruck wandelt sich aber vielleicht schnell, wenn man bspw. auf Nachfrage bei einem Adresshändler (siehe *datum* 01/06) einen Ausdruck von mehreren A4-Seiten mit Informationen über den eigenen Gesellschaftsstatus, einen allfälligen Telefon-Zweitanschluss, das Auto oder den Lifestyle (kreativ? bodenständig? Powerfrau?) erhält. Da sagt die Rubrik „Sternzeichen“ wohl noch am Wenigsten aus.

Nicht jeder „Little Brother“ bereitet uns Sorgen

Während der Staat seine Personendatensammlungen vornehmlich aus „Sicherheitsgründen“ ausweiten will, verspricht sich die Wirtschaft von möglichst umfassenden Kenntnissen über (potenzielle) Kundinnen und Kunden Wettbewerbsvorteile. Mittels Data Mining, der automatischen Auswertung von Datenbeständen auf der Suche nach bestimmten Mustern, werden Kunden gruppiert und zielgerichtet mit Angeboten bedient. Dabei spielen, gerade im Bankenbereich, bei den Versicherungen und im Handel, Kriterien wie Kreditwürdigkeit durchaus eine Rolle.

Die Gefahren dieser Entwicklung liegen auf der Hand: Es besteht das Risiko einer Diskriminierung von Kunden, die den Kriterien einer bestimmten Zielgruppe nicht entsprechen, da ihnen gewisse Angebote gar nicht erst unterbreitet werden. Zudem weckt erwiesenermassen jede Datensammlung neue Bedürfnisse, und ursprünglich ökonomisch ausgerichtete Datenbanken werden europaweit mehr und mehr auch für die Strafverfolgung hinzugezogen. Die Frage ist, ob die Verhältnismässigkeit hier immer gewährleistet ist.

Am Ende ist Überwachung, ganz im Sinne des Sprichworts „Vertrauen ist gut, Kontrolle ist besser“, auch ein Zeichen von Misstrauen. Soziale Beziehungen basieren jedoch auf Vertrauen – deshalb garantiert der Rechtsstaat den Bürgerinnen und Bürgern bis zum Gegenbeweis die Unschuldsvermutung, die Verfassung das Recht auf Privatsphäre. Wie bei Orwell erfordert der Versuch, sich diese zu erhalten, weiterhin eigene Wachsamkeit und Anstrengung. Im Gegensatz zu Orwells Romanfiguren aber haben wir heute tatsächlich noch Möglichkeiten, unsere Privatsphäre einigermassen abzuschirmen. Gegenüber dem Big Brother, aber auch gegenüber den vielen Little Brothers.

Quellen:

- Surveillance Studies Network, A Report on the Surveillance Society: http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_report.aspx
- NZZ Dossier, 01.06.2007
- Facts, 08.02.2007
- http://daten-chaos.de/2007/09/11/die-rfid-disco-in-rotterdam/
- http://whatis.techtarget.com/definitionsAlpha/0,289930,sid9_alpA,00.html ◄

WLAN – Drahtloses Surfen nicht ganz ohne Fallstricke

Total praktisch: mit dem Laptop im Wohnzimmer nach dem aktuellen Fernsehprogramm surfen, im Schlafzimmer E-Mails versenden, in der Küche Internetradio hören … und das alles ohne Kabelsalat und Stolpergefahr. WLAN macht's möglich – aber gewisse Vorsichtsmassnahmen sind unverzichtbar, wenn das böse Erwachen vermieden werden soll.

Ein böses Erwachen, so berichtete im Sommer dieses Jahres die NZZ am Sonntag, bereitete die Polizei einem Paar, über dessen WLAN kinderpornografisches Material heruntergeladen worden war. Das Paar war unschuldig in Verdacht geraten, weil es sein Funknetz unzureichend geschützt und somit Drittpersonen eine Pforte ins Internet geöffnet hatte. Um solche Unannehmlichkeiten zu vermeiden, müssen Sie entsprechende Vorkehrungen treffen. Dazu hat der EDÖB kürzlich einige Erläuterungen aufgeschaltet.

Privates WLAN

WLAN steht für Wireless local area network – also ein drahtloses, lokales Netzwerk, dessen angeschlossene Geräte (Rechner, Drucker, Scanner und andere) via Funk untereinander und oft auch mit dem Internet kommunizieren. Die Vorteile des kabellosen Betriebs liegen auf der Hand – die Nachteile allerdings auch: Ein Funknetz lässt sich nicht durch Hausmauern begrenzen. Ist es also nicht (genügend) geschützt, können Dritte in Reichweite des Netzes unerkannt mitsurfen. Mit verheerenden Konsequenzen.

Es können zwei Probleme entstehen:

- Problem Trittbrettfahrer: Drittpersonen surfen auf Ihre Kosten in Ihrem WLAN, schmälern dadurch für Sie die Bandbreite und laden eventuell illegale Inhalte herunter. Je nach Inhalt verstösst der Trittbrettfahrer damit meist unerkannt gegen das Urheberrechtsgesetz oder gar gegen das Strafgesetzbuch, nicht jedoch gegen das Datenschutzgesetz.
- Problem Hacker: Drittpersonen hören die Funkkontakte innerhalb Ihres Netzwerks ab oder schleusen sich gar direkt in Ihre Geräte, Ihren Rechner ein und lesen, manipulieren oder stehlen Ihre Daten. Hier liegt die Verletzung der Privatsphäre und damit des Datenschutzgesetzes auf der Hand.

Ergreifen Sie daher die nötigen Massnahmen, um Ihr Funknetz zu schützen. Dazu gehören sichere Passwörter, das Verbergen der Netzwerkidentifikation, die Beschränkung des Zugangs zum eigenen Access Point auf bestimmte Endgeräte und das Ausschalten des Access points bzw. der Geräte bei Nicht-Gebrauch – womit auch noch Strom gespart wird.

Öffentliches WLAN

Es gibt kommerzielle Anbieter, die an öffentlichen Orten (städtische Gebiete, Bahnhöfe, Flughäfen etc.) WLAN-Infrastrukur zur Benutzung anbieten. Umfragen zeigen, dass immer mehr User diese Möglichkeit zum Surfen bereitwillig nutzen. Natürlich ist die Vorstellung, im Stadtpark zu sitzen oder am Flughafen zu warten und dabei seine Emails beantworten zu können, durchaus reizvoll. Auch hier besteht jedoch für den User die Problematik des Hackens.

Stellen Sie also den Schutz des eigenen Gerätes sicher, bevor Sie öffentlich surfen. Richten Sie eine gute Firewall ein, halten Sie Viren- und Spywareschutz auf neustem Stand, benutzen Sie nur verschlüsselte Funkstrecken zum Access point und schalten Sie das Funkelement an Ihrem Laptop aus, wenn Sie gerade nicht auf dem Internet sind. Das spart erst noch Akku-Power.

In einem öffentlichen Netz können Sie zwar nicht wegen illegaler Downloads anderer Benutzer unter Verdacht geraten. Mit den beschriebenen Schutzmassnahmen verhindern Sie jedoch, dass Ihre persönlichen Daten, Fotos oder Filme plötzlich auf dem Internet verbreitet werden.

Nähere Informationen zu den Schutzmassnahmen finden Sie unter

- http://www.edoeb.admin.ch/themen/00794/01124/01160/index.html?lang=de

Quelle:

- NZZ am Sonntag, 03.06.2007 ◄

Kurz beleuchtet

Verschlüsselung – ganz einfach

Das kostenlose Programm „LockNote" der Firma Steganos ermöglicht es, auf unkomplizierte Weise Textdateien zu verschlüsseln. Eine aufwendige Softwareinstallation ist nicht erforderlich: Es genügt, die Programmdatei nach dem Herunterladen an einem geeigneten Ort abzulegen – bspw. auch auf einem USB-Stick. LockNotes kann zweierlei: erstens ist es ein einfacher Texteditor, mit dem Sie Ihre Ideen, aber auch Ihre Passwörter und Zugangsdaten in verschlüsselter Form festhalten können (sofern Sie für letztere kein spezielles Passwort-Verwaltungsprogramm wie „Password Corral" verwenden); zweitens können Sie mit dem Programm bereits bestehende Textdateien nachträglich verschlüsseln. Das Programm generiert in beiden Fällen ausführbare (exe-)Dateien, die nur nach Eingabe des richtigen Passworts geöffnet werden können. Für technisch interessierte Leserinnen und Leser: Als Algorithmus verwendet LockNote einen AES 256-bit-Schlüssel.

- http://www.steganos.com

Aus der Presse

Piercing mal ein wenig anders

Im April 2006 berichtet der Tages-Anzeiger über den Selbstversuch eines Amerikaners, sich das alltägliche Leben mittels implantierten RFID-Chips etwas zu vereinfachen. RFID steht für Radio Frequency Identification, zu Deutsch in etwa „Funkidentifizierung". Diese Funkchips waren ursprünglich für wirtschaftliche Zwecke entwickelt worden und werden zur Warensicherung, zur Lagerbewirtschaftung und seit einiger Zeit auch, als Ersatz für den Strichcode, bei Self-Scanning-Systemen in Supermärkten eingesetzt. Sie haben den Vorteil, dass sie auf bestimmte Distanz berührungslos ausgelesen werden können. In den USA werden implantierte Chips bereits im Gesundheitswesen eingesetzt. Der Amerikaner

Amal Graafstra benutzt die Chips in seinen Händen, um die Haustüre aufzuschliessen oder den Computer zu entsichern. Er sieht sich als Pionier „einer neuen Generation von Menschen, die Computertechnologie ganz selbstverständlich in ihren Körper integrieren“, und hat über seine Erfahrungen ein Buch geschrieben (s. unten). Der EDÖB warnt, im Verbund mit anderen Datenschützern, immer wieder vor zu exzessivem Gebrauch dieser Technologie, die die Privatsphäre massiv gefährden könnte, ermöglicht sie doch Verknüpfungen mit der Identität des Trägers, unbefugtes Orten seines Aufenthalts und damit die Erstellung seines Bewegungsprofils.

Quelle:

- Tages-Anzeiger 3.4.2006

Literaturhinweis:

- Graafstra, Amal. RFID Toys: 11 Cool Projects for Home, Office and Entertainment.

Tipps

Krankengeschichte: Wie kommen Sie an Ihre Daten heran?

Laut Bericht des Beobachters vom letzten Frühjahr haben Patientinnen und Patienten immer wieder Probleme damit, Einsicht in ihre eigene Krankengeschichte zu erlangen. Eine Krankengeschichte besteht aus einer Sammlung von Personendaten, und das Datenschutzgesetz räumt jedem Individuum das Recht ein, jederzeit Auskunft über die eigenen Daten zu verlangen – und zwar grundsätzlich kostenlos. Offensichtlich ist dies nicht allen Ärztinnen und Ärzten bekannt.

Einsicht in die Krankengeschichte ist vor allem bei Arztwechsel, vor dem Einholen einer Zweitmeinung oder beim Verdacht auf Fehlbehandlungen ratsam. Auf der Website des EDÖB finden Sie die entsprechenden Musterschreiben und weitere, detaillierte Informationen zu diesem Thema.

Quelle:

- Beobachter, 30.03.2007

Weitere Informationen:

- http://www.edoeb.admin.ch/themen/00574/index.html?lang=de
- http://www.privatim.ch/content/pdf/_PRIVATIM_Patientenbrosch_D.pdf

Update

Unter Themen/Datenschutz/Sonstige Themen/Schwarze Listen finden Sie neu die Vorgaben des EDÖB für die Erstellung von Schwarzen Listen über ungebetene Gäste.

Unter Themen/Datenschutz/Internet/Peer-to-Peer nimmt der EDÖB Stellung zu den Anstrengungen in der Bekämpfung der Produktepiraterie im Internet.

In der Zeitschrift Managed Care 5/07 erläuterte ein Spezialist des EDÖB die Bedeutung der Einverständniserklärung im Zusammenhang mit der Speicherung medizinischer Daten auf der Versichertenkarte. Den Artikel finden Sie auf unserer Webseite unter Dokumentation/Datenschutz/Artikel, Referate, Gutachten.

Weiterhin werden unter Dokumentation/Öffentlichkeitsprinzip/Empfehlungen laufend die neuen Empfehlungen im Rahmen des Öffentlichkeitsgesetzes aufgeschaltet.

- http://www.derbeauftragte.ch

Agenda 2008

28. Januar	2. Europäischer Tag des Datenschutzes – Der EDÖB wird an diesem Tag mit Chat- und Hotline-Angeboten der Bevölkerung zur Verfügung stehen.
März	*datum* 01/2008