Wie Sie online Ihre Privatsphäre (halbwegs) behalten

War früher die Preisgabe persönlicher Informationen an ein Gegenüber oder an eine Form von Korrespondenz geknüpft, so geschieht sie heute beiläufig und unbemerkt. Schon bei der einfachen Benutzung von Internetdiensten, beim Akzeptieren von Dialogrückfragen, beim Auswählen von Artikeln und natürlich bei der ubiquitären Google-Suche entstehen Datenspuren. Diese werden gespeichert, ja gehortet, aggregiert zu Nutzerprofilen, ausgewertet und gehandelt. Die Dimension dieser Vorgänge ist nur schwer vorstellbar. Alle digitalen Daten sind sofort verfügbar, können jederzeit verdoppelt, verteilt und auf der ganzen Welt gespeichert und ausgewertet werden. Jetzt und für immer.

Kritische Auseinandersetzung mit dem allgegenwärtigen Dienst, seinen Ablegern und Praktiken tut Not und beginnt sich auch im deutschsprachigen Raum zu etablieren. www.googlefalle.com/googlefalle/ bzw. www.googlefalle.com

Scroogle „anonymisiert" Ihre Suchanfrage und sendet sie dann zu Google und werbefrei zurück. www.scroogle.org/

Privatsphäretipp 1

Geben Sie möglichst wenig Informationen von sich weiter.
Widerstehen Sie Verlockungen und Versprechungen, die meist nur zum Abgreifen von Daten entwickelt werden. Machen Sie keine Branchen-, Umsatz- oder andere sensible Angaben. Erinnern sie sich, dass alles, was Sie eingeben (praktisch immer mehrfach) gespeichert, ausgewertet und weitergegeben wird. Internationale Anbieter (wie Google) agieren frei von deutschen Datenschutzgesetzen.

Privatsphäretipp 2

Nehmen Sie Ihren Browser an die Leine.
Vom Browser werden kleine Dateien abgelegt, die eine Identifizierbarkeit ermöglichen. Für den Nutzer bringen sie nur eine kleine Bequemlichkeit, für den Seitenbetreiber die Möglichkeit, ihr Verhalten (auf seinen Seiten) zu verfolgen. Löschen Sie daher regelmäßig die Browser-Cookies. Bei Firefox unter Einstellungen/Datenschutz/Cookies anzeigen, dann löschen. Wer genau wissen möchte, was sich hinter den Datenplätzchen verbirgt, der findet alles nötige hier: http://de.wikipedia.org/wiki/HTTP_Cookie

Lassen Sie Ihren Browser möglichst wenig speichern. Neben Cookies werden auch auf andere Art Daten auf Ihrem Rechner gesichert. Beispielsweise mit der Flash-Animationstechnologie, deren Einstellungen können Sie unter www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager03.html selbst verändern. Achtung, das ist keine herkömmliche Website, sondern alle Einstellungen, die Sie sehen, wirken auf Ihren Rechner. Stellen Sie die erlaubte Speichergröße auf 0 KB im Reiter „Globale Speichereinstellungen".

Eine weitere Ablagemöglichkeit sind so genannte „Supercookies" (DOM Storage). In Firefox können Sie die Einstellungen vornehmen indem Sie in die Adresszeile eingeben: about:config. Dann suchen Sie nach dem Eintrag „dom.storage.enabled" und setzen ihn durch Doppelklick auf „false".

Sichere Browsereinstellungen finden sich unter: www.pcwelt.de/start/sicherheit/firewall/praxis/195075/so_schuetzen_sie_ihren_browser/ oder www.computerwoche.de/mittelstand/1891877/

Privatsphäretipp 3

Geizen Sie mit Ihrer E-Mail-Adresse.
Viele Dienste verlangen Ihre Mail-Adresse für die Zusendung eines Links, einer Kennung etc. Danach werden Sie meist zum Adressaten für Werbemails. Verwenden Sie daher eine eigene Mail-Adresse für Kataloganfragen, Kundenformulare, Umfragen etc. Diese Adresse muss nicht Ihren Namen enthalten, verwenden Sie lieber ein Pseudonym.

Für einmalige zum Beispiel Zusendung einer Registrierung für einen Dienst oder eine Software hilft ein eigener Dienst. Mailinator das Einmal-Postfach ist originell und hilfreich. Im Handumdrehen lassen sich so Registrierungen vornehmen oder einmalige Anfragen stellen, ohne dass anschließend das Postfach überquillt www.mailinator.com.

Privatsphäretipp 4

Hören Sie nicht auf Hoaxes.
Hoaxes sind E-Mail-Scherze, bei denen die Welle der Weiterleitungen von den Urhebern als „Erfolg" verbucht wird.

Aktuelle Meldungen sowie den Stand der Dinge zu offiziellen Vorhaben, Bestimmungen etc. findet man beim Beauftragten der Bundesregierung für Informationstechnik. www.cio.bund.de

Der Spion in meinem Rechner oder was ist eigentlich Spyware? Ausführlich erklärt und gleich mit Links zu Test- und Säuberungssoftware. Ein Service des Datenschutzbeauftragten in Bremen. www.datenschutz-bremen.de/sv_internet/spyware.php

Wenn Sie jemand davon überzeugen will, dass eine Firma etwas verschenkt, wenn Sie eine Nachricht an alle Ihre Kontakte weiterleiten oder aber ein armes krankes Kind sich immer schon die Weiterleitung einer E-Mail gewünscht hat oder viele andere „gute" Gründe Sie zum Weiterschicken einer Nachricht überreden wollen, seien Sie kritisch, halten Sie ein. Meist handelt es sich um einen E-Mail-Kettenbrief auch Hoax genannt. Auch verschickt weder Microsoft noch irgendeine andere Firma Viruswarnungen unaufgefordert. Dafür gibt es Informationsdienste, die man bestellen kann. Welche Ketten-Mails bereits bekannt sind und zahlreiche andere Sicherheitsinformationen bietet die TU-Berlin gut aufbereitet http://hoax-info.tubit.tu-berlin.de/hoax/.

Privatsphäretipp 5

Widerstehen Sie Verlockungen.
Das unschlagbar günstige Auto auf eBay, die kostenlose Wundersoftware oder die ganz besonders günstige (weil illegale) Markensoftware hat schon viele teures Lehrgeld zahlen lassen. Die Betrugsmöglichkeiten und Methoden wachsen schneller als man sie im Blick behalten kann. Lassen Sie den gesunden Menschenverstand walten. Professionell genutzte Rechner benötigen professionelle Software, die ihren Preis hat. Vermeintliche Superschnäppchen sind meist Fallen. Bei Ihnen unbekannten Händlern suchen sie zum Beispiel „Firma XYZ Erfahrungen", um zu sehen, wie es anderen beim Kauf erging.

Privatsphäretipp 6

Meiden Sie Google-Dienste.
Ja, Sie haben richtig gelesen. Google befindet sich auf dem Weg zum alles beherrschenden Datenriesen mit vollkommen unkalkulierbaren Folgen. Alle Mails an und vom Google Mail-Dienst werden auf Stichworte durchsucht und alle, auch gelöschte Mails, werden von Google gespeichert! Google zensiert und manipuliert nicht nur in China seine Suchergebnisse. Suchbegriff, IP-Adresse, Browsereinstellungen, Datum und Uhrzeit sowie der Ort werden bei jeder (!) Suchanfrage gespeichert. Vor diesem Hintergrund ist die Aussage, Google sei ein gigantischer Trojaner, der unbemerkt Daten für unbekannte Zwecke sammelt, durchaus berechtigt.

Immer mehr Bereiche werden mit „kostenlosen" Angeboten von Google abgedeckt, Google, Gmail, GoogleMaps, GoogleBooks, GoogleDocs, Picasa, Youtube, ... Kritische Stimmen und Fakten nehmen zu. Eine Studie aus der Universität Graz zeigt die realen Gefahren www.iicm.tu-graz.ac.at/iicm_papers/dangers_google.pdf. Eine kritische Themensammlung erläutert die Lage www.google-watch.org/

In Wikipedia werden viele Sicherheitsaspekte betrachtet http://en.wikipedia.org/wiki/Google_and_privacy_issues.

Alternative Suchdienste:
www.bing.com/?cc=de
http://de.search.yahoo.com/

Privatsphäretipp 7

Machen Sie einen Sicherheitscheck.
Verschiedene technische Ebenen greifen ineinander und gehören überprüft und gegebenenfalls abgesichert oder richtig eingestellt, um sicher online arbeiten zu können. Betriebssystem, Browser, Programme, DSL- und WLAN-Router, Mobilgerät/Handy etc. Organisatorische Maßnahmen und das Einhalten der obigen Grundregeln ergänzen den Checkup. Fertigen Sie eine Liste an, was Sie wann kontrolliert und wie eingestellt haben.

Den aktuellen Stand von Sicherheitsempfehlungen und Warnungen bietet Bürger CERT, ein Dienst des Bundesamtes für Sicherheit in der Informationstechnik (BSI) www.buerger-cert.de und www.sicher-im-netz.de.

Professioneller und umfangreicher sind die IT-Grundschutzkataloge und Informationen, die sich beim BSI finden. www.bsi.bund.de/cln_164/ContentBSI/grundschutz/kataloge/kataloge.html

Privatsphäretipp 8

Sichern Sie Ihre Daten.
Es kann nur immer wieder wiederholt werden. Es gibt Menschen, die Daten verloren haben und welche, die noch Daten verlieren werden (weil sie sie nicht gesichert haben). Die Gefahrenquellen sind so zahlreich, dass hier nur die Spitze des Eisbergs anklingen kann: Versagen (von Mensch, Maschine und Software), Verlust, Beschädigung, Fehlbedienung, Diebstahl, Unfall usw. Installieren Sie eine professionelle automatische Sicherungssoftware, lagern Sie Sicherungen aus und testen Sie die Wiederherstellung. Nur so können Sie einem Ausfall halbwegs gelassen gegenübertreten (siehe Bayerisches Ärzteblatt, 11/2009, www.blaek.de/presse/aerzteblatt/2009/BAB_1109_584_585.pdf).

Persönliche Datensicherheit ist ein wichtiges und auch komplexes Thema. Hier kann nur ein Einstieg in das Thema vermittelt werden. Eine Beschäftigung mit der eigenen Position und daraus abgeleitetem Verhalten ist nötig und vermittelt nebenbei einen besseren Einblick in die Mechanismen des Web.

Seien Sie ein sicherer Surfer!

Dr. Marc M. Batschkus, Arzt, Medizinische Informatik, Spezialist für eHealth, eLearning & Mac OS X, Steinstraße 40, 81667 München, E-Mail: mail@batschkus.de