Private Sicherheit im Internet

Studie und Lösungshinweise

Autor Kay Golze

Inhaltsverzeichnis

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Bei der Zusammenstellung der Texte, Verweise und Abbildungen wurde mit größter Sorgfalt vorgegangen; trotzdem ist ein vollständiger Fehlerausschluß nicht möglich. Die nachfolgende Dokumentation erfolgt daher ohne Gewähr für Richtigkeit, Vollständigkeit oder Funktionalität der gemachten Angaben, für deren Verifizierung oder Nutzung allein der Anwender die Verantwortung trägt. Die WIPN Gruppe oder der Autor übernimmt für aus der Verwendung dieser Dokumentation entstehende Schäden, gleich aus welchem Rechtsgrund, eine Haftung nur im Falle vorsätzlichen oder grob fahrlässigen Handelns für die eigenen Texte; im übrigen ist die Haftung von der WIPN Gruppe oder des Autors ausgeschlossen. Die WIPN Gruppe oder der Autor übernimmt keine Verantwortung oder Haftung für Programme, Inhalte von anderen Studien, Inhalte von Internetseiten oder Veröffentlichungen Dritter.

Die Studie basiert auf Informationen aus dem Internet, der Studie von der Firma Xamit Bewertungsgesellschaft mbH und der SAP AG im Rahmen des SAP Pocketseminar, Herausgegeben für die Sicherheitsinitiative „Deutschland sicher im Netz“ (https://www.sicher-im-netz.de). Alle Daten wurden in 2007 bzw. teilweise bis Feb. 2008 erhoben.

Im folgenden wird der Begriff **Datenschutz** verwendet. Er bezeichnet den Schutz personenbezogener Daten vor Missbrauch.

Kurze Lesezeit

In kurzer Zeit können Sie das ganze Buch lesen. Sollten Sie jedoch über weniger Zeit verfügen, können Sie gezielt nur die Stellen lesen, die für Sie wichtige Informationen enthalten.

- Kapitel „Übersicht“ leitet in das Thema ein und bringt das Thema auf den Punkt. Das Kapitel sollte gelesen werden, wenn keine Zeit für Details vorhanden ist und nur die grobe Linie erfaßt werden soll. Das Kapitel „Datengipfel des BMI im Sommer 2008“ sollte wegen aktueller Entwicklungen mitgelesen werden.
- Kapitel „Zusammenfassung“ faßt den Inhalt und die Aussagen der Studie zusammen. Das Kapitel eignet sich für den Einstieg zur Entwicklung eines Verständnisses zum eigenen präventiven Schutz. Das Kapitel „Datengipfel des BMI im Sommer 2008“ sollte wegen aktueller Entwicklungen mitgelesen werden.
- Details ab dem Kapitel „Internetbeobachtung im Jahr 2007“.
- Hinweise auf aktuelle Entwicklungen im Kapitel „Datengipfel des BMI im Sommer 2008“.
- Konkrete Anleitungen für die Verbesserung der Sicherheitsmaßnahmen im Kapitel „Lokale Programme“. Für Details sollte ab „Einstieg in ein Sicherheitskonzept“ begonnen werden.
- Ein Verzeichnis am Anfang des Buches erleichtert das Nachschlagen.

Copyright © 2008 Kay Golze

Übersicht

Das Internet hat sich zu einem der wichtigsten und zukunftsweisenden Medien für Privatpersonen, Unternehmen, Universitäten, öffentlichen Einrichtungen und Anderen des gesellschaftlichen Lebens entwickelt. Mit dieser Entwicklung entstehen und entstanden neue Märkte, über die die Öffentlichkeit in der Regel keine Kenntnis hat. Ein bereits jetzt Milliarden umfassender Markt hat sich mit dem Handel von persönlichen Daten und Datenprofilen weltweit entwickelt. Die Erfassung von Daten aus dem Internet und die damit erstellten Profile sind eine im Bewusstsein der Öffentlichkeit nicht bekannte Ware. Die Profile werden u.a. durch Beobachtung von Web-Seiten und anderen Internetbenutzern erstellt. Dabei ist dem normalen Benutzer in der Regel nicht bekannt, daß seine lokalen Sicherheitseinrichtungen, einschließlich Firewalls, prinzipbedingt gegen die zur Beobachtung eingesetzten Technologien keinen Schutz bieten. Jeder Mensch und jedes Unternehmen, jedes Institut, jeder Verein, jede öffentliche Einrichtung und jedes Ministerium hat Geheimnisse. Alle Informationen, die nicht für Dritte bestimmt sind, benötigen Schutz und Vertraulichkeit, die im Internet nicht gegeben ist. In der hier erarbeiteten Studie konnte festgestellt werden, das im Bereich der Internetbeobachtung erhebliche Defizite im Umgang mit persönlichen Daten zu verzeichnen sind. Private Unternehmen wie z.B. eTracker, Google und Andere bieten zur Ermittlung von statistischen Daten Services an, die den Besuch auf Internetseiten beobachten und zu Profilen zusammenstellen. Dabei werden Techniken angewandt, die eine Individualisierung der erstellen Profile ermöglichen. Die über diese Technik ermittelten Daten entziehen sich jeder öffentlichen oder rechtlichen Kontrolle. Durch die Internationalisierung der Unternehmen und dem länderübergreifenden Internet, entstehen somit unbekannte Datenströme von privaten Informationen, Profilen und persönlichen Daten, die als Ware in internationalen Märkten ohne jegliche Kontrolle gehandelt werden. So können z.B. Unternehmen mit ihren leitenden Mitarbeitern beobachtet werden und von Investmenthäusern zur Analyse von Übernahmen herangezogen werden. Möglicherweise können ausländische Unternehmen Profile von deutschen Unternehmen mit ihren Beziehungen zu Lieferanten, Universitäten, Anwälten, Patentämtern oder anderen Unternehmen käuflich erwerben, um Informationen über Innovationen, Projekte oder andere wichtige Firmendaten zu erhalten. Werden persönliche Profile z.B. von Entscheidungsträgern zu einer internationalen Ware, mit der Milliarden verdient werden können, liegt die Gefahr der Manipulation in greifbarer Nähe. Sind von vielen Entscheidungsträgern einer Gesellschaft die Profile eine Ware, mit der Geld in anderen Ländern verdient werden kann, besteht die Gefahr für eine Gesellschaft, ihren „freien Willen“ zu verlieren. Ein Schutz SEINER persönlichen Daten ist also bereits bei jedem Internetbesuch ein Anliegen, das bisher noch darauf wartet entdeckt zu werden. Die Entwicklung von Technologien und Infrastrukturen zur Sicherung der persönlichen Daten wird ein weiterer Schritt in der Entwicklung des Internet sein, der zu einem weiteren Nutzungsschub beitragen wird.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Zusammenfassung

Die Erfassung von Daten aus dem Internet und der Handel mit den daraus erstellten Profilen ist ein Milliarden schweres Geschäft, in dem der Staat bereits mit integriert ist. Bei dieser hier vorgestellten ersten Betrachtung werden die Themenbereiche von direkten Einbrüchen in Rechner (Stichwort „Bundestrojaner“) nicht behandelt. Auf dieses Thema wird in den Kapiteln (siehe auch Lokale Programme) des Dokuments gesondert eingegangen, jedoch wegen der eigenen Komplexität nicht ausführlich behandelt. Die hier beschriebenen Techniken werden lediglich für Beobachtungen im Internet eingesetzt. Die sich aus diesen indirekt ermittelten Daten ergebenen Profile sind jedoch bereits sehr umfangreich und aussagekräftig. Deshalb muss an dieser Stelle darauf hingewiesen werden, daß ein Einsatz einer Firewall – wie gut sie auch direkte Angriffe aus dem Internet abwehren mag – prinzipbedingt keinen Schutz vor dem Ausspionieren von Unternehmen oder Privatperson bietet.

Jeder Mensch und jedes Unternehmen, jedes Institut, jeder Verein, jede öffentliche Einrichtung und jedes Ministerium hat Geheimnisse. Alle Informationen, die nicht für Dritte bestimmt sind, benötigen Schutz und Vertraulichkeit. Kein Unternehmen möchte seine Kundenbeziehungen, Forschungspläne, Steuerdaten oder Projektaktivitäten anderen Konkurrenten zur Verfügung stellen. Keine Privatperson möchte seine Krankengeschichte, finanziellen Verhältnisse oder andere persönliche Dinge (Familienverhältnisse; sexuelle Neigungen oder Vorlieben; zukünftige persönliche Absichten; Suche nach neuer Arbeit wenn z.B. Jobbörsen im Internet aufgesucht werden, etc.) öffentlich von Dritten verwertet wissen.

Die Xamit-Studie, auf die hier Bezug genommen wird (siehe auch Internetbeobachtung im Jahr 2007), hat gezeigt, daß bereits in dem Feld der Internetbeobachtung erhebliche Defizite im Umgang mit persönlichen Daten zu verzeichnen sind. Im besonderen wenn die Unternehmen, die ihren Service zur Internetbeobachtung anbieten, keinen Sitz in Deutschland haben, sondern ihren Statistikservice von einem anderen Firmensitz außerhalb Deutschlands anbieten. Berücksichtigt man noch die weltweite Vernetzung des Internets, wandern Daten somit grenzenlos durch alle Länder und können von unzähligen „Mithörern“ zu ganz eigenen Profilen zusammengestellt werden. Ein Schutz SEINER persönlichen Daten ist also bereits bei jedem Internetbesuch ein Anliegen, das bisher noch darauf wartet entdeckt zu werden.

Diese Vorgänge sind vor allem dann von erheblicher Bedeutung, wenn auf der einen Seite vom Bundesverfassungsgericht Urteile zur Informellen Selbstbestimmung verfaßt werden, diese Rechtsprechungen jedoch in der Praxis von staatlichen Einrichtungen offensichtlich missachtet werden (siehe auch Internetbeobachtung im Jahr 2007). Die in der Studie ermittelten Fakten bekommen eine noch größere Bedeutung, wenn davon ausgegangen werden muss, daß in Zukunft immer mehr Dienste der öffentlichen Hand über das Internet angeboten werden sollen (eGovernment). Bürger und Unternehmen werden über diese Angebote gezwungen, ihre Verwaltungsvorgänge über das Internet abzugeben. Diese sehr persönlichen

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Verwaltungsvorgänge gehen jedoch keinen Dritten etwas an (Urteil BVG vom 11.03.2008 BvR 256/08, 27.02.2008 BvR 370/07). Die Studie hat bewiesen, daß die Anonymität, die für diese persönlichen Daten notwendig ist, damit die Daten vertraulich zwischen der Verwaltungsbehörde und einer Privatperson oder einem Unternehmen ausgetauscht werden können, nicht vorhanden ist. Der Staat hilft außerdem mit der Nutzung von Profilern aktiv ausländischen Unternehmen (Google, eTracker, NetStat, WebTrack und andere Profiler), Daten über seine Staatsbürger und Unternehmen preis zu geben. Zusätzlich gibt der Staat den Profilern einen tiefen Einblick in sein eigenes Handeln von Verwaltungsaufgaben.

Zur Vollständigkeit soll hier darauf hingewiesen werden, daß nach §15 Abs. 3 TMG Nutzungsdaten „für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien“ verwendet werden, wenn diese mit Pseudonymen arbeiten und der Besucher nicht widersprochen hat! Der Benutzer muss also explizit gefragt werden, ob er sein Widerspruchsrecht ausüben will oder nicht, wenn ein Profiler seine Daten ermitteln sollte. Dieses Widerspruchsrecht konnte jedoch nach Auswertung der Xamit-Studie in keinem Fall aktiv bei einem Besuch der untersuchten Internetpräsenzen ausgeübt werden. Die erstellten Profile werden u.a. von Google nicht gelöscht, so daß auch zukünftige Auswertungen mit Personenbezug nach Googles Ermessen möglich sind. Haftung und Verantwortung für eine gesetzeskonforme Handhabe der ermittelten Daten verbleiben indes beim Betreiber als Auftraggeber. Wie der Widerspruch gegen die Erstellung eines Profils/Bewegungsprofils von einem Unternehmen oder einer Privatperson technisch umgesetzt werden soll, lässt der Gesetzgeber offen.

Es muss auch darauf hingewiesen werden, daß es bereits fortgeschrittene Techniken gibt, die die Beauftragung eines Profilers zur Erhebung von Besuchsdaten auf einer Internetseite nicht benötigt. Zusätzlich muss nochmals unterstrichen werden, daß offensichtlich ein prinzipieller Mangel eines Rechtsvollzug/Rechtsverfolgung im Internet, egal welches Rechtssystem offensichtlich zur Anwendung kommen würde, vorhanden ist. Die Folge ist, daß ein wirksamer Schutz aller Menschen eines Staates/Rechtsraumes und eine wirkungsvolle Verfolgung gegen Rechtsverstöße nicht mehr von den dafür zuständigen Organen umgesetzt wird. Wenn sich zusätzlich staatliche Bundes- und Landeseinrichtungen nicht an die gesetzlichen Rahmenbedingungen des eigenen Landes halten, ist eine gesellschaftlich gefährliche Entwicklung in Gang gesetzt.

Die Sicherheit eines Rechners, und die darin enthaltenen Daten, wird durch die lokalen Programme selbst und die Kommunikation über das Internet bestimmt. Die Kommunikation eines Rechners mit einem anderen Rechner über das Internet kann und wird beobachtet, protokolliert und ausgewertet. Wer mit wem eine Verbindung aufbaut, welche Internetseiten aufgerufen werden und welche Eingaben auf Internetseiten vorgenommen werden, wird mit anderen Daten z.B. bei Google, Yahoo, etc. zu individuellen Profilen zusammengestellt. Dabei spielen Cookies eine besondere Rolle. Bei der Identifikation eines individualisierten Rechner sind Cookies eine einfache aber wirksame Schlüsseltechnologie.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Wenn unsere Daten in Tausenden internationaler Datenbanken abgelegt sind, müssen wir uns damit abfinden? Ist vor diesem Hintergrund ein freier Wille noch realisierbar? Nach der Auffassung des Autors muss der erste Schritt darin bestehen, daß bei Unternehmen, Instituten, Wissenschaft, Gerichten und privaten Personen ein Bewußtsein für die wirklichen Verhältnisse im Internet entsteht. Wie im Kapitel „Zusammenfassung zur Netzbeobachtung“ (siehe ausführliche Beschreibung) angemerkt, wäre eine Kapitulation vor der Sammel- und Auswertewut eine Wende in der gesellschaftlichen Entwicklung, daß von keiner Seite gewollt werden kann. Durch die immer detaillierteren Profile von Unternehmen und Personen als Grundlage/Ware für internationale Geschäfte von anderen privaten Unternehmen, kann die Gefahr ausgehen, daß die Ausübung des freien Willen z.B. von Unternehmensführungen nicht mehr möglich ist. Sind detaillierte persönliche Profile von Entscheidungsträgern eine Ware die gehandelt wird, dann liegt die Gefahr der Manipulation in greifbarer Nähe. Sind von vielen Entscheidungsträgern einer Gesellschaft die Profile eine Ware, mit der Geld verdient werden kann, dann besteht die Gefahr für eine Gesellschaft, ihren „freien Willen“ zu verlieren.

Der Verbindungsaufbau zu einem Provider gilt für jeden Internetnutzer in gleicher Weise/Prinzip, egal ob er sich privat oder geschäftlich, von einer Behörde oder aus einer Organisation in das Internet einwählt. Ein Profiler hat nun über eine IP-Adresse, egal ob dynamisch oder statisch, eine Zusatzinformation über den Ort, also das nähere örtliche Umfeld eines Providers, an dem der Internetnutzer gerade angemeldet ist. Auf der Internetseite http://webtools.live2support.com/misc_locate_ip_address.php kann eine IP-Adresse eines beliebigen Computers eingegeben werden. Die Seite ist mit „Location of User Country, State & City by IP address.“ überschrieben und zeigt die entsprechenden Daten über eine IP-Adresse an. Durch den Einsatz von Cookies/Scripten kann ein einzelner PC eindeutig identifiziert werden, auch wenn eine dynamische IP vom Provider vergeben wird. Mit diesen beiden Informationen, IP-Adresse und Cookie, kann ein individueller PC an einem beliebigen Ort eines Landes weltweit lokalisiert und identifiziert werden. Die Erstellung von individuellen Bewegungsprofilen ist somit nur eine Frage, ob sie erstellt werden und nicht ob es machbar ist.

In der Regel müsste ein Missbrauch dieser privaten Daten durch ein Rechtssystem verfolgt werden (siehe erstes Kapitel Internetbeobachtung im Jahr 2007). Das erfolgt jedoch in Deutschland nicht. Obwohl nach dem deutschen Kommunikationsgesetz das Erstellen von Bewegungsprofilen/Kommunikationsprofilen nur durch hohe rechtliche Hürden und bei schweren Straftaten möglich ist, verdienen ohne Rechtsverfolgung internationale Unternehmen genau mit diesen illegalen Praktiken Milliarden Dollar. Vom deutschen Rechtssystem ist also keine Hilfe für den Schutz seiner persönlichen Daten von Unternehmen oder Privatpersonen zu erwarten. Somit muss sich jedes Unternehmen und jede Privatperson, in diesem durch den Rückzug des Rechtssystems frei gegebenen Raum, selbst schützen. Die dazu notwendige Technologie ist bereits vorhanden und kann eingesetzt werden.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

In diesem Dokument sollen einfache, wirkungsvolle und praxistaugliche Hinweise auf Sicherheitsstrategien, einsatzfähige Programme und sinnvolle Konfigurationen z.B. bei Internetbrowsern gegeben werden. Das Dokument ist für Entscheidungsträger in Unternehmen geschrieben, die ein Interesse am Schutz ihres Unternehmens haben. Das Dokument gibt Auskunft über nicht in der Öffentlichkeit bekannte Gefährdungen von Unternehmen und Privatpersonen, die durch den Umgang mit dem Internet in den letzten Jahren verdeckt entstanden sind.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Internetbeobachtung im Jahr 2007

Ende 2007 wurde von dem Unternehmen Xamit Bewertungsgesellschaft mbH eine breit angelegte Studie zur Beobachtung von Internetnutzern durchgeführt. Dabei wurde analysiert, welche Unternehmen und Branchen im Zusammenhang mit ihrem Internetauftritt Statistikanbieter beauftragten, um Daten über den Besuch ihrer Internetseiten zu ermitteln. Insgesamt wurden zwischen August und September 2007 mehr als 655.000 Webseiten von 14.400 Unternehmen und öffentlichen Einrichtungen in der Studie ausgewertet. Jeder Internetauftritt eines Anbieters wurde daraufhin untersucht, welcher Statistikanbieter – wir werden diese Unternehmen im folgenden Profiler nennen – mit eigener Datenerhebung genutzt wird, ob Logfiles des Internetauftritts vom Profiler ausgewertet werden und ob Besucher der Internetseiten über den Einsatz des Profilers informiert werden.

Insgesamt wurden 1250 öffentliche Anbieter und zahlreiche mittelständische Unternehmen aus folgenden Branchen ausgewertet:

- Werbung
- Unternehmensberatung
- Informationstechnik
- Verarbeitendes Gewerbe
- Grundstücks- und Wohnungswesen
- Handel, Instandhaltung und Reparatur von Kfz und Gebrauchsgütern
- Gesundheitswesen
- Rechtsanwälte & Steuerberater
- Gastgewerbe
- Hotel mit Restaurant

Jede Branche war mit 853 bis 2.048 Web-Präsenzen vertreten. Analysiert wurden jeweils die 6.000 zu erst gefundenen Webseiten pro Internetpräsenz. Die Untersuchung bezog sich auf Deutschland. In Deutschland ist Google Analytics der Marktführer unter den Profilern. In anderen europäischen Ländern ist z.B. Yahoo oder andere Unternehmen, die Internetstatistiken anbieten, marktführend.

Die Studie hat ergeben, daß Profiler vor allem in der Werbebranche mit Abstand am häufigsten eingesetzt werden, gefolgt von Unternehmensberatungen, Unternehmen der Informationstechnikbranche und dem verarbeitenden Gewerbe. Im letzten Drittel der Branchenauswertung stehen alle anderen Unternehmen aus den oben aufgelisteten Branchen. Dabei wurden aus methodischen Gründen in der Studie nur die Angebote berücksichtigt, in denen lediglich eigene Datenerhebungen durch die Profiler erhoben wurden. Daten durch Analysen der Logfiles des Provider, der den Internetauftritt eines Unternehmens im Internet zur Verfügung stellt, wurden dabei in der Datenerhebung nicht berücksichtigt.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Die Studie von Xamit ermittelte, daß insgesamt 7% der Internetpräsenzen Google Analytics für die Ermittlung ihrer Web-Statistiken benutzten. 1% nutzte nach den Erhebungen der Studie andere Anbieter. Mit Abstand nutzten Unternehmen aus der Werbebranche den Service der Profiler am meisten.

Google kennt die IP-Nummer, den Zeitpunkt des Besuchs, den Browser, häufig das Betriebssystem und weitere Daten eines Besuchers. Um einen Benutzer eindeutig identifizieren zu können, hat sich der Einsatz von Cookies bewährt. Die Standardeinstellung fast aller Internetbrowser ist eine stille Akzeptanz von Cookies. Im Normalfall wird damit beim Besuch einer Internetseite ein Cookie auf den Rechner des Besuchers abgespeichert, das eine weltweit eindeutige Nummer enthält. Besucht der Internetbesucher eine Seite, kann dieses Cookie ausgelesen werden und über die eindeutige Nummer mit Daten beim Profiler verglichen werden, die dank der Nummer im Cookie eindeutig zugeordnet werden können. Häufig wird diese Cookie-Technik mit Scripten kombiniert. Hat z.B. ein Benutzer das Setzen von Cookies deaktiviert, wird häufig die Nutzung von Scripten für den Besuch der Internetseite verlangt. Durch das aktivieren der Scripte kann nun indirekt ein Cookie oder eine andere Datei (z.B. kleine Bilddatei) auf dem Rechner des Besuchers abgespeichert werden, in dem u.a. eine eindeutige Nummer oder ein eindeutiger Code (z.B. Bilddatei) enthalten sein kann. Diese Nummer/Code identifiziert in Verbindung mit den anderen Daten den Benutzer eindeutig. Nach der eindeutigen Identifikation des Rechners/Internetbenutzers können die aktiven Klicks, also welche Seiten oder Inhalte der Benutzer auswählt, gespeichert und dieser eindeutigen Kennung zugeordnet werden. Aus diesen gespeicherten Daten entstehen Profile. So bietet z.B. der Internetdienst WEB-GPS (http://www.web-gps.de/index.php) seine Produkte mit folgendem Satz an: „WEB-GPS bietet Ihnen die Möglichkeit, zu sehen, aus welchen Städten und Ländern ihre Webseitenbesucher kommen."

Da z.B. Google Analytics alleine nur in Deutschland tausende von Internetauftritten mit seinem Statistikservice betreut, entsteht bei dem Profiler ein Bewegungsbild und Angaben über Präferenzen/Vorlieben des Benutzers, welche Internetseiten/Inhalte von ihm bevorzugt werden. Wird z.B. der Service eines Profilers auf Internetseiten wie z.B. Quelle, Neckermann, Otto Versand, Bader oder anderen großen Warenhäusern angewendet, kann über einen längeren Zeitraum ein umfassendes Bild von wünschenswerten/interessanten Waren (Bedürfnissen) einer Person/Kennung entstehen. Benutzt der Internetbesucher bei den großen Online-Warenhäusern den Bezahlservice oder benutzt er Online-Banking, können sehr einfach seine Bedürfnisse mit seinen wirtschaftlichen Verhältnissen verbunden werden. Google bietet zusätzlich zur Erhebung von statistischen Informationen weitere Services wie Google Apps, Google Mail, Google Earth, Google Calendar, Google Addwords an, in dem eine persönliche Anmeldung – generell aber aktive Scripte – notwendig sind.

In dem Bewegungsbild kann durch die Verknüpfung von Internetseiten und Besuchszeitpunkt ein detailliertes Profil des Internetbesuchers erstellt werden. Benutzt der Internetbesucher Internetseiten, in dem er seinen Namen oder E-Mail eingeben muss (sich Iden-

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

tifizieren muss), werden diese Daten dem bisher anonymen Profil zugeordnet. Durch diese Zuordnung kann nun direkt auf eine Person geschlossen werden, in welchen wirtschaftlichen Verhältnissen sie sich befindet und welche Bedürfnisse (Vorlieben) sie hat, wer der Arbeitgeber ist und an welchen Orten/Urlaubsorten/Einsatzorten sie war. Gibt der Internetnutzer seine Daten einmal von einem Arbeitsplatz-PC ein und z.B. abends von seinem Heim-PC, können weitere Details seines Profils zusammengestellt werden. Das gilt vor allem dann, wenn er seine E-Mails in seinem Urlaubsort abruft und dazu Internetseiten benutzt, in dem er sich Identifizieren muss (siehe weiter oben z.B. Google Mail). Durch die Kombination von IP-Adresse (wird vom Provider automatisch vergeben), die auf den Ort schließen läßt wo er sich zur Zeit aufhält, und seiner Identifikation/E-Mailadresse, kann damit ein umfassendes persönliches Bewegungsprofil nach einiger Zeit aufgebaut werden.

Wie in der Xamit-Studie und auch hier klar ausgewiesen wurde, kann nicht behauptet werden, daß Google oder andere Profiler eine Zusammenführung aller Daten tatsächlich vornimmt. Hier soll lediglich darauf hingewiesen werden, daß dazu die Profiler in der Lage wären. Ob die Daten bei den Profilern in Deutschland tatsächlich zusammengeführt werden oder nicht, wurde bisher offensichtlich nie kontrolliert. Ebenfalls gibt es darüber keine Untersuchungen oder Studien. Das die Daten von Profilern zusammengeführt werden, ist jedoch aus anderen Ländern (z.B. USA) bekannt.

In der Werbeindustrie sind diese Daten/Profile besonders wertvoll, wenn sie viele Details von Personen enthalten, die auf das Konsumverhalten und die Bedürfnisse schließen lassen. Die Werbebranche ist an detaillierten Berichten interessiert, wie Besucher von Internetseiten auf Werbung reagieren. Unternehmen investieren viel Geld in Werbung und wollen möglichst effizient ihre Werbebotschaften an den Konsumenten übermitteln. Damit treffen sich die Interessen von bestimmten Unternehmen, möglichst effizient ihre Werbemittel einsetzen zu wollen und andererseits das Interesse von Profilern, ihre Daten so genau wie möglich ihren Kunden anbieten zu können. Kennt ein Werbeunternehmen die Anschrift eines Kunden, ist eine direkte „Ansprache“ des Kunden möglich. Über diesen Weg werden sogenannte Streuverluste in der Werbung verringert.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Rechtslage und die Wirklichkeit

Der Kunde bezahlt also häufig mit seinen persönlichen Daten und möglichen Bewegungsprofilen die kostenlosen Angebote von Internetanbietern. Dabei ergibt sich die Frage, wie werden diese persönlichen Daten kontrolliert und wie lange werden diese Daten gespeichert. Diese Fragen sind vor allem vor dem Hintergrund der Novellierung des Telemediengesetzes (TMG) in 2007 interessant, in dem Datenspeicherungen von persönlichen Daten neu geregelt worden sind. Zusätzlich hat das Bundesverfassungsgericht Anfang 2008 eine grundsätzliche Klarstellung zur Anwendung des neuen TMG vorgenommen.

Im folgenden soll anhand des Marktführers Google diese Frage exemplarisch für die Branche der Profiler analysiert werden. In den Geschäftsbedingungen von Google ist verankert, daß Google in §8.1 seiner Nutzungsbedingungen vom Internetanbieter verlangt, daß die Bewegungsprofile von Besuchern nicht mit personenbezogenen Daten verknüpft und die Nutzung von Google Analytics an „prominenter“ Stelle dokumentieren wird. Google schreibt den Wortlaut dieser Information vor und behält sich ein Kontrollrecht vor.

Nach den Analysen der Xamit-Studie ignorieren jedoch im Durchschnitt ca. 99% aller Kunden diesen Paragraph der Geschäftsbedingungen zur Kennzeichnungspflicht. In der Studie wird darauf hingewiesen, daß z.B. bei dem Konkurrenzunternehmen eTracker in den Nutzungsbedingungen nur eine Empfehlungen zur Kennzeichnung ausgesprochen wird. Bei Unternehmensberatungen halten sich nach der Xamit-Studie von allen Unternehmen, die Google Analytics nutzen, ca. 1%, in der Informationstechnik ca. 1,7% und in der Werbebranche ca. 2% an die Kennzeichnungspflicht.

Der Internetservice zur Verwaltung von Domains und Domainnamen DENIC (www.denic.de) hat in 2007 unter der Kennung „.DE“ mehr als 11 Mio. Domains registriert. Bei einem Marktanteil von Google Analytics von ca. 7% nutzen rechnerisch ca. 770.000 Internetauftritte Google Analytics (Mehrfachregistrierungen eines Internetauftritts unter verschiedenen Domains werden dabei nicht berücksichtigt). Wie die Studie ermittelt hat, verheimlichen demnach also über 760.000 Internet-Präsenzen ihre Überwachung durch Google Analytics. Zusätzlich ist darauf hinzuweisen, daß in der Regel ein normaler Internetnutzer die Konsequenzen nicht bewerten kann, wenn auf der besuchten Internetseite an „prominenter“ Stelle auf einen Statistikanbieter hingewiesen wird. Auf Basis der Daten aus der Studie kann gefolgert werden, daß in der Praxis keine Anerkennung, Einhaltung oder Kontrolle der gültigen Rechtsnormen erfolgt, weder von den staatlichen Organen (siehe nächstes Kapitel), noch von den Profilern oder deren Kunden selbst. Der Internetbesucher ist sich selbst überlassen.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Wie in der Xamit-Studie weiter festgestellt wurde, nutzen staatliche Bundes- und Landeseinrichtungen ebenfalls die Services der Profiler. Bis zum Stichtag am 8.10.2007 nutzte das **Bundesministerium für Finanzen** Google Analytics. Das Ministerium wies in seinem Impressum – eine Seite, die in der Regel nicht oder nur in Ausnahmen besucht wird – auf die Nutzung dieses Services hin. Die Studie ergab, Zitat: „*Sitestat/Nedstat wird vom **Bundesministerium für Arbeit und Soziales** genutzt und Webtrekk vom **Auswärtigen Amt**. Beide Ministerien weisen nicht auf die Datenerhebung durch externe Dienstleister hin. Das Auswärtige Amt verzichtet gleich ganz auf eine (auffindbare) Datenschutzerklärung, obwohl es eine Bestellfunktion, vergleichbar einem Webshop, anbietet.*“

Auf der Landesebene konnte die Studie weitere „gesetzesunkonforme“ Internetangebote ermitteln. Zitat aus der Studie: „*Im Unterschied zum Bundesministerium der Finanzen verschleierten in NRW u.a. sowohl das **Landesministerien für Justiz** als auch die **Landesministerien für Innovation, Wissenschaft, Forschung und Technologie** die Nutzung von Google Analytics. Beide Ministerien stellten die Nutzung von Google Analytics ein, nachdem Xamit sie angesprochen hatte. In seinen Datenschutzerklärungen (Abbildung 4) schreibt das **Justizministerium** des Landes NRW: „Nach Ablauf von 6 Wochen werden die Zugriffsdaten anonymisiert, indem die IP-Adresse in den betreffenden Datensätzen gelöscht wird.“ Wie das Ministerium diese Löschung bei Google durchsetzt und kontrollieren will, bleibt sein Geheimnis. Weiter in seiner Datenschutzerklärung verspricht das Ministerium: „Die Website des Justizministeriums verwendet keine Cookies.“ Google Analytics setzt trotzdem Cookies. Das Ministerium suggeriert ein Datenschutzniveau, das faktisch nicht existiert. Das **Ministerium für Innovation, Wissenschaft, Forschung und Technologie** des Landes NRW verschleiert die Datenerhebung mit Google Analytics auf ähnliche Weise (Abbildung 5). Zusätzlich verspricht das Ministerium keine Java Script einzusetzen („Aktive Elemente auf HTML-Seiten (Java-Script, ActiveX, usw.) werden grundsätzlich nicht eingesetzt.“11). Google Analytics baut auf Java-Script auf!*“

Diese Vorgänge sind vor allem dann von erheblicher Bedeutung, wenn auf der einen Seite vom Bundesverfassungsgericht Urteile zur Informellen Selbstbestimmung verfaßt werden, diese Rechtsprechungen jedoch in der Praxis von staatlichen Einrichtungen offensichtlich missachtet werden. Die in der Studie ermittelten Fakten bekommen eine noch größere Bedeutung, wenn davon ausgegangen werden muss, daß in Zukunft immer mehr Dienste der öffentlichen Hand über das Internet angeboten werden sollen (eGovernment). Bürger und Unternehmen werden über diese Angebote gezwungen, ihre Verwaltungsvorgänge über das Internet abzugeben (siehe auch Angebote privater Unternehmen zu weitreichenden Verwaltungsvorgängen wie http://www.arvatogov.de/?action=eastriding oder http://www.empolis.com/de/sicherheit/). Diese sehr persönlichen Verwaltungsvorgänge gehen jedoch keinen Dritten oder sogar privaten Unternehmen etwas an (Urteil BVG>>>). Die Studie hat bewiesen, daß die Anonymität, die für diese persönlichen Daten notwendig

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

ist, damit die Daten vertraulich zwischen der Verwaltungsbehörde und einer Privatperson oder einem Unternehmen ausgetauscht werden können, nicht vorhanden ist. Der Staat hilft außerdem mit der Nutzung von Profilern aktiv ausländischen Unternehmen (Google, eTracker und andere Profiler), Daten über seine Staatsbürger und Unternehmen preis zu geben. Zusätzlich gibt der Staat den Profilern einen tiefen Einblick in sein eigenes Handeln von Verwaltungsaufgaben.

Zur Vollständigkeit soll hier darauf hingewiesen werden, daß nach §15 Abs. 3 TMG Nutzungsdaten „für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien“ verwendet werden, wenn diese mit Pseudonymen arbeiten und der Besucher nicht widersprochen hat! Der Benutzer muss also explizit gefragt werden, ob er sein Widerspruchsrecht ausüben will oder nicht, wenn ein Profiler seine Daten ermitteln sollte. Dieses Widerspruchsrecht konnte jedoch nach Auswertung der Xamit-Studie in keinem Fall aktiv bei einem Besuch der untersuchten Internetpräsenzen ausgeübt werden. Die erstellten Profile werden u.a. von Google nicht gelöscht, so daß auch zukünftige Auswertungen mit Personenbezug nach Googles Ermessen möglich sind. Haftung und Verantwortung für eine gesetzeskonforme Handhabe der ermittelten Daten verbleiben indes beim Betreiber als Auftraggeber. Wie der Widerspruch gegen die Erstellung eines Profils/Bewegungsprofils von einem Unternehmen oder einer Privatperson technisch umgesetzt werden soll, lässt der Gesetzgeber offen.

Welche Daten zur Verwaltung des Internets permanent erfasst werden, kann unter http://www.internetworldstats.com/stats.htm („The Big Picture“) nachgesehen werden. Für eine einfache Sofortanalyse, welche Daten man selbst aktuell an Profiler übermittelt, kann auf der Seite https://www.astalavista.net/?cmd=net angesehen werden. Eine interessante Übersicht von Zugriffen ist unter http://www.holzrank.de/Statistik.html zu finden. Auf dieser Seite kann u.a. die Anzahl der Suchanfragen von fast allen Suchmaschinen über die letzten Jahre abgefragt werden (Es wird also protokolliert, wer in welcher Suchmaschine nach was sucht!). Ebenfalls werden Zugriffe nach bestimmten Branchen und Themen (Krankenkassen, Banken, Versicherungen, Kapitalmarkt, Beruf, Arbeitslosigkeit, Haushalte) über die letzten Jahre aufgelistet. Natürlich sind die Daten nicht mit einer IP-Adresse oder mit einem Namen verbunden, sondern reine statistische Daten. Mit der Seite wird aufgezeigt, daß über einen weiten Bereich des täglichen Handelns Daten von Profilern erfaßt und zusammengestellt werden. Wie und bei welchem Profiler die Daten verknüpft werden, kann und wird nicht kontrolliert. Vor allem dann nicht, wenn die Unternehmen, die diese Daten zusammenstellen, nicht in Deutschland ansässig sind. Auf der Internetseite wird auch der folgende Hinweis auf den Einsatz mächtiger Statistikmethoden gegeben: „*Das Buch "Großstädte-Ranking" dient insbesondere auch der Vorstellung moderner Informationstechniken, die mittels Excel- und VBA-Implementierungen zur Verfügung gestellt sind. Es sind leistungsfähige Data-Mining und OLAP-Techniken realisiert, die besonders auch neuere Evidenz-Theorien berücksichtigen. Ein implementierter Cluster-Algorithmus ermöglicht zudem die Darstellung von Copulas.*„

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Im folgenden werden einige zufällig ausgewählte und bekannte Seiten exemplarisch dargestellt, ob und wie persönliche Daten rechtssicher erfaßt werden. Die Auswertung der Seiten erfolgte im Main und Juni 2008. Im folgenden werden einige wichtige Informationen zu den Profilern aufgelistet, die von den Internetseiten eingesetzt worden sind. Die hier beispielhaft aufgelisteten Seiten werden nicht vollständig beschrieben, da es den hier vorgegebenen Rahmen sprengen würde. Die hier aufgelisteten Angaben haben deshalb nicht den Anspruch der Vollständigkeit sondern geben einen Hinweis auf die Prinzipien der in dieser Studie zugrunde liegenden Informationsindustrie, sowohl deren Verzahnung und Verflechtungen.

tfag.de

Unternehmen: Tomorrow Focus AG.

Aus der Seite des Anbieters zur Selbstdarstellung:

Der Geschäftsbereich Portal zählt zu den größten Vermarktern für Onlinewerbung in Deutschland. Zum Portfolio von über 50 Onlineangeboten zählen eigenen redaktionellen Onlineportale bekannter Marken wie FOCUS, AMICA, CINEMA, FITFORFUN, MAX, PLAYBOY und TV SPIELFILM. Darüber hinaus vermarktet der Geschäftsbereich Portal redaktionelle Partnerangebote wie BUNTE Online, CHIP Online oder FAZ.NET sowie erfolgreiche Internet-Communitys wie PICZO oder SEVENLOAD. Dank der breiten Basis verschiedener Marken und Plattformen bietet TOMORROW FOCUS maßgeschneiderte Themenwelten für jede Zielgruppe und Anforderung.

ivwbox.de

Ein deutsches Unternehmen der Medienindustrie.

Aus der Seite des Anbieters zur Selbstdarstellung:

Die INFOnline GmbH wird von sieben großen deutschen Medienverbänden getragen. Gesellschafter des Unternehmens sind zu gleichen Teilen der

- Bundesverband Deutscher Zeitungsverleger (BDZV)
- Verband Deutscher Zeitschriftenverleger (VDZ)
- Bundesverband Digitale Wirtschaft (BVDW)
- Markenverband
- Organisation der Media-Agenturen im GWA
- Verband Deutscher Auskunfts- und Verzeichnismedien (VDAV)
- Verband Privater Rundfunk und Telemedien (VPRT)

Das Leistungsangebot von INFOnline umfasst

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

- die Zählung und Messung von Zugriffen auf offene Seiten, die über das http-Protokoll ausgeliefert werden, mit dem bewährten Skalierbaren Zentralen Messverfahren (SZM)
- die Zählung und Messung von Zugriffen auf SSL-verschlüsselte Seiten, die das https-Protokoll nutzen, mit dem SZM plus zwischengeschalteten SSL-Offloader (der die https-Requests in http-Requests umwandelt und damit für das SZM messbar macht)
- das Controlling der Nutzung von Webseiten: Welche Inhalte wurden von wie vielen Besuchern mit welcher Dauer genutzt? Für die Analyse von Webseitensetzen wir unser Website-Controlling-Cockpit (WCC) ein, das ab Dezember 2005 zur Verfügung steht und auf der bewährten Analyseplattform "HEATMAP" von spring, basiert.

doubleclick.net

Ein deutsches Tochterunternehmen einer amerikanischen Muttergesellschaft. Google ist Mehrheitsaktionär bei DoubleClick Inc..

Aus der Seite des Anbieters zur Selbstdarstellung:

DoubleClick ist ein global aufgestellter Anbieter von Technologien und Dienstleistungen für das digitale Marketing. Weltweit vertrauen führende Media-Agenturen, Werbungtreibende und Web-Publisher auf DoubleClicks Erfahrung in den Bereichen Ad-Management, Rich-Media, Videowerbung, Suchmaschinenmarketing und Mobile Adserving, um optimal von ihren Investitionen in das digitale Marketing zu profitieren. Aufgrund dieser Position ist DoubleClick in der Lage, Know-how mit einzigartiger Informationstiefe zur Verfügung zu stellen.

Googleanalytics.com

Der Marktführer in Deutschland von Analyse und Informationsdiensten. Google ist an zahlreichen anderen Unternehmen, die Informationsdienste anbieten, beteiligt. Google ist ein amerikanisches Unternehmen, dass zahlreiche Server in verschiedenen Staaten betreibt. Eine Kontrolle von Daten nach Deutschem Recht auf diesen Servern, einschließlich den Betreibergesellschaften dieser Server, ist realistisch nicht möglich.

Internetseite „Www.Focus.De“

Beim Aufruf dieser beliebten Seite werden folgende Dienste im Hintergrund aktiviert

- tfag.de
- ivwbox.de
- doubleclick.net

Die Seite weist auf seiner Datenschutzseite u.a. wie folgt auf die Erhebung privater Daten hin:

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

> Cookies werden von Tomorrow Focus ferner dazu verwendet, um die Nutzung der Websites, insbesondere der Online-Werbung zu analysieren und Ihnen anhand Ihrer Vorlieben spezielle, Sie interessierende Angebote und Services auf den Webseiten zu präsentieren. Darüber hinaus soll Anzeigenkunden ermöglicht werden, ihre Zielgruppe möglichst genau und ohne große Streuverluste anzusprechen. Hierzu werden z.B. anonyme Nutzerstatistiken erstellt und die Daten zu Marktforschungszwecken verwendet. Keinem der Anzeigenkunden werden jedoch Daten zur Verfügung gestellt, die einen Rückschluss auf eine bestimmte Person ermöglichen. Zur Erfolgsanalyse verwenden wir ggf. die oben bezeichneten Cookies, die generelle Vorlieben eines Nutzers speichern. Diese Daten werden unter Umständen bei **OnSite-Befragungen** mit weiteren demographischen Daten (z.B. Alter und Geschlecht) angereichert. Hierauf werden Sie auch gesondert bei der OnSite-Befragung hingewiesen. Die Daten werden in dem Cookie auf Ihrem Computer gespeichert. Durch die Speicherung des Profils unter einem Pseudonym wird Ihr Datenschutz verstärkt, weil die im Cookie gespeicherten Daten keine Rückschlüsse auf Ihren konkreten Namen zulassen. Sie sind berechtigt, jederzeit Auskunft über die unter Ihrem Pseudonym gespeicherten Daten zu verlangen. Ferner sind Sie berechtigt, der Erstellung eines Nutzerprofils jederzeit mit Wirkung für die Zukunft zu widersprechen.

Hinweis: Auf der Datenschutzseite werden die eingesetzten Profiler-Dienste nicht explizit ausgewiesen. Der grün markierte Satz beschreibt das Verfahren, in dem die individuellen Informationen rechtlich sicher von einem Profiler genutzt werden. In dem Satz wird klargestellt, daß ein persönliches Datenprofil in einem Cookie unter einem Pseudonym auf dem persönlichen Computer eines Internetbenutzers gespeichert werden. Der Profiler hat also persönliche „Vorlieben“ in einem „Profil“ zusammengestellt und auf Ihrem Computer in einem „Cookie“ abgelegt. Das Cookie wird von dem Profiler ausgelesen und nach belieben mit weiteren persönlichen Daten auf ihrem Computer ergänzt. Das Profil ist unter einem Pseudonym eindeutig für den Profiler identifizierbar und wird bei jedem Besuch einer Internetseite ausgewertet. Die Zuordnung eines realen Namens zu dem Pseudonym kann jederzeit durch andere Dienste vorgenommen werden. Damit ist der Besucher in seinen persönlichen „Vorlieben“ transparent und ein wirtschaftliches Gut.

Internetseite „Www.stern.de“

Beim Aufruf dieser beliebten Seite werden folgende Dienste im Hintergrund aktiviert

- ivwbox.de
- betarget.de
- doubleclick.net
- proximic.com

Die Seite weist auf seiner Datenschutzseite u.a. wie folgt auf die Erhebung privater Daten hin:

> stern.de setzt Cookies insbesondere für die Verteilung von Werbung und für die Zählung von Seitenaufrufen. Hierbei wird beim Nutzer eine Zufallszahl - eine Art Pseudonym - in Form des Cookies gesetzt, anhand derer der Server erkennt, dass die Anfrage vom selben Nutzer erfolgt, ohne aber Informationen über die Identität oder sonstige Daten des Nutzers zu erhalten. Dies ist vor allem wichtig, um Anzeigenkunden eine Vorstellung davon vermitteln zu können, wie viele verschiedene Nutzer innerhalb welcher Zeit seine Werbung zu sehen bekom-

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

men. Derartige Cookies haben überdies in der Regel nur eine Lebensdauer von 24 Stunden. Ebenso setzt stern.de Cookies - teilweise mit längerer Lebensdauer - wenn Sie sich (z.B. im Shop- oder Community-Bereich) registrieren: Ihre personenbezogenen Daten werden bei stern.de auf einem besonders geschützten Server in Deutschland gespeichert, der eine Zufallszahl als Cookie auf Ihrem Rechner setzt, mit der er Ihren Rechner beim nächsten Besuch wieder erkennt. Ebenso kann stern.de ein Cookie mit langer Lebensdauer setzen, das die technischen Einstellungen ihres Browser überprüft und als erste Information beim neuen Besuch auf stern.de ausgelesen wird.

Hinweis: Auf der Stern-Datenschutzseite wird auf die eingesetzten Profiler-Dienste nicht explizit ausgewiesen. Im Datenschutz wird klargestellt, daß eine eindeutige Nummer zur Identifikation des persönlichen Rechner verwendet wird. Dieses Pseudonym kennzeichnet also den persönlichen Rechner eindeutig.

Internetseite „Www.faz.de“

Beim Aufruf dieser beliebten Seite werden folgende Dienste im Hintergrund aktiviert

- googleanalytics.com
- gacela.eu
- doubleclick.net

Die Seite weist auf seiner Datenschutzseite u.a. wie folgt auf die Erhebung privater Daten hin:

Während Sie das Portal besuchen, erheben unsere Webserver zum Betrieb des Angebotes allgemeine technische Informationen, insbesondere über die von Ihnen verwendete Soft- und Hardware, die IP-Adresse Ihres Rechners, welche Webseiten Sie aufgerufen haben, sowie den Zeitpunkt und die Dauer Ihres Besuches. Diese Daten haben keinen Personenbezug zu Ihnen. Eine Verknüpfung der erhobenen Daten mit etwaigen Registrierungsdaten erfolgt nicht.

Hinweis: Auf der Datenschutzseite wird auf die eingesetzten Profiler-Dienste nicht explizit ausgewiesen. Der in den Datenschutzbestimmungen gegebene Hinweis auf „unsere Webserver“ ist irreführend, da weitere Profiler wie z.B. googleanalytics Daten erheben. Ein Hinweis auf diese Datenerhebungen und ob Informationsabgleiche zwischen den eigenen Webservern und den beauftragten Profilern erfolgt fehlt.

Beispiel eines Profilings anhand des deutschen Profilers AGOF

Link: http://www.agof.de/

Methodenbeschreibung in Auszügen aus der Präsentation des Profilers AGOF. Die Auszüge wurden aus den öffentlichen Darstellungen zu den Methoden des Profilers im Mai 2008 erfaßt.

...

Die methodische Grundlage der internet facts ist daher ein Drei-Säulen-Modell, in dessen Zentrum die elektronische Messung der Nutzung (Basiserhebung)

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

steht, und die durch eine OnSite-Befragung sowie eine bevölkerungsrepräsentative Telefonbefragung ergänzt wird.

Die drei Basismodule haben dabei die folgenden Funktionen: Die rein technische Messung, die nahezu eine Vollerhebung der gesamten Kontakte auf den deutschen Online-Werbeträger-angeboten darstellt, beinhaltet die Erhebung gelernter Größen wie Visits, Page Impressions und zwar auf Basis jeden einzelnen Rechners, dessen Internetnutzung gemessen wird. Diese Rechner werden als Unique Clients bezeichnet.

Während die Grundgesamtheit der technischen Messung Unique Clients sind, dient die OnSite-Befragung dazu, Informationen über die Nutzer hinter den Rechnern zu generieren. Die Grundgesamtheit hier ist die Internetnutzerschaft ab 14 Jahren. In der OnSite-Befragung werden neben personenbeschreibenden soziodemografischen Größen auch Informationen zur Nutzung des Rechners gewonnen.

...

Die wichtigste Innovation der internet facts ist die Umwandlung von Unique Clients in Unique User, also in die Nutzer hinter den Rechnern. Unique Clients sind nicht eins zu eins auf Personen übertragbar: Zwar machen die Single User (der Rechner wird von einer Person genutzt, die keinen anderen Internetzugang nutzt - ein Unique Client ist gleich ein Unique User) einen wesentlichen Teil der Internetnutzer aus. Allerdings existieren daneben auch Rechner, deren Nutzung von verschiedenen Nutzern ausgelöst wird, so genannte Multi User.

Zum anderen gibt es Rechner, deren Nutzung nur einen Teil ihrer gesamten Internetnutzung ausmacht, da die Person mit verschiedenen Rechnern, zum Beispiel zu Hause und am Arbeitsplatz online geht, so genannte Multi Clients.

Für die Umwandlung von Unique Clients auf Unique User müssen somit in einem ersten Schritt Multi-User-, Multi-Client- und Single-User-Profile aus den Daten der ersten Säule ermittelt werden.

Danach werden die soziodemografischen Daten jedes idealtypischen Nutzers nach dem Identitäts- bzw. Ähnlichkeitsprinzip auf diejenigen Nutzer projiziert bzw. prognostiziert, von denen lediglich das tatsächliche Internetnutzungsverhalten aus der technischen Messung vorliegt und mit dem eines der idealtypischen Nutzer korrespondiert.

Auf diese Weise werden fehlende soziodemografische Daten ergänzt und vollständige Nutzerprofile generiert (Modelling). Die Umwandlung von Unique Clients in Unique User ist damit abgeschlossen.

...

Zusammenfassung:

Der Profiler erfaßt Daten von Personen über mehrere Medien (Drei-Säulen-Modell). Die Daten werden zu einer Grundgesamtheit, den „Unique Clients“ zusammengestellt. Über eine „**OnSite-Befragung**“ werden die „Informationen über die Nutzer hinter den Rechnern“ erfaßt. Bei dieser Erfassung werden auch „Informationen zur Nutzung des Rechners“ erhoben. Durch die „Umwandlung von Unique Clients auf Unique User“ werden die erhobenen Daten zu „vollständige Nutzerprofilen“ zusammengestellt.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Zusammenfassung der Netzbeobachtung

Vor dem Hintergrund der dargestellten Fakten wird deutlich, daß persönliche Daten oder Daten von Unternehmen im Internet nicht sicher sind. Die Erfassung von Daten aus dem Internet und der Handel mit den daraus erstellten Profilen ist ein milliardenschweres Geschäft, in dem der Staat bereits mit integriert ist. Bei der bisherigen Betrachtung wurden die Themen von direkten Einbrüchen in Rechner (Stichwort „Bundestrojaner“) nicht behandelt. Auf dieses Thema wird in dem nächsten Kapitel eingegangen. Die oben beschriebenen Techniken werden lediglich für Beobachtungen im Internet eingesetzt.

Die sich aus diesen indirekt ermittelten Daten ergebenen Profile sind jedoch bereits sehr umfangreich und aussagekräftig. Deshalb muss an dieser Stelle darauf hingewiesen werden, daß ein Einsatz einer Firewall – wie gut sie auch direkte Angriffe aus dem Internet abwehren mag – prinzipbedingt keinen Schutz vor dem Ausspionieren von Unternehmen oder Privatperson bietet.

Jeder Mensch und jedes Unternehmen, jedes Institut, jeder Verein, jede öffentliche Einrichtung und jedes Ministerium hat Geheimnisse. Alle Informationen, die nicht für Dritte bestimmt sind, benötigen Schutz und Vertraulichkeit. Kein Unternehmen möchte seine Kundenbeziehungen, Forschungspläne, Steuerdaten oder Projektaktivitäten anderen Konkurrenten zur Verfügung stellen. Keine Privatperson möchte seine Krankengeschichte, finanziellen Verhältnisse oder andere persönliche Dinge (Familienverhältnisse; sexuelle Neigungen oder Vorlieben; zukünftige persönliche Absichten; Suche nach neuer Arbeit wenn z.B. Jobbörsen im Internet aufgesucht werden, etc.) öffentlich von Dritten verwertet wissen. Deshalb soll in diesem Beitrag darauf verwiesen werden, wie bereits mit einfachen Mitteln der Sammelwut entgegen gewirkt werden kann.

Die in der Xamit-Studie untersuchte Technik basiert auf dem Willen eines Internetanbieters, Daten über seine Internetbesucher zu erhalten. Die Studie hat gezeigt, daß bereits in diesem Feld erhebliche Defizite im Umgang mit Daten zu verzeichnen sind. Im besonderen wenn die Unternehmen keinen Sitz in Deutschland haben, sondern ihren Service von einem anderen Firmensitz außerhalb Deutschlands anbieten. Berücksichtigt man noch die weltweite Vernetzung des Internets, wandern Daten somit grenzenlos durch alle Länder und können von unzähligen „Mithörern“ zu ganz eigenen Profilen zusammengestellt werden. Ein Schutz SEINER persönlichen Daten ist also bereits bei jedem Internetbesuch ein Anliegen, das bisher noch darauf wartet entdeckt zu werden.

An dieser Stelle soll auch darauf hingewiesen werden, daß es bereits fortgeschrittene Techniken gibt, die die Beauftragung eines Profilers zur Erhebung von Besuchsdaten auf einer Internetseite nicht benötigt. In den folgenden Kapiteln wird darauf noch eingegangen. Zusätzlich muss nochmals unterstrichen werden, daß offensichtlich ein prinzipieller Mangel eines Rechtsvollzug/Rechtsverfolgung im Internet, egal welches Rechtssystem offensichtlich zur Anwendung kommen würde, vorhanden ist. Die Folge ist, daß ein wirksamer Schutz aller Menschen eines Staates/Rechtsraumes und eine wir-

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

kungsvolle Verfolgung gegen Rechtsverstöße nicht mehr von den dafür zuständigen Organen umgesetzt wird! Wenn sich zusätzlich staatliche Bundes- und Landeseinrichtungen nicht an die gesetzlichen Rahmenbedingungen des eigenen Landes halten oder aktiv Daten sammeln, ist eine gesellschaftlich gefährliche Entwicklung in Gang gesetzt.

Aufgrund der durch die jetzt erneut bekannt gewordenen Datenmissbräuche erhält diese Studie eine hohe Aktualität. Aus diesem Grund wurde auch ein neues Kapitel „Datengipfel des BMI im Sommer 2008“ eingeführt. Das Kapitel zeigt die für eine Gesellschaft gefährlichen Entwicklungen anhand aktueller und konkreter Fälle auf.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Nachtrag

„Man gebe mir sechs Zeilen, geschrieben von dem redlichsten Menschen, und ich werde darin etwas finden, um ihn aufhängen zu lassen."

- Kardinal Richelieu

Artikel vom 25.02.2008, Streit zwischen Google und Anderen:

Thema: IP-Adressen sind keine personenbezogenen Daten. Streit mit Art.29-Gruppe im Rahmen einer Anhörung vor dem Bürgerechtsausschuss des EU-Parlaments (Presseinformation des EU-Parlaments)

Auszug aus dem Protokoll

...

Peter Fleischer, Datenschutzsprecher von Google, wendete sich gegen diese Ansicht: "Manchmal kann eine IP-Adresse ein personenbezogenes Datum darstellen, andermal nicht. Es kommt dabei immer auf den Zusammenhang an." Zudem betonte er die Rolle der IP-Adressen für Googles Geschäftsmodell: "Wir müssen wissen, wer wonach fragt - andernfalls könnte unser Unternehmen nicht funktionieren".

In der Anhörung vor dem Bürgerrechtsausschuss des EU-Parlaments, aus der die obigen Zitate stammen, gab Fleischer auch zu, **dass Google den Inhalt von E-Mails, die über seinen Dienst Gmail verschickt werden, zu Werbezwecken auswertet.** -- O. Langfeldt (ULD)

Link zum Artikel:
http://www.datenschutz.de/privo/news/alle/detail/?nid=2683

Ergänzung:
http://www.europarl.europa.eu/news/expert/infopress_page/019-19258-022-01-04-902-20080121IPR19236-22-01-2008-2008-false/default_en.htm

Tagesspiegel vom 01.10.2007: Der falsche Klick

Wer auf der Internetseite des Bundeskriminalamts recherchiert, wird registriert - und möglicherweise zurückverfolgt. Weil Internetprovider Daten ihrer Kunden oft nur kurz speichern, soll nun das Gesetz geändert werden.

Die Internetseite des Bundeskriminalamtes hat nur 14 Zeilen. Unter „offene Tatkomplexe" beschreibt die Behörde die nach ihrer Darstellung linksterroristische Vereinigung „Militante Gruppe". Sie erwähnt etwa Bekennerschreiben zu zehn Brandanschlägen in Berlin und Umgebung – und die Beschäftigung der Aktivisten „mit verschiedenen linksradikalen Themenfeldern, aktueller Schwerpunkt ist die beabsichtigte Kürzung von Sozialleistungen", dazu gibt es ein paar Links. Wer sich im Netz diese offizielle Information einholt, riskiert was: Ausweislich eines Vermerkes der Behörde, der dem Tagesspie-

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

gel vorliegt, werden seit September 2004 die IP-Adressen – es geht um Zahlenkolonnen, die der eindeutigen Identifizierung von Rechnern dienen – aller Besucher dieser Internetseite registriert. Zudem versuchte die Behörde, einen Teil der Computerbesitzer zu identifizieren, die die betreffende BKA-Website besucht hatten.

...

Das BKA wollte zu der Speicherung und Auswertung der IP-Adressen keine Stellung nehmen und verwies auf die Bundesanwaltschaft. Dort hieß es, dass Internetüberwachung zu den Fahndungsmitteln zähle. Der innenpolitische Spreche der Unionsfraktion im Bundestag, Wolfgang Bosbach, sagte, dass die Registrierung von IP-Adressen im Zusammenhang mit Ermittlungsverfahren zum „täglichen Geschäft“ der Sicherheitsbehörden gehöre. Er sagte aber auch, er könne das „Motiv nicht erkennen, warum das BKA mit einer solchen Website in die Öffentlichkeit geht“. Der SPD-Innenpolitiker Dieter Wiefelspütz wollte den Vorgang nicht kommentieren, er habe sich „damit noch nicht befasst“.

Christian Ströbele, Fraktionsvize der Grünen, sagte, seine Fraktion werde den Fall zum Anlass nehmen, „im Bundestag weitere Aufklärung über die Motive des Bundeskriminalamtes zu verlangen“. Er bezweifle, dass ein solches Vorgehen zulässig sei. Man könne nicht übersehen, dass hier „eine große Zahl völlig unverdächtigter Personen in ein Raster kommen und unbequemen polizeilichen Maßnahmen ausgesetzt werden.“ Denn es sei nicht auszuschließen, dass die Polizei bei den Betreffenden anrücke – auch wenn gegen diese nichts vorliegt. Die innenpolitische Sprecherin der Linksfraktion, Ulla Jelpke, sprach von einer „Fangschaltung“ des Bundeskriminalamtes, dies sei ein „absoluter Skandal“. Es sei doch legitim, sich über die „Militante Gruppe“ zu informieren – und empörend, wenn Menschen deshalb „unter Generalverdacht zu geraten“.

(Erschienen im gedruckten Tagesspiegel vom 01.10.2007)

Link zum Artikel:
http://www.tagesspiegel.de/politik/deutschland/BKA-Datenschutz;art122,2390884#

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Datengipfel des BMI im Sommer 2008

Bis zum Sommer 2008 wurden einige schwere Datenschutzverstöße in der Bundesrepublik öffentlich bekannt. Diese Datenschutzverstöße waren so schwer, daß das Innenministerium deshalb einen „Datengipfel“ einberief, an dem u.a. auch die Ministerien für Wirtschaft und Justiz, sowie die Datenschützer von Bund und Ländern teilnahmen und eine Verbesserung des Datenschutzes beschlossen. Da diese hier vorgelegte Studie Anfang 2008 gestartet wurde, konnten verschiedene Mißstände bereits ein halbes Jahr vor den öffentlich bekannt gewordenen Verstößen aufgezeigt werden.

Ein erhebliches größeres Problem entsteht für jeden einzelnen Bundesbürger durch die Kombination unterschiedlicher Datenquellen, wie z.B. die gesetzliche Einführung einer lebenslangen Steueridentifikationsnummer (von der Geburt eines Menschen an!). Damit schafft der Staat die Voraussetzung, personenbezogene Daten direkt durch staatliche Organisationen und wirtschaftlich orientierte Unternehmen einer natürlichen Person lebenslang zuordnen zu können. Mit dieser ID kann zukünftig ein Profil einer Person auch ohne Cookie- oder Browser-Technologie (siehe auch Internetbeobachtung im Jahr 2007) hergestellt werden. Um diese Zuordnung herstellen zu können, muß einem Profiler die persönliche lebenslange Steuer-ID einmal bekannt gemacht werden. Das könnte z.B. über das Internet erfolgen, in dem ein Profiler einfach die Seiten des Finanzamtes (siehe auch Service für staatliche Bundes- und Landeseinrichtungen) beobachtet. Es wird vermutlich auch möglich sein, die Steuer-ID einer Person über die Meldeämter „bei einem berechtigten Interesse“ abzurufen! Ebenfalls wird es möglich sein, durch zwingende Abfragen, z.B. bei Internetbestellungen oder anderen Internetservices wie z.B. bei Bankservices, sie ermitteln zu können. Mit der einmaligen Preisgabe der lebenslangen Steuer-ID einer Person im Internet kann jeder Profiler dieser eindeutigen ID sämtliche Internetbesuche, Bestellungen, Forenbesuche, Kommunikation mit Freunden, persönliche Beziehungen, Kollegen etc., Bewegungsprofile und alle weiteren persönlichen privaten Dinge, die eine Person nutzt, zuordnen. Damit erhält ein Profiler mit Hilfe dieser staatlich zwangsweise verordneten ID die Möglichkeit, persönliche Profile z.B. durch ausländische Profiler zu erstellen und damit einen Datenhandel zu betreiben.

Heute werden bereits bei Bewerbern von qualifizierten Jobs Internetrecherchen durchgeführt, um die Persönlichkeit zu durchleuchten. In Zukunft ist eine Recherche nicht mehr notwendig. Eine Anfrage bei einem Profiler über eine ID würde ein tief strukturiertes Persönlichkeitsprofil eines Bewerbers liefern. Hat ein Bewerber z.B. in seiner Jugend Informationen im Internet hinterlassen, die sein persönliches Profil aus Sicht des Arbeitgebers belasten, könnte dieser Bewerber in bestimmten Berufen keine Einstellung mehr erhalten. Die Ablehnung eines Bewerbers durch einen Arbeitgeber würde niemals in Bezug auf die Auswertung eines Persönlichkeitsprofils gestellt werden. Der Bewerber würde die genauen Gründe einer Einstellungsablehnung nicht erfahren und hätte auch keine Möglichkeit der Rechtfertigung oder Korrektur. Ein Bewerber hätte damit niemals die freie Wahl eines Berufes oder einer Karriere, da er weder die erstellten

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Profile noch die dafür verwendeten Daten einsehen oder kontrollieren könnte.

Die Problematik wird vor diesem Hintergrund besonders bedrohlich, wenn dieses Prinzip der Datenzuordnung und Verwendung auf Führungskräfte von Unternehmen angewendet wird. Ein mittelständisches Unternehmen wird in der Regel durch einen Eigentümer geführt. Werden Persönlichkeitsprofile dieses Eigentümers Konkurrenten bekannt, oder hat der Eigentümer besonders interessante Patente oder Produkte, kann mit Hilfe des Persönlichkeitsprofils ein Angriffspunkt zur kostengünstigen Übernahme des Unternehmens, der Produkte oder der Patente durch ein konkurrierendes Unternehmen gefunden werden. Das gleiche Profil des Unternehmers oder Entscheidungsträgers könnte auch für Kreditbewilligungen, Versicherungsabschlüsse oder Ausschreibungsvergaben verwendet werden.

Sind diese persönlichen Profile erst einmal vorhanden, ist eine Kontrolle ihrer Anwendung und Verbreitung nicht mehr möglich. Die Kontrolle wird unmöglich, wenn die Profile durch ausländische Unternehmen weltweit erstellt worden sind (was zur Zeit der Trend im Internet ist). Ein Mißbrauch von Profilen erfolgt bereits heute (siehe öffentlich bekannt gewordene Datenschutzverstöße mit Bankdaten etc.) und wird in Zukunft in ihrer Verwendung an Subtilität und Unfang zunehmen. Durch eine gezielte Anwendung dieser Datensammlungen ist langfristig der freie Wille einer ganzen Gesellschaft in Gefahr und in der Hand weniger Datenmonopolisten, wie sie heute bereits entstehen. Die Gefahr der „Lenkung und Kontrolle“ ganzer Volkswirtschaften über deren Schlüsselpersonen, deren intime persönliche Daten bei Datenmonopolisten bekannt sind, wird dann um so realistischer, je stärker die Verbindung zwischen den Datenmonopolisten und den jeweiligen Regierungen - mit denen diese Datenmonopolisten zusammenarbeiten - ist. Natürlich kann auch eine Regierung selbst ein Datenmonopolist sein/werden und damit den freien Willen ihrer Bürger „abschaffen“.

Diese Szenarien sollten nicht unterschätzt werden, da sie bereits seit einigen Jahren in verschiedenen Think Tanks diskutiert worden sind und Bestandteil von Überlegungen in entsprechenden staatlichen Stellen unterschiedlicher Regierungen geworden sind. Sind die Daten von Personen mehrerer Generationen bekannt, können diese Daten auch über das ganze Leben Einzelner entscheiden.

Es ist zukünftig bei der Anwendung dieses Prinzips zur „*Anwendung intimer personenbezogenen Datenprofile*“ aus dem Internet und anderer Datenquellen auch denkbar, daß Kredit- oder Versicherungsbewilligungen diese Profile einschließen. In der hier erstellen Studie wird aufgezeigt, daß der Staat bereits in den Datenhandel indirekt integriert ist. Diese Aussage wurde vor dem Hintergrund der aktuellen Datenmißbräuchen belegt (siehe Kommentare zu den Meldeämtern). Die im Umfeld der jetzt öffentlich bekannt gewordenen Datenmißbräuche haben jedoch nicht nur diese Fakten bestätigt, sondern auch noch weitergehende Bezugsquellen, wie Banken, Lottogesellschaften, etc. öffentlich gemacht.

Betrachtet man die großen Datenquellen, wie Internet (tiefe persönliche Daten, wie Neigungen, Meinungen, Einstellungen, Ansichten, persönlicher Geschmack, intime Daten, Beziehungen, etc.), Schufa-

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

und Bankdaten (persönliche Wirtschaftskraft, gesellschaftliche Stellungen, Berufliche Funktion und Aktivität, etc.), Ämter (Wohnsitz, Steuerdaten, etc.), werden durch die Zusammenführung dieser Datenquellen umfangreiche Datenprofile eines jeden Menschen möglich. In dieser Studie wird darauf hingewiesen, daß ein Schutz vor diesem persönlichen „Datendiebstahl“ nur schwer möglich ist und das zur Zeit eine entsprechende politisch ausreichende Sensibilität gegenüber dem Thema fehlt. Zusätzlich sind die wenigen Schutzmechanismen der Masse der Internetnutzer nicht bekannt und finden deshalb auch keine weit verbreitete Anwendung.

Viel gravierender ist jedoch die extremen Naivität der gesellschaftlichen Führungseliten, die Datensammlung von international agierender Konzerne lediglich national in Bezug auf den Deutschen Staat zu sehen. Die nationale Souveränität eines Staates basiert auch auf der Hoheit des Staates über die Daten seiner Bürger. Diese Hoheit ist bereits für die jetzt lebenden Menschen vom eigenen Staat aufgegeben worden bzw. beteiligt sich der Staat an der Entwicklung einer vollständigen Überwachung und Aufzeichnung aller persönlichen Daten aller Personen eines Rechtsraums (siehe Pressemitteilung vom 11.09.2008 weiter unten). Diese Informations- und Datenhoheit besitzen bereits jetzt international agierende Konzerne (Aktiengesellschaften, die an der Börse notiert sind und IHRE Daten als eigenes Unternehmenskapital sehen, daß zukünftig im Wert entwickelt werden muß!), die mit personenbezogenen Daten eines Landes Geld verdienen (das kann auch z.B. dadurch erfolgen, daß wesentliche Datenprofile von den Eliten eines anderen Landes an die Regierung verkauft werden, in dem die Konzerne ihre Sitz haben!). Bei diesen Bestrebungen verliert das Individuum, und damit auch jeder Entscheidungsträger, die Hoheit und Kontrolle über seine persönlichen Daten, die die Grundlage seiner Persönlichkeit, seines Denkens, seiner Innovationen und seiner Entscheidungsgrundlagen sind.

Zu den aktuellen Entwicklungen auf EU-Ebene wurde folgende Pressemitteilung 11.09.2008 in Heise Online gemeldet:

(Verweis auf Aktikel:
http://www.heise.de/newsticker/EU-Innenpolitiker-wollen-saemtliche-digitalen-Nutzerspuren-ueberwachen--/meldung/115770)

EU-Innenpolitiker wollen sämtliche digitalen Nutzerspuren überwachen

Der von Bundesinnenminister Wolfgang Schäuble einberufenen "Zukunftsgruppe" zur Brüsseler Innenpolitik schwebt laut Statewatch vor, Sicherheitsbehörden uneingeschränkte Befugnisse zum Sammeln und Auswerten riesiger Datenmengen aus dem täglichen Leben der Bürger zu geben. Jeder Gegenstand, den ein Individuum nutze, jede Transaktion und jeder Schritt erzeuge einen detaillierten digitalen Eintrag in Datenbanken, zitieren die britischen Bürgerrechtler aus EU-Papieren für den künftigen Fünfjahresplan für die Sicherheitspolitik. "Dies wird einen Reichtum an Informationen für Sicherheitsorganisationen generieren und riesige Möglichkeiten für effektivere und produktivere Bemühungen um die öffentliche Sicherheit schaffen." Laut Statewatch droht so die Privatsphäre von dem in Brüssel ausgemachten "digitalen Tsunami" fortgespült zu werden.

Die Bürgerrechtler haben in einer Analyse verschiedener Berichte für das geplante "Stockholmer Programm" herausgearbeitet, dass das Prinzip, nach dem verfügbare Daten für Belange der Sicherheitsbehörden genutzt werden, künftig durch einen Ansatz der "Konvergenz" auch von Datenbanksystemen der Strafverfolger und Geheimdienste sowie von Abhöreinrichtungen ergänzt werden soll. Zudem schwebe der "Future Group" vor, die Grenzen zwischen innerer

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

und äußerer Sicherheit ebenfalls weiter zu verwischen und einen "gemeinsamen Kooperationsraum" mit den USA zu bilden. Nur eine ausführliche öffentliche Debatte könne die Verwandlung der EU in eine Überwachungsgesellschaft und ein autoritäres Staatengebilde noch verhindern.

Einzelheiten bringt ein Hintergrundbericht in c't – Hintergrund:

*(*http://www.heise.de/ct/hintergrund/meldung/115759*)*

siehe auch

http://www.heise.de/newsticker/Protest-gegen-Anti-Piraterieabkommen-ACTA--/meldung/116095

Werden diese international erstellten und gehandelten persönlichen Datenprofile auf die Spitzenkräfte und Entscheidungsträger einer Gesellschaft angewendet, besteht die Möglichkeit der gesellschaftlichen Lenkung und Beeinflussung. Für die Beeinflussung eines Entscheidungsträgers aus Politik und Wirtschaft können mit den Erkenntnissen aus diesen Datenprofilen subtile Methoden der Beeinflussung wie z.B. öffentliche Ehrungen, gesellschaftliches öffentliches Mobbing, Verweigerung von Wirtschaftskontakten, Verlust von Aufträgen, Ausschluß von Ausschreibungen, Verbreiten von Gerüchten im persönlichen Beziehungsgeflecht (das dann Fremden bekannt ist), Angebote bezogen auf persönliche Meinungen, Neigungen, Vorlieben und Bedürfnisse etc. zum Einsatz kommen.

Die in dieser Studie gemachten Aussagen und „Vermutungen“ zu den Entwicklungen mit und durch das Internet, und den damit verbundenen gesellschaftlichen Konsequenzen, werden in Zukunft erhebliche Bedeutung für eine wirtschaftliche Unabhängigkeit von externen Einflüssen einer Volkswirtschaft erlangen. Diese Einflüsse und Seiteneffekte im Bereich der Datenanwendungen sind jedoch nicht Bestandteil dieser Studie, sondern nur eine Konsequenz aus den hier aufgezeigten Fakten. In dieser Studie soll auf diese Konsequenzen aufmerksam gemacht, jedoch nicht weiter vertieft werden.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Einstieg in ein Sicherheitskonzept

Diese Abhandlung wurde vor dem Hintergrund zunehmender Beobachtungsanalyseaktivitäten von privaten Unternehmen im Internet geschrieben (siehe vorheriges Kapitel). Diese Unternehmen sammeln durch die Beobachtung von anderen Firmen Daten über deren Geschäftsverbindungen, Projekte, Mitarbeiter, Produkte, Bankverbindungen und vieles mehr. Nach dem Deutschen Recht sind diese Beobachtungstätigkeiten illegal, vor allem wenn sie von privaten Unternehmen durchgeführt werden. Ein Deutsches Unternehmen sollte aber sein Recht wahrnehmen können und sein „Recht auf informelle Selbstbestimmung“ zu mindestens ausüben können. Hier werden einige Praxistips gegeben, wie ein Unternehmen mit kleinem Etat sich schützen kann und eine bessere Kontrolle über die Daten erhält, die es im Internet preis gibt. Sicherheit und Anonymität von Internetaktionen (senden und empfangen von Daten, Surfen im Internet, E-Mail Verkehr, etc.) sind ein weites Feld. Hier sollen nur wesentliche und einfache Hinweise gegeben werden, die erprobt sind und einen effizienten Schutz gegen die meisten privatwirtschaftlich arbeitenden Datensammler im Internet geben.

In den heutigen Sicherheitskonzepten hat sich das Angriffsszenario über einen zerstörerischen Virus auf das Ausspähen von privaten oder geschäftlichen Informationen verschoben. Ein Angriff eines Virus kann heute in der Regel besser erkannt und in seinen Auswirkungen verkraftet werden, als ein nicht erkanntes Ausspähen eines Rechners oder eines Firmennetzwerks. Dabei ist ein Angriff auf einen Rechner von dem Betroffenen nicht differenzierbar, ob der Angreifer eine staatliche Organisation ist („Bundestrojaner“), ein Unternehmen oder eine Privatperson ist. Deshalb muss ein Schutz eines Rechner generell gegen alle Angriffe funktionieren.

Die Sicherheit eines Rechners, und die darin enthaltenen Daten, wird durch die lokalen Programme selbst und die Kommunikation über das Internet bestimmt. Die Kommunikation eines Rechners mit einem anderen Rechner über das Internet kann und wird beobachtet, protokolliert und ausgewertet. Wer mit wem eine Verbindung aufbaut, welche Internetseiten aufgerufen werden und welche Eingaben auf Internetseiten vorgenommen werden, wird mit anderen Daten z.B. bei Google, Yahoo, etc. zu individuellen Profilen zusammengestellt. Dabei spielen Cookies eine besondere Rolle. Bei der Identifikation eines individualisierten Rechner sind Cookies eine einfache aber wirksame Schlüsseltechnologie.

Das Internet kennt durch seinen strukturellen Aufbau prinzipbedingt keine Privatsphäre eines Benutzers. Das Internet wurde nicht für ein anonymes „Surfen“ entworfen und sieht auch deshalb keine entsprechenden Mechanismen vor. Aus diesem Grund müssen zusätzliche Technologien für diesen Anspruch zum Schutz der Privatsphäre entwickelt und eingesetzt werden. Bei der Beobachtung des Netzes wird zwischen den Verbindungen der Rechner untereinander und den Dateninhalten unterschieden. Die Verbindung, wer mit wem verbunden ist, sagt noch nichts über die ausgetauschten Informationen aus. Deshalb wird auch von Profilern und Anderen versucht zu erkennen, welche Daten ausgetauscht worden sind. Generell werden

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

die Inhalte z.B. von E-Mails analysiert. Das erfolgt durch große Unternehmen, wie auch durch staatliche Organisationen. Deshalb sollten in festen Benutzergruppen ausschließlich verschlüsselte E-Mails ausgetauscht werden.

Ein offizielles - wenn auch nicht legales (siehe Kapitel „Internetbeobachtung im Jahr 2007“) - Feld ist die Ermittlung des Konsumverhaltens in Form von Persönlichkeitsprofilen, daß auf den gleichen Techniken basiert, die oben beschrieben worden sind. Diese gesammelten Daten werden zu komplexen Konsumlandkarten zusammengestellt. Durch die Individualisierung von Profilen können z.B. die Konsumenten aus einem Gebiet einer Stadt mit viel Kaufkraft persönlich angesprochen werden. Ihnen kann aufgrund der Datenanalyse ein individuelles Angebot unterbreitet werden. Natürlich werden über den gleichen Mechanismus Firmen ausspioniert. In diesem Feld sind in den letzten Jahren durch ihre Tätigkeiten vor allem die Chinesen, Amerikaner, Israelis und Franzosen öffentlich bekannt geworden. Mann kann davon ausgehen, daß in der Regel heute alle relevanten europäischen Unternehmen beobachtet werden. Deshalb wissen häufig auch Konkurrenzunternehmen in Asien sehr früh, welche Produkte zu kopieren sind.

Die Frage ist, gibt es einen Schutz und wie kann man sich schützen?

Sicherheit beginnt mit Vertrauen. Ein Unternehmen kann z.B. in Verbindung mit staatlichen Organisationen Programme verkaufen, die Hintertüren enthalten (Sicherheitssoftware die Backdoors von Geheimdiensten enthalten wurden bereits in der Presse veröffentlicht. Der BND und andere Geheimdienste wenden diese Strategie und Technik an). Jedes private Softwareunternehmen kann prinzipiell durch einen anderen Interessenten (Unternehmen, Privatperson, Organisationen oder Institutionen) aufgekauft werden. Dieser Interessent kann als Eigentümer oder Mehrheitsaktionär nun bestimmen, welche Eigenschaften eine Software besitzt. Welche Unternehmen heute Backdoors in ihren Produkten verwenden, kann nicht abgeschätzt werden. Vor allem vor dem sich weiter entwickelnden Trend zum Handel mit Informationen von Firmen und Privatpersonen, mit dem bereits zahlreiche Unternehmen große Gewinne erwirtschaften (siehe auch Schufa und andere Auskunftsdienste und Suchmaschinen wie Google, Yahoo, und Profiler wie z.B. eTracker, etc.).

Wenn unsere Daten in Tausenden internationaler Datenbanken abgelegt sind, müssen wir uns damit abfinden? Ist vor diesem Hintergrund ein freier Wille noch realisierbar? Nach der Auffassung des Autors muss der erste Schritt darin bestehen, daß bei Unternehmen, Instituten, Wissenschaft, Gerichten und privaten Personen ein Bewußtsein für die wirklichen Verhältnisse im Internet entsteht. Wie bereits im Kapitel „Zusammenfassung zur Netzbeobachtung“ angemerkt, wäre eine Kapitulation vor der Sammel- und Auswertewut eine Wende in der gesellschaftlichen Entwicklung, daß von keiner Seite gewollt werden kann. Durch die immer detaillierteren Profile von Unternehmen und Personen als Grundlage/Ware für internationale Geschäfte von anderen privaten Unternehmen, kann die Gefahr ausgehen, daß die Ausübung des freien Willen z.B. von Unternehmensführungen nicht mehr möglich ist. Sind detaillierte persönliche

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Profile von Entscheidungsträgern eine Ware die gehandelt wird, dann liegt die Gefahr der Manipulation in greifbarer Nähe. Sind von vielen Entscheidungsträgern einer Gesellschaft die Profile eine Ware, mit der Geld verdient werden kann, dann besteht die Gefahr für eine Gesellschaft, ihren „freien Willen“ zu verlieren.

In den Sicherheitsdoktrin geht man von der These aus, daß prinzipbedingt Programme von Softwareunternehmen weniger vertrauensvoll sind als öffentlich kontrollierte Programme. Hier gilt das Prinzip, daß ein Programm, daß durch viele Entwickler öffentlich im Sourcecode kontrolliert werden kann, vertrauenswürdiger ist, als ein Programm, das nicht öffentlich kontrolliert werden kann. Open Source spielt nach der Einschätzung des Autors damit eine immer stärker werdende Bedeutung, die durch entsprechende Marketingstrategien weiter ausgebaut werden könnte. In den Sicherheitsstrategien gilt das zur Zeit nur für Programme, die eine Kommunikation mit dem Internet eingehen oder Daten zur Übertragung durch das Internet herstellen. Wie im ersten Kapitel bewiesen, reichen Selbstverpflichtungen von Unternehmen zum Schutz privater Daten nicht aus. Zur Zeit erscheint die öffentliche Kontrolle der Sourcecodes (Transparenz) als einzige Strategie akzeptabel und wirksam.

Sicherheit im Internet beginnt bei den Programmen, die auf dem Rechner mit Internetzugang eingesetzt werden. Dabei spielt die Administration des PC's oder eines Unternehmenssystems eine wichtige Rolle. Werden nach der Installation der Programme (z.B. Internet-Browser, E-Mail-Programm, etc.) die voreingestellten Werte verwendet, kann davon ausgegangen werden, daß die persönlichen Daten eines Unternehmens oder einer Privatperson nicht geschützt werden. Dabei beschränkt sich die Sicherheit eines PC's nicht nur auf Virenscanner und Firewalls (siehe auch erstes Kapitel). Zum Schutz der persönlichen Daten müssen alle Programme in eine Sicherheitsstrategie einbezogen werden, mit denen Daten über das Internet übertragen werden, wie auch Programme, mit denen Daten erstellt werden, die über das Internet verschickt werden (z.B. Textprogramm, Tabellenkalkulation, etc.).

Im folgenden wird zwischen

1. einfachen und wirkungsvollen Methoden von lokalen Programmen und
2. wirksamen Methoden zur Erschwerung bei der Beobachten der Kommunikation im Internet

unterschieden (siehe auch „Schutz durch vertrauensvolle Programme“).

In der Studie „Faktor Mensch“ von SAP wird ausführlich auf weitere Schwachstellen außerhalb des Internets eingegangen (lesenswert).

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Lokale Programme

Die hier beschriebenen Programme beziehen sich auf eine Microsoft Windows Betriebssystemumgebung. Das Betriebssystem Windows ist mit großem Abstand weltweit marktführend und gilt somit als Standard. Die Auflistung der folgenden Programme ist nicht als eine Präferenz für oder gegen irgend einen Hersteller zu werten. Grundsatz der Empfehlungen sind lediglich Sicherheitsaspekte zum Schutz der eigenen Daten.

Die folgenden Beschreibungen müssen vor dem Hintergrund verstanden werden, daß Angriffe über das Internet nur von Experten durchgeführt werden. Deshalb können Abwehrmaßnahmen gegen diese Angriffe nur wirkungsvoll mit einem Minimum an Know How begegnet werden. Die folgenden Beschreibungen setzen dieses Minimum voraus.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Schutz durch vertrauensvolle Programme

Wie oben bereits beschrieben, sollten die Programme, die täglich für eine Kommunikation mit dem Internet genutzt werden, durch Programme ausgeführt werden, die durch eine breite Öffentlichkeit im Sourcecode kontrolliert werden können. Dazu zählen die Programme Internet Explorer, E-Mail Programm, Terminverwaltung, Verschlüsselungssoftware, Office-Programme (Textverarbeitung, Präsentation, Tabellenkalkulation) und wenn möglich Firewalls und Virenscanner.

Um einen Rechner, der ein Microsoft-Betriebssystem nutzt, sicherer zu machen, sollten die folgenden vorinstallierten Programme gegen Open Source Programme ausgetauscht werden. Die Programme lassen sich in folgende Kategorien unterteilen:

- Proxy Server
- Firewall
  (kein Open Source-Produkt guter Qualität z.Z. verfügbar)
- Anti Virus Programm
  (kein Open Source-Produkt guter Qualität z.Z. verfügbar)
- Internet Explorer
- E-Mailprogramme
- Terminplaner
- ggf. Office Software, wenn der Rechner direkt als Internetrechner genutzt wird.

Zu jeder Kategorie werden in den folgenden Kapiteln Empfehlungen gegeben. Fast alle oben aufgelisteten Kategorien können kostenlos in hoher Qualität aus dem Internet als Open Source bezogen werden. Teilweise sind die kostenlosen Programme leistungsstärker als die kostenpflichtigen Konkurrenzprodukte.

Bei den Firewalls und den Antivirusprogrammen sind zur Zeit keine leistungsstarken Open Source Programme dem Autor bekannt. Hier kann man auf getestete Programme von bekannten Softwareanbietern zurückgreifen. Die breiten öffentlichen Tests dieser Programmgruppe garantiert einen gewissen Schutz vor Hintertüren, die für das Ausspähen von Rechner genutzt werden können. Auch die Programme, die nicht als Open Source angeboten werden, können häufig als Freeware kostenlos bezogen werden.

In den folgenden Kapiteln werden Programmvorschläge für die drei sicherheitsrelevanten Bereiche eines Rechner mit Internetzugang unterbreitet:

- Lokale Programme
- Interfaces zum Internet
- Aktivitäten im Internet

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Zu 0: Proxy Server

Proxy Server können lokale Programme auf dem Internetrechner sein, eigenständige Rechner im eignen LAN oder Rechner außerhalb des eigenen Netzwerks. Hier soll nur auf die Variante der „lokalen Programme“ eingegangen werden.

Proxy Server sind kleine Programme, die zwischen die Kommunikation des Rechners und dem Internet geschaltet werden und zu der Kategorie der „Interfaces zum Internet“ zählen. Ein Proxy Server entkoppelt also den Rechner mit dem Internet. Zusätzlich kann der Datenstrom über den Proxy Server sehr effizient kontrolliert werden. Mit diesen „Filtern“ können z.B. Informationen des eigenen Rechner anonymisiert werden, lästige Popups beim Surfen unterdrückt und die eigene Identifikation für Beobachtungsprogramme im Internet verändert werden.

Ein kleines kostenloses und extrem leistungsfähiges Programm ist Proxomitron (und sein Nachfolger Proximodo), daß als lokaler Proxy Server installiert wird. Für einen Download kann folgender Link genutzt werden.

Download Link: http://www.buerschgens.de/Prox/Seiten/Download/

Download Link Proximodo: http://proximodo.sourceforge.net/

Nach dem Download (Standard- oder Profiversion) kann das Programm einfach installiert werden. Es sollte durch den Start von Windows automatisch gestartet werden. Die mitgelieferten Filter sind für einen sicheren Schutz im Standardfall ausreichend. Nach der Installation des Programms muss der Zugang zum Internet (Modemeinwahl, DSL-Konfiguration, LAN-Konfiguration) auf den Proxy Server eingestellt werden. Diese Einstellung vorzunehmen ist sehr einfach. Folgen sie dabei der Beschreibung auf der oben angegebenen Internetseite.

Weitere kostenlose lokale Proxy Server können alternativ eingesetzt werden. Alle Proxy Server können auch alternativ im Tor Projekt eingesetzt werden. Zu empfehlen sind

Privoxy:
Ein Proxy Server, der im Tor-Projekt enthalten ist (siehe auch Tor Projekt).

Download Link und Homepage: http://www.privoxy.org/

Polipo:
Ein Proxy Server, der mit einer Cache-Funktion ausgestattet ist. Damit besonders schnelles Surfen möglich. Unterstützt IPv6.

Download Link und Homepage: http://www.pps.jussieu.fr/~jch/software/polipo/

3Proxy:
Proxy Server für fast alle Internetprotokolle und Dienste, einschließlich FTP, POP3, SMTP.

Download Link und Homepage: http://3proxy.ru/documents/

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Weitergehende Informationen über externe Proxys und welche man nicht nutzen sollte (Proxy Server z.B. vom Militär oder Geheimdiensten etc.), können auch unter

http://www.proxy-listen.de/Tutorials/Allgemeine-Informationen-uber-Proxies.html

abgerufen werden.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Zu 1: Firewall

Anstelle der Standard-Firewall von Microsoft, die ab dem Betriebssystem XP ausgeliefert wird, sollten folgende Firewalls eingesetzt werden: Comodo Firewall Pro 3.0.19.318 oder höher, Online Armor Personal Firewall 2.1.0.112 Free oder höher. Die Programme wurden nach einem Ranking der Internetseite Matousec (http://www.matousec.com/projects/firewall-challenge/results.php) vom 30. März 2008 als einer der besten kostenfreien Programme eingestuft. Für Windows 98 oder Windows 2000 PC's empfiehlt sich die Firewall von NetVeda „Safety.Net“. Sie ist unter den älteren Betriebssystemen voll einsatzfähig. Alle Programme sind kostenlos für den privaten Gebrauch erhältlich und in der kostenlosen Version fast perfekt im Schutz vor externen Angriffen. Für die Installation in einer Firma muss eine Lizenz erworben werden, die jedoch in der Regel preisgünstig erworben werden kann.

Download Link Comodo Firewall:
http://www.heise.de/software/download/comodo_firewall_pro/30612

oder

Download Link Online Armor:
http://online-armor-free.softonic.de/

Installieren sie eine der oben angegebenen Firewalls. Deaktivieren oder deinstallieren sie vorher die Standard-Firewall von Windows.

Nach der Installation der neuen Firewalls sollten kleinere Anpassungen erfolgen, die jedoch an dieser Stelle nicht beschrieben werden können, da für jedes Programm andere Einstellungen gelten. Die Voreinstellungen der oben angegebenen Firewalls sind jedoch bereits viel sicherer, als die Standardeinstellungen der Firewall von Windows. Alle angegebenen Firewalls konzentrieren sich nur auf ihre eigentliche Aufgabe, den Datenverkehr zu kontrollieren. Deshalb sind die Belastungen des Rechners minimiert.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Zu 2: Antivirus

In der Ergänzung zu der Firewall und dem Proxy Server können einfache Antivirusprogramme eingesetzt werden. Vollversionen mit Firewall-Funktionen sind nicht notwendig. Ein aktueller Test von Antivirusprogammen kann in der Zeitschrift PCWelt (Online link http://www.pcwelt.de/start/sicherheit/antivirus/tests/144166/) oder bei CHIP (mit Ranking) http://blog.chip.de/0-security-blog/maerz-2008er-security-suiten-im-vergleich-20080310/ nachgelesen werden. Zur Zeit können folgende kostenlose Produkte für das Betriebssystem XP oder höher empfohlen werden:

Download Link AV Antivir:
http://www.free-av.de/de/download/1/avira_antivir_personal__free_antivirus.html

oder

Download Link ALWIL Software AVAST: (auch für W98 einsetzbar)
http://www.avast.de/index.php/Desktop-Produkte/Desktop-Losungen/

oder ab Windows 98 (Windows 9) und höher

http://www.avast.com/ger/avast_4_home.html

Bei der Antivirussoftware AVAST ist eine empfehlenswerte Sonderfunktion vorhanden, die VRDB ("Virus Recovery Database"). Mit dieser Funktion können infizierte Dateien sicherer wieder hergestellt werden.

Bei der AVAST-Firewall ist eine Registrierung notwendig, mit dem gegenüber dem Hersteller versichert wird, daß eine kostenlose Benutzung nur dann zulässig ist, wenn sie privat und nicht kommerziell ist.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Zu 3: Internet Explorer

Grundsätzlich ist der Internet-Explorer von Microsoft offener und „informationsfreudiger“ als andere Internet-Explorer wie z.B. Firefox von Mozilla. Der Internet Explorer von Microsoft kann durch eine manuelle Konfiguration in seiner voreingestellten „Informationsfreudigkeit“ eingeschränkt werden. Der Firefox basiert auf Open Source. Deshalb sollte für ein sicheres Surfen im Interne auf Mozilla Firefox umgestiegen werden. Für den Firefox können zusätzliche kostenlose Addons installiert werden, die den Explorer mit Funktionen ausstatten, die der Internet-Explorer von Microsoft nicht besitzt. Der Firefox-Browser ist sehr gut zu bedienen und funktioniert auf allen Windows Betriebssystemen wie Win98, Win2000, XP, Vista. Die zahlreichen Addons müssen für Firefox einzeln heruntergeladen und installiert werden. Diese Arbeit gestaltet sich sehr einfach. Wichtiger ist, die richtigen Addons zu kennen, die die Sicherheit des Explorers erweitern. Eine detaillierte Konfiguration kann auf Wunsch geliefert werden. Im folgenden werden die wichtigsten Sicherheits-Addons aufgelistet. Sie können direkt über den Browser installiert werden. Geben sie in dem Suchfeld der Addon-Internetseite die unten aufgelisteten Begriffe ein, damit das entsprechende Modul gefunden werden kann.

- MR Tech Local Install
- CS Lite
- NoScript
- RefControl
- AddBlock Plus
- FoxyProxy (empfehlenswert. Notwendig nur wenn Tor-Privacy Shield installiert werden soll)
- CacheViewer
- SafeCache
- SafeHistory
- Live IP Address
- Stealther

Für eine deutsche Rechtschreibkontrolle sollte das deutsche Wörterbuch heruntergeladen werden. Nach der Installation aller Addons erscheinen verschiedene Angaben in der Statusleiste. Mit diesen "Icons" können z.B. Java-Scripte für jede Internetseite individuell aktiviert werden. Ein weiteres Icon/Schalter stellt eine wirkungsvolle Steuerung von Cookies zur Verfügung. Generell sollten alle Cookies beim Surfen abgelehnt werden. Die Grundeinstellung erfolgt beim Firefox im Menü „Extras“, „Einstellungen“, auf der Seite „Datenschutz“. Klicken sie im Feld „Cookies akzeptieren“, so das ein Haken erscheint. Tragen sie anschließend in der darunter liegenden Auswahlliste „Behalten bis...“ den Wert „jedes mal nachfragen“ ein. Bestätigen sie anschließend den Dialog mit OK. Ebenfalls sollten Java-Scripte nur temporär für entsprechende Seiten zugelassen werden. In der Regel werden aktive Scripte nicht zur Anzeige von Webseiten

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

benötigt, sondern nur für Zusatzfunktionen wie z.B. Animationen, Downloads etc. Mit Hilfe der empfohlenen Addons kann für jede aufgerufene Internetseite ein Cookie akzeptiert oder abgelehnt werden. Die Regel sollte sein, daß Cookies vollständig abgelehnt werden (nach der oben angegebenen Einstellung). Mit der angegebenen Einstellung wird vom Browser im Bedarfsfall ein Dialog automatisch ausgegeben, in dem der Internetbesucher einfach auf den Button „Annehmen“ drücken kann, sofern es zwingend notwendig ist. In der Regel sollte immer der Button „Ablehnen“ gedrückt werden. Der Browser hat sich für diese Web-Seite die Einstellung gemerkt und wird den Dialog nicht mehr ausgeben.

Bei Java-Scripten verhält sich Firefox ähnlich wie bei den Cookies. Sollte eine Seite nicht korrekt angezeigt werden, können sie das notwendige Java-Script temporär aktivieren. Auch diese Einstellungen werden vom Browser für jede aufgerufene Internetseite gespeichert, so daß nach und nach individualisierte Einstellungen pro Internetseite entstehen. Damit ist ein Höchstmaß an Sicherheit und maximalem Komfort gegeben.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Zu 4: E-Mail Programm

Ein sehr gutes E-Mail Programm, das den oben beschriebenen Sicherheitskriterien genügt, ist Mozilla Thunderbird. Es läuft auf allen Windows-Plattformen. Nach der Installation können alle Datenbestände, Adressen etc. z.B. aus Outlook importiert werden. Thunderbird bietet zahlreiche Sicherheitsfunktionen als integrierte Funktionen an, die bei Outlook zusätzlich käuflich erworben werden müssen. In Thunderbird lassen sich Terminplanfunktionen integrieren, so daß für einen Outlook-Benutzer alle gewohnten Funktionen (wie bei Outlook selbst) verfügbar sind. Zusätzlich können zahlreiche Addons installiert werden, die das Programm mit Funktionen ausstattet, die bei anderen Programmen nicht vorhanden sind.

Der Terminplaner ist ein Addon mit dem Namen "Lightning", der zusätzlich installiert werden muss. Wichtig ist, daß alle Einstellungen, wie z.B. Konten, in externe Backup-Dateien gespeichert werden können. Sollte eine Neuinstallation von Thunderbird notwendig werden, können diese Profile wieder importiert werden. Damit entfällt eine erneute Konfiguration der Konten. Viele weitere nützliche Sicherheitsfunktionen, z.B. eine Junk-Lernfunktion, sind ebenfalls vorhanden. Mit Hilfe der Junk-Lernfunktion können Spam-Mails markiert werden. Nach der Markierung merkt sich Thunderbird den Absender. Eine erneute Zusendung einer beliebigen E-Mail von diesem Absender wird damit sofort in einen gesicherten Bereich verschoben oder kann automatisch gelöscht werden. Das Programm Thunderbird ist kostenlos als Open Source erhältlich.

Die integrierte Kalenderfunktion *Lightning* arbeitet mit einem zusätzlichen externen Kalenderprogramm mit dem Namen Mozilla Sunbird zusammen. Mit dem Kalenderprogramm können alle Kalender und Zeitmanagementaufgaben unabhängig vom E-Mailprogramm, also auch offline vom Internet, durchgeführt werden. Mit diesem separaten Programm können weitergehende Funktionen für den Kalender genutzt werden. Beide Programme arbeiten mit den gleichen Kalender. Details siehe auch unter Terminplaner.

Verschlüsselungssoftware

Thunderbird arbeitet reibungslos mit der Open Source Verschlüsselungssoftware *OpenPGP*, mit dem Namen *Enigmail*, zusammen. Sie sollte nach der Installation von Thunderbird installiert werden. Mit diesem Addon kann der gesamte E-Mailverkehr, wie auch Daten auf dem Rechner selbst verschlüsselt werden. Kostenlose Trustserver für die Schlüsselverwaltung werden ebenfalls zur Verfügung gestellt. Damit können Empfänger von E-Mails auch verschlüsselte E-Mail erhalten und ohne Probleme lesen. Interne Firmenangaben oder private Namen sollten in den Schlüsselangaben vermieden werden, da in der Vergangenheit von einigen Trustservern die Schlüssel zur Identifikation von E-Mails und anderen Absendern verwendet worden sind. Deshalb sollten öffentliche Schlüssel auf Trustservern nur pseudonyme/anonymisierte Daten enthalten (siehe weiter unten „Tip“). Thunderbird ist kostenlos und Open Source.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Mit der Verschlüsselung des Datenverkehrs zwischen Absender und Empfänger wird eine einfache Auswertung von E-Mails nach Schlüsselbegriffen unmöglich oder erschwert! Für einen festen Kreis von E-MailEmpfängern sollten generell nur gesicherte Daten (verschlüsselt) ausgetauscht werden. Bei Thunderbird und OpenPGP erfolgt die Verschlüsselung und Entschlüsselung automatisch, ohne daß der Benutzer nach der Einrichtung von diesem sicheren Datenverkehr etwas merkt.

Download Link OpenPGP (deutsche Version)
http://www.gpg4win.de/

Der hier vorgestellte Download enthält alle Programme und Dokumentationen, die für die Software und einen komfortablen Gebrauch notwendig sind. Nach der Installation der Software können Schlüssel erzeugt und verwendet werden. Die Software ist auf Windows 98 lauffähig. Es werden zwei Schlüsselverwaltungen installiert. Für Windows XP sollte das Programm GPA verwendet werden. Es kann auch WinPT eingesetzt werden (Win98). Beide Programme können alternativ ab Windows XP eingesetzt werden.

Tip:

Generell sollten keine persönlichen E-Mailadressen im Internetverkehr oder bei Anmeldungen/Identifikation auf Internetseiten verwendet werden. Aus einer privaten E-Mail kann häufig der Name einer Person ermittelt werden oder ein direkter Bezug zwischen E-Mailadresse und einem Vertrag mit einem Provider abgeleitet werden. In Verbindung mit der IP-Adresse ihres Providers kann der persönliche Wohnort und andere Daten ermittelt werden. Nutzen sie generell zusätzlich zu ihrer persönlichen E-Mailadresse, die in der Regel durch ihren Provider vergeben wird, weitere E-Mailadressen. Ihre persönliche E-Mailadresse sollte geheim bleiben und bei keinem Internetverkehr auftreten. Ratsam ist die Einrichtung mehrerer Pseudonyme und E-Mailadressen in Abhängigkeit von den Gruppen, mit denen sie kommunizieren. Sie können z.B. ein reserviertes Pseudonym für den privaten E-Mailverkehr mit Freunden und Bekannten nutzen. Für den persönlichen Geschäftsverkehr sollten ebenfalls Pseudonyme in der E-Mailadresse verwendet werden, in denen nicht der persönliche Name enthalten ist. Im Geschäftsverkehr sollten anonyme E-Mailadressen z.B. für Projekte oder andere zeitlich begrenzten Prozesse zusätzlich eingerichtet werden. Alle zusätzlich eingerichteten E-Mailadressen sollten bei mehreren Anbietern von kostenlosen E-Mailaccounts eingerichtet werden. Der Eingang/Empfang von E-Mails über diese Pseudonyme wird zum privaten/persönlichen/zentralen (geheimen) E-Mailaccount weitergeleitet. In dem empfohlenen Programm Firefox können ausgehende E-Mails über eingerichteten Pseudonyme flexibel verschickt werden. Vor allem bei Kleinen- und Mittelständischen Unternehmen (KMU) sollte eine klare Vorgabe im eigenen Interesse von der Geschäftsführung für die Strukturierung des E-Mailverkehrs und deren Kommunikationskonten vorhanden sein.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Zu 5: Terminplaner

Ein zusätzlicher Terminplaner zum Addon im Firebird ist eigentlich nicht notwendig. Das hier vorgestellte und empfohlene Mozilla Sunbird ist eine Ergänzung zum oben (zu Absatz 4) erwähnten Lightning. Durch den Einsatz von Sunbird wird eine Entkopplung des Zeitmanagements vom E-Mailverkehr erreicht. Mit dem Sunbird stehen weitere Funktionen zur Verfügung, wie z.B. der Import von Kalenderdaten aus Outlook. Beide Programme (Sunbird und Lightning) arbeiten auf dem gleichen Terminplan, so daß ohne Probleme in beiden Programmen im gleichen Kalender Termine verwaltet werden können. Der Terminplan kann innerhalb eines Netzwerks auch auf einem Server abgelegt werden, so daß Kollegen gemeinsam auf einen Terminplan zugreifen können. Das Programm ist kostenlos und Open Source.

Das Quartett Thunderbird, Lightning, Sunbird und OpenPGP ergänzen sich bestens und stellen eine höhere Leistungsfähigkeit und bessere Sicherheitsfunktionen zur Verfügung als die vergleichbaren Produkte, die nach dem Erwerb eines Rechner in der Regel vorinstalliert sind.

Download Link Thunderbird:
http://www.mozilla-europe.org/de/products/thunderbird/

Download Link Lightning: über Addons in Thunderbird installieren.

Download Link Sunbird:
http://www.sunbird-kalender.de/downloads.php (Lightning und Kalender)

Download Link OpenPGP (GnuPG) für Windows:
http://www.gpg4win.de/

Alle Programme stehen in Deutsch und kostenlos zur Verfügung.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Zu 6: Office Programme

Häufig kommunizieren die MS-Office Programme mit dem Internet. Nach den oben beschriebenen Doktrin (siehe auch Kapitel Einstieg in ein Sicherheitskonzept) kann das gesamte MS-Office Paket ebenfalls gegen ein leistungsfähigeres kostenloses Softwarepaket ausgewechselt werden, das auf Basis von Open Source basiert. Es wird als OpenOffice bezeichnet und ist von der Firma Sun Microsystems. Mit dieser Software stehen ebenfalls Funktionen für Animationen, Erstellung von Grafiken, Erstellung von 3D-Grafiken, Excel-ähnliches Tabellenkalkulationsprogramm und vieles mehr zur Verfügung. Es ist auf allen MS-Windows Plattformen lauffähig. Die Dateien können in den jeweiligen Formaten von MS-Office gespeichert werden. Es ist eine gute Daten- und Formatkompatibilität vorhanden. Sehr komfortabel sind die im OpenOffice integrieren Exportfunktionen in das PDF-Format.

Download Link OpenOffice:
http://de.openoffice.org/downloads/quick.html

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Absicherung gegen Profiling im Internet

Nach dem Kapitel „Lokale Programme“, daß die Aspekte der Sicherheit auf einem lokalen Rechner thematisiert hat, wird im folgenden Kapitel der Bereich der „Absicherung gegen Profiling im Internet“ thematisiert. Im folgenden werden nur praxistaugliche Methoden für geringe Etats empfohlenen, die auch eine möglichst hohe Sicherung seiner eigenen Persönlichkeitsrechte ermöglichen.

Viele am Markt angebotenen Programme sind häufig unbrauchbar und bieten diesen Schutz nicht. Die hier empfohlenen Technologien bieten einen ziemlich hohen Schutz, jedoch wird dieser Schutz durch eine Verringerung der Kommunikationsgeschwindigkeit mit den aufgerufenen Internetseiten „erkauft“. Dabei sollte beachtet werden, daß häufig Bezahldienste nicht unbedingt wesentlich mehr Kommunikationsleistung bieten. Bevor endgültige Verträge mit Bezahldiensten abgeschlossen werden, sollte die Kommunikationsleistung über mindestens eine Woche (7 Tage) stichprobenartig geprüft werden. Alle hier empfohlenen Technologien bieten jedoch bereits in der kostenlosen Version einen akzeptablen Datendurchsatz, der natürlich Abhängig von der Tageszeit und dem zu diesem Zeitpunkt vorhandenen Internetverkehr ist.

Was ist eine „Beobachtung“ und worin bestehen die Gefahren (siehe „Internetbeobachtung im Jahr 2007“). Wie funktioniert eine Beobachtung von Internetnutzern? (siehe „Funktionsprinzip der Technologie“) Warum werden Unternehmen und Privatpersonen im Internet beobachtet? Ist die Erstellung von Kommunikationsprofilen nicht strafbar? (siehe „Rechtslage und Wirklichkeit“) Hilft mir das Kommunikationsgesetz bei der Verfolgung von Rechtsverstößen im Internet? Hilft mir eine deutsche oder europäische Behörde bei Rechtsverstößen durch ausländische Unternehmen? (siehe „Service für staatliche Bundes- und Landeseinrichtungen“)

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Funktionsprinzip und Technologie

Das Internet ist ein offenes Netzwerk, in dem jeder Teilnehmer über Adressen mit anderen Teilnehmern kommuniziert. Eine Internetadresse funktioniert wie eine normale Postadresse, mit Angaben eines Namens, der Straße, der Postleitzahl und Stadt. In der Welt des Internets werden all diese Daten in Form von Zahlen ausgedrückt. Eine Adresse im Internet wird auch als IP-Adresse bezeichnet, die den persönlichen Anschluss eines Internetnutzers eindeutig identifiziert.

Jeder Internetnutzer benutzt für den Zugang zum Internet einen Provider. Der Provider hat die Aufgabe, viele Internetnutzer mit geringen Bandbreiten z.B. über ISDN oder DSL zu bündeln und über einen sehr schnellen Anschluß an andere Sammler (Provider) weiterzuleiten. Jeder Provider ist also ein wesentlicher Bestandteil des Internets.

Möchte nun ein Internetnutzer, von seinem Arbeitsplatz oder von Zuhause, sich in das Internet einwählen, verbindet er sich zuerst mit dem Provider. Damit der Internetnutzer sich mit dem Provider verbinden kann, wurde für diese Dienstleistung ein Vertrag zwischen Internetnutzer und Provider geschlossen. In diesem Vertrag wird festgelegt, wie sich der Internetnutzer mit dem Provider technisch verbinden darf.

Nachdem sich der Internetnutzer mit dem Provider technisch verbunden hat (Einwahl), besitzt der Anschluß des Internetnutzers eine weltweit eindeutige IP-Adresse, also eine eindeutige Postanschrift. Diese IP-Adresse wird in der Regel dynamisch vergeben. Das bedeutet, daß eine eindeutige IP-Adresse so lange gültig ist, bis der Benutzer sich wieder vom Provider abmeldet. Ist der Internetnutzer länger als 24 Stunden bei einem Provider angemeldet, wird in der Regel eine neue IP-Adresse vergeben. Statische IP-Adressen müssen explizit beantragt werden. Sie werden in der Regel nur für sehr schnelle Datenverbindungen zwischen großen Unternehmen und Providern eingesetzt. Damit übernimmt ein Rechenzentrum einer großen Firma die Funktion eines Providers. In der Regel werden im Netz einer großen Firma die IP-Adressen zwischen dem Rechenzentrum und dem Arbeitsplatz-PC's ebenfalls dynamisch vergeben.

Der Verbindungsaufbau zu einem Provider gilt für jeden Internetnutzer in gleicher Weise/Prinzip, egal ob er sich privat oder geschäftlich, von einer Behörde oder aus einer Organisation in das Internet einwählt. Ein Profiler hat nun über eine IP-Adresse, egal ob dynamisch oder statisch, eine Zusatzinformation über den Ort, also das nähere örtliche Umfeld eines Providers, an dem der Internetnutzer gerade angemeldet ist. Auf der Internetseite http://webtools.live2support.com/misc_locate_ip_address.php kann eine IP-Adresse eines beliebigen Computers eingegeben werden. Die Seite ist mit „Location of User Country, State & City by IP address.“ überschrieben und zeigt die entsprechenden Daten über eine IP-Adresse an. Durch den Einsatz von Cookies/Scripten kann ein einzelner PC eindeutig identifiziert werden, auch wenn eine dynamische IP vom Provider vergeben wird. Mit diesen beiden Informationen, IP-Adresse

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

und Cookie, kann ein individueller PC an einem beliebigen Ort eines Landes weltweit lokalisiert und identifiziert werden.

Da das Internet für alle offen ist, kann ein Dritter die Aktivitäten in diesem Netzwerk mit bestimmten Hilfsprogrammen analysieren (siehe auch WEB GPS unter http://www.web-gps.de/index.php). Bei dieser „Beobachtung“ werden nicht die Datenströme zwischen zwei Kommunikationspartnern analysiert, sondern lediglich festgestellt, daß eine Verbindung von einer Adresse mit einer anderen Adresse aufgenommen worden ist. Technisch ist auf der einen Seite die Analyse der Datenverbindungen und deren Datenströme wichtig, damit Kommunikationslasten auf unterschiedliche Wege im Internet verteilt werden können. In den letzten Jahren hat jedoch die Tendenz zugenommen, daß die Netzbeobachtungen für die Erstellung von Kommunikationsprofilen, Betriebsspionagezwecke oder andere nicht legale Aktivitäten – zu denen gehört z.B. Spam Mail, Virusattacken, auslesen von Festplatteninhalten, etc. – weiterentwickelt wurden. Mit der Netzbeobachtung kann z.B. heute festgestellt werden, welche Kommunikationsbeziehung eine Firma pflegt und wer seine Kommunikationspartner sind. Wird zusätzlich der Datenverkehr (z.B. unverschlüsselter E-Mail-Verkehr) einer Firma analysiert, können rechtzeitig Akquisitionen, Projekte oder Marketingaktivitäten von Konkurrenzunternehmen ermittelt werden. Mit diesen Daten von Unternehmen, und auch den Daten von Privatpersonen, ist eine eigene weltweit agierende „Spionage“-Industrie entstanden, die Milliarden umsetzt.

Die Beobachtung von Verbindungsdaten (Analyse des Netzverkehrs) ist also innerhalb eines Netzwerks technisch sinnvoll, um eine gute Lastverteilung zu ermöglichen (siehe auch „The big picture“ http://www.internetworldstats.com/stats.htm). Auf der anderen Seite können diese Daten für andere Zwecke missbraucht werden. Wenn jemand Quelle und Ziel des Internetverkehrs eines Unternehmen oder einer Privatperson kennt, kann er das persönliche Verhalten und die Vorlieben nachvollziehen. Es kann sogar den Arbeitsplatz und die körperliche Unversehrtheit bedrohen, wenn öffentlich wird, wer ein Benutzer ist und wo er wohnt. Wenn z.B. ein Angestellter eines Unternehmens sich im Ausland auf Dienstreise befindest und sich mit dem Computer des Arbeitgebers verbindet, kann er ungewollt seine Nationalität und den Arbeitgeber jedem offenbaren, der das Netzwerk beobachtet, auch wenn die Verbindung verschlüsselt ist. Damit erfährt ein Beobachter, wo Mitarbeiter sich zu welchen Zeiten und wie lange sich aufhalten. Werden nun zusätzlich die ausgetauschten Daten oder vorher erstellten Profile von Personen ausgewertet, kann ein Beobachter ggf. erkennen, ob in einem Projekt im Ausland Schwierigkeiten auftreten oder nicht. Bei großen Projekten können aus diesen Informationen sehr schnell gefährliche Situationen für die Mitarbeiter des Unternehmens vor Ort entstehen, wenn andere Konkurrenten dieses Projekt übernehmen wollen.

Wie funktioniert nun die Analyse des Netzverkehrs? Die Datenpakete, die bei einer Kommunikation im Internet ausgetauscht werden, haben zwei Teile: die Nutzlast, die die eigentlichen Daten trägt und der Kopf, wo verschiedene Informationen zum Routing – der Wegbeschreibung, die ein Datenpaket vom Sender zum Empfänger nimmt – zu finden sind. Auch wenn die Nutzlast verschlüsselt wird, enthüllt

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

diese Art der Analyse, was ein Benutzer getan hat und eventuell auch, was jemand dem Anderen mitgeteilt hat. Die Analyse kann diese Informationen deshalb ermitteln, da sie sich auf die Kopfdaten fokussiert, die die Quelle, Ziel, Umfang (Größe) der Daten etc. enthalten. Das „Was“ kann nur über die Analyse der Dateninhalte erfolgen (siehe im Folgenden).

Ein grundlegendes Problem ist für jemanden, der am Schutz seiner Privatsphäre interessiert ist, daß der Empfänger alleine bereits an den Kopfdaten eines Datenpakets erkennen kann, daß jemand Daten an einen bestimmten Empfänger versandt hat. Diese Auswertung der Kopfdaten können autorisierte Vermittler, wie ISPs (Internet Service Provider oder kurz Provider genannt), und auch Unautorisierte vornehmen. Eine sehr einfache Form der Verkehrsanalyse kann irgendwo zwischen dem Sender und Empfänger erfolgen, indem die Kopfdaten von einem aktiven Rechner ausgewertet und verfolgt werden (Trace Analyse). Diese Netzanalyse kann im Prinzip jeder im Internet durchführen, sofern er die dazu notwendigen Programme besitzt. Ein Beispiel einer einfachen oft genutzten und sehr bekannten Netzwerkbeobachtung ist auf der folgenden Internetseite zu finden:

http://whois.domaintools.com/

Ein Beispiel einer Online-Netzbeobachtung ist unter der folgenden Adresse zu finden:

http://www.caida.org/analysis/routing/reversetrace/

oder ein Zugang zu allen Ländern der Welt, die mit dem Internet verbunden sind kann über folgende Internetseite abgefragt werden:

http://www.traceroute.org/

Ein Dienst zur Ermittlung des Orts, woher Internetbesucher einer Internetseite kommen, bietet

http://www.web-gps.de/index.php

Eine deutsche Internetseite für Beschwerden illegaler Netzwerkaktivitäten jeglicher Art kann unter der folgenden Internetseite aufgerufen werden:

http://www.naiin.org/de/content/beschwerdestelle/inhalt.php

Diese Internetseite hat jedoch keine rechtliche Relevants, sondern stellt lediglich eine Veröffentlichung „Schwarzer Schafe“ dar.

Natürlich existieren auch mächtigere Formen der Verkehrsanalyse. Einige Angreifer spionieren in verschiedenen Teilen des Internets und nutzen fortgeschrittene statistische Methoden, um die Kommunikationsmuster von verschiedenen Organisationen und Menschen zu verfolgen. Die Verschlüsselung der Daten z.B. mit OpenPGP hilft nicht gegen diese Angreifer. Denn eine Datenverschlüsselung verbirgt nur den Inhalt der Kommunikation und nicht die Verbindungsdaten/Kopfdaten der Datenpakete! Deshalb ist also zusätzlich zu der Verschlüsselung von Daten auch eine Anonymisierung der Verbindungsdaten notwendig. Dieser Grundsatz sollte vor allem für

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

jedes Unternehmen gelten, daß nicht daran interessiert ist, seine Unternehmenstätigkeiten über das Internet anderen Konkurrenten im Inn- und Ausland mitzuteilen.

In der Regel müßten illegale Praktiken und ein Missbrauch bei der Erhebung, Speicherung und Vermarktung der persönlichen Daten durch ein Rechtssystem verfolgt werden (siehe erstes Kapitel Internetbeobachtung im Jahr 2007). Das erfolgt jedoch in der Regel in den Staaten nicht. Obwohl nach dem deutschen Kommunikationsgesetz das Erstellen von Bewegungsprofilen/Kommunikationsprofilen nur durch hohe rechtliche Hürden und bei schweren Straftaten möglich ist, verdienen ohne Rechtsverfolgung Unternehmen genau mit diesen illegalen Praktiken Milliarden Dollar. Vom deutschen Rechtssystem ist zur Zeit unter Berücksichtigung der realen Verhältnisse im Internet keine Hilfe für den Schutz der persönlichen Daten von Unternehmen oder Privatpersonen zu erwarten. Somit muss sich jedes Unternehmen und jede Privatperson, in diesem durch den Rückzug des Rechtssystems frei gegebenen Raum, selbst schützen. Die dazu notwendige Technologie ist bereits vorhanden und kann eingesetzt werden.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Technologien zum Schutz seiner Persönlichkeitsrechte

Der Markt von Software-Lösungen zur Anonymisierung ist groß und unübersichtlich. Auch hier gilt die oben formulierte Doktrin, in dem öffentlich kontrollierbare Softwarelösungen prinzipbedingt mehr Sicherheit bieten, als Systeme von Unternehmen. Im folgenden soll ein wenig auf die Technologiekonzepte eingegangen werden, die zur Zeit verfügbare Lösungen anbieten.

Verbindungsaufbau im Internet

Eine Verbindung zwischen einem Internetbesucher und einer Internetseite erfolgt in der Regel über einen Provider und zahlreichen weiteren Servern, die zwischen dem Provider und dem Rechner, auf dem die Internetseite abgelegt ist, vorhanden sind. Wählt ein Internetbesucher eine Seite an, ist ein Verbindungsaufbau zwischen beiden Seiten bereits aufgebaut worden. Für den Verbindungsaufbau wurden zwischen dem Rechner des Internetbesuchers (auch Client genannt) und der „Internetseite“ (auch Host genannt) Daten ausgetauscht. Diese Daten dienen dem Verbindungsaufbau. Die Daten werden in Form von einzelnen Paketen, den Datenpaketen, übertragen (siehe auch „Funktionsprinzip und Technologie„). Der Weg, den diese Datenpakete nehmen, ist vor dem Verbindungsaufbau nicht bekannt. Er ist also nicht statisch. Er wechselt sogar im Verlauf einer Verbindung. Dieser dynamische Aufbau der Verbindung ist eine grundlegende Funktion des Internets. Dadurch ist das Internet selbst besonders ausfallsicher, weil auch bei einer Unterbrechung einer Verbindung automatisch ein neuer Weg von den Datenpaketen gesucht wird.

Damit eine Verbindung zwischen zwei Rechnern (Client und Host) zustande kommt, werden für den Zeitpunkt des Verbindungsaufbaus eindeutige IP-Adressen verwendet. Diese IP-Adressen geben immer den Rechner an, von dem ein Paket gesendet worden ist und an welche Adresse eine Antwort geschickt werden soll. Die Liste aller IP-Adressen eines einzelnen Datenpakets gibt also den Weg an, auf dem Daten zwischen dem Client und dem Host ausgetauscht werden. Diese Liste nennt man auch Routing Table. Befinden sich mehrere Rechner zwischen dem Client und dem Host, kann die IP-Adresse zwischen jedem einzelnen Zwischenrechner neu vergeben werden. Lediglich der erste Rechner, der vom Host oder Client angesprochen worden ist, kennt die eigentliche Zieladresse des Host oder Clients. Mann nennt diese „ersten Rechner“ auch Eingangsrechner in einen Mix, auf den später noch eingegangen wird. Ein Mix ist also alles zwischen zwei Rechner, dem Client (PC des Internetbesuchers) und dem Host (dem Rechner, der die Internetseite eines Anbieters verwaltet), das zur Verbindung an Zwischenrechnern zusätzlich benötigt wird.

Zusammenfassend kann festgehalten werden: Ein Internetbesucher verbindet sich über zahlreiche andere Computer mit einer Internetseite. Der Verbindungsweg ist dabei dynamisch und steht vor der Verbindung nicht fest. Dieser dynamische Aufbau eines Verbindungsweges ist eine grundsätzliche Funktion des Internets.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Konzepte zum Schutz der eigenen Verbindungsdaten

Das Internet ist also ein sehr dynamisches System. Wenn eine Verbindung geschützt werden soll, muss also jedes Datenpaket und die damit verknüpften Verbindungsdaten, bearbeitet werden. Im folgenden werden einige Konzepte kurz angedeutet, wie eine Verbindung von einem Internetbesucher mit einer Internetseite geschützt werden kann.

Für kleine und mittelständische Unternehmen bieten sich vor allem Virtuelle Privates Netzwerke (auch VPN genannt) an. Sie können dann einen relativen Schutz für Mitarbeiter des zu schützenden Unternehmens bieten, wenn die Mitarbeiter z.B. mit mobilen Laptops oder mobilen PC's (z.B. bei Bauprojekten in Baucontainern, etc.) eine direkte Verbindung mit ihrem Firmensitz aufbauen wollen. Es reicht jedoch bereits der Verbindungsaufbau aus, daß ein Profiler diesen Verbindungsaufbau erkennt und im späteren die Kopfdaten auswerten kann.

Externe Proxy Server

Im einfachsten Fall wird zwischen dem Internet und dem Internetbesucher ein externer Rechner zwischengeschaltet. Dieser Rechner empfängt von dem Internetbesucher alle Datenpakete und versendet die empfangenen Daten unter seiner neutralen eigenen IP-Adresse in das Internet. Damit kann ein Netzbeobachter nicht direkt auf einen Internetbesucher zurückschließen. Dieser Zwischenrechner wird auch als Proxy Server bezeichnet. Für diesen Dienst können externe fremde Rechenzentren und Dienstleister beauftragt werden. Weltweit wird dieser Dienst in unterschiedlichen Qualitäten angeboten. Ein sehr bekannter Proxy Server Dienst wird z.B. von der Firma Steganos (siehe auch https://www.steganos.com/de/produkte/privatkunden/) mit einem gesamten Sicherheitspaket angeboten. Dieses Sicherheitsangebot ist kostenpflichtig. Erweiterte kostenpflichtige Sicherheitsdienste auf Basis dieser VPN-Technologie wird u.a. von der gleichen Firma (siehe auch www.steganos.com) angeboten.

Über ein Virtuelles Privates Netzwerke (VPN) wird ein Verbindungsaufbau zwischen dem Internetbesucher und dem Dienstleistungsunternehmen aufgebaut. Dadurch entsteht ein „virtueller Tunnel“ zwischen dem Dienstleister und dem Kunden, der seine Internetverbindung schützen möchte. Der Rechner des Dienstleisters übernimmt dabei die Funktion eines externen Proxy Servers. Die Daten des Internetbesuchers werden durch diesen Tunnel an den Dienstleister verdeckt gesendet. Der Dienstleister versendet unter der eigenen Identifikation die Daten des Internetbesuchers in das Internet. Damit wird ein direkter Rückschluß durch Profiling von einer besuchten Internetseite auf einen Internetbesucher erschwert. Problematisch ist die Situation dann, wenn ein Anbieter von Sicherheitslösungen selbst ein Profiling durchführt. Es muss jedoch auch beachtet werden, daß häufig die Provider selbst (z.B. nationale Telekommunikationsanbieter und Andere) bereits Profiler einsetzen oder selbst Profiler sind. Das heißt, das bereits bei der Anmeldung auf der Homepa-

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

ge eines Providers einem Profiler bekannt wird, daß ein bestimmter Internetbesucher sich angemeldet hat.

Bei den weiter unten empfohlenen neueren Technologien können jedoch auch diese Schwachstellen absichert werden. Wie im ersten Kapitel beschrieben, besteht eine sehr geringe Gefahr für alle national ansässige Profiler kontrolliert zu werden, da vom deutschen Rechtssystem keine Kontrollen durchgeführt werden und die nationalen Profiler mit ihren Profilen viel Geld verdienen.

Lokale Proxy Server

Ein Proxy Server kann auch als Programm zwischen dem Internetzugang und den Programmen auf dem lokalen Rechner eingesetzt werden. Der Vorteil bei diesem Konzeptansatz besteht darin, daß der Proxy Server vor der Verbindung mit dem Provider bereits aktiviert werden kann. Dieser Konzeptansatz wird bei den weiter unten empfohlenen Programmen eingesetzt.

Stealth-Technologie

Diese Technologie basiert häufig auf der Technologie von externen Proxy Servern (siehe auch weiter oben). Häufig werden in den angebotenen Produkten lediglich Cookie-Blocker und andere Programmzusätze eingebaut. Einen guten Schutz vor dem Profiling bieten sie in der Regel nicht. Die Stealth-Technologie ist aus Sicht des Autors nicht zu empfehlen, da sie eine Sicherheit vorgaukelt, die tatsächlich nicht gegeben ist (siehe auch http://download.freenet.de/archiv_s/stealther_3814.html). Über die Stealth-Technologie wurden in vielen deutschen PC-Zeitschriften berichtet, auf die hier nur verwiesen werden soll.

Mix-Technologie

In der folgenden kurzen Beschreibung kann nur auf einen kleinen Teil der Mix-Technologie eingegangen werden. Was ein Mix ist, kann auch im Kapitel „Verbindungsaufbau im Internet“ nachgelesen werden. Im folgenden werden die Technologien behandelt, auf denen auch die Empfehlungen basieren.

Onion Routing (englisch für „Zwiebel-Routing“) ist eine Anonymisierungstechnik im Internet. Hierbei werden die Web-Inhalte über ständig wechselnde Routen von mehreren Mixen geleitet, welche in diesem Zusammenhang auch Knoten genannt werden. Diese Knoten stellen jeweils eine Art externen verschlüsselnden Proxy Server dar. Dadurch bleibt die wahre Identität desjenigen, der die Daten von einer anderen Internetseite oder einem anderen Internetdienst angefordert hat, für den Webserver auf der anderen Seite anonym. Auch die Betreiber der Knotens selbst sind aufgrund des Verschlüsselungsschemas nicht in der Lage, eine Zuordnung zwischen dem Nutzer und seinen angeforderten Web-Inhalten herzustellen, es sei denn alle Knoten der jeweiligen Route arbeiten zusammen.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Im Gegensatz zu Diensten die auf festen Mix-Kaskaden basieren, d.h. die stets eine für alle Nutzer gleiche Route zwischen den Mixen verwenden, wird beim Onion-Routing die Auswahl und Reihenfolge der benutzten Knoten immer wieder individuell durch jeden Nutzer geändert. Somit scheint auch ein späterer erneuter Zugriff auf einen Server aus Sicht dieses Servers von einem neuen Benutzer zu kommen, da sich die IP-Adresse zwischenzeitlich ebenso geändert hat. Dies gilt allerdings nur, falls nicht auf Grund der übertragenen Daten/ Internetseite eine weitere Identifikation möglich ist, z.B. mit Hilfe von Cookies, Java-Scripten oder personalisierten Links.

Konzeptvergleich zu Mix-Kaskaden

Der Hauptunterschied zwischen dem Konzept von festen Mix-Kaskaden und freiem Routing liegt in der Übertragungskapazität und der Anzahl der benötigten Knoten. Während bei festen Mix-Kaskaden alle Nutzer die gleichen Mixe verwenden, diese Mixe also entsprechend große Kapazitäten zur Verfügung stellen müssen, sind beim Onion-Routing-Konzept sehr viele Knoten nötig, die aber geringere Bandbreiten benötigen, da der einzelne Knoten jeweils nur durch wenige Nutzer in Anspruch genommen wird. Dadurch kann Onion-Routing innerhalb eines „Graswurzelansatz“ (viele kleine Rechner mit geringer Bandbreite) verwirklicht werden, da Nutzer mit einem DSL-Zugang (mit ausreichen Upstream-Kapazität) oftmals in der Lage sind, selbst einen Knoten zu betreiben. Andererseits ist eine niedrige Beteiligungsschwelle und damit die fehlende Zentralkontrolle auch das größte Risiko: ein solcher Dienst kann mit verhältnismäßig wenig Aufwand zu großen Teilen unterwandert und damit auch kontrolliert werden, indem einzelne Personen unter vielen Pseudonymen Knoten betreiben. Auch wenn immer noch ausreichend "sichere" Knoten (=nicht unterwanderte Knoten) im Netzwerk existieren, ergibt sich eine entsprechend erhöhte Wahrscheinlichkeit, daß ein Nutzer eine Route komplett aus der Menge der kontrollierten Knoten zusammenstellt und damit seine Aktionen für den Betreiber dieser Knoten nachvollziehbar werden. Begünstigt wird dies sogar noch durch die ständig neu stattfindende Wahl der Ruten. Damit ist zwar die Wahrscheinlichkeit geringer, daß alle Aktionen des Nutzers kontrolliert werden können, da er ständig neue Knoten wählt. Allerdings steigt die Wahrscheinlichkeit, daß zumindest einzelne seiner Aktionen erfolgreich deanonymisierbar (=einem Internetbesucher zugeordnet) werden können.

Anwendung

Ein bekanntes und verbreitetes Programm zur Nutzung von Onion-Routing ist der Anonymisierungsdienst „Tor“. Dagegen ist die in Deutschland entwickelte „JAP“-Software ein auf festen Mix-Kaskaden basierender Dienst.

Beide Technologien sind aus Sicht des Schutzes der Privatsphäre empfehlenswert. Aus diesem Grund werden in den folgenden Absätzen die angebotenen Programmlösungen kurz eingegangen.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

In den jeweiligen Abschnitten sind Kapitel enthalten, die einige Hintergrundinformationen über die Strukturen der Organisationen oder Hersteller geben. Diese Hintergrundinformationen sind vor allem deshalb von besonderem Interesse, da sie den Technologietransfer zwischen den engagierten Personen und Unternehmen und den staatlichen Organisationen und Sicherheitsbehörden widerspiegeln. Analytisch wird dadurch eindeutig aufgezeigt, daß eine absolute Sicherheit vor staatlicher Beobachtung fremder Staaten und des eigenen Staates generell nicht im Internet möglich ist. Die Analyse zeigt auch das Interesse von staatlichen Stellen wie z.B. das BKA oder die DARPA an dieser Entwicklung und der damit sich entwickelnden Technologie. Die Hersteller der derzeit führenden Technologielösungen stehen also in direkter oder indirekter Beziehung zu staatlichen Stellen. Der Einfluß der staatlichen Organe ist jedoch durch den Open Source Ansatz teilweise transparent und damit kalkulierbar. Der Einfluß der staatlichen Organe ist jedoch in der Infrastruktur, auf denen die Technologien aufsetzen (Mix-Betreiber), nicht transparent.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Tor Projekt

Tor ist ein Softwaresystem zum Schutz der Privatsphäre im Internet. Die Software verschlüsselt die Verbindungsdaten und tarnt die Verbindung zwischen Client und Host. Der Zugang zu den Mixen, die die Anonymisierung vornehmen, ist kostenlos. Das Softwaresystem basiert auf Open Source und ist kostenlos erhältlich. Eine große öffentliche Entwicklergemeinde arbeitet an der weiteren Entwicklung des Systems. Das System basiert auf dem Konzept von dynamischen Mixen.

Das Softwarepaket „Tor“ der „The Tor Project Inc.“ anonymisiert den Netzwerkverkehr zwischen einem Rechner und einer aufgerufenen Seite im Internet, Downloads und anderen Internetservices, das im folgenden auch zu der Kategorie der „Privacy Shield-Methoden„ zugerechnet wird. Das Projekt, die Software und die Infrastruktur werden von Personen und Unternehmen aus unterschiedlichen Ländern entwickelt und betrieben. Der Tor-Service bietet eine zuverlässige Technologie und eine weltweit aufgestellte Infrastruktur an, mit der ein Bezug zwischen einem Internet-PC und der vom Rechner aufgerufenen Verbindung für einen außenstehenden Beobachter mit einfachen Mitteln nicht mehr möglich ist. Für die Anonymisierung der Netzwerkverbindungen, die Unternehmen mit ihren Mitarbeitern, Zulieferern oder Kunden per Internet eingehen, bietet diese Technologie einen wirkungsvoll Schutz. Die Technologie wurde nach Angaben der Tor-Betreiber auch vom amerikanischen Militär zur Tarnung von Einsätzen in anderen Ländern eingesetzt. Dieser in der Projektbeschreibung als werbende Aussage gemeinter Hinweis muss vor dem Hintergrund der amerikanischen Industriestruktur und der Mentalität verstanden werden. Aus europäischer Sicht ist diese Aussage eher dahingehend zu interpretieren, daß möglicherweise auch jetzt nach Bedarf Knotenrechner vom amerikanischen Militär oder anderen Diensten nahe stehenden Betreiber für die Mixe verwendet werden.

Hinweis: Der Schutz kann durch die Aktivierung von Cookies und/oder Java-Scripten unterwandert werden. Deshalb sollten die im Kapitel „Internet Explorer“ angegebenen Empfehlungen befolgt werden.

Die Organisation „The Tor Project Inc.“ ist in den USA eine Non-Profit-Organisation nach Chapter 501(c)(3). Die Organisation listet alle Schlüsselpersonen auf und ist an einer Transparenz ihrer Organisation und Öffentlichkeit interessiert. Der Sourcecode der Technologie, wie auch die weltweite Infrastruktur, ist öffentlich und kann von einer breiten Öffentlichkeit kontrolliert werden. Software und Dienste sind kostenlos. Die Non-Profit-Organisation finanziert sich aus Spenden. Mit dem folgenden Link kann das Programm heruntergeladen werden.

Tor Download:
http://www.torproject.org/download.html.de

Nach dem Download kann das Softwarepaket installiert werden.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Hinweis: Wurde bereits vorher der Proxy Server Proxomiton installiert, ist die Installation des im Softwarepaket enthaltenen Proxy Servers „Privoxy“ nicht notwendig. Die Installation des mitgelieferten Proxy Servers wird einfach dadurch verhindert, daß bei der Installation der Haken vor dem Dienst „Privoxy“ deaktiviert wird.

Eine genaue Beschreibung, wie die Zusammenarbeit zwischen dem Mozilla Firefox Browser, Tor und einem Proxy funktioniert, kann unter

http://www.netzwelt.de/news/74366-firefox-anonym-unerkannt-surfen-mit.html

nachgelesen werden. Tor bietet also einen wirksamen Schutz vor Profilern. Generell muss hier darauf hingewiesen werden, daß durch eine Anonymisierung prinzipbedingt mit einer Verringerung der Kommunikationsgeschwindigkeit gerechnet werden muss.

Hintergrundinformationen

Sponsoren des TorProject

1. 2001-2007: DARPA und ONR via Naval Research Laboratory
   Internet link: http://chacs.nrl.navy.mil

Quelle Wikipedia:

Defense Advanced Research Projects Agency

Die Defense Advanced Research Projects Agency (DARPA) ist eine Behörde des Verteidigungsministeriums der Vereinigten Staaten, die Forschungs-Projekte für das US-Militär durchführt, u. a. auch Weltraumprojekte. Ihr jährliches Budget beträgt etwa 3 Milliarden Dollar (Stand 2004).

Gegenwärtige Tätigkeitsbereiche

Heute widmet sich die DARPA vorrangig der Terrorismusbekämpfung. In diesem Zusammenhang wurde beispielsweise das sehr umstrittene Information Awareness Office (IAO) von der DARPA gegründet.

2003 rief die DARPA Forscher im Bereich Maschinelle Übersetzung zu einem „Blind“-Wettbewerb auf. Sie sollten innerhalb eines Monats ein Übersetzungssystem von einer fremden Sprache nach Englisch entwickeln. „Blind“ heißt, dass den Forschern erst am Starttag des Wettbewerbs mitgeteilt wurde, um welche Ausgangssprache es sich handelte, so dass sie gezwungen waren, Methoden vorzubereiten, die möglichst jede Sprache verarbeiten könnten. Das Ziel war, für die Sprachen der kaum vorhersehbaren Konfliktherde (z. B. Afghanistan, Irak) möglichst schnell Übersetzungssysteme bereitstellen zu können, ohne die üblichen mehrere Jahre an Forschung und Entwicklung. Blindsprache war schließlich Hindi; der Wettbewerb wurde von dem Deutschen

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Franz-Josef Och mit einem Statistisch-Basierten Übersetzungssystem gewonnen.

IAO Information Awareness Office:

Das Information Awareness Office (IAO) war ein Projekt, das von der DARPA, einer Agentur des Verteidigungsministeriums der USA, gegründet wurde. Aufgabe des IAO war es, innerhalb einer Datenbank alle verfügbaren Merkmale der Bürger des Staates zu suchen und diese später auf verdächtige Muster auszuwerten. Dies sollte vor allem zum Schutz vor Terrorismus geschehen.

2. 2004-2005: Electronic Frontier Foundation
   Internet Link: https://www.eff.org

Electronic Frontier Foundation

From the Internet to the iPod, technologies are transforming our society and empowering us as speakers, citizens, creators, and consumers. When our freedoms in the networked world come under attack, the Electronic Frontier Foundation (EFF) is the first line of defense. EFF broke new ground when it was founded in 1990 — well before the Internet was on most people's radar — and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today. From the beginning, EFF has championed the public interest in every critical battle affecting digital rights.

Blending the expertise of lawyers, policy analysts, activists, and technologists, EFF achieves significant victories on behalf of consumers and the general public. EFF fights for freedom primarily in the courts, bringing and defending lawsuits even when that means taking on the US government or large corporations. By mobilizing more than 50,000 concerned citizens through our Action Center, EFF beats back bad legislation. In addition to advising policymakers, EFF educates the press and public.

EFF is a donor-funded nonprofit and depends on your support to continue successfully defending your digital rights. Litigation is particularly expensive; because two-thirds of our budget comes from individual donors, every contribution is critical to helping EFF fight —and win—more cases.

3. 2006: Omidyar Network Enzyme Grant
   Internet Link: http://www.omidyar.net

Omidyar Network Enzyme Grant

Pierre Omidyar, the founder of eBay, and his wife, Pam, established Omidyar Network based on the belief that every person has the potential to make a difference. Since 2004, Omidyar Network has worked with its partners to create opportunities for people to tap that potential, enabling them to improve their lives and make powerful, lasting contributions to their communities.

Our Work

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

We support, scale, and champion the work of our partners in order to maximize social impact.Omidyar Network is a philanthropic investment firm that is committed to creating and fostering opportunity for people around the world. We make both grants and investments, identifying likeminded organizations that we support, scale, and champion to maximize their social impact.

4. 2006: Bell Security Solutions Inc (BSSI)
   Internet Link: http://www.bce.ca/en/

Bell Security Solutions Inc.

Bell Security Solutions Inc. is a national provider of scaleable, integrated, end-to-end security solutions for the government, healthcare, financial, manufacturing, transportation and retail industries. A wholly-owned subsidiary of Bell Canada, BSSI is headquartered in Ottawa, with offices in Toronto, Montreal, Quebec City, Calgary, Vancouver and Victoria. BSSI has the largest team of dedicated security specialists in the country. BSSI's mandate is to be the premier nationwide security solutions provider, by developing innovative services that address the continued escalation of threats and vulnerabilities, as well as increasingly stringent legal and regulatory obligations.

5. 2006-2007: NSF über die Rice Universität
   Internet Link: http://seclab.cs.rice.ed/lab/2005/08/01/seclab-awarded-grant-to-study-security-of-p2p/

NSF National Science Foundation

Die National Science Foundation (NSF) ist eine unabhängige Einrichtung der Regierung der Vereinigten Staaten mit Sitz in Arlington, Virginia, deren Aufgabe die finanzielle Unterstützung von Forschung und Bildung auf allen Feldern der Wissenschaften, mit Ausnahme der Medizin ist. Mit einem jährlichen Budget von 5,6 Milliarden Dollar (2006) repräsentiert sie 20 Prozent der gesamten Zuschüsse der US-Regierung für Grundlagenforschung an Hochschulen. In einigen Bereichen wie Mathematik, Informatik, Wirtschaftswissenschaften und Sozialwissenschaften ist die NSF die Hauptdrittmittelquelle für Forschung.

6. Eine anonyme europäische Nicht-Regierungsorganisation (2006-2007)
7. 2006-2008: Über 500 Einzelspenden
8. 2006-2008: International Broadcasting Bureau
   Internet Link: http://www.ibb.gov/

Quelle Wikipedia

International Broadcasting Bureau

Das International Broadcasting Bureau (IBB) ist eine US-amerikanische Behörde in Washington D.C., die für die technische Betreuung, die Verwaltung und den Betrieb der Sendeanlagen und Sendeeinrichtungen aller nicht-militärischen internationalen

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Rundfunksender der USA verantwortlich ist. Das IBB ist dem Broadcasting Board of Governors (BBG) unterstellt.

Gegründet wurde das IBB 1994 und unterstand zunächst der United States Information Agency (USIA). Nach deren Auflösung im Jahr 1999 und der Gründung des BBG untersteht das IBB dem BBG als unabhängige US-Regierungsbehörde.

9. 2006-2008: Cyber-TA Projekt
   Internet Link: http://www.cyber-ta.org/

Cyber-TA Projekt

This website is the home page of the Cyber-Threat Analytics (Cyber-TA) research project. Cyber-TA is an initiative to accelerate the ability of organizations to defend against Internet-scale threats by delivering technology that will enable the next-generation of privacy-preserving digital threat analysis centers. These centers must be fully automatic, scalable to alert volumes and data sources that characterize attack phenomena across millions of IP addresses, and higher fidelity in their ability to recognize attack commonalities, prioritize, and isolate the most critical threats. Cyber-TA brings together leading researchers in large-scale network intrusion defenses with leaders from the information privacy community to develop next-generation wide-area collaborative defense technologies that maximally balance the needs for contributor privacy with the need for rich-content data to drive new threat detection and mitigation systems. This web site provides links to our research publications, software releases, web portal access to our live threat reconnaissance center, and registration information for becoming an active data contributor.

10. 2007: Human Rights Watch
    Internet Link: http://www.hrw.org/

Human Rights Watch

Human Rights Watch setzt sich für Opfer und Menschenrechtsaktivisten ein, um Diskriminierungen zu verhindern, politische Freiheiten aufrecht zu erhalten, Menschen in Zeiten des Krieges zu schützen und Menschenrechtsverbrecher vor Gericht zu stellen.

Wir untersuchen Menschenrechtsverletzungen, veröffentlichen die Ergebnisse und ziehen die Täter zur Verantwortung.

11. 2007, 2008: Google Summer of Code
    Internet Link: http://code.google.com/soc/

Google Summer of Code™

Google Summer of Code 2008 is on! Over the past three years, the program has brought together over 1500 students and 2000 mentors from 90 countries worldwide, all for the love of code. This year, we're welcoming 1125 student contributors and 175

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Free and Open Source projects into the program. You can find out more about each participating organization and abstracts of their accepted students' proposals by visiting each organization's page, below. We'll be posting regular news about the program to the Google Open Source Blog.

If you are interested in participating in future instances of Google Summer of Code, now is an excellent time to begin further exploration: check out our mentoring organizations' ideas lists below, our Frequently Asked Questions, and the program wiki. If you are a student, the best way to prepare for Google Summer of Code is to learn more about Open Source development before the program begins.

JonDonym Produkt

JAP aus dem Softwarepaket „Jondonym“ ist ein Softwaresystem zum Schutz der Privatsphäre im Internet. Die Software verschlüsselt die Verbindungsdaten und tarnt die Verbindung zwischen Client und Host. Der Zugang zu den Mixen, die die Anonymisierung vornehmen, ist teilweise kostenlos. Die Qualität des privaten Schutzes kann durch kostenpflichtige Anonymisierungsdienste verbessert werden. Ein kostenloser Testdienst ist vorhanden, der jedoch in der Regel überlastet ist. Das Softwaresystem basiert teilweise auf Open Source und ist kostenlos erhältlich. Das Unternehmen JonDos und eine öffentliche Entwicklergemeinde arbeitet an der weiteren Entwicklung des Systems. Das System basiert auf dem Konzept von statischen Mixen.

JAP ist das Produkt der JonDos GmbH aus Deutschland. Das Softwarepaket „Jondonym“ anonymisiert den Internetverkehr zwischen einem Rechner und einer aufgerufenen Internetseite, das im folgenden auch zu der Kategorie der „Privacy Shield-Methoden„ zugerechnet wird. Das Projekt Jondonym ist die geschäftliche Basis des Unternehmens. Die Software wird von der Firma entwickelt und als Open Source betreut. Die Infrastruktur/Mixe wird zur Zeit vor allem von deutschen Unternehmen, die sich vertraglich an die JonDos GmbH binden müssen, betrieben. Der Jondonym-Service bietet konzeptionell eine zuverlässige Technologie an, mit der ein Bezug zischen einem Internet-PC und den vom Rechner aufgerufenen Verbindungen für einen außenstehenden Beobachter mit einfachen Mitteln nicht mehr möglich ist. Für die Anonymisierung der Netzwerkverbindungen, die Unternehmen mit ihren Mitarbeitern, Zulieferern oder Kunden per Internet eingehen, bietet diese Technologie einen wirkungsvoll Schutz, der jedoch nicht kostenlos ist. Nach Sichtung der Foren (Februar 2008), die für dieses System unterhalten werden, muss an dieser Stelle darauf hingewiesen werden, daß offensichtlich auch die Bezahldienste häufiger ausfallen und deshalb auch häufiger mit erheblichen Kommunikationseinbußen für die Nutzer dieser Dienste gerechnet werden muss. Ebenfalls muss auf eine Protokollierungsfunktion nach dem Telemediengesetz für alle deutschen Mix-Betreiber in der Software hingewiesen werden, die es staatlichen Stellen ermöglicht, die Anonymisierung aufzuheben.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Das Unternehmen JonDos GmbH ist eine Ausgründung mit Studenten der Uni Regensburg und der Uni Dresden. Das Unternehmen hatte zum Stichtag dieser Arbeit eine Angestelltenbasis von weniger als 20 Angestellte. Die Technologie geht auf ein Universitätsprojekt mit dem Namen „An.On“ unter der Leitung von Prof. Dr.-Ing. Hannes Federrath zurück. Das Unternehmen JonDos GmbH ist rechtlich zur Erwirtschaftung von Profiten verpflichtet (siehe auch „Einstieg in ein Sicherheitskonzept“). Es ist deshalb genau zu Prüfen, ob das Konzept des Open Source längerfristig durch das Unternehmen durchgehalten werden kann und welche bisher öffentlich kenntlich gemachten „Hintertüren“ zur Aufhebung der Anonymität noch eingebaut werden „müssen“. Zur Zeit finanziert sich das Unternehmen nach eigenen Angaben im wesentlichen aus öffentlichen Fördergeldern. Die Räumlichkeiten des An.On-Projekts wurde im Juni/Juli 2003 von der Staatsanwaltschaft und dem Amtsgericht durchsucht und die Rechner wurden beschlagnahmt. Das Landgericht Frankfurt hat die Rechtswidrigkeit „*der vom Amtsgericht Frankfurt am 29. August 2003 gegen das Projekt erlassenen Durchsuchungsanordnung für die Räume des AN.ON-Projektes*“ festgestellt.

(siehe auch dazu http://anon.inf.tu-dresden.de/strafverfolgung/anonip4.html).

Die Software wird als „quelloffener Dienst“ beschrieben. Der Client ist kostenlos. Die Verschlüsselungsdienste sind, bis auf den Testdienst, kostenpflichtig. Das Unternehmen unterliegt dem Deutschen Recht und dem Telemediengesetzt (TMG). Demzufolge ist folgendes bei der Nutzung dieses Dienstes zu berücksichtigen: Zitat aus dem An.On-Projektbeschreibung: „*Die im AN.ON-Projekt konzipierte und implementierte Lösung verdeutlicht außerdem, daß Strafverfolgung bei hinreichendem Anfangsverdacht durch den Anonymisierungsdienst nicht ausgeschlossen ist. Der AN.ON-Dienst sieht bei Vorliegen einer richterlichen Anordnung im definierten Einzelfall ein Mitspeichern von bestimmten Nutzungsdaten vor.*“ Siehe dazu auch unter

http://anon.inf.tu-dresden.de/strafverfolgung/index_de.html

und

http://anon.inf.tu-dresden.de/publications/index.html#RevocableAnonymity.

Download

JonDos Download:
https://www.jondos.de/de/download/windows

Das technologische Konzept erscheint überzeugend. Das Geschäftskonzept des Unternehmens erscheint überprüfungswürdig. Das Produkt selbst erscheint nicht ausgereift. Bezugnehmend bis zum Stichtag Februar 2008: In den Foren wird häufig darauf hingewiesen, daß der kostenlose Testdienst, wie auch die Bezahldienste sehr langsam sind und teilweise über längere Zeiträume (es wird auch von Tagen und Wochen in den Foren berichtet) ausfallen. Weitergehende rechtliche Fragen sind unter der folgenden Seite zu finden:

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

https://www.datenschutzzentrum.de/projekte/anon/20070316-rechtliche-grundlagen.htm

Hintergrundinformationen JonDos GmbH

Eigener Beschreibungstext:

JonDos gibt ihren Kunden quelloffene Hilfsmittel bzw. Werkzeuge zur Durchsetzung ihres Rechts auf informationelle Selbstbestimmung an die Hand. Außerdem möchten wir die Marktfähigkeit von Datenschutzwerkzeugen demonstrieren.

JonDos als Unternehmen agiert als Vermittler zwischen Benutzern des Anonymisierungsdienstes JonDonym, den "JonDonauten", und den unabhängigen Betreibern des Dienstes, den "Mixbetreibern". Die Basis unseres Geschäftsmodells ist der Verkauf von Zugangsberechtigungen zum Dienst an die JonDonauten, während wir gleichzeitig die Mixbetreiber dafür bezahlen, dass sie deren Datenverkehr über ihre Mixe weiterleiten.

Die Entwicklung und Bereitstellung der quelloffenen Software, die nötig ist um den JonDonym-Dienst zu betreiben und zu nutzen, übernehmen wir kostenlos in Zusammenarbeit mit Mitarbeitern der deutschen *Universitäten TU Dresden* und *Universität Regensburg*.

Universitäten TU Dresden

Technische Universität Dresden, Institut für Systemarchitektur

Professur Datenschutz und Datensicherheit

Lehrstuhlinhaber Prof. Dr. Andreas Pfitzmann

Verantwortlich Dipl.-Inf. Stefan Köpsell

D-01062 Dresden

Kooperationen und Partnerschaften des Lehrstuhls

- …
- Projektbezogene Partnerschaften
- IBM Forschungslabor Zürich, Schweiz
- JonDos GmbH, Deutschland
- London School of Economics and Political Science, Vereinigtes Königreich
- Netherlands Forensic Institute, Niederlande
- T-Systems Enterprise Services GmbH, Systems Integration, Deutschland

Universität Regensburg

Universität Regensburg, Institut für Wirtschaftsinformatik

Lehrstuhl Management der Informationssicherheit

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Prof. Dr. Hannes Federrath
D-93040 Regensburg
Projekt: AN.ON - Anonymität.Online

Kooperationen und Partnerschaften des Lehrstuhls

- …
- Art of defence GmbH
- Bundeskriminalamt (BKA)
- Initiative IT-Sicherheit
- IT-Security Cluster Ostbayern
- Siemens VDO

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Weitere Methoden zur Sicherung der Privatsphäre

In diesem Kapitel werden weitere Hinweise auf andere Konzepte, Produkte und Dienste gegeben. Die beiden oben aufgezeigten Lösungen stehen jedoch derzeit an der Spitze aller bisher angebotenen Lösungen, da sie eine - im Vergleich mit anderen Diensten – wirkungsvolles Gesamtkonzept und eine in weiten Teilen funktionierende Technologie anbieten. Um anonym im Internet sich bewegen zu können, werden insgesamt zahlreiche Methoden in Form von Produkten und kombinierten Lösungen mit Diensten angeboten. Unter der folgenden Adresse kann eine weitergehende Beschreibung über wirkungsvolle alternative Methoden abgerufen werden:

http://www.proxy-listen.de/Tutorials/Welche-Methoden-gibt-es-noch-um-anonym-zu-sein.html

Eine Alternative für die oben beschriebenen Privacy Shield-Methoden kann auch unter

http://www.proxy-listen.de/Tutorials/Was-sind-Wingates.html

abgerufen werden.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

Fazit

Einen absoluten Schutz der Persönlichkeitsrechte im Internet kann nicht erreicht werden. Das ein Internetbesucher beobachtet wird, ist eine Tatsache. Das Datenprofile von Unternehmen und Privatpersonen hergestellt werden ist ebenfalls eine Tatsache. Profiler verdienen weltweit mit detaillierten Datenprofilen von anderen Unternehmen Milliarden Dollar. Das Geschäft mit diesen Daten hat sich über Jahre und weitestgehend von der Öffentlichkeit unbeobachtet zu einem eigenen weltweiten Industriezweig entwickelt. Ob Datenprofile auch von in Deutschland ansässigen Profilern individualisiert und personalisiert werden, bleibt ungeklärt. Datenprofile werden auch auf Veranlassung von Bundes- und Landesbehörden ohne Verdachtsgründe allgemein mit Hilfe von privaten Unternehmen erstellt. Ausländische Profiler erhalten damit Einsicht in Deutsche Verwaltungsabläufe einzelner Ministerien und deren Kundenstruktur. Dabei werden offenbar Gesetzesverstöße auf allen Ebenen bewußt seit Jahren in Kauf genommen. Dazu trägt auch bei, dass sich hinter dem unscharfen Begriff der „statistischen Erfassung und Auswertung“ von Daten, die im Internet kostenlos und massenhaft vorhanden sind, zahlreiche Aktivitäten im Internet durchgeführt werden. Die eindeutige Definition einer „statistischen Erhebung“ und welche Daten dazu von Personen und Unternehmen erfaßt werden dürfen, ist nicht bekannt. Eine gründliche Überprüfung und Verfolgung von möglichen massenhaften Gesetzesverstößen in Deutschland ansässiger Unternehmen, einschließlich von Behörden und öffentlichen Einrichtungen, findet durch entsprechende Organe, trotzt neuester Klarstellung durch das BVG (Bundesverfassungsgericht), nicht statt. Eine private Person, ein Unternehmen und anderen Internetbesucher sind somit beim Schutz ihrer persönlichen Daten und ihrer Persönlichkeitsrechte auf sich selbst gestellt. Die Technologie für diesen Schutz ist vorhanden und kann kostenlos eingesetzt werden. Ein zuverlässiger Schutz der Privatsphäre im Internet ist zur Zeit nicht gegeben, obwohl dazu ein erheblicher Bedarf besteht. Der Schutz der Privatsphäre im Internet ist also bereits ein weltweiter Markt, der noch zu besetzen ist.

Beispiel eines einfachen Profils:

- Eindeutige Kennziffer einer Person, die durch ein Cookie auf dem persönlichen Computer gespeichert wird.

Daten des Profils nach Datenklassen auf einem externen Server. Verbindung zwischen Cookie und Profil ist die Kennziffer.

- Berufliche Position
- Kaufkraft
- Kredite und andere Verbindlichkeiten
- Bankverbindungen
- Versicherungen
- Eigenkapital
- Bedürfnisse

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.

- Abhängigkeiten
- Meinungen
- Erwartungen
- Interessen
- Neigungen
- Bewertung, Ranking

Einen relativen Schutz vor Profilern bietet der vollständige Einsatz der in diesem Dokument vorgestellten Lösungen. Im folgenden werden die vorgestellten Lösungen zum „**Schutz der Persönlichkeitsrechte im Internet**“ zu den „10 Internet-Geboten“ zusammengefaßt:

1. Nutzung von „auf Source-Code-Ebene“ öffentlich kontrollierbarer Programme.
2. Cookies und Scripte im Internetbrowser nicht zulassen. Maximal selektiv zulassen. Wenn sie zugelassen werden müssen, Cookies und Scripte nur temporär speichern lassen (wird im Firefox automatisch angeboten).
3. Internetbesuche generell nur mit lokalem Proxy Server, Firewall, Vierenschutzsoftware und Privacy Shield (Anonymisierungstechnologie) (siehe auch Technologien zum Schutz seiner Persönlichkeitsrechte) durchführen.
4. Die persönliche E-Mailadresse ist geheim. Bei der Angabe von E-Mailadressen auf Internetseiten pseudonyme E-Mailadressen verwenden.
5. E-Mails innerhalb fester Benutzergruppen generell verschlüsseln.
6. Keine Chats, Messenger oder ähnliche Online-Kommunikation im Geschäftsverkehr nutzen.
7. Keine Plattformen wie z.B. YouTube oder ähnliche Angebote nutzen. Ihre persönlichen Daten können von Profilern bei Bewertungen zum Abgleich z.B. in Bewerbungen, Bonitätsprüfungen, Versicherungs- oder Kreditanträgen verwendet werden.
8. Unsichere oder nicht vertrauensvolle Internetseiten zukünftig nicht mehr besuchen. Geben sie keine persönlichen Informationen in unsichere Internetseiten ein.
9. Kein Online-Banking, wenn keine von Ihnen kontrollierbare Verschlüsselung z.B. mit PGP oder OpenPG bei der Übertragung ihrer Daten möglich ist. Eine PIN oder/und TAN bietet keinen Schutz.

Hinweis: Lassen sie nach dem Verlassen des Internets alle historischen Daten im Internetbrowsers automatisch löschen. Der Verzicht auf Komfort erhöht die persönliche Datensicherheit. Der Komfort ist der Köder der Profilern, persönliche Daten zu erhalten.

Copyright © 2008, Kay Golze WIPN Group
No disclosure, reproduction, or use of any part thereof may be made except by written permission.