UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Schleswig-Holsteins
Servicezentrum für Datenschutz
und Informationszugang

In Zusammenarbeit mit

Technische Universität Dresden

veritas iustitia libertas
Freie Universität Berlin

Gefördert vom

Bundesministerium für Wirtschaft und Technologie

Sicherheit im Internet durch

Anonymität

HERAUSGEBER

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98 · 24103 Kiel
Homepage: www.datenschutzzentrum.de
Telefon: 0431 / 988 - 12 00
Telefax: 0431 / 988 - 12 23
E-Mail: mail@datenschutzzentrum.de

IN ZUSAMMENARBEIT MIT

Technische Universität Dresden >> Fakultät Informatik
Institut für Systemarchitektur · 01062 Dresden

und

Freie Universität Berlin >> Institut für Informatik
Takustraße 9 · 14195 Berlin
Homepage: www.anon-online.de
E-Mail: jap@inf.tu-dresden.de

ANSPRECHPARTNER:

Dr. Claudia Golembiewski
Martin Rost
Telefon: 0431 / 988 - 13 95 oder -13 91
E-Mail: anon@datenschutzzentrum.de

AUFLAGE:

August 2002

GESTALTUNG:

Eyekey Design, Kiel | Martin Papp
www.eyekey.de

Sicherheit im Internet durch Anonymität

1. Das Recht auf Anonymität

Manchmal sind Dinge so selbstverständlich, dass wir sie tun, ohne lange darüber nachzudenken oder gar fundierte Begründungen zu geben. Wir entscheiden im täglichen Leben häufig intuitiv, ob wir namentlich auftreten, oder ob wir „anonym“ bleiben wollen. In aller Regel gehen dem keine tiefschürfenden Reflexionen voraus, sondern wir verhalten uns so wie uns gerade zu Mute ist oder so wie es unserem üblichen, ganz persönlichen Verhaltensmuster entspricht. Vermutlich ist uns dabei gar nicht bewusst, dass wir ein Grundrecht ausüben, nämlich das auf informationelle Selbstbestimmung. Es ist gerade so, wie wenn wir atmen, essen und trinken, ohne dass wir überhaupt daran denken, dass wir dabei eigentlich unser Grundrecht auf Leben in Anspruch nehmen.

Jeder Mensch braucht zu einem selbstbestimmten Leben die Möglichkeit, in bestimmten Situationen anonym aufzutreten, so wie er die Atemluft zum Überleben braucht. Wer sich in allen Lebenslagen namentlich zu erkennen geben müsste, gewissermaßen seinen Namen für jedermann und jederzeit deutlich sichtbar eintätowiert tragen müsste, dem wäre das Recht auf informationelle Selbstbestimmung entzogen, denn er könnte nicht mehr wissen, geschweige denn selbst bestimmen, wer was wann und bei welcher Gelegenheit über ihn weiß.

Vielleicht ist dieses Recht auf Anonymität so selbstverständlich, dass man darüber weder schreiben noch sprechen muss? Gewiss, die Grundfesten des Datenschutzes ruhen auf der Annahme, dass die Verarbeitung personenbezogener Daten nur zulässig ist, wenn der Betroffene eingewilligt hat oder wenn ein Gesetz die Verarbeitung erlaubt. Das „Außergewöhnliche“ der Verarbeitung personenbezogener Daten und damit der Regelfall des nicht personenbezogenen Auftretens liegt unausgesprochen dem gesamten Datenschutzgedanken zu Grunde.

Auch die Tatsache, dass die „Identitätsfeststellung“ ein relevanter Vorgang ist, der nach allen Polizeigesetzen nur unter bestimmten Voraussetzungen zulässig ist, zeigt das Regel-Ausnahme-Verhältnis. Welch leidenschaftliche Debatten wurden noch vor zwei

Jahrzehnten geführt, als es darum ging, das Recht der polizeilichen Identitätsfeststellung zu erweitern und sogar auf jedermann auszudehnen, der sich an gefährlichen oder gefährdeten Orten aufhält. Die Polizei setzte sich seinerzeit mit ihren Vorstellungen bekanntlich durch. Dann kam das Zentrale Verkehrsinformationssystem ZEVIS, das es der Polizei technisch ermöglichte, im fließenden Straßenverkehr jederzeit unauffällig durch eine Computerabfrage festzustellen, wer da im Auto vor ihr fuhr. Schon bald verbreiteten sich weitere technische Systeme, die das Recht auf Anonymität faktisch aushöhlen, bevor eine Dogmatik dieses Rechts auch nur ansatzweise entwickelt war. So sucht man in den Bänden der Entscheidungen des Bundesverfassungsgerichts vergeblich nach dem Stichwort „Recht auf Anonymität“, wiewohl das Gericht, vor allem im Volkszählungsurteil, selbstverständlich der Sache nach auch zu dieser Frage judiziert hat. Auch in der juristischen Literatur ist das Recht auf Anonymität nur spärlich vertreten. In den neueren Datenschutzgesetzen ist von Anonymisierung, d. h. von der nachträglichen Wiederherstellung der Anonymität die Rede.

Manchmal wird den Menschen der Wert einer Errungenschaft, die sie täglich in Anspruch nehmen, erst dann bewusst, wenn sie bedroht ist. Unsere Anonymität ist inzwischen massiv gefährdet. ZEVIS war erst der Anfang in einer Kette von Technologien, die es ermöglichen, Menschen zu identifizieren und ihren Aufenthaltsort und ihre Bewegungen zu registrieren, ob ihnen das passt oder nicht. Wer ein Handy benutzt, kann geortet werden, sobald es eingeschaltet ist, wer nicht bar bezahlen möchte, muss seinen guten Namen hinterlassen. Videokameras oder gar Satelliten aus dem Weltall zeichnen auf, wer was wann wo gemacht hat. Ubiquitous Computing könnte der Freiheit zur Anonymität bald den Rest geben. Erst langsam dämmert den Menschen, dass da etwas bedroht ist, was für sie bislang zur selbstverständlichen Lebensqualität gehörte.

Und im Internet? Dort lauern überall die Schnüffler. Es ist ja auch einfach zu verführerisch, den Menschen heimlich über die Schultern schauen zu können, wie sie sich in der virtuellen Welt bewegen. Wer den Clickstream eines ausgedehnten Spaziergangs durch das Web analysieren kann, der ist nahe dran an der Gedankenwelt seines Opfers. Der alte Menschheitstraum, die Gedanken eines anderen lesen zu können, bekommt im Internet durchaus eine reale Basis. Menschen sind zumeist Opfer und Täter zugleich, auch

wenn wir schon früh gelernt haben: „Was du nicht willst, dass man dir tu, das füg auch keinem anderen zu“. Die Bedrohungen der Anonymität kommen im Internet von den staatlichen Sicherheitsbehörden ebenso wie von der privaten Wirtschaft oder vom Hacker von nebenan. Persönlichkeitsprofile von Menschen zu besitzen, die dies noch nicht einmal ahnen können, schafft Macht zur Unterdrückung, Manipulation und Ausbeutung.

In dieser Situation ist es besser, die Anonymität von Grund auf, gewissermaßen an der Quelle, zu schützen, als sich gegen die jeweils unterschiedlichen Angreifer mit unterschiedlichen Methoden zur Wehr zu setzen. Das hat auch der Gesetzgeber erkannt, der im Teledienstedatenschutzgesetz jedem das Recht eingeräumt hat, sich anonym durch das Netz zu bewegen. Kein Provider darf aufzeichnen, wer was wann im Netz getan hat, wenn dies nicht ausnahmsweise für Abrechnungszwecke erforderlich ist. Und dann dürfen die Daten auch nur für diesen Zweck verwendet werden. Klingt nicht nur gut, sondern ist auch ein gutes Datenschutzkonzept. Leider halten sich die wenigsten im Internet an die Spielregeln. Zu attraktiv ist offenbar der Gedanke, mit Hilfe von Protokolldaten nachzuvollziehen, wer was wann getan hat.

Deshalb muss das Recht auf Anonymität, das der Gesetzgeber den Internetnutzern ausdrücklich zugebilligt hat, in der Realität noch einmal erkämpft werden. Technische Vorkehrungen sind notwendig, um das Recht auf Anonymität tatsächlich in Anspruch nehmen zu können, denn das Internet darf kein rechtsfreier Raum sein. Das Projekt AN.ON, das die Technische Universität Dresden, die Freie Universität Berlin und das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein gemeinsam betreiben und das vom Bundeswirtschaftsminister gefördert wird, stellt allen Internetnutzern kostenlos eine Software zur Verfügung, mit deren Hilfe sie sich anonym im Internet bewegen können. Es ist ein Instrument, um Recht und Ordnung, in diesem Fall ein Bürgerrecht, im Internet durchzusetzen.

Beim Thema Anonymität im Internet fällt manchen nicht viel mehr als Kinderpornografie oder generell Strafverfolgung ein. In der Tat, anonym handelnde Menschen sind innerhalb wie außerhalb des Internet die eigentliche Herausforderung für die Kriminalpolizei. Niemand würde auf die absurde Idee kommen – oder doch ? – unser gesamtes Leben, jeden Schritt, jede Aktivität, lückenlos aufzuzeichnen, nur weil im Falle einer Straftat die Strafermittlungen dann leichter möglich wären. Im Internet soll plötzlich angehen, was in der realen Welt grob verfassungswidrig wäre? Die Begehrlichkeiten sind bei manchen Sicherheitspolitikern groß. Das Foucault'sche Panoptikum, das ansonsten nur in einem speziell gebauten Gefängnis funktionieren kann, soll plötzlich im Internet Realität werden. Das den Bürgern im Teledienstedatenschutzgesetz ausdrücklich bestätigte Recht auf Anonymität ist noch gar nicht überall in die Praxis umgesetzt, da soll es bereits wieder abgeschafft und in sein Gegenteil verkehrt werden. Statt endlich gegen rechtswidrige Protokolldatenbestände vorzugehen, soll die Schaffung solcher Vorratsdaten sogar ausdrücklich vorgeschrieben werden. Verrückte Welt, in der, statt den Bürgern zum Recht zu verhelfen, dieses kurzerhand entzogen werden soll.

Die Diskussion um die Durchsetzung des Rechts auf Anonymität im Internet zeigt, dass inzwischen auch Selbstverständliches der Begründung und Verteidigung bedarf. Rechte, die wir schon sicher zu besitzen glaubten, müssen plötzlich gegen eine omnipotente Überwachungstechnologie und gegen ein maßlos übersteigertes Sicherheitsdenken von neuem verteidigt werden. Unser Recht auf Anonymität, das wir bis dato einfach hatten und das – von Prominenten einmal abgesehen – jeder von uns selbstverständlich tagtäglich in Anspruch nahm, bedarf jetzt vorsichtshalber der ausdrücklichen Ableitung aus den Grundrechten. Beim Gang über den Marktplatz, bei der Teilnahme an einem Musikfestival, beim Besuch im Fußballstadion, in der U-Bahn oder nur beim Bäcker nebenan verhalten wir uns nicht nur völlig natürlich, wenn wir kein großes Namensschild vor uns hertragen, sondern wir nehmen auch ein Grundrecht in Anspruch, nämlich selbst zu entscheiden, wem gegenüber wir uns in welcher Situation zu erkennen geben. Ganz zu schweigen von besonderen Nutzungen des Internet z. B. im Rahmen von Ehe- oder Drogenberatung, Seelsorge oder Telemedizin.

Das Recht auf informationelle Selbstbestimmung gibt, wie sein Name unschwer verrät, jedem das Recht, grundsätzlich selbst zu entscheiden, welche Informationen er über sich selbst preisgibt. Dies schließt selbstverständlich das Recht ein, auch gar nichts von sich preisgeben zu wollen. Solange nicht ein staatliches Eingriffsgesetz oder die Rechte anderer entgegenstehen, kann jeder Mensch sein Recht auf informationelle Selbstbestimmung in der Form ausüben, dass er nicht namentlich, eben anonym, auftritt. Wer hätte gedacht, dass unsere Freiheit eines Tages so in Gefahr kommen würde, dass es ratsam erscheint, auf solchen Selbstverständlichkeiten wie dem Recht auf Anonymität ausdrücklich zu bestehen, bevor auch dieses Grundrecht soweit ausgehöhlt ist, dass nicht mehr viel Substanz bleibt. Die Informationsgesellschaft beruht auf genialen technischen Erfindungen, aber sie zwingt auch dazu, vermeintlich selbstverständliche Rechte neu zu begründen und zu festigen, deren Verlust die schönsten Errungenschaften der Informationstechnik nicht aufwiegen könnten.

Dr. Helmut Bäumler
Landesbeauftragter für den Datenschutz und
Leiter des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

2. Das technische Konzept hinter AN.ON

Wer beobachtet mich beim Surfen im Internet?

Eigentlich kann doch niemand mitbekommen, was ich daheim auf meinem Computer so mache!? Ich surfe zwar im Internet, aber das machen doch so viele andere auch – da falle ich doch gar nicht auf!

In diesem Kapitel wird erklärt, weshalb diese Einschätzung so nicht richtig ist. Es wird beschrieben, was beobachtet werden kann, und vor allem, wer dazu in der Lage ist. Es soll aber hier auch gleich klargestellt werden, dass nicht jeder, der zur Beobachtung in der Lage wäre, dies auch tut. Im Gegenteil: für Internet Service Provider (ISP) ist es mehrheitlich eher eine Last, Nutzungsdaten zu sammeln. Diese Daten wecken schließlich Begehrlichkeiten bei Polizei und Geheimdiensten, deren Wünsche in erster Linie Kosten für die ISP verursachen.

Wann immer ein Nutzer ohne Schutzmechanismen im Internet surft, kann die Kommunikationsbeziehung, z. B. welche Webseite gerade abgerufen oder an wen eine E-Mail verschickt wird, belauscht werden. Meistens sind auch problemlos die Inhalte abhörbar. Eine E-Mail ist von jedem lesbar, der auf dem Weg lauscht, den die Daten im Netz nehmen. Ebenso wie eine Postkarte vom Briefträger und von den Angestellten in den Briefverteilzentren gelesen werden könnte.

WER KANN BEOBACHTEN?

Beobachter können alle diejenigen sein, die in irgendeiner Weise Infrastruktur für das Internet bereitstellen oder auf diese zugreifen können. In der Praxis sind dies vor allem der eigene Internet Service Provider, Betreiber von Routern, die die jeweiligen Datenpakete

weiterleiten, der Netzwerkadministrator in der Firma oder andere Nutzer, die sich lokal im gleichen Netz befinden. Externe Beobachter, die nicht über diese Möglichkeiten verfügen, können nicht ohne weiteres andere Nutzer beobachten. Dazu wären sie auf die aktive Mithilfe des Beobachteten bzw. seines Rechners angewiesen. Eine Möglichkeit wäre es beispielsweise, auf dem Rechner des Beobachteten ein spezielles Überwachungsprogramm (z. B. einen Virus) zu installieren, das den Nutzer direkt beobachtet und seine Erkenntnisse an den externen Beobachter sendet. Auf diese Weise gehen z. B. einige Firmen vor, die dem Nutzer für das Surfen Geld bezahlen, dafür aber einen Teil des Bildschirms blockieren, um ihre Werbung anzuzeigen.

WAS KANN BEOBACHTET WERDEN?

Jeder mit dem Internet verbundene Rechner wird innerhalb des Internet über die so genannte IP-Adresse identifiziert. Ein permanent an das Internet angebundener Rechner hat eine fest zugewiesene IP-Adresse. Private Nutzer wählen sich in der Regel per Telefon über einen ISP in das Internet ein. Von diesem erhalten sie für die Dauer ihrer Einwahl eine dynamisch zugewiesene IP-Adresse. Auf die Frage, ob und inwieweit eine IP-Adresse ein personenbezogenes Datum darstellt, wird im 3. Kapitel eingegangen.

Im Internet werden alle Informationen in kleinen Datenpaketen transportiert, die immer die IP-Adressen von Absender und Adressat enthalten. Dadurch weiß der adressierte Rechner, wohin er seine Antwort, z. B. die vom Browser angefragten Webseiten oder die für einen Nutzer zwischengespeicherten E-Mails, senden muss. Die IP-Adresse ist vergleichbar mit einer realen Postadresse – im Falle temporärer Adressen mit zeitlich beschränkt gültigen Postfächern. Alle Datenpakete, die zu einer IP-Adresse gesendet werden, sind für Beteiligte (Betreiber der angefragten Webseite, ISP) und Außenstehende (z. B. Betreiber von Routern) verkettbar. Sowohl die Datenpakete als auch die IP-Adressen sind für alle oben aufgezählten Beobachter sichtbar.

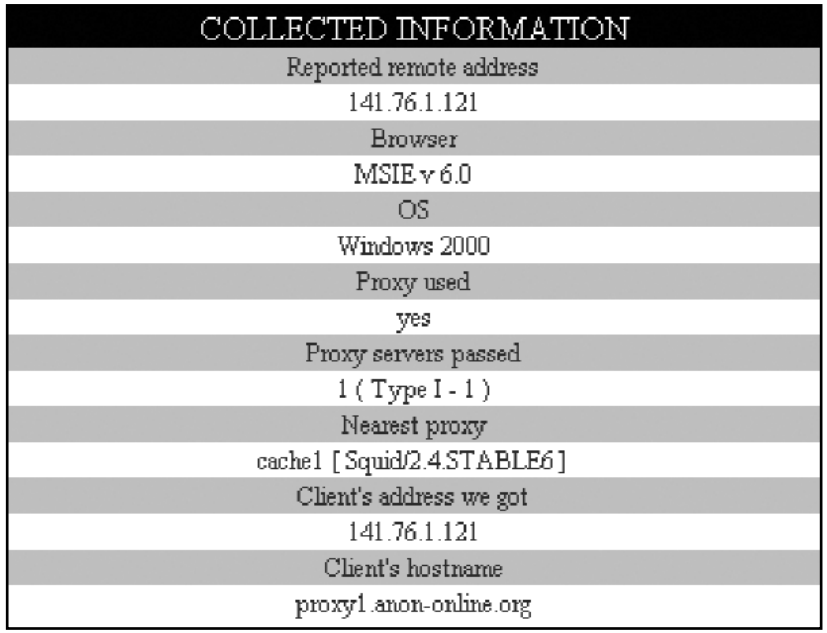
Fest zugewiesene IP-Adressen sind innerhalb eines Teilnetzes durch dessen Betreiber einem Nutzer zugeordnet. Jeder Beobachter, der die Zuordnung zwischen diesem und der

IP-Adresse kennt, kann exakte Benutzungsprofile erstellen. Um eine derartige Zuordnung vornehmen zu können, genügt es einem Beobachter bereits, eine E-Mail vom beobachteten Nutzer empfangen zu haben, da diese die IP-Nummer seines Rechners enthält. Dynamisch zugewiesene IP-Adressen sind für den ISP mit dem Telefonanschluss, von dem er angewählt wurde, verknüpft. Er weiß, welchem Nutzer er in welchem Zeitraum welche IP-Adresse zugewiesen hat, und er wird in der Regel auch eine Logdatei darüber führen. Solange der ISP eines Nutzers bzw. der Betreiber des von seiner Nutzergruppe verwendeten Rechners die erhobenen Daten gegen unbefugte Zugriffe schützt, nicht weitergibt und nicht selbst zur Beobachtung verwendet, ist der Nutzer vor externen Beobachtern und den Betreibern der angefragten Webseiten theoretisch anonym. Praktisch gilt die Anonymität nur so lange, wie der Nutzer Cookies und Java-Script abschaltet und auch sonst keine identifizierenden Daten an fremde Server übergibt. Cookies untergraben die Anonymität, indem sie den Nutzer mit einer eindeutigen Kennung versehen, die beim Surfen an den Webserver übermittelt wird, der den Cookie gesetzt hat. Aktive Inhalte sind in der Lage, eindeutige Kennungen, z. B. die IP-Nummer, zu übermitteln.

Leider lassen sich aber ohne Aktivierung von Cookies, JavaScript etc. viele Webseiten nicht mehr anzeigen bzw. Webservices nicht nutzen. Außerdem werden zunehmend bei den ISP Nutzerdaten gesammelt, da diese ihnen eine attraktive Nebeneinnahme bescheren können.

Zusätzlich werden noch zahlreiche Informationen über den Nutzerrechner innerhalb des Kommunikationsprotokolls zum Abfragen von Webseiten (HTTP-Protokoll) an den Webserver übertragen. Dazu zählen u. A. das verwendete Betriebssystem und der verwendete Browser. Häufig wird argumentiert, dieses habe insbesondere den Vorteil, dass Betreiber von Webseiten dem Nutzer eine auf seinen Browser optimierte Darstellung ihrer Webseite bereitstellen können. Abbildung 1 illustriert einen Teil der beim Webserver über den Rechner des Nutzers verfügbaren Informationen. Dabei hat ein Nutzer mit einem üblichen Browser (in diesem Fall Internet Explorer) auf eine entsprechende Testseite *http://www.leader.ru/secure/who.html* zugegriffen.

Abbildung 1



COLLECTED INFORMATION
Reported remote address
141.76.1.121
Browser
MSIE v 6.0
OS
Windows 2000
Proxy used
yes
Proxy servers passed
1 (Type I - 1)
Nearest proxy
cache1 [Squid/2.4.STABLE6]
Client's address we got
141.76.1.121
Client's hostname
proxy1.anon-online.org

Höchstwahrscheinlich kann jedoch ein Webserver allein anhand dieser Daten (außer der IP-Adresse) einen einzelnen Nutzer nicht identifizieren oder wiedererkennen. Betriebssystem, Webbrowser usw. unterscheiden zwar Nutzergruppen voneinander, aber jede der Gruppen dürfte noch so groß sein, dass einzelne Nutzer nicht identifiziert werden können. Wie bereits oben beschrieben ist allerdings die Abschaltung von Cookies und aktiven Inhalten erforderlich.

FILTERPROGRAMME

Insbesondere gegen die Erstellung von Nutzungsprofilen mithilfe von Cookies existieren eine Reihe von Tools, z. B. Webwasher (*http://www.webwasher.com*) und CookieCooker (*http://cookie.inf.tu-dresden.de*). Die Idee dieser Tools ist es, Cookies zwar erst einmal anzunehmen, diese aber nur für die aktuelle Sitzung zu verwenden. Webseiten, die auf der Nutzung von Cookies bestehen, können dies nicht feststellen und Nutzer somit nicht aussperren. CookieCooker geht dabei noch einen Schritt weiter: Cookies werden nicht einfach nur gelöscht, sondern über ein Netz von Cookie-Servern mit denen anderer Nutzer ausgetauscht. Webserver werden dadurch verwirrt und ihre gespeicherten Nutzerprofile durchmischt.

Anonym oder unbeobachtbar surfen

In diesem Abschnitt werden die Grundlagen zum Verständnis der Funktionsweise von Anonymisierungsdiensten gelegt.

ANONYMITÄT

Ein einzelner Internetnutzer kann gegenüber einem Beobachter nicht absolut anonym sein. Anonym ist ein Einzelner immer in einer Gruppe, die sich in allem, was ein Beobachter sehen kann, gleich verhält: Für den Beobachter ist nicht entscheidbar, welches Mitglied der Gruppe eine bestimmte Webseite abgerufen hat. Zudem bezieht sich die Anonymität meistens auf den Kommunikationspartner: Beispielsweise ist der Sender vor dem Empfänger anonym.

UNBEOBACHTBARKEIT

Unbeobachtbarkeit ist eine viel stärkere Forderung. Ein Internetnutzer ist unbeobachtbar gegenüber einem beliebigen Beobachter, wenn dieser nicht einmal feststellen kann, ob der Nutzer überhaupt kommuniziert. Effizient lässt sich völlige Unbeobachtbarkeit nur in Verteilnetzen wie z. B. dem Kabelfernsehen realisieren. In Vermittlungsnetzen müsste zur Erreichung völliger Unbeobachtbarkeit zusätzlich ein hoher Prozentsatz an leerem Datenverkehr, so genannter Dummy-Traffic, stattfinden.

Auch wenn die Anfrage eines Internetnutzers auf eine bestimmte Webseite gegenüber außen stehenden Beobachtern unbeobachtbar oder anonym ist, müssen Nutzer und Betreiber der Webseite nicht anonym voreinander sein; für viele Anwendungen ist es sogar sinnvoll oder erforderlich, dass sie sich kennen (z. B. Online-Banking oder personalisierte Webseiten).

WIE KANN MAN ANONYM SURFEN?

Die Internet-Anfragen einer Gruppe von Internetnutzern können innerhalb dieser Gruppe anonymisiert werden, wenn sich die Computer der Nutzer nicht direkt zum Webserver verbinden, sondern ihre Kommunikationsverbindungen über einen Umweg schalten. Die dabei verwendete Methode beeinflusst die maximale “Stärke” der Beobachter, vor denen die Nutzer gerade noch anonym sind, sowie den Grad ihrer Anonymität. Soll Anonymität oder Unbeobachtbarkeit erreicht werden, dann muss es immer einen Bereich geben, den der Beobachter nicht überwachen kann. Ansonsten könnte er ja einer Nachricht einfach auf ihrem gesamten Weg folgen. Zwar kann keine Methode gegen einen allmächtigen Beobachter schützen, man kann den notwendigen “sicheren” Bereich jedoch immer kleiner machen oder diesen sogar so verteilen (räumlich oder organisatorisch), dass die Methode noch sicher ist, wenn der Beobachter auch nur einen von vielen “sicheren” Bereichen nicht beobachtet. Eine solche Verteilung der Sicherheit auf mehrere Parteien wird z. B. durch das nachfolgend beschriebene Konzept der Mixe realisiert. Gegenüber externen Beobachtern und Webservern erreicht bereits die Einwahl über den ISP

(dynamisch vergebene IP-Nummer) oder die Benutzung eines Rechners durch mehrere Personen die Anonymität eines einzelnen Nutzers innerhalb der betreffenden Gruppe von Internetnutzern. Ein Nutzer, der durch eine einzelne IP-Adresse identifizierbar ist oder der die Anonymität seiner einzelnen Handlungen gegenüber seinem ISP oder dem Betreiber des von seiner Nutzergruppe verwendeten Rechners wünscht, sollte zusätzliche Anonymisierungsdienste nutzen, die seinen Webzugriff über Umwege leiten.

EINFACHE LÖSUNG: ANON-PROXIES

Ein Proxy (zu Deutsch: Stellvertreter) kann zwischen den Browser eines Internetnutzers und die von ihm angefragten Webserver geschaltet werden. Er hat die Aufgabe, angefragte Webseiten anstelle des Nutzers abzurufen. Manche Institutionen erlauben ihren Mitgliedern (z. B. Mitarbeiter und Studierende von Universitäten) den Internet-Zugriff sogar nur über so genannte Zwangs-Proxies. Es ist dadurch möglich, bestimmte unerwünschte Webserver für die Nutzer, die über diesen Zwangs-Proxy auf das Internet zugreifen, zu sperren. Beispielsweise erlauben einige Staaten ihren Bürgern nur den Zugriff auf einen Teil des Internet.
Gegenüber einem Browser (Client) erscheint der Proxy als Webserver, während er gegenüber einem Webserver einen Client darstellt.

WAS IST EIN ANON-PROXY?

Ein so genannter Anon-Proxy nutzt das obige Prinzip aus. Der Webserver oder auch ein hinter dem Anon-Proxy befindlicher Lauscher erfährt nicht, wer eigentlich auf die Webseite zugreifen wollte, da der Anon-Proxy stellvertretend als Anfragender auftritt.

Es existieren mehrere Anbieter von Anon-Proxies im Internet, z. B. Anonymizer (*http://www.anonymizer.com*) oder Rewebber (*http://www.rewebber.com*), die sich durch den Vorteil auszeichnen, dass auf dem eigenen Rechner keine zusätzlichen Programme

installiert werden müssen.
Einige Tools für den Bereich Sicherheit, z. B. Steganos (*http://www.steganos.com*), bieten anonymes Websurfen, indem sie Webseitenaufrufe über allgemein zugängliche, so genannte “offene” Proxies umleiten, die damit als Anon-Proxis fungieren (mitunter unbeabsichtigt durch die Betreiber dieser Proxies). Um eine hohe Verfügbarkeit zu erreichen, verwalten diese Programme ganze Listen der verwendbaren Proxies, die während des Surfens regelmäßig gewechselt werden.

Bei allen obigen Realisierungsarten ruft der Anon-Proxy dann die angefragte Webseite in seinem eigenen Namen auf, so als wäre er der Nutzer. Anon-Proxies realisieren damit zwar Anonymität gegenüber dem Webserver und, falls verschlüsselt wird, auch vor dem eigenen ISP, nicht jedoch gegenüber dem Betreiber des Anon-Proxies. Dieser kann die dem Nutzer zugeordnete IP-Adresse natürlich mit der angefragten Webseite verknüpfen. Es kann daher wohl nur eine Frage der Zeit sein, bis potenzielle Datensammler selbst Anon-Proxies betreiben.

Häufig wird für die Programme, die anonymes Websurfen über freie Proxies realisieren, damit geworben, dass die Verwendung mehrerer Proxies für die Anonymisierung vorteilhaft sei. Da aber zu einem Zeitpunkt immer nur ein Proxy verwendet wird, ist dem jeweils verwendeten Proxy die Zuordnung zwischen IP-Nummer und angefragter Webseite bekannt. Anon-Proxies realisieren auch keine Unbeobachtbarkeit gegenüber externen Beobachtern, die Leitungen überwachen (Big Brother) und damit (zumindest theoretisch) genau wissen, zu welchem Zeitpunkt die Anfrage einer Webseite im Anon-Proxy eingegangen ist. Da der Proxy diese sofort bearbeitet, kann “Big Brother” Anfrage und angefragte Webseite leicht miteinander verknüpfen. Gegen diese Beobachtung hilft selbst Verschlüsselung nicht, da die zeitliche Zusammengehörigkeit nach wie vor beobachtbar bleibt. Eine Verschlüsselung zwischen Nutzer und Proxy sowie zwischen Proxy und Zielserver verbirgt zwar vor fremden Blicken, für welche Inhalte (z. B. welche Webseiten) sich der Nutzer interessiert. Die Kommunikationsbeziehung als solche, d .h. welcher Webserver aufgerufen wird, ist dagegen trotzdem beobachtbar.

Lösung gegen “Big Brother”: Mix-Netze

WAS IST EIN MIX-NETZ?

Ein Mix-Netz besteht aus einer Menge von Rechnern, den Mixen, die über das Internet verbunden sind. Das Mix-Konzept wurde von David Chaum 1981 eingeführt. Es wurde für den anonymen E-Mail-Versand entwickelt.

Diese Idee lässt sich mit einigen Anpassungen auch zum anonymen Websurfen verwenden. Ein Internetnutzer kann die Anfrage einer Webseite über eine Folge von Mixen leiten, statt diese direkt an den entsprechenden Webserver zu richten. Entsprechende praktische Realisierungen von anonymer E-Mail und anonymem Websurfen werden nachfolgend beschrieben.

Mixe sind nicht einfach eine Aneinanderreihung von Anon-Proxies, sondern realisieren vielmehr auch Schutz gegenüber einem Angreifer, der Leitungen überwacht. Um zu verhindern, dass dieser den Weg einer Anfrage verfolgt, werden in jedem Mix die ankommenden Anfragen verwürfelt, in ihrem Aussehen verändert und schließlich wieder ausgegeben. Selbst wenn Big Brother alle Verbindungen zwischen Nutzern, Mixen und Webservern beobachtet, verliert er die Zuordnung, welcher Nutzer welche Webseite anfragt. Die Funktionsweise eines Mixes gleicht einem Postamt, das jeden eingehenden Brief öffnet und darin wieder einen verschlossenen Briefumschlag vorfindet, den es an die darauf stehende Adresse, meist wieder ein Postamt, weiterleitet. Das nächste Postamt verfährt ebenso, bis der Brief – entsprechend verzögert – schließlich beim Empfänger landet.

In der Welt des Internet entsprechen die Briefe den Datenpaketen und die Postämter den Mixen. Damit die Weiterleitung funktioniert, müssen auf dem Rechner des Nutzers die Datenpakete entsprechend vorbereitet werden. Sie werden so verpackt (verschlüsselt), dass sie nur dann ausgepackt (entschlüsselt) werden können, wenn sie von allen zu verwendenden Mixen in der vom Sender vorgesehenen Reihenfolge entschlüsselt wurden. Dazu verschlüsselt der Nutzer zunächst die Anfrage für den letzten Mix, sodass nur dieser sie lesen kann. Das Ergebnis dieser Verschlüsselung wird nun erneut verschlüsselt, dies-

mal jedoch für den vorletzten Mix und so fort. Diese nun mehrfach verschlüsselte Nachricht wird an den ersten Mix gesendet. Nur er kann die erste Verschlüsselungsschale entschlüsseln (den äußersten Briefumschlag entfernen) und verschickt sein Ergebnis an den folgenden Mix. Der letzte Mix der Folge leitet die Anfrage dann an den vom Nutzer gewünschten Webserver weiter. Dabei wird diese Adresse auf Grund der Verschlüsselung eben erst beim letzten Mix offenbart.

WIE SCHÜTZEN MIXE GEGEN BIG BROTHER?

Die Kryptographie stellt an Verschlüsselungsverfahren die Anforderung, dass ohne Kenntnis des zugehörigen geheimen Schlüssels kein Zusammenhang zwischen einer Menge von Verschlüsselungstexten und der entsprechenden Menge von Klartexten bestehen darf, d. h. zu jedem Verschlüsselungstext könnte mit etwa gleicher Wahrscheinlichkeit jeder Klartext gehören.

Das Mix-Konzept nutzt diese Eigenschaft von Verschlüsselungsverfahren aus, um Anonymität der Internetnutzer zu gewährleisten. Ein Beobachter, der alle Leitungen eines Mixes belauscht, sieht, wie verschlüsselte Datenpakete den Mix erreichen und ihn entschlüsselt wieder verlassen. Wenn der Mix seine Entschlüsselung durchgeführt hat, ist es einem Beobachter, der nicht über den Schlüssel des Mixes verfügt, nicht möglich, eine Beziehung zwischen eingehenden und ausgehenden Datenpaketen herzustellen.

Damit für einen Beobachter auch keine zeitliche Verkettung der ein- und ausgehenden Datenpakete möglich ist, sammeln Mixe mehrere Nachrichten, bevor sie sie wieder ausgeben. Vor der Ausgabe wird die Reihenfolge der Nachrichten noch “durcheinander gemixt”. Ein Beobachter kann also nicht davon ausgehen, dass die dritte eingehende Nachricht zu der dritten vom Mix gesendeten Nachricht gehört.

Damit es einem Beobachter auch nicht möglich ist, den Weg einer Nachricht anhand ihrer Länge zu verfolgen, haben alle Datenpakete die gleiche Länge.

Um völlige Unbeobachtbarkeit jedes Nutzers zu gewährleisten, ist es notwendig, dass die Nutzer eines Mix-Netzes auch dann Daten senden, wenn sie eigentlich keine Webseiten abfragen möchten. Diese leeren Daten werden als Dummy-Traffic bezeichnet. Ohne Dummy-Traffic ist zumindest beobachtbar, welche Teilnehmer gerade anonym kommunizieren. Für alle Teilnehmer bedeutet dies, dass sie nur in der Gruppe der gerade aktiv surfenden Teilnehmer anonym sind.

WESHALB GENÜGT NICHT EIN MIX?

Chaum ging bei der Entwicklung der Mixe davon aus, dass der Big Brother nicht nur das gesamte Netz überwacht, sondern zusätzlich einen Großteil der Mixe kontrolliert. Damit eine Nachricht unbeobachtbar durch das Kommunikationsnetz transportiert wird, muss lediglich ein einziger Mix vertrauenswürdig sein. Würde der Nutzer nur einen Mix verwenden bzw. nur Mixe benutzen, die von genau einem Betreiber verwaltet werden, wäre er von diesem beobachtbar. Um neben dem Schutz gegenüber externen Beobachtern auch Schutz gegenüber den Betreibern der Mixe zu gewährleisten, müssen wenigstens zwei Mixe verwendet werden, damit keiner von beiden alles über die Zuordnung von Nutzer und angefragter Webseite erfährt: Der erste Mix weiß, welcher Nutzer welche Anfrage absendet und dass er ihn an einen Mix weiterleiten muss. Der letzte Mix weiß, wohin eine Anfrage gesendet werden soll, aber nicht, von welchem Nutzer diese stammt. Solange die beiden Mixe nicht zusammenarbeiten, bleibt die Kommunikationsbeziehung vor allen externen Beobachtern und den Betreibern der Mixe verborgen.

Die Anzahl der Mixe, für die sich ein Nutzer entscheidet, hängt letztendlich von seinem Vertrauen in die betreibenden Institutionen ab. Technisch spielt es für die erreichbare Anonymität keine Rolle, wie viele korrupte Mixe eine Folge enthält, solange wenigstens ein Mix vertrauenswürdig ist.

Die Betreiber der Mixe müssen sorgfältig ausgewählt werden, damit diese nicht mit vereinten Kräften an der Enttarnung ihrer Nutzer arbeiten. Mögliche Beispiele sind Datenschutzbeauftragte des Bundes und der Länder, Bürgernetzvereine, kirchliche Organisa-

tionen und Institutionen, deren Geschäftsfeld sowieso typischerweise Diskretion erfordert, z. B. Banken, Beratungsstellen oder die Post. *

Wenn die Mixe von unabhängigen Betreibern angeboten werden, ist die Chance, dass doch alle Mixe mit dem Beobachter zusammenarbeiten, sehr gering. Aus Kostengründen ist es sinnvoll, alle Mixe in einem Rechenzentrum – aber physisch separat gesichert (Tresor) – aufzustellen, da bei einer Aufstellung an verschiedenen Orten die Daten zwischen den Mixen andernfalls über das Internet oder teure Standleitungen übertragen werden müssten.

ANGRIFFE VON BIG BROTHER

Ein Beobachter, der die Anonymität von Internetnutzern aufheben möchte, kann nicht nur versuchen, alle Leitungen zu überwachen und einzelne Mixbetreiber unter seine Kontrolle zu bekommen, sondern er kann auch versuchen, aktiv ins Geschehen einzugreifen.

Zwei Beispiele werden im Folgenden erklärt:

Der erste Angriff ist der so genannte Replay-Angriff. Dabei zeichnet der Beobachter eine Anfrage auf und spielt sie später noch einmal ein, so dass dem Mix eine bereits versendete Nachricht zur erneuten Bearbeitung vorgelegt wird. Dieser führt die Entschlüsselung durch und sendet das Ergebnis weiter. Dabei entsteht eine zur ursprünglichen Verarbeitung identische Nachricht. Vergleicht ein Beobachter nun die Ausgaben des Mixes, kann er die wiederholt gesendete Nachricht entdecken, da nur sie in beiden Ausgaben vorhanden ist. Er hat somit diesen Mix überbrückt.

Um solche Replay-Angriffe zu verhindern, besitzt jeder Mix eine Datenbank, in der er bereits bearbeitete Nachrichten speichert. Genau genommen speichert er nicht die Nachricht selbst, sondern nur einen aus der Nachricht berechneten “Fingerabdruck”. Wird dem Mix nun eine Nachricht zur Bearbeitung vorgelegt, überprüft er zunächst, ob sie

* Die Betreiber der Mixe im Rahmen des AN.ON-Projektes sind derzeit die Technische Universität Dresden, die Freie Universität Berlin (spline – studentisches projekt linux netz), die Medizinische Universität Lübeck (Projekt Ecstasy Online) und ab 2002 das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein.

nicht bereits bearbeitet wurde, ansonsten ignoriert er die Nachricht. Um ein unbegrenztes Anwachsen der Datenbank zu verhindern, ist jede Nachricht nur begrenzte Zeit gültig, d. h. es wird ein Haltbarkeitsdatum hineinkodiert. Der Mix kann dadurch Fingerabdrücke veralteter Nachrichten aus der Datenbank löschen.

Eine weitere Angriffsmöglichkeit stellt der *(n-1)*-Angriff dar. Die Größe *n* bezeichnet dabei die Anzahl der Nutzer eines Mix-Netzes. Das Prinzip des Angriffs beruht darauf, dass der Beobachter von den *n* zu einem Zeitpunkt verarbeiteten Nachrichten *n-1* kennt und deren Weg bestimmen kann. Als einzige Unbekannte bleibt somit die Nachricht des angegriffenen und nun enttarnten Nutzers übrig.

Durchführbar ist dieser Angriff z. B., indem ein Nutzer allein *n-1* Nachrichten generiert oder *n-1* Nutzer zusammenarbeiten. Der erste Fall, dass mehrere Nachrichten eines Schubes vom selben Nutzer stammen, lässt sich mittels kryptographischer Verfahren verhindern. Technisch nicht kontrollierbar ist hingegen der zweite Fall, dass Nutzer zusammenarbeiten, um andere zu enttarnen.

MIX-KASKADE ODER NUTZERBESTIMMTE FOLGE IM MIX-NETZ?

Im Wesentlichen gibt es zwei verschiedene Methoden, Mixe in einem Netz zu betreiben. Bei der im später ausführlich erläuterten Anonymisierungsdienst JAP verwendeten Methode werden die Mixe zu einer Kaskade zusammengeschlossen. Für den Nutzer bedeutet dies, dass er nicht einzelne Mixe auswählt, sondern sich für eine komplette Mix-Kaskade (vorgegebene Anzahl und Reihenfolge von Mixen) entscheidet.

Die andere Möglichkeit ist folgende: Jeder Mix bietet seine Dienste für sich allein an. Jeder Nutzer stellt aus den verfügbaren Mixen eine eigene Kette zusammen, über die er seine Nachrichten schickt.

Auf den ersten Blick scheint die zweite Möglichkeit nutzerfreundlicher, da dieser die Mixe seines Vertrauens selbst auswählen kann. Technisch führt die freie Mixwahl aber schon

deshalb zu einer geringeren Anonymität, da diese ja dadurch entsteht, dass sich möglichst viele Nutzer möglichst gleich verhalten. Wenn jeder Nutzer eine andere Route wählt, so kann der Beobachter bei längerer Beobachtung seine Schlüsse ziehen. So sind z. B. die zwischen den einzelnen Mixen durch unterschiedliche Wegewahl hervorgerufenen Lastschwankungen aufschlussreich.

Weitere Informationen und wissenschaftliche Papiere zum Thema finden Sie auf der Webseite *http://www.inf.tu.dresden.de/~hf2/anon*.

Anonyme Internetnutzung über Mix-Netze

Momentan existiert am Markt nur der Anonymisierungsdienst JAP als ein System für mixbasiertes anonymes Websurfen. Für anonyme E-Mail stehen so genannte Type-2-Remailer, z. B. Mixmaster (*http://www.obscura.com/*), zur Verfügung.

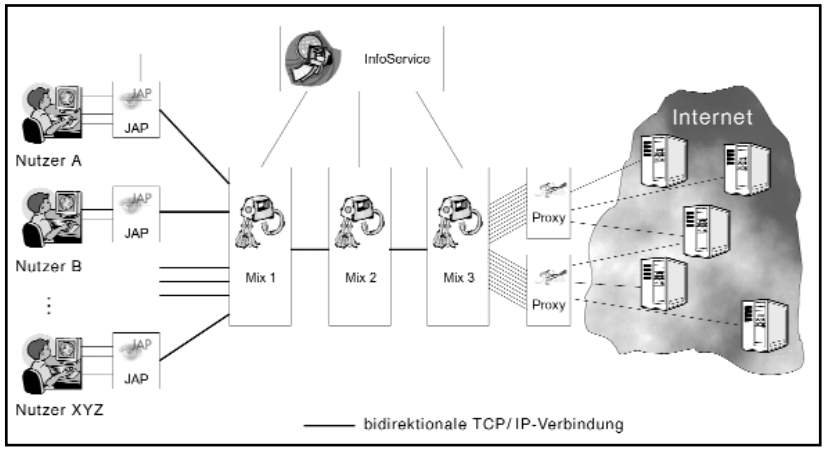
ANONYMISIERUNGSDIENST "JAP"

Im Rahmen des Projektes "AN.ON - Starke Unbeobachtbarkeit und Anonymität im Internet", das in Zusammenarbeit zwischen der TU Dresden, der FU Berlin und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein durchgeführt und vom Bundesministerium für Wirtschaft und Technologie gefördert wird, wird die Software **JAP** (*www.anon-online.de*) entwickelt und ein Anonymisierungsdienst betrieben, um Internetnutzern anonymes Websurfen zu ermöglichen. Dem System liegt das vorstehend beschriebene Mix-Konzept zu Grunde.

KOMPONENTEN

Die entwickelte Software besteht aus drei Komponenten, die in Abbildung 2 schematisch dargestellt sind:

Abbildung 2

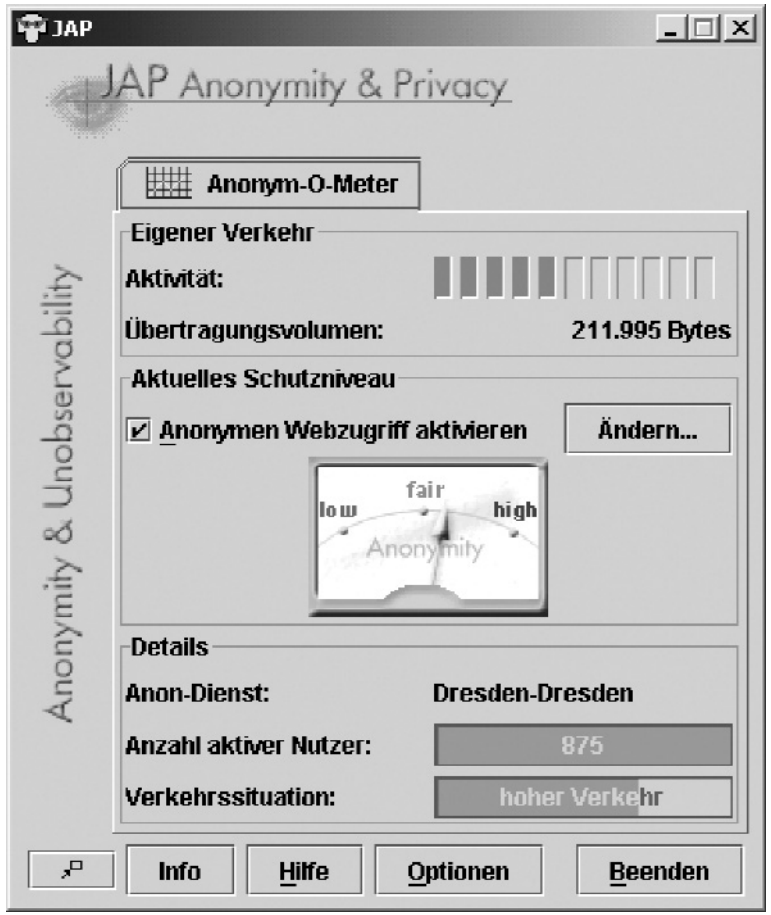


Der Anonymisierungsdienst selbst besteht aus mehreren möglichen Mix-Kaskaden, über die die Anfragen der Nutzer geleitet werden. Die Mixe sind für die weitere Verarbeitung der Daten gemäß dem jeweiligen Mix-Protokoll zuständig.

Auf der Nutzerseite gibt es ein Client-Programm (JAP), das die Verschlüsselung der Daten und den Versand an die Mix-Kaskaden auf dem Rechner des Nutzers erledigt. Dieses Client-Programm muss sich jeder Nutzer auf seinem Rechner installieren. Es ist auch möglich, dass mehrere Nutzer gemeinsam einen JAP benutzen. Existiert z. B. ein firmeninternes Intranet, so kann der JAP auf einem Rechner installiert werden, der sowohl Zugang zum Intranet als auch zum Internet hat. Der JAP arbeitet als lokaler Proxy für einen Browser, d. h. er nimmt dessen Anfragen entgegen, sendet sie über den Anonymisierungsdienst (mit dem er über das Internet verbunden ist), empfängt vom Anonymisierungsdienst die Antwort des Webservers und leitet diese an den Browser weiter.

Um die Benutzung des Anonymisierungsdienstes zu erleichtern und dem Nutzer eine Rückmeldung über sein aktuelles Schutzniveau zu geben, wurde der so genannte InfoService konzipiert. Dieser ist mit einer Datenbank vergleichbar und hält Informationen über die aktuell verfügbaren Mix-Kaskaden, deren Auslastung etc. bereit. So kann mithilfe der beim InfoService vorliegenden Daten dem Nutzer visuell mit dem so genannten Anonym-O-Meter (vgl. Abbildung 3) eine Vorstellung über seine aktuelle Anonymität vermittelt werden.

Abbildung 3



TECHNISCHE DETAILS

In JAP kommt ein erweitertes Mixkonzept zum Einsatz. Zwar werden vom Mix so genannte MixPakete als grundlegende Kommunikationseinheit verarbeitet, mehrere MixPakete jedoch zu ein em anonymen MixKanal zusammengefasst. Die Zuordnung eines MixPakets zu einem Kanal wird dabei über eine Kanal-ID erreicht, wobei eine Kanal-ID natürlich nur jeweils zwischen zwei Mixen bzw. zwischen Client und erstem Mix gültig ist. Wäre dies nicht so, könnten dazwischenliegende Mixe anhand gleicher IDs leicht überbrückt werden. Das erste vom Client gesendete MixPaket initialisiert den MixKanal, indem es jedem Mix einen so genannten Sitzungsschlüssel übergibt. Der Mix hat nun die Aufgabe, die Zuordnung zwischen Sitzungsschlüssel und den Kanal-IDs (Ein- und Ausgang) während der Existenz des Kanals zu speichern, erhaltene Pakete zu entschlüsseln und mit der jeweils anderen Kanal-ID weiterzusenden.

Zur Verschlüsselung wird so genannte hybride Verschlüsselung verwendet. Der größte Teil der über den Kanal zu sendenden Daten wird aus Effizienzgründen mit einem symmetrischen Verschlüsselungsverfahren (AES im OFB Modus mit 128 Bit Schlüssellänge) verschlüsselt. Der zur Entschlüsselung benötigte symmetrische Sitzungsschlüssel wird mit dem bei weitem langsameren asymmetrischen Verschlüsselungsverfahren RSA mit 1024 Bit verschlüsselt und mit dem ersten MixPaket an jeden Mix übergeben. Asymmetrische Verschlüsselungsverfahren zeichnen sich dadurch aus, dass sie zwei Schlüssel verwenden - einen öffentlich bekannten Schlüssel zum Verschlüsseln der Nachricht und einen geheimen Schlüssel zum Entschlüsseln. Den geheimen Schlüssel kennt nur der jeweilige Mix allein, der öffentliche Schlüssel ist hingegen systemweit bekannt, damit die Clients die jeweils ersten MixPakete erstellen können.

Ein weiterer Vorteil der MixKanäle ist, dass auf diese Weise die Antwort eines Webservers einfach über den bestehenden Kanal anonym zurückgesendet werden kann. Die Daten werden dazu mithilfe der in jedem Mix noch gespeicherten symmetrischen Schlüssel verschlüsselt. Da der Client die Schlüssel seines Kanals kennt – schließlich ist der Kanal von ihm aufgebaut worden –, kann er die mehrfach verschlüsselte Antwort wieder entschlüsseln.

Normalerweise werden die Datenpakete nicht verschlüsselt bis zum Webserver gesendet, der Nachrichteninhalt also nicht geschützt. Für die Sicherung der übertragenen Inhalte ist deshalb noch eine zusätzliche Verschlüsselung (z. B. per SSL) notwendig, die vom Webserver unterstützt werden muss. JAP verschlüsselt nur auf der Verbindung zwischen Nutzer und Mixen. Nach dem letzten Mix werden die Daten unverschlüsselt bis zum jeweiligen Server weitergesendet. Die Verschlüsselung durch JAP ist also nur ein Mittel, um Anonymisierung zu erreichen, dient jedoch nicht der Geheimhaltung der übertragenen Daten bis hin zum Webserver.

AUFBAU DER MIX-KASKADEN

Aus Performancegründen werden nur feste Mix-Kaskaden angeboten. Jeder Mix ist Bestandteil höchstens einer Kaskade und eine Kaskade besteht aus mindestens zwei Mixen. Die Betreiber der Mixe sollten unabhängige Institutionen sein, die in einer Selbstverpflichtung erklären, dass sie weder Log-Files über die transportierten Verbindungen speichern, noch mit den anderen Mix Betreibern Daten austauschen, die dazu führen könnten, dass ein Nutzer von JAP enttarnt wird. Der JAP bietet dem Nutzer die Möglichkeit, aus den vorhandenen Mix-Kaskaden diejenige auszuwählen, die seiner Meinung nach am vertrauenswürdigsten ist.

ERREICHTE ANONYMITÄT

Unser Ziel ist es, einen Anonymisierungsdienst zu schaffen, der gegen einen Angreifer sicher ist, der alle Leitungen abhören, alle Daten manipulieren und löschen, neue Daten einfügen sowie mehrere Mixe und Nutzer kontrollieren kann. Solange wenigstens ein Mix nicht von ihm kontrolliert wird, ist der Nutzer immer noch anonym unter allen den Anonymisierungsdienst gleichzeitig verwendenden Nutzern, die nicht mit dem Angreifer zusammenarbeiten.

Derzeit ist JAP gegen einen so starken Angreifer noch nicht sicher. Es wurde beispielsweise bisher kein Dummy-Traffic implementiert, sodass jeder Nutzer zu jeder Zeit gleich viel senden und empfangen würde. Dies ist aus Effizienzgründen in der Form auch zurzeit nicht umzusetzen: Die Nutzer haben unterschiedlich schnelle Netzanbindungen und sind zudem zu einem gegebenen Zeitpunkt unterschiedlich aktiv. Wollte man erreichen, dass sich zumindest alle diejenigen Nutzer gleich verhalten, die über einen gleich schnellen Zugang zum Internet verfügen, müssten die Mixe bei vergleichbarer Dienstqualität ein Vielfaches des momentanen Datenvolumens bewältigen. Zudem würde sich jede Verzögerung bei einem Teilnehmer auf alle anderen auswirken, da ja auf diesen gewartet werden müsste. Eine teilweise Realisierung von Dummy-Traffic durch Einteilung der Nutzer in Gruppen mit gleichem Sende- und Empfangsvolumen ist eine unserer

aktuellen Forschungsfragen. Dazu führen wir sporadisch, zeitlich eng begrenzt und auf eine ganz spezifische Forschungsfrage zugespitzt statistische Verkehrsanalysen durch, um Erkenntnisse darüber zu gewinnen, wie viele Datenpakete üblicherweise von wie vielen Nutzern gesendet werden.

Auch die erste Form der oben beschriebenen *(n-1)*-Angriffe ist theoretisch möglich. Ein einzelner Angreifer könnte im Prinzip die angegebenen Nutzerzahlen manipulieren, indem er viele Clientprogramme startet. Damit kann er den übrigen Nutzern zumindest eine höhere Anonymität vortäuschen. Könnte er zudem noch alle bis auf einen echten Nutzer blockieren, wäre die Anonymität des einen aufgehoben. Um diesen Angriff zu verhindern, wäre es nötig, jeden Nutzer bei der Anmeldung zu authentifizieren – beispielsweise per digitaler Signatur.

Momentan sind weitere Angriffe möglich, da die Mix-Grundfunktionen noch nicht vollständig implementiert sind. Allerdings müsste für alle bekannten Angriffe der Angreifer sehr stark sein. Gegen einen Lauscher, der das Netz an nur einer einzigen Stelle abhören kann bzw. nur einen der Mixe kontrolliert, ist das System im Vergleich zu den oben beschriebenen Anon-Proxies bereits sicher.

BETRIEB VON JAP

Der Anonymisierungsdienst “JAP” wird momentan von der TU Dresden und der FU Berlin in Zusammenarbeit mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein im Rahmen des vom Bundesministerium für Wirtschaft und Technologie geförderten Forschungsprojektes “AN.ON – Starke Unbeobachtbarkeit und Anonymität im Internet” in Kooperation mit einem von der deutschen Forschungsgemeinschaft (DFG) geförderten Projekt entwickelt. Auf Grund der Förderung und der Unterstützung durch die TU Dresden wird der Dienst zurzeit in einem Probebetrieb kostenlos der Öffentlichkeit zur Verfügung gestellt. Allerdings überraschten der große Erfolg und die hohe Nutzerakzeptanz. Momentan wird von ca. 20.000 regelmäßigen Nutzern weltweit ausgegangen.

Dies bedeutet jedoch, dass die Mix-Server die Verkehrslast von eben diesen 20.000 Nutzern bewältigen müssen. Dies verursacht erhebliche Kosten, die auf Dauer weder durch Forschungsmittel noch von der TU Dresden getragen werden können.

Es werden deshalb Konzepte und technische Lösungen entwickelt, um die Kosten zu verteilen. Eine Möglichkeit wäre es, dass staatliche Stellen den JAP-Betrieb als Grundschutz für aller Bürgerinnen und Bürger zur Verfügung stellen. Eine andere Möglichkeit bestünde darin, den Dienst den Nutzern zum Selbstkostenpreis anzubieten.

3. Rechtliche Grundlagen des Anonymisierungsdienstes

WELCHE PERSONENBEZOGENEN DATEN FALLEN EIGENTLICH BEIM SURFEN IM INTERNET AN?

Beim Abruf von Informationen von einer Webseite fallen zahlreiche Informationen über den einzelnen Nutzer an. Selbst dann, wenn der Nutzer keine Internet-Formulare ausfüllt oder seine E-Mail-Adresse nicht angibt, zieht er eine Datenspur hinter sich her, die u. A. aus IP-Adressen, Kennungen in Cookies von besuchten Webseiten oder Werbeanbietern sowie den URLs der besuchten Webseiten besteht.

Interessant ist besonders die sog. IP-Adresse. Sie ist die eindeutige Adresse eines Rechners im Internet, die jeder Rechner – vergleichbar einer Telefonnummer in herkömmlichen Telefonnetzen – benötigt, um einen anderen Rechner adressieren zu können. Im Internet ist jede einzelne IP-Adresse nur einmal vergeben, sodass sie grundsätzlich eine Identifizierung des einzelnen Nutzers ermöglichen und auf diese Weise ein personenbezogenes Datum darstellen kann. Der Personenbezug einer IP-Adresse ist in der Praxis jedoch nicht so eindeutig festzustellen. Es ist zwischen statischen und dynamischen IP-Adressen zu unterscheiden. Während die Internet-Server statische, d. h. feste IP-Adressen haben, gilt dies für die meisten Nutzer nicht. Wer sich über einen sogenannte Access-Provider oder einen Online-Dienst an das Internet anschließt, bekommt von diesem eine sog. dynamische IP-Adresse für die jeweilige Internet-Session zur Verfügung gestellt. Teilweise wird dem Nutzer aus technischen Gründen auch während eines Zugriffs eine neue IP-Adresse zugeordnet. Es ist also davon auszugehen, dass ein Nutzer in der Regel bei jedem neuen Login eine neue IP-Adresse zugeordnet bekommt.

Die Betreiber von Webservern speichern Protokolldateien (sog. Logfiles). Diese enthalten u. A. die IP-Adressen, über die auf die Webseiten zugegriffen wurde, die exakten Zugriffszeiten, Informationen über das genutzte Betriebssystem, den verwendeten Browser sowie etwaige URLs von Seiten, über die der Nutzer weitergeleitet wurde. Die anfal-

lenden Logfiles dienen u. A. der Funktionsprüfung, der statistischen Analyse sowie der Prüfung von Fehlfunktionen. Zusätzlich können sie aber auch der Erstellung von Nutzungsstatistiken und damit der Auswertung des Nutzerverhaltens dienen. Obwohl der Betreiber des Webservers insoweit Kenntnis von der IP-Adresse des Nutzers erlangt, kann er dennoch nicht ohne weiteres feststellen, welcher Nutzer sich hinter der IP-Adresse verbirgt, da die Nutzer in der Regel dynamische Adressen zugewiesen bekommen. Die dynamischen IP-Adressen lassen aber nur Rückschlüsse auf den Access-Provider bzw. Online-Dienst zu, dem der IP-Adressbereich zugewiesen ist. Für den Betreiber des Webservers handelt es sich bei der IP-Adresse insoweit nicht um ein personenbezogenes Datum. Insbesondere ist er rechtlich nicht befugt, von dem Access-Provider Auskunft über die Identität des Nutzers, dem eine bestimmte IP-Adresse zugeordnet ist, zu verlangen.

Anders sind die sogenannten statischen IP-Adressen zu bewerten, die beim Surfen im Internet in den Protokolldateien der aufgerufenen Webserver anfallen. Obwohl auch die statische IP-Adresse zunächst als rechnerbezogenes, nicht jedoch von vornherein personenbezogenes Datum einzuordnen ist, lassen sich fest vergebene IP-Adressen leichter dem dahinter stehenden Nutzer zuordnen, als es bei den dynamischen IP-Adressen der Fall ist. In der Regel ist deshalb bei fest vergebenen IP-Adressen von einem Personenbezug auszugehen.

Für den Access-Provider als Zugangsanbieter ist es allerdings kein Problem, auch bei dynamisch vergebener IP-Adresse, die Identität des Nutzers zu ermitteln. Der Access-Provider hat nämlich zumindest zum Zeitpunkt der Nutzung Kenntnis davon, welchem Nutzer zu einem bestimmten Zeitpunkt welche IP-Adresse aus dem dem Access-Provider zur Verfügung gestellten Pool an IP-Adressen zugewiesen ist. Diese Informationen lassen sich regelmäßig den Logfiles des Access-Providers entnehmen. Im Unterschied zum Betreiber des Webservers stellt die IP-Adresse für den Access-Provider insoweit regelmäßig ein personenbezogenes Datum dar, so dass für ihn die Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) gelten.

WER INTERESSIERT SICH DENN FÜR DIESE DATEN?

Interessenten können die unterschiedlichsten Akteure sein. Die von den Nutzern im Internet hinterlassenen Datenspuren werden von Marketingfirmen verwendet, um detaillierte Kundenprofile zusammenzustellen und auf diese Weise Kundeninteressen zu analysieren. Aber auch Arbeitgeber, Versicherungen, Geheimdienste und Strafverfolgungsbehörden haben Interesse an den bei der Internet-Nutzung anfallenden Daten der einzelnen Nutzer. Interessant wird es insbesondere auch dann, wenn das Internet-Angebot von Beratungsstellen, z. B. im Bereich der Seelsorge, aufgerufen wird. Es ist schwerlich vorstellbar, dass es Nutzern entsprechender Angebote gleichgültig ist, wenn sie hierbei beobachtet werden.

IST ANONYMES SURFEN ÜBERHAUPT RECHTLICH ZULÄSSIG?

Anonymes Surfen ist nicht nur zulässig, sondern sogar rechtlich geboten. Der Gesetzgeber hat im Jahre 1997 mit der Schaffung des Teledienstedatenschutzgesetzes (TDDSG) sowie des Mediendienstestaatsvertrages (MDStV) Regelungen geschaffen, die die anonyme und pseudonyme Nutzungsmöglichkeit vorsehen und damit ein Recht auf Anonymität jedes Einzelnen normieren. So lautet der für den Schutz personenbezogener Daten bei Telediensten geltende § 4 Absatz 6 TDDSG im Wortlaut: „Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.“ § 18 Absatz 6 MDStV enthält eine gleich lautende Vorschrift für die Anbieter von Mediendiensten.

Mit dieser Verpflichtung, die anonyme oder pseudonyme Nutzung zu ermöglichen, hat der Gesetzgeber die im Bundesdatenschutzgesetz (BDSG) sowie in verschiedenen Landesdatenschutzgesetzen (LDSG) normierten allgemeinen Grundsätze der Datenvermeidung und Datensparsamkeit für die Diensteanbieter nach dem TDDSG bzw. MDStV konkret geregelt. Die Grundsätze zielen darauf, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen und sehen die Pflicht vor,

von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen (vgl. § 3 a BDSG, § 4 Absatz 1 LDSG-SH).

Dem jeweiligen Diensteanbieter wird die Verpflichtung auferlegt, die Inanspruchnahme anonym oder unter Pseudonym zu ermöglichen. Bei der nachträglichen Anonymisierung oder Pseudonymisierung werden die Daten zunächst mit Personenbezug erhoben, der Personenbezug wird später entfernt. Sofern die Anbieter von Tele- und Mediendiensten ihrer Verpflichtung nachkommen, eine Möglichkeit zur anonymen oder pseudonymen Nutzung zu schaffen, wird dagegen von vornherein vermieden, dass personenbezogene Daten überhaupt erst entstehen. Die Verpflichtung steht allein unter dem Vorbehalt der technischen Möglichkeit und Zumutbarkeit. Die TU Dresden, die FU Berlin sowie das Unabhängige Landeszentrum für Datenschutz haben es sich zum Ziel gesetzt, im Rahmen des Projektes „AN.ON – Starke Unbeobachtbarkeit und Anonymität im Internet“ gerade diesem Auftrag des Gesetzgebers nachzukommen und einen gesetzeskonformen Dienst zu implementieren. Hierzu gehört auch die Möglichkeit einer anonymen bzw. pseudonymen Bezahlung. Während der restlichen Laufzeit des Forschungsprojektes wird die Entwicklung einer entsprechenden Funktion einen wichtigen Raum einnehmen.

WELCHE DATEN DARF EIN PROVIDER ÜBER SURFER SPEICHERN?

Die gesetzlichen Voraussetzungen für die Zulässigkeit der Speicherung personenbezogener Daten sind im Teledienstedatenschutzgesetz (TDDSG) detailliert geregelt und aus datenschutzrechtlicher Sicht im Allgemeinen recht positiv zu bewerten. Der Anwendungsbereich der Vorschriften des TDDSG erstreckt sich auf alle Anbieter von Telediensten. Es werden insoweit sowohl die Access-Provider als auch diejenigen erfasst, die Webserver oder sonstige Server im Internet betreiben.

Bei der Inanspruchnahme des Internet fallen sog. Nutzungsdaten an. Eine Definition dieser Daten lässt sich § 6 Absatz 1 TDDSG entnehmen. Der Diensteanbieter darf nach dieser Vorschrift personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben,

verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen. Hierbei gelten als Nutzungsdaten insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Teledienste. Es handelt daher bei diesen Daten um besonders sensible Informationen, da sie das Kommunikationsverhalten des Nutzers im Internet präzise beschreiben. Im Gegensatz zu den bloßen Verbindungsdaten, die lediglich die anrufende und angerufene Nummer sowie Zeit und Dauer einer Verbindung umfassen, schließen die Nutzungsdaten auch Inhalte der Kommunikation, wie z. B. URLs aufgerufener Seiten oder aber die Anfragen bei Suchmaschinen ein. Sie sind damit durchaus geeignet, die inhaltlichen Interessen der Nutzer zu offenbaren.

Die Erhebung und Speicherung der Nutzungsdaten ist nur dann zulässig, soweit dies technisch erforderlich ist, um den Dienst zu erbringen. Sofern ihre Erhebung und Speicherung zulässig ist, sind die Daten allerdings unmittelbar nach Ende des Nutzungsvorgangs zu löschen. Etwas anderes gilt nur dann, wenn es sich bei den Nutzungsdaten um Daten handelt, die für die Abrechnung des Dienstes erforderlich sind.

Sofern die Nutzung eines Teledienstes personenbezogen erfolgt, werden für Zwecke der Abrechnung die anfallenden Nutzungsdaten mit den sog. Bestandsdaten verknüpft. § 5 TDDSG enthält eine Definition der Bestandsdaten. So handelt es sich um personenbezogene Daten eines Nutzers, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit ihm über die Nutzung von Telediensten erforderlich sind. Z. B. handelt es sich um Daten, die von einem Access-Provider im Rahmen einer Vertragsbeziehung mit dem Kunden erhoben werden. Hierzu können Personalien, Angaben über die Bankverbindung, E-Mail-Adressen etc. gehören.

Da die Abrechnung bei den meisten Access-Providern nach Zeit oder Datenvolumen erfolgt, ist es beispielsweise erforderlich, festzustellen, welcher Nutzer zu welcher Zeit wie lange den Dienst in Anspruch genommen hat. Die Provider dürfen daher, wenn dies zu Abrechnungszwecken erforderlich ist, speichern, von wann bis wann ein Nutzer eingeloggt war bzw. welches Datenvolumen transferiert wurde. Zu betonen ist in diesem

Zusammenhang, dass tatsächlich nur diejenigen Daten gespeichert werden dürfen, die wirklich erforderlich sind. Erfolgt die Abrechnung nach der Nutzungszeit, dürfen mithin nicht die abgerufenen Inhalte mitprotokolliert werden, sondern lediglich die Abrufzeiten. Gleiches gilt für die übertragenen Datenmengen. Werden Flatrates verwendet, ist die Erhebung personenbezogener Nutzungsdaten von vornherein nicht erforderlich und damit unzulässig.

Anders als die Access-Provider sind die Betreiber von Webservern im Internet zu beurteilen. Da die überwiegende Anzahl der Webseiten kostenlos zur Verfügung gestellt wird, entfällt eine Abrechnung, sodass IP-Adressen grundsätzlich gar nicht gespeichert werden dürfen.

Obwohl die Zulässigkeit der Erhebung und Speicherung der bei der Internet-Nutzung anfallenden Daten präzise geregelt ist, zeigt der Blick in die Praxis, dass in diesem Bereich trotz detaillierter Regelungen nicht selten gegen die präzisen Bestimmungen des Teledienstedatenschutzgesetzes bzw. Mediendienstestaatsvertrages verstoßen wird. So wird an den Webservern häufig aufgezeichnet, mit welchen IP-Adressen welche Angebote abgefragt wurden. Häufig wird von Access-Providern auch über den Nutzungszeitraum hinaus gespeichert, welche IP-Adresse welchem Nutzer zugeordnet war.

WELCHE DATEN WERDEN GESPEICHERT, WENN MAN DEN JAP BENUTZT?

Bei der Entwicklung des Anonymisierungsdienstes wird bereits seit Beginn des Projektes besonderer Wert darauf gelegt, von vornherein die relevanten datenschutzrechtlichen Fragestellungen zu berücksichtigen. Dies ist auch der Grund für die enge Kooperation zwischen dem Unabhängigen Landeszentrum für Datenschutz und der Technischen Universität Dresden sowie der Freien Universität Berlin bei der Entwicklung und Implementierung des Dienstes. Das dem Anonymisierungsdienst zu Grunde liegende Konzept vermeidet bereits auf technischer Ebene durch Verwendung unterschiedlicher Mixe die Zuordnung von IP-Adressen zu einzelnen Nutzern. Da der Anonymisierungsdienst

derzeit kostenlos angeboten wird, ist die Erhebung personenbezogener Nutzungsdaten auch zum Zwecke der Abrechnung nicht erforderlich. Die Vorgaben des § 6 TDDSG werden beim Betrieb des JAP strikt eingehalten.

Neben der Entwicklung eines Anonymisierungsdienstes, der die anonyme Inanspruchnahme von Internet-Diensten ermöglicht, stellt auch die Entwicklung einer anonymen oder pseudonymen Bezahlfunktion einen wichtigen Gegenstand des Forschungsprojektes dar. Der Gesetzgeber hat den Diensteanbietern in § 4 Abs. 6 TDDSG nämlich nicht nur die Verpflichtung auferlegt, die Inanspruchnahme von Telediensten anonym oder unter Pseudonym zu ermöglichen, sondern hat diese Verpflichtung auch auf die Bezahlung des Dienstes erweitert. Es ist unser Ziel, im Rahmen des Forschungsprojektes auch dieser Verpflichtung des Gesetzgebers nachzukommen.

WIRD DER ANONYMISIERUNGSDIENST NICHT DURCH KRIMINELLE MISSBRAUCHT?

Eine missbräuchliche Nutzung des Anonymisierungsdienstes ist natürlich nicht auszuschließen. Nachdem der Prototyp des Tools JAP so weit implementiert war, dass dieser auch praktisch genutzt werden konnte, dauerte es nicht allzu lange, bis die Projektpartner mit den ersten Fällen konfrontiert wurden, in denen missbräuchliche Nutzungen des Dienstes beklagt wurden. Sowohl Privatpersonen bzw. Firmen als auch Strafverfolgungsbehörden wendeten sich an die Technische Universität Dresden oder das Unabhängige Landeszentrum für Datenschutz.

Unter Benennung der vom jeweiligen Server mitgeloggten IP-Adresse sowie des Datums und der präzisen Uhrzeit der missbräuchlichen Handlung versuchten die anfragenden Stellen, den hinter der IP-Adresse verborgenen Nutzer zu ermitteln. Da jedoch keine personenbezogenen Daten der Nutzer des Anonymisierungsdienstes erhoben und gespeichert werden, ist die Erteilung von Auskünften über entsprechende Daten von vornherein nicht möglich.

Das ist ungefähr so, wie wenn es für die Polizei wichtig wäre zu erfahren, wer wann mit seinem Auto auf einem bestimmten Autobahnabschnitt gefahren ist. Auch darüber gibt es keine Aufzeichnungen, also auch keine Möglichkeit der Auskunft.

Es ist in diesem Zusammenhang aber auch zu betonen, dass die Anfragen, die den Verdacht einer missbräuchlichen Nutzung des Dienstes bzw. den Verdacht einer Straftat begründeten, im Vergleich zu den Nutzerzahlen des Dienstes lediglich einen verschwindend geringen Anteil einnehmen. Keineswegs wird der Dienst daher in erster Linie von Kriminellen genutzt.

An dieser Stelle sei ergänzend hinzugefügt, dass Diensteanbietern nach geltender Gesetzeslage keine Verpflichtung obliegt, personenbezogene Bestands- oder Nutzungsdaten für Strafverfolgungsbehörden vorzuhalten. Zwar dürfen Diensteanbieter Auskunft über Bestandsdaten an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung nach Maßgabe der hierfür geltenden Bestimmungen erteilen (§ 5 Satz 2 TDDSG). Hierbei handelt es sich allerdings um eine lediglich klarstellende Vorschrift, die die Strafverfolgungsbehörden auf die bereits bestehenden Rechtsgrundlagen – zu nennen sind die einschlägigen Vorschriften der Strafprozessordnung (StPO) – verweist. Gleiches gilt auch für Auskünfte über Nutzungsdaten gemäß § 6 Absatz 5 Satz 5 TDDSG. Sofern Auskünfte von Strafverfolgungsbehörden verlangt werden, bedarf es hierzu eines richterlichen Beschlusses nach Maßgabe der §§ 100 g, h StPO.

STEHT DER ANONYMISIERUNGSDIENST IN EINKLANG MIT DEN INTERESSEN DER STRAFVERFOLGUNGSBEHÖRDEN?

Das Angebot des Anonymisierungsdienstes steht in Einklang mit den Interessen des Gesetzgebers. Die Implementierung eines in jeder Hinsicht gesetzeskonformen Dienstes war und ist das Ziel des Projektes. Der Gesetzgeber hat bei der Schaffung der Regelungen über die anonyme und pseudonyme Inanspruchnahme von Telediensten im TDDSG durchaus die Interessen der Strafverfolgungsbehörden berücksichtigt. So hat der Bundesrat im Gesetzgebungsverfahren um Prüfung der Frage gebeten, ob die Ermöglichung

der anonymen Inanspruchnahme von Telediensten nicht die Zwecke der Strafverfolgung vereiteln könnte. Die Bundesregierung hat hierzu ausgeführt, mit den im TDDSG getroffenen Regelungen werde ein angemessener Ausgleich zwischen dem Recht auf informationelle Selbstbestimmung einerseits und den Interessen der Strafverfolgungsbehörden andererseits herbeigeführt. Informationelle Selbstbestimmung in globalen Netzwerken könne wirksam nur durch größtmögliche Anonymität des Nutzers gewährleistet werden. Dabei seien die verschiedenen Nutzungskostellationen zwischen dem Nutzer und einer Vielzahl von Diensteanbietern zu berücksichtigen. Den Interessen der Strafverfolgungsbehörden könne durch die Ausschöpfung der in der Strafprozessordnung vorgesehenen Ermittlungsmöglichkeiten Rechnung getragen werden (BT-Drucksache 13/7385, Seite 71).

Diese Auffassung hat der Gesetzgeber auch im Rahmen der neuesten und umfassenden Novellierung des TDDSG zum 1. Januar 2002 beibehalten. Die Vorschrift des § 4 Abs. 6 TDDSG, die die Verpflichtung der Diensteanbieter zur anonymen und pseudonymen Inanspruchnahme und Bezahlung von Telediensten regelt, blieb in ihrem Wortlaut nämlich unberührt. Die Einräumung einer anonymen bzw. pseudonymen Möglichkeit der Inanspruchnahme von Telediensten ist daher nach wie vor ein wichtiges Anliegen des Gesetzgebers.

WIE KANN AUF DER EINEN SEITE DAS RECHT AUF ANONYMITÄT GEWÄHRLEISTET WERDEN UND AUF DER ANDEREN SEITE DEN INTERESSEN DER STRAFVERFOLGUNGSBEHÖRDEN RECHNUNG GETRAGEN WERDEN?

Ziel des Projektes ist es auch, am Ende seiner Laufzeit eine möglichst allen Seiten gerecht werdende Lösung gefunden zu haben, die sowohl das garantierte Recht des Einzelnen auf Anonymität effektiv durchzusetzen unterstützt, auf der anderen Seite aber auch berechtigten Interessen der Strafverfolgungsbehörden an einer wirkungsvollen Bekämpfung der Kriminalität Rechnung trägt.

4. Warum ist die Möglichkeit zur anonymen Kommunikation so wichtig?

EIN BEITRAG AUS SOZIOLOGISCHER SICHT

Auf die Frage, warum die Möglichkeit zur anonymen Kommunikation wichtig ist, lässt sich eine knappe, umstandslose Antwort geben: Weil Anonymität für die moderne Gesellschaft konstitutiv ist.

Es gibt in der modernen Gesellschaft an vielen Stellen Bedarf nach Nichtzurechenbarkeit von Kommunikationen und Handlungen auf Personen. Als erstes denkt man da vielleicht an die gleichen und geheimen Wahlen des demokratischen Rechtstaats. Die Nichtzurechenbarkeit der Stimmabgabe erleichtert es auf der individuellen Ebene, “Nein!” zu sagen, und auf der sozialen Ebene, dass politische Programme wechseln. Oder man denke an die Wissenschaft: Die Begutachtung von Artikeln für massgebliche wissenschaftliche Zeitschriften geschieht ohne das Wissen darum, wer als Autor und Gutachter agiert. Auch nach der Publikation stellt sich die Feststellung der Wahrheit erst in einem diskursiven, ergebnisoffenen Verfahren ein, an dem viele namentlich nicht festgelegte Personen die Chance haben, sich zu beteiligen. Nicht zuletzt spielt Anonymität ökonomisch eine Rolle: Man gibt Geld hin und nimmt das Gewünschte entgegen, ohne dass mit diesem Tausch auch zwangsläufig die persönlichen Daten gewechselt werden müssen. Es bedarf auch keiner Emotionen füreinander. Man geht in der Form des Geldtausches eine soziale Beziehung auch mit demjenigen ein, den man nicht kennt, der einem gleichgültig ist und der dies üblicherweise auch weiterhin bleiben kann.

Auch in anderen Zusammenhängen wird die Bedeutung der Anonymität deutlich. Man denke nur an die Anonymen Alkoholiker, die einander helfen, ohne sich beim Namen zu kennen. Anonymität ist für sie unverzichtbar, ohne Übertreibung in einigen Fällen sogar überlebenswichtig. Das AN.ON-Projekt nahm seinen Anfang aus einer ganz ähnlichen

Problemlage: Mögliche Ecstasy-Konsumenten sollten sich per Internet anonym an eine Drogenberatung wenden können, ohne dass die Hilfesuchenden in Sorge sein mussten, dass allein durch die Kontaktaufnahme ihre Identität zwangsläufig offenkundig wurde oder durch Dritte hätte beobachtet werden können.

Kurzum: Ohne Chance auf Anonymität wäre kein demokratisches System denkbar, keine Wissenschaft, deren Wahrheitsabsicherung einzig auf vorbehaltloser Kommunikation gründet, kein freies, offenes Marktgeschehen und schließlich in vielen Fällen keine Hilfe selbst in extremen Notlagen möglich.

ANONYMITÄT IST EIN PHÄNOMEN DER MODERNE

Die Bezeichnung “anonym” entstand im Zusammenhang mit Schriften (”Anonyma”), die ohne Namen der Verfasser überliefert sind oder deren Verfasser sich selbst nicht zu erkennen geben wollen. Mit dem Buchdruck, also einer frühen Informationstechnik, entstand erstmals systematisch die Möglichkeit zur Entkoppelung von Urheberschaft und der Zurechnung von Gesagtem zu einer bestimmten Person. Die Verbreitung von Gedrucktem für die Allgemeinheit, das sich anders als ein Brief an viele unbekannte Leser richtete, veränderte auch die Form der Argumentation. Der Autor musste seinen Text auf einen generalisierten Leser ausrichten und deshalb abstrakter, das heisst: von konkreten Kontexten unabhängiger, argumentieren, mit der Folge, dass die Argumentation zunehmend Halt an übergreifenden Standards (wie Gewicht, Länge, Ort, Zeit, Material, Variationen von Themen zunächst primär aus dem allgemeinen religiösen Wissensfundus) sowie logisch an sich selber finden musste.

In den großen Metropolen bricht, spätestens zu Beginn des 20. Jahrhunderts, zunehmend die Zuordnung von sozialen Funktionen und Bezirken auf. Man denke an die Zünfte der Gerber, Korb- und Radmacher, Schneider, Kunsthandwerker, Buchhändler, Geldleiher, Arbeiter usw. Allein die grosse Zahl der mit dieser Entwicklung entstehenden “unsortierten” Begegnungen nötigt in einer Großstadt zu einem Modus der gegenseitigen Beobachtung, der sich zunächst weitgehend darauf beschränken kann, die Körper so zu-

einander zu arrangieren, dass sie bei zufälligen Begegnungen nicht miteinander kollidieren. Stadtluft macht frei. Wie bei den Technikfolgen des Buchdrucks so ist auch diese Entwicklung von einer Generalisierung begleitet: Es entsteht die Option, jemanden als einen “bloß Anderen” wahrzunehmen und nicht zwangsläufig als “Freund oder Feind”, “gehört-zu-uns oder gehört-nicht-zu-uns” oder als “nützlich oder unnütz”.

Diese städtische Kultur des kalkulierten Ignorierens breitet sich heutzutage, im Zuge der Nutzung moderner Kommunikationstechniken sozusagen “stadtübergreifend”, global aus. Durch diese verallgemeinerte Verstädterung werden neue Formen vertrauensbildender Massnahmen eingeübt. “Der Andere” wird zu einem generalisierten Anderen, der weder Zuneigung noch Abneigung beansprucht oder provoziert, sondern der mit universalisierter Achtung rechnen darf bzw. diese schlicht beansprucht. Niemand muss sich im Alltag grundlos legitimieren oder kann von anderen eine Rechtfertigung verlangen – selbst Missgeschicke, wie etwa das Auffahren auf ein anderes Auto, werden zunehmend weniger moralisiert, sondern schlicht funktional abgewickelt. Man wird im positiven Sinne – darf man sagen: in einem zen-buddhistischen Sinne? – füreinander gleich-gültig. Die Kehrseite dieser Medaille ist, dass nicht-gleich-gültige Beziehungen gestiftet werden müssen, um der unter Umständen auch als bedrückend empfundenen Anonymität unter Wohnungsnachbarn eines städtischen Hochhauses zu entgehen. Gemeinschaft versteht sich dann, entgegen dem traditionellen Verständnis, eben nicht länger von selbst.

In vormodernen Zeiten gab es derartig anonyme Sozialbeziehungen eher nicht. Bei jeder Begegnung in einer mittelalterlichen “Stadt” taxierte man einander und wies sich, auch wenn man sich nicht beim Namen kannte, oder möglicherweise zum Teil kaum über einen Namen verfügte, einen eindeutigen Status zu, wofür vermutlich schon die strenge Kleiderordnung hilfreich war. Es war klar, wer auf wen in welchem Maße mehr oder weniger willkürlich zugreifen durfte. Es gab für alles in der Welt eine logisch oder mental befriedigende, meist hierarchisch organisierte Ordnung der Dinge. Diese soziale und mentale Eindeutigkeit ging in Westeuropa, im Zuge der Umstellungen der Moderne, dann weitgehend verloren bzw. wurde, wie etwa Religion, zur Privatsache erklärt. Das Gute, Wahre und Schöne fiel auseinander. Genau an diesem Punkt der Differenzierung, diese Nebenbemerkung sei gestattet, stehen nunmehr die als fundamentalistisch-religiös bezeichneten Staaten.

DAS POTENZIAL DER MODERNE

Parallel zur oben kurz geschilderten Generalisierung in der Wahrnehmung des Anderen entstanden Ordnungsmuster, die die traditionellen Ordnungskapazitäten von den bis dahin führenden Organisationformen, hierbei denke man an Manufakturen, Klöster, Zünfte, Märkte in den Schatten der Kirchen, Höfe usw., überstiegen. John Locke provozierte um 1660 herum die Anhänger zentral-absolutistischer Führungskonzepte mit Überlegungen zu komplizierten Regelungsmechanismen durch eine “Drei-Gewalten-Teilung” mit einer gegenseitigen Kontrolle von Exekutive, Legislative und Jurisdiktion. Adam Smith formulierte etwa 100 Jahre später die rätselhafte “invisible hand” des Marktes, die deutsche Hochphilosophie spürte den Offenbarungen der Vernunft in der Natur, des Ichs und der Geschichte nach. Und knapp ein weiteres Jahrhundert später schüttelten Charles Darwin und Karl Marx die Welt der Theorien ein weiteres Mal mit ihren Thesen durch, wonach es organisationsübergreifend-allgemeine Ordnungsmuster der ganz eigenen Art gäbe.

Inzwischen sind die Mechanismen derartig organisationsübergreifender Ordnungsmuster, speziell im sozialen Bereich, besser freigelegt und verstanden. Diese übergreifenden sozialen Ordnungen werden als “gesellschaftliche Subsysteme” (Niklas Luhmann) bezeichnet, die dazugehörige soziologische Theorie ist die der “funktionalen Differenzierung”. Im Kern besagt diese Theorie, dass sich Kommunikationssysteme speziell für Ökonomie, Politik, Wissenschaft und Recht herausgebildet haben, die sich anhand der Reproduktion von kommunikativen Elementarereignissen selbst organisieren.

Jedes dieser Systeme reproduziert seine ganz spezifische Form durch Oszillation zwischen zwei Seiten eines kommunikativen Codes, wobei nicht eine der beiden Seiten, sondern die Oszillation zwischen ihnen, und damit beide einander widersprechende Seiten stabilisiert werden. Konkret heisst das: das Wirtschaftssystem verarbeitet Informationen durch die permanente Oszillation zwischen den beiden Seiten Zahlung/Nichtzahlung, das politische System oszilliert zwischen Macht/Nichtmacht, das Rechtsystem zwischen Recht/Nichtrecht und das Wissenschaftsystem zwischen wahr/falsch. Ökonomisch interessiert fortan allein die Verzinsung des Kapitals, die Politik oszilliert zwischen Regierung

und Opposition und die wissenschaftliche Wahrheit gründet sich, überaus riskant, weil unababschließbar vorläufig, auf die an Wahrheit/Falschheit orientierte Kommunikation von Experten.

Als Ergebnis dieser neu sich zunächst vornehmlich in Europa herausbildenden übergreifenden Ordnungsmuster verändern sich die Formen der Organisationen und die Selbstbestimmung der Menschen. Im philosophischen Diskurs werden Menschen fortan als dem Wesen nach autonome Individuen, im politischen Diskurs zumindest im Prinzip als freie, souveräne Bürger ausgewiesen. Und Organisationen sehen sich vor das Problem gestellt, diese systematisch geschiedenen Funktionalitäten der gesellschaftlichen Subsysteme und die Selbstbestimmung der Menschen miteinander zu synthetisieren. Seitdem gilt: Nur diejenigen Organisationen, die über eine optimale Wissensverarbeitung und Marktinteraktion verfügen sowie politischen Einfluss nehmen und ihr komplexes Personal optimal in ihre Workflows einbinden, können sich in einer turbulenten Umwelt behaupten.

Die generelle Funktion von Organisationen besteht darin, Entscheidungen herzustellen. Dafür müssen sie, bei Strafe ihres sonstigen Unterganges, heutzutage mit Hilfe der modernen Informations- und Kommunikations-Technik die aus ihrer Sicht notorisch chaotische Umwelt und ihre ebenfalls komplexe Binnenwelt ihrer Mitglieder ordnen. Organisationen sehen sich deshalb permanent aufgefordert, ihre internen und externen Kommunikationsformen zu effektivieren, insbesondere um Einfluss auf ihre Umwelt zu nehmen und so die Transformationskosten in der Interaktion mit der Umwelt möglichst gering zu halten.

Im Übergang zur Moderne mussten Organisationen ihre einstigen Allbindungen von Menschen zu einem massgeblichen Anteil an die gesellschaftlichen Subsysteme abgeben. Während des Übergangs entstanden all die heute kursierenden Programmatiken zu demokratischen Verhältnissen in Staat, Ökonomie und Wissenschaft. Durch die enormen Informationsverarbeitungskapazitäten in den Händen moderner Organisationen gewinnen diese wieder beschleunigt, den Eindruck muss man heute gewinnen, die massgebliche Hoheit über die Menschen. Firmen basteln zum Beispiel an ihrem Customer-

Relationship-Management (“CRM”) herum, um durch hoch auflösende Kundenprofile die Bindungen zu den Kunden zu intensivieren.

Werbefirmen wie Doubleclick verfolgen den Clickstream der Interessenten über verschiedene Webseiten vieler Marktführer hinweg und erstellen zentralisiert Kundenprofile. Es werden Kundenkarten ausgegeben, die für einen geringen Preisnachlass Kunden zu Quasi-Mitgliedern von Firmen machen und es erlauben, sie in ihrem Kaufverhalten ebenfalls unter genaue Beobachtung zu stellen. Strafverfolgungsbehörden tragen, trotz des Labels “Rasterfahndung” von der Öffentlichkeit weitgehend unproblematisiert, behördliche Datenbestände von Energie- und Wasserversorgern und aus vielen anderen Wirtschaftsbranchen sowie von Hochschulen zusammen, um diese zentral auswerten und nach verdächtig/unverdächtig sortieren zu können. Wissenschaftler vermessen Menschen bis in die Gene hinein, legen sie dadurch auf bestimmte Dispositionen fest und könnten somit, wenn bei Einstellungsverhandlungen Gen-Untersuchungen als Grundlage zur Abschätzung von Krankheitsrisiken genutzt würden, maßgeblichen Einfluss auf die Biografien von Menschen nehmen.

Diese Zunahme an wieder mehr organisierter, sozusagen “stramm festgezurrter” Gesellschaftlichkeit bedeutet gesellschaftstheoretisch, zumindest auf den ersten Blick, eine gewisse Zurücknahme der bereits vollzogenen gesellschaftlichen Differenzierung. Diese Differenzierung war bislang dadurch ausgezeichnet, dass sie ein höheres Maß an Risiken erzeugte, mit dem Effekt einer enormen Verbesserung der ökonomischen, politischen, juristischen und wissenschaftlichen Systemleistungen.

DIE NEUE BEDEUTUNG DER ANONYMITÄT

Aus dieser Sicht bedeutet das Verteidigen der Möglichkeiten zur anonymen Kommunikation ein Verteidigen der Funktionalität der gesellschaftlichen Subsysteme, deren zentrale Kommunikationen auch ohne namentlichen Bezug auf die jeweils konkret beteiligten Menschen auskommen. Anders formuliert: Sie bedeutet ein In-die-Schranken-Weisen der Ordnungsansprüche der informationstechnisch wieder mächtig gewordenen Organisationen. Wer für die Möglichkeit auch anonymer Kommunikationen plädiert, spricht insofern für Modernisierung.

In einer erweiterten Perspektive besteht die Funktion speziell des Datenschutzes darin, Organisationen permanent auf die Risiken der Moderne einzustimmen und diese zu einer Optimierung der Formen ihrer „Kommunikationsverwaltung“ zu bringen. Dies gelang „dem Datenschutz“ von dem Moment, an dem ihm, organisiert und somit sozusagen auf Augenhöhe zu anderen Organisationen, ebenfalls die modernen Informations- und Kommunikationsmittel zur Verfügung standen. Datenschutz ist somit eine der wenigen auch praxisrelevanten Reflexionsinstanzen zum Management von Modernisierungsrisiken. Die Moderne sieht sich dabei immer der ergebnisoffenen Bewertung ausgesetzt, ob die Bilanz zwischen Chancen und Risiken stimmt. Politisch geht es um die Fortsetzung des Ausbaus der Vormachtstellung einer gewissen „Kultur der Gleich- Gültigkeit“ gegenüber dem „generalisierten Anderen“, um die politische Abwehr von „Wiedervergemeinschaftungsbestrebungen“ mit unreflektierten, vorvertraglich- traditionellen, im Ergebnis vermutlich anti-demokratisch-patriarchischen Verhältnissen. Nur in einer Kultur der reflektierten Gleich-Gültigkeit kann es ein tatsächlich realisiertes Recht auf informationelle Selbstbestimmung geben.

Die Potenziale der Moderne sind dabei noch nicht ausgeschöpft. Sie ist noch nicht an ihrem Ende angelangt, wie es vielleicht die seit 25 Jahren wohlfeile Formulierung der „Postmoderne“ suggeriert. Sicher, naive Vorstellungen der Moderne über die Möglichkeiten zur Ausbübung gesellschaftlicher Kontrolle sind passé, jedoch lässt sich eine andere starke Traditionslinie moderner Argumentation ziehen: Im Zuge des Ausbaus der globalen, computergestützten Vollvernetzung steht derzeit die Durchdigitalisierung der Welt an. War das Industrialisierungsprojekt Anfang des 19. Jahrhunderts noch mit Materialbearbeitung befasst, so setzt sich die Entwicklung heute mit Informationsbearbeitung fort und rundet sozusagen das Gesamtprojekt ab. Stehen heute jedem Haushalt in Form von Elektrizität und Kleinstelektromotoren „universalisierte Dampfmaschinen“ zur Verfügung, so bietet das Internet einen über die Welt gezogenen, generalisierten Transmissionsriemen, der sogar bis in die Privathaushalte hineinreicht. Derzeit kann man durch die Vernetzung eine nochmals gesteigerte Beschleunigung der Industrialisierung

in solchen Bereichen wie der Planung und Entwicklung, des Managements, der Verwaltung, oder genereller der Wissenschaft und der Dienstleistungen beobachten. Kennzeichnend ist, dass der Technisierung die Standardisierung von Kommunikation vorausgeht. Mit den Risiken, die mit dieser Technisierung einhergehen, wachsen zugleich auch die Mittel zu deren Beherrschung. Das ist der Stress, den die Moderne permanent auszuhalten verlangt. Konkret kann man, angesichts der durch Internetnutzung gestiegenen Datenschutz- Risiken, dabei an die im AN.ON-Projekt realisierten Mixe denken.

IDENTITÄTSMANAGEMENT

Es ist heute recht klar absehbar, dass schon bald sämtliche gesellschaftlich relevanten Kommunikationen, insbesondere die von Organisationen und deren Klientel, per Internet, oder zumindest: computergestützt, abgewickelt werden. Insofern muss Anonymität auch unter diesen Bedingungen gewährleistet sein, weil andernfalls, wie oben dargelegt, eine gesellschaftliche Entdifferenzierung droht. Insbesondere sind die Anforderungen an Anonymisierungstechnik in Computernetzen hoch, weil diese sich, als Ergebnis der Industrialisierung auch des Ausübens sozialer Kontrolle, besonders bequem – eben: weitgehend automatisiert – beobachten lassen.

Die Technisierung der Kommunikation kann ein Bürger/Kunde/Arbeitnehmer nur dann schadensfrei bewältigen, wenn ihm seinerseits moderne Kommunikationstechnik dafür zur Verfügung steht, oder er es sich leisten kann, dass andere diese Arbeit für ihn übernehmen. Insbesondere müssen Techniken zur Verfügung stehen, die den differenzierten Umgang mit verschiedenen Organisationen unterstützen. Aus Nutzersicht gilt es, den Überblick zu behalten und zugleich vieles weitgehend automatisiert ablaufen lassen zu können. Als eine der ersten Entwicklungen in diese Richtung ist, neben AN.ON P3P (”Platform for Privacy Preferences”) zu nennen. Es handelt sich um einen Standard zum automatisierten Aushandeln formalisierter Privacy-Policies zwischen Web-Browser und Web-Server.

Ungleich komplexere Überlegungen zu einer solchen Datenschutz verbessernden Technik (”Privacy-Enhancing Technology” [PET]) firmieren unter dem Begriff des “technisch

gestützten Identitätsmanagements”. Die Kernidee besteht darin, dass jeder Bürger über einen, problemlos bei sich zu tragenden, leistungsstarken persönlichen Computer (im Wortsinne eines tatsächlichen “Personal Digital Assistant”) verfügt, der maximal abgesichert eine Fülle persönlicher Daten im ausschließlichen Zugriff seines Besitzers vorhält, die in bestimmten sozialen Situationen für die Lösung einer konkreten Interaktion herausgegeben oder besser noch: in den Rechner hereingeholt und prozessiert werden können. Hierbei denke man an Interaktionen mit der Stadt oder Gemeinde, mit der Krankenkasse und dem Krankenhaus, mit der Polizei, mit der Schule, zwischen Arbeitgeber und Arbeitnehmer usw.

Eine sehr wichtige Technik in diesem Szenario besteht aus “Convertible Credentials”. Credentials sind Beglaubigungen, die von einem Bereich in einen anderen Bereich umgerechnet werden können, ohne dass dadurch Daten zwischen den Bereichen getauscht werden müssen, und ohne dass die Reputation durch den Transfer verloren geht. Generell macht die Nutzung eines Identitätsmanagementsystems aber nur Sinn, wenn dieses auf einer verlässlich Anonymität gewährleistenden Infrastruktur aufsetzt. Deshalb kommt dem Gelingen des AN.ON-Projekts eine perspektivisch grundsätzliche gesellschaftliche Bedeutung zu.

Virtuelles Datenschutzbüro

Ich will da mitreden.
Geht das?

Datenschutz –
gibt's da was im Internet?

Ich hab' da mal
'ne Frage!

Kontakt:

Virtuelles Datenschutzbüro
c/o Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Postfach 7121, 24171 Kiel

international im Web: **http://www.privacyservice.org**
deutsche Sektion im Web: **http://www.datenschutz.de**
schweizer Sektion im Web: **http://www.datenschutz.ch**

E-Mail: **info@privacyservice.org**

PGP-Schlüssel: RSA 2048 Bit, Key-ID: 0x49E9CA0D, erzeugt am 2000-10-18
Fingerprint: 7475 DDB5 6542 1754 08EB 1617 E3D7 DE96