Anonym im Netz – eine neue Gefahr?

Stefan Köpsell

Fakultät Informatik
Institut für Systemarchitketur
TU Dresden
01062 Dresden
sk13@inf.tu-dresden.de

Zusammenfassung: Anonymität im Internet bewegt sich in dem Spannungsfeld zwischen den berechtigten Interessen der Nutzer nach Selbstdatenschutz einerseits und andererseits den ebenso berechtigten Interessen der Strafverfolgungsbehörden nach Aufklärung von kriminellen Handlungen im Zusammenhang mit dem Internet. Dieses Spannungsfeld wird unter Berücksichtigung der gewonnenen Erkenntnisse aus dem praktischen Betrieb eines eigenen Anonymisierungs-Dienstes und der gegenwärtigen Gesetzeslage beleuchtet.

1 Das „anonyme“ Internet?

Das Internet als das Medium des Gedanken- und Informationsaustausches unserer Zeit wird auf Grund seiner scheinbar unübersichtlichen, geradezu gigantischen Strukturen und den zig Millionen Nutzern die sich hinter einer ebenso großen Menge von kryptischen Kürzeln (IP-Adressen) verbergen, gern als „anonymes Internet“ bezeichnet. Oft wird damit die Vorstellung verbunden bzw. suggeriert, daß ein einzelner Nutzer nicht zu identifizieren und sein Kommunikationsverhalten nicht nachvollziehbar ist.

Daß dies jedoch nicht zutrifft ist den Experten, die sich mit der tatsächlichen Struktur und den Protokollen des Internets und mit den Überwachungsmöglichkeiten bzw. Abhörschnittstellen auskennen, längst klar. Und auch der Privatanwender muß in zunehmendem Maße erkennen, daß seine Internetaktivitäten trotz dynamisch vergebener IP-Addressen sehr wohl überwachbar sind und daß er keinesfalls anonym handelt. Insbesondere seitdem die internationale Musik- und Filmindustrie verstärkt gegen Raubkopierer vorgeht und mit Hilfe von Überwachungsmaßnahmen versucht die Verursacher zu ermitteln, um diese dann mit Hilfe der Provider abzumahnen [Heise1] oder zu verklagen [Heise2], dürfte vielen Internetnutzer klar sein, wie „gläsern“ ihre Netznutzung ist.

In Abbildung 1 ist symbolisch ein kleiner Ausschnitt des weltweiten Netzes dargestellt. Jede Nachricht wird über eine Vielzahl von Zwischenstationen geleitet, die von einer ebenso großen Zahl von unterschiedlichen Organisationen oder Personen betrieben werden. Gerade diese Diversität bildet einen wesentlichen Unterschied zu der Zeit des BTX, bei der die Netzinfrastruktur von einem (staatlichen) Unternehmen betrieben wurde. Die privaten Internetzugangsprovider und Inhalteanbieter sind vor allem der Erzielung maximaler Gewinne verpflichtet und erkennen mehr und mehr den Wert der Daten, die sie transportieren. Persönlichkeits- und Interessenprofile werden zum Wirtschaftsgut, um in einer zunehmend

individualisierten Gesellschaft das Marketing von Produkten und Dienstleistungen maßgeschneidert für den einzelnen Kunden betreiben zu können.

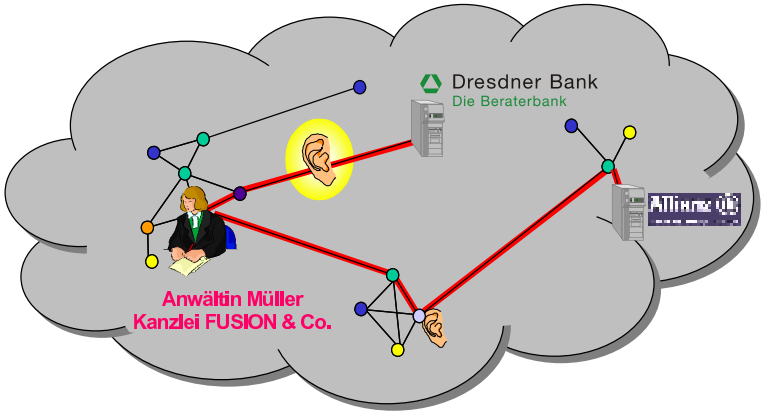

Abbildung 1: Ein symbolischer Ausschnitt des Internet mit seinen Abhörmöglichkeiten

Aber auch von staatlicher Seite wird die Überwachung in starkem Maße zu den unterschiedlichsten Zwecken betrieben. So existieren globale Überwachungssysteme wie z. B. das vornehmlich von den USA betriebene ECHELON-System. Dabei handelt es sich um ein Netzwerk von Abhörstationen, die über den Globus verteilt auf interessante Informationen lauschen. Daß es dabei nicht nur um die Durchsetzung berechtigter Interessen geht, wie etwa dem Schutz vor Terrorismus oder der Kriminalitätsbekämpfung, zeigt der Abschlußbericht des europäischen ECHELON-Untersuchungsausschusses. Das EU-Parlament stellt diesbezüglich in [EU] fest:

> „ . . . daß nunmehr kein Zweifel mehr daran bestehen kann, daß das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient, . . . “

und fordert deshalb:

> „ . . . ihre Bürger und Unternehmen über die Möglichkeit zu informieren, daß ihre international übermittelten Nachrichten unter bestimmten Umständen abgefangen werden; besteht darauf, daß diese Information begleitet wird von praktischer Hilfe bei der Entwicklung und Umsetzung umfassender Schutzmaßnahmen, auch was die Sicherheit der Informationstechnik anbelangt; . . . “

Gleichzeitig gehen die Bemühungen der sogenannten Bedarfsträger (Polizei, Geheimdienst etc.) dahin, durch Änderung von Gesetzen ihre Überwachungsbefugnisse auf dem Gebiet der Telekommunikation ständig zu erweitern. Während in den USA an einem neuen Überwachungssystem dem „Total Information Awareness (TIA) System“ [TIA] gearbeitet wird und in Großbritannien eine bis zu siebenjährige Speicherung von Kommunikationsdaten diskutiert wird [Heise7], Dänemark vorschlägt innerhalb der EU Verbindungsdaten

ein Jahr lang zu speichern [Heise6], kommt aus Bayern der Vorstoß uneingeschränkte Überwachung auch von besonders geschützten Personengruppen wie z. B. Rechtsanwälten, Abgeordneten, Geistlichen und Journalisten zu erlauben, wobei dies auch präventiv zur Gefahrenerkennung und -abwehr gestattet sein soll [Heise3].

Datenschützer und Juristen beklagen seit langem die immer stärkere Einschränkung des Grundrechts auf Unverletzlichkeit des Fernmeldegeheimnisses (Artikel 10 GG). Gleichzeitig steigt jedes Jahr die Anzahl durchgeführter Überwachungsmaßnahmen. Die Statistik der Regulierungsbehörde für Telekommunikation (RegTP) weist für 2002 mit 21 874 Abhöraktionen gegenüber dem Vorjahr einen erneuten Anstieg um zehn Prozent aus [Heise4]. Dabei wurde die Wirksamkeit von Überwachungsmaßnahmen bis heute nicht belegt. Momentan wird dies in einer Studie untersucht [Heise5], um so erstmals Aufschluß über den Sinn und Erfolg zu erlangen.

Berücksichtigt man die vielen Sicherheitsprobleme, die sich immer wieder bei dem Entwurf und Betrieb von komplexen Systemen zeigen, so ist es mehr als fraglich, ob auf die zum Zwecke der Strafverfolgung geschaffenen Abhörschnittstellen auch wirklich nur Berechtigte zugreifen können und ob die Daten vor Unbefugten geschützt sind – insbesondere da diese Schnittstellen so ausgelegt sein müssen, daß die Telekommunikationsunternehmen von etwaigen Abhörmaßnahmen keine Kenntnis erlangen.

Nicht vergessen werden soll an dieser Stelle, daß neben der staatlichen Überwachung und dem privatwirtschaftlichen Datensammeln auch die Gefahr des Lauschen durch Administratoren von Netzknoten oder Kollegen besteht. In einer Zeit, in der Sendungen wie „Big Brother“ höchste Einschaltquoten erzielen oder Mobbing am Arbeitsplatz ein ernst zunehmendes Thema ist, sollte man auch darüber nachdenken.

Zusammenfassend kann also festgestellt werden, daß Anonymität im Internet auf keinen Fall gegeben ist und daß nicht „Anonymität im Netz“ eine neue Gefahr darstellt – sondern eher die unkontrollierte Überwachung.

2 Technische Maßnahmen zur Wahrung der Anonymität im Netz

Zu den bekanntesten Verfahren für Vertraulichkeit und Integrität von Daten im Internet zählen sicherlich Verschlüsselungsverfahren wie RSA und AES bzw. die digitale Signatur. Eine ganze Reihe von Programmen wie PGP oder der freie GPG (www.gnupg.org/) ermöglichen es jedem, auf einfache Art seine Kommunikationsinhalte zu schützen. Die Verfahren sind seit vielen Jahren gut untersucht und gelten als sicher.

Allerdings löst Verschlüsselung alleine das Problem der Anonymität im Netz nicht, da neben den Inhalten auch die Kommunikationsumstände (also *wer* hat *wann* von *wo* mit *wem* etc. kommuniziert) geschützt werden müssen. In Abbildung 1 ist dies beispielhaft dargestellt. Das Problem ist, daß sich aus den Kommunikationsumständen Rückschlüsse über die Kommunikationsinhalte ziehen lassen. Ein anderes Beispiel sei etwa eine plötzlich einsetzende, rege Kommunikation zwischen dem deutschen Transrapid Konsortium und der Stadt Shanghai. Wird dies durch das amerikanische ECHELON-System registriert, so könnte es eine wertvolle Information für die US-Wirtschaft darstellen – selbst wenn die Inhalte verschlüsselt sind.

Um Anonymität im Netz zu gewährleisten sind daher weitere, technische Maßnahmen notwendig. In den letzten Jahren wurden eine ganze Reihe von Anonymitäts-Techniken entwickelt. Einige nur als Forschungsprototypen – andere sind (oder waren) als Produkt bzw. Dienstleistung erhältlich.

Am häufigsten trifft man dabei auf sogenannte „Proxy-Lösungen“. Dabei werden zwischen dem eigenen Web-Browser und dem Web-Server im Internet ein (oder mehrere) Proxies geschaltet. Diese Proxies (Stellvertreter) stellen dann die eigentlichen Web-Anfragen und leiten die Antworten an den Browser weiter. Der Web-Server erfährt auf diese Weise nur die IP-Adresse des Proxy – nicht jedoch die des eigenen Rechners. Es gibt eine Reihe von „Spielarten“ dieses Verfahrens.

Abbildung 2: Formularbasierte Proxies am Beispiel von Rewebber.de und Anonymizer.com – Die zu anonymiserenden URL wird mit Hilfe eines Web-Formulars aufgerufen

Rewebber (www.rewebber.de/) bzw. *Anonymizer* (www.anonymizer.com/) gehören zu den Web-Formular basierten anonymisierenden Proxies. Dabei trägt der Nutzer in ein Formular auf den Internetseiten des Anbieters die URL ein, zu der er surfen möchte. Neben verräterischen Informationen in der HTTP-Anfrage wird auch die vom Web-Server gesendete Antwort gefiltert und z. B. aktive Inhalte entfernt. Außerdem werden die in der Seite enthaltenen Verweise (Links) so geändert, daß damit verbundene Anfragen automatisch wieder über den Proxy geleitet werden (siehe Abbildung 2).

Natürlich bieten derartige Lösungen nur einen schwachen Schutz. Zum einem muß dem Betreiber des Proxy vertraut werden, da er ja sämtliche Surfdaten erfährt. Zum anderen kann natürlich auch ein Überwacher, der vor und hinter dem Proxy lauscht, weiter seine Rückschlüsse ziehen. Ist die Verbindung vom Nutzer zum Proxy nicht verschlüsselt, so ist dies besonders einfach. Aber selbst wenn Verschlüsselung eingesetzt wird, so kann er doch mittels zeitlicher Verkettung oder Verkettung über die Größe von ein- und ausgehenden Daten ermitteln, welche Anfrage von welchem Nutzer stammt.

Proxy-Tools wie beispielsweise *Steganos Internet Anonym* (www.steganos.de/) oder *Anon4Proxy* (www.inetprivacy.com/) greifen auf offene, im Internet vorhandene Proxies zurück, die optional automatisch nach vorgegebenen Regeln gewechselt werden können(z. B. jede Minute). Zwar kann dies die Überwachung erschweren – eine ernst zunehmende Hürde ist es jedoch nicht.

Einzig die kanadische Firma ZeroKnowledge hat mit *Freedom* einen Dienst angeboten, der durch die Verwendung von mehreren hintereinander geschalteten Proxies (verbunden mit einem speziellen, kryptographischen Protokoll und Verschlüsselung) einen ernsthaften Schutz gegen Lauscher im Netz darstellte. Dieser Dienst wurde jedoch aus wirtschaftlichen Gründen im Oktober 2001 eingestellt.

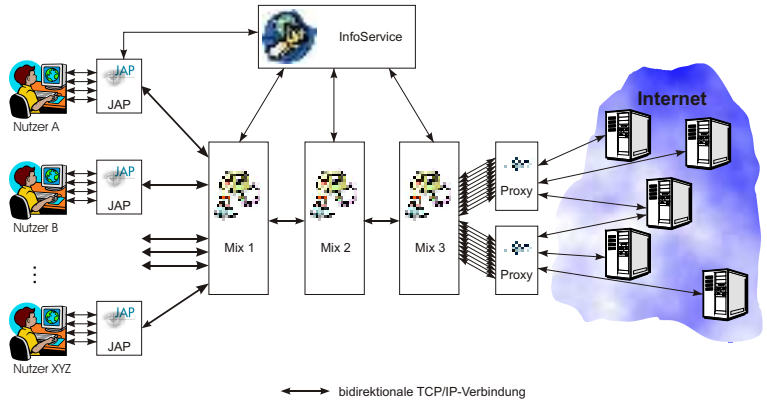

Abbildung 3: Architektur des Anonymiserungsdienstes *JAP*

An der TU Dresden wird seit Anfang 2000 am Institut für Systemarchitektur ein Anonymisierungsdienst entwickelt, der ebenfalls Anonymität auch gegenüber „starken Angreifern“ bieten soll. Schutz soll also gegenüber einem mächtigen Beobachter bestehen, der über umfangreiche Ressourcen verfügt und beispielsweise in der Lage ist, große Teile des Internets zu überwachen, die auf den Verbindungen übertragenen Daten zu manipulieren, eigene Pakete einfügen oder vorhandene löschen kann oder sogar einen Teil der Anonymisierungsserver kontrolliert. Selbst wenn solch ein mächtiger Angreifer nicht real existieren sollte, so ist man mit der Annahme seiner Existenz doch auf „der sicheren Seite“.

Das System selbst besteht aus einer Client-Software (genannt: JAP) und aus einer Reihe von Servern – den sogenannten Mixen (siehe Abbildung 3). Die Grundlagen für das Verfahren gehen auf Ideen von David Chaum aus dem Jahre 1981 zurück [Chau81].

Der JAP muß auf dem Rechner des Nutzers installiert werden und stellt als lokaler Proxy für den Browser die Schnittstelle zum Anonymisierungsdienst dar. Dieser besteht aus einer festen Folge von hintereinandergeschalteten Mixen. Diese Folge wird als Mix-Kaskade bezeichnet. Ein Mix ist dabei im wesentlichen ein „Datenweiterleitungsserver“.

Er nimmt Datenpackete entgegen, puffert sie, kodiert sie um und gibt sie in veränderter Reihenfolge wieder aus. Die Datenpakete sind mehrfach verschlüsselt und die Umkodierung besteht aus einer Entschlüsselung. Es wird also quasi eine „Verschlüsselungsschicht“ entfernt. Sinn des Ganzen ist, daß ein Beobachter, der vor und nach einem Mix lauscht, nicht erfährt, welches eingehende Paket zu welchem ausgehenden Paket gehört. Die Umkodierung sorgt dabei dafür, daß ein einfacher Vergleich des Bitmusters von eingehenden und ausgehenden Paketen keine Rückschlüsse zuläßt. Die Pufferung und die Umsortierung verhindern einen Angriff über zeitliche Verkettung. Außerdem besitzen alle Pakete dieselbe Länge, so daß auch hierüber keine Zuordnung möglich ist (siehe Abbildung 4).

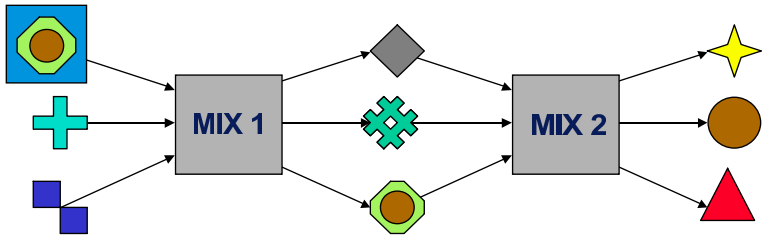

Abbildung 4: Mix-Prinzip: Datenpakete werden gepuffert, umkodiert und umsortiert – die Ein- — Ausgabe-Zuordnung wird verborgen

Der JAP bereitet die Anfragen des Browsers auf, so daß sie über den Anonymisierungsdienst versendet werden können. Dies bedeutet im wesentlichen, Nachrichten in die Pakete zu zerteilen, diese mehrfach zu verschlüsseln und an den ersten Mix einer Kaskade zu senden bzw. von dort Pakete zu empfangen, zu entschlüsseln und an den Browser weiterzuleiten.

Ein wesentlicher Vorteil der Verwendung von mehreren Mixen liegt darin, daß nur einer in der Kette vertrauenswürdig sein muß, damit das gesamte Verfahren sicher ist. Die Mixe sollten daher von unabhängigen Betreibern betrieben werden, um die Vertrauenswürdigkeit einer Mix-Kaskade zu erhöhen. Auf diese Weise ist auch sicher gestellt, daß nicht einmal die Entwickler bzw. Betreiber des Anonymisierungsdienstes wissen, wer welche Seiten abruft.

Das Projekt wurde durch Förderung des Bundeswirtschaftministerium und der Deutschen Forschungsgemeinschaft (DFG) ermöglicht. Es wird in Kooperation mit der Freien Universität Berlin und dem Unabhängigen Landeszentrum für Datenschutz Schleswig Holstein durchgeführt. Momentan läuft eine öffentliche Testphase. Jeder kann sich die Software unter http://anon.inf.tu-dresden.de/ herunterladen und ausprobieren.

3 Gesellschaftliches Spannungsfeld von Anonymität

Leider (oder vielleicht: natürlich) wird solch ein Anonymisierungsdienst auch mißbraucht. Anonymität im Internet bewegt sich daher im Spannungsfeld zwischen den berechtigten Interessen der Nutzer nach Selbstdatenschutz einerseits und andererseits den ebenso

berechtigten Interessen der Strafverfolgungsbehörden nach Aufklärung von kriminellen Handlungen im Zusammenhang mit dem Internet.

Daß es sehr schwierig ist, einen „richtigen“ Weg im Umgang mit Anonymität, Vertraulichkeit und Datenschutz zu finden, zeigt sich auch durch die vielen unterschiedlichen und zum Teil gegensätzlichen politischen Aktivitäten.

So werden zum einen Maßnahmen beschlossen, die eine Ausweitung der Überwachung bedeuten, wie etwa die Telekommunikationsüberwachungsverordnung (TKÜV), das Gesetz zur Neureglung von Beschränkungen des Brief- Post- und Fernmeldegeheimnisses (G-10 Gesetz), das Europäische Abkommen zur Cyberkriminalität oder die Erarbeitung eines europäischen Standards für Abhörschnittstellen (ETSI 201671).

Gleichzeitig werden Projekte, wie das „AN.ON“-Projekt zum anonymen Surfen oder die Entwicklung des Verschlüsselungstools GNU Privacy Guard (GnuPG) vom Bundeswirtschaftsministerium gefördert. Dies weist klar den Weg in Richtung mehr Vertraulichkeit und mehr Datenschutz. Daß der Gesetzgeber die Notwendigkeit von Anonymität im Internet erkannt hat, zeigt sich auch in diversen gesetzlichen Regelungen.

Im §4 Absatz 6 des Teledienstedatenschutzgesetzes (TDDSG) heißt es:

> „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.“

Das TDDSG wurde zum 1. Januar 2002 umfassend novelliert – der Wortlaut des § 4 Absatz 6 blieb jedoch unverändert. Daraus läßt sich ableiten, daß die Möglichkeit der anonymen bzw. pseudonymen Nutzung von Telediensten dem Gesetzgeber weiterhin ein wichtiges Anliegen ist.

„Anonymität“ im Sinne des § 4 Absatz 6 TDDSG ist dabei gegeben, wenn ein Personenbezug auch mit Hilfe von zusätzlichem Wissen nicht mehr hergestellt werden kann. Der an der TU Dresden entwickelte Anonymisierungsdienst JAP soll genau das leisten: eine Rückverfolgung und damit Deanonymisierung einer Anfrage, die durch eine Mix-Kaskade geschickt wird, ist ausgeschlossen, solange nur ein einziger Mix-Betreiber vertrauenswürdig ist.

Eine weitere Frage, die das TDDSG regelt, betrifft die Daten, die ein Provider speichern darf. Im § 6 Absatz 1 TDDSG heißt es dazu:

> „Der Diensteanbieter darf personenbezogene Daten eines Nutzers ohne Einwilligung nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (Nutzungsdaten).“

Als Nutzungsdaten gelten dabei solche Daten, die der Identifikation des Nutzers dienen bzw. beschreiben wann, wie lange welcher Dienst genutzt wurde. Nach Auffassung der Datenschützer zählt dabei z. B. auch die IP-Adresse zu den Nutzungsdaten. Damit ist klar, daß Betreiber von Web-Servern gegen die Datenschutzbestimmungen verstoßen, wenn sie

bei kostenlosen Web-Angeboten mitprotokollieren, von welcher IP-Adresse welche URL aufgerufen wurde.

Neben dem TDDSG wird auch in der Neufassung des Bundesdatenschutzgesetzes (BDSG) vom 23. Mai 2001 das Prinzip der Datensparsamkeit und Datenvermeidung hervorgehoben:

> „§**3a Datenvermeidung und Datensparsamkeit**
> Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

Zwar wurde durch einen Gesetzesentwurf des Bundesrates vom 31. Mai 2002 (BT-Drucksache 275/02) versucht, diese starken Datenschutzbestimmungen einzuschränken, indem eine Pflicht zur Vorratsdatenspeicherung in das TDDSG aufgenommen werden sollte, jedoch hat das Bundesverfassungsgericht bereits am 15. Dezember 1983 im sogenannten Volkszählungsurteil ein generelles Verbot der Vorratsdatenspeicherung festgestellt:

> „ . . . Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. . . . "

Ferner führte das Gericht aus:

> „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

Zur Begründung führt das Gericht aus:

> „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine dies ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.
> Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."

Man kann also feststellen, daß der Betrieb eines Anonymisierungsdienstes momentan im Einklang mit dem Willen des Gesetzgebers steht. Natürlich kann sich dies in einem demokratischen Staat durch Änderung der entsprechenden Gesetze jederzeit ändern – etwa wenn die Mehrheit der Bevölkerung die Interessen der Strafverfolgungsbehörden für wichtiger erachtet als den Datenschutz. Angemerkt sei, daß dieser Interessensausgleich zwischen

Datenschutz und Strafverfolgung bereits im Gesetzgebungsverfahren zum TDDSG diskutiert wurde, wobei der Gesetzgeber der Auffassung war, daß die Interessen der Strafverfolgungsbehörden ausreichend berücksichtigt wurden:

> „ . . . 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 könne in globalen Netzwerken wirksam nur durch größtmögliche Anonymität der Nutzer gewährleistet werden. . . .
> . . . Den Interessen der Strafverfolgungsbehörden könne durch Ausschöpfung der in der StPO vorgesehenen Ermittlungsmöglichkeiten Rechnung getragen werden. . . . " [BT 13/7385]

Gleichzeitig ergibt sich als Problem, daß die Strafverfolgungsbehörden ihre Anforderungen nicht konkret formulieren. Die generelle Vorstellung, erst einmal alles auf unbestimmte Zeit zu speichern, ist für einen Interessensausgleich sicher wenig hilfreich. Der Abschlußbericht zum „Projekt der Strategischen Kriminalitätsanalyse im BKA" (Juni 2002) merkt dazu an:

> „ . . . Zudem fehlt noch immer das polizeiliche Anforderungsprofil für die Begrenzung des Datenschutzes, in dem sie aus ihrer Sicht notwendiger- und begründeterweise längerfristig zu speichernde Daten beschreibt . . .
> Die Polizei muss ihre Wünsche endlich präzisieren . . . " [BKA02]

Ausführlichere Untersuchungen der rechtlichen Situation findet man z. B.auch in [Gole03].

4 Erfahrungen aus dem Betrieb des Anonymisierungsdienstes

Bei dem Anonymiserungsdienst JAP wurde von Anfang an versucht, die von ihm ausgehenden „Gefahren" (also das Mißbrauchspotential) so gering wie möglich zu halten. So ist die Möglichkeit der Anonymisierung einer allgemeinen TCP/IP-Verbindung zwar implementiert – aber nicht aktiviert, um Hacking bzw. Denial Of Service Angriffe zu verhindern. Momentan unterstützt der Dienst nur das Abrufen von Informationen aus dem Web. Ein vollständige, vorrausschauende Einteilung der zu anonymisierenden Anfragen in „Gut" und „Böse" wäre zwar wünschenswert, ist aber natürlich nicht möglich.

So kam es zu einer Reihe von Mißbrauchsfällen. Dies betrifft sowohl strafrechtlich relevante Tatbestände als auch Aktivitäten die „nur" zu Unannehmlichkeiten führen. Daß auch strafbare Handlungen über den Dienst durchgeführt werden verwundert insofern, als daß noch nicht alle Schutzfunktionen auch tatsächlich implementiert sind. Somit ist eine Deanonymisierung z. B. durch Strafverfolgungsbehörden unter bestimmten Umständen möglich – worauf auch deutlich auf den Web-Seiten des Projektes hingewiesen wird.

Eventuell ist letzteres auch eine Ursache dafür, daß seit Beginn des Testbetriebes vor über zwei Jahren nur ca. 20 Anfragen von deutschen Strafverfolgungsbehörden auf Grund eines strafrechtlich relevanten Anfangsverdachtes eingegangen sind (Stand August 2002) – bei bis zu 10 Millionen abgerufenen URLs und geschätzten 5000 Nutzern täglich. Diese Statistik sagt natürlich nichts über die Dunkelziffer von nicht zur Anzeige gebrachten Taten

aus. Polizeibeamte gaben zusätzlich zu bedenken, daß sie manche Anfragen gar nicht erst weiterleiten, da sie bereits wüßten, daß keine sachdienlichen Hinweise zu erwarten sind. So läßt sich auch die vom Bayrischen Landeskriminalamt genannte Zahl erklären, wonach bei 7%-8% der Fälle mit Internetrelevanz IP-Adressen von Anonymisierungsdiensten im Spiel waren [GeTi03]. Hingewiesen werden soll auch auf eine Mißbrauchsanalyse [BrEl03], die die Betreiber des *Freedom*-Dienstes (siehe oben) veröffentlich haben – wobei ebenfalls von einer nur geringen Mißbrauchsrate (ca. 2%) die Rede ist.

Die Anfragen der Polizei verlaufen alle nach demselben Schema: In einem Schreiben wird darum gebeten alle Informationen bzgl. der IP-Adressen 141.76.1.121 bzw. 141.76.1.122 zu dem Zeitpunkt x herauszugeben. Der Zeitpunkt liegt meist Monate vor dem Eingang des Schreibens. So traf beispielsweise die erste Anfrage am 24. Juli 2001 ein, bei dem es um den Mißbrauchszeitpunkt 25. April 2001 ging. Gegenwärtig treffen etwa ein bis zwei Auskunftsersuchen pro Monat ein.

Da die IP-Adressen nicht unmittelbar dem Anonymisierungsdienst, sondern zunächst einmal der TU Dresden zuzuordnen sind (mittels „whois"-Abfrage), wurden die Anfragen vielfach an den Leiter des Universitätsrechenzentrums gesandt, der dann weiterleitete. Außerdem entstand auf diese Weise der Eindruck, daß der Mißbrauch unmittelbar durch Mitarbeiter oder Studenten der TU Dresden begangen wurde. Um derartige Imageschäden zu vermeiden, wird der Dienst zukünftig IP-Adressen aus einem eigenen Adressbereich verwenden, der direkt dem Projekt zugeordnet ist.

Auf Grund der Art des Dienstes und da keine Informationen mitgeloggt werden, können auch keine sachdienlichen Hinweise gegeben werden. Dies wurde in allen Fällen mittels eines „Standardschreibens" mitgeteilt, das zusätzlich einen Verweis auf das Forschungsprojekt und eine kurze Erläuterung der Funktionsweise des Dienstes enthält. Die Anfragen werden generell vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (als Projektpartner) beantwortet.

Da der Betrieb unseres Dienstes gesetzeskonform erfolgt, wurden die Antwortschreiben von Seiten der Strafverfolgungsbehörden akzeptiert. Weiterführende Maßnahmen, wie etwa Verhöre, Durchsuchungen oder Beschlagnahme von Geräten, fanden nicht statt.

Bei dem Großteil der Fälle handelt es sich um Betrug – insbesondere Kreditkartenbetrug. Über das Internet werden mit gefälschten Angaben Waren bestellt, die anschließend nicht bezahlt werden. Eine Spielart des Betruges ist es, daß die Identität einer anderen Person vorgetäuscht wird, um diese „zu ärgern". So wurde z. B. ein Wohnhaus mittels Inserat im Internet zu einem sehr günstigen Preis angeboten, obwohl der Hausbesitzer gar nicht verkaufen wollte. Durch eine Vielzahl von kauf- und besichtigungswilligen Interessenten wurden die Nerven des Hausbesitzers auf's äußerste strapaziert.

Auch Drohungen und Beschimpfungen gehören zu den Tatbeständen. In zwei Fällen bestand der Verdacht, daß jemand kinderpornographisches Material aus dem Internet herunter geladen hat.

Neben den strafrechtlich relevanten Fällen gab es auch eine Reihe von Anfragen von Firmen oder Privatpersonen, die sich durch den Dienst geschädigt fühlen. Oft ging es dabei um Beleidigungen, die in Gästebüchern oder Web-Foren hinterlassen wurden oder die

Polizeidirektion XY
Kommissariat 3

Technische Universität Dresden
Systemadministratoren

Ermittlungsverfahren gegen Unbekannt wegen des Verdachtes auf Computerbetrug

Sehr geehrte Damen und Herren,

im Rahmen des oben genannten Ermittlungsverfahrens wurde festgestellt, daß dem Täter eine IP-Adresse zugeordnet werden kann, die durch Sie verwaltet wird:

IP-Adresse: 141.76.1.121
Datum/Uhrzeit (Ortszeit): 25.06.2001, 09:05:46 Uhr

Sie werden nun gebeten alle Ihnen bekannten Verbindungs- und Nutzungsdaten, die oben genannte IP-Adresse und Zeitpunkt betreffen mitzuteilen.
Es wird auch um Mitteilung gebeten, falls keine Daten zum Beispiel auf Grund der bereits verstrichenen Zeit vorliegen.

Mit Dank und freundlichen Grüßen
Meier, KK

Abbildung 5: Beispiel eines Auskunftsersuchens

Foren wurden mit sinnlosen Daten „zugemüllt“. Als Lösung dieses Problems besteht das Angebot, den Zugriff auf die betreffenden Seiten über den Anonymisierungsdienst zu sperren. Dazu muß der Betreiber der Seite lediglich mitteilen, welche Seiten gesperrt werden sollen. Bevor eine Sperrung erfolgt, wird überprüft, ob der Beantragende tatsächlich verantwortlich für die Seite ist. Auf diese Weise soll willkürliche Zensur verhindert werden. Außerdem wird mitgeteilt, daß Sperrwünsche veröffentlicht werden, um dem Vorwurf der Zensur zu begegnen. Es ist auch möglich, daß der Webseiten-Betreiber selbst eine eigene Sperre einrichtet, da die Ausgangs-IP-Adressen des Dienstes bekannt sind und im Web abgefragt werden können.

Aus Sicht der Netzwerksicherheit ist insbesondere interessant, daß immer wieder Vorwürfe bezüglich Hacking-Versuchen auf Web-Server eintreffen, obwohl die restriktive Konfiguration des Dienstes dies eigentlich ausschließen sollte (siehe oben). Diese Angriffe geschehen dabei regelmäßig unter Ausnutzung bekannter Schwachstellen der Server, (z. B. unter Ausnutzung bekannter Sicherheitslücken im Microsoft Internet Information Server) – für die oftmals bereits seit längerem Patches vorhanden sind. Dabei handelt es sich jedoch nicht um eine speziell von Anonymisierungsdienst ausgehende Gefahr. Vielmehr zeigt sich, daß die generellen (Sicherheits-)Risiken des Internet unterschätzt und nicht hinreichend beachtet werden. Letztlich ist für die Sicherheit z. B. eines Web-Servers auch der entsprechende Administrator verantwortlich.

Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein

Polizeidirektion XY
Kommissariat 3

Übermittlung von Nutzungsdaten; Ermittlungsverfahren wegen Computerbetrugs

Sehr geehrter Herr Meier,

Sie haben um Auskunft bezüglich ... gebeten. Die Mitarbeiter der TU Dresden haben Ihre Anfrage zuständigkeitshalber an uns weitergeleitet. Ich kann Ihnen zu Ihrer Anfrage Folgendes mitteilen:

Der von Ihnen genannten Server mit der IP-Adressen 141.76.1.121 ist Teil eines Forschungsprojektes, das gemeinsam von der Technischen Universität Dresden, Fakultät für Informatik, und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein durchgeführt wird. Ziel des Projektes, das vom Bundesministerium für Wirtschaft und Technologie gefördert wird, ist es, anonyme und unbeobachtbare Webzugriffe zu realisieren (http://anon-online.de).
Dabei geht es darum, die Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) umzusetzen, die verlangen, dass Diensteanbieter den Nutzern die anonyme oder pseudonyme Nutzung ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 4 Abs. 6 TDDSG). Dabei wird bereits auf technischer Ebene die Zuordnung von IP-Adressen zu einzelnen Nutzern oder sonstigen identifizierenden Merkmalen vermieden. Aus diesem Grunde liegen hier keine Daten vor, über die (bei Vorliegen eines richterlichen Beschlusses) Auskunft gegeben werden könnte.
Es tut mir leid, Ihnen insoweit nicht weiterhelfen zu können.

Mit freundlichen Grüßen

Abbildung 6: Beispiel eines Antwortschreibens

Neben den erwähnten Maßnahmen zur Mißbrauchsverhinderung gibt es auch Überlegungen, wie in berechtigten Fällen (richterliche Anordnung etc.) eine Deanonymisierung durchgeführt werden kann. Dabei darf es natürlich nicht zu einer Massenüberwachung kommen, da sonst der Sinn des Dienstes in Frage gestellt ist. Die Überlegungen zielen in Richtung einer „Online“-Überwachung, bei der ähnlich der Telefonüberwachung nur der im Moment ausgeführte Zugriff zurückverfolgbar ist. Eine Vorratsdatenspeicherung, die eine rückwirkende Deanonymisierung ermöglicht, ist nicht geplant. Um die Wirksamkeit dieser Maßnahmen abschätzen zu können, wäre ein Dialog mit den Strafverfolgungsbehörden notwendig. Obwohl sogar Planspiele zur Bekämpfung von Internetkriminalität unter Verwendung von JAP durchgeführt werden, zeigen sich die Behörden leider sehr zögerlich bei der Bekanntgabe ihrer Anforderungen und lassen sich nicht „in die Karten schauen“ (siehe oben).

Zum Schluß soll noch erwähnt werden, daß es auch „positiven Mißbrauch“ des Dienstes gibt. So wird er für Zwecke benutzt, für die er nicht unmittelbar entwickelt wurde. Dazu zählt insbesondere die Umgehung von Internet-Zensurmaßnahmen. Menschen aus Ländern mit restriktivem Internetzugang benutzen den Dienst, um darüber auf das gesamte Netz zugreifen zu können. Aus Saudi-Arabien ist beispielsweise bekannt, daß der Zugriff auf das Netz nur über einen staatlich kontrollierten Proxy möglich ist, der unerwünschte Kommunikation filtert.

Da momentan nur einige wenige Zugangspunkte zum Anonymisierungsdienst (Mix-Kaskaden) existieren, ist aber auch eine Sperre des Dienstes leicht möglich. So hat China mittlerweile den Zugriff gesperrt, wie ein Hilferuf von DPA Peking vom Oktober 2002 belegt:

> „... einige Wochen hat uns die JAP-Software gute Dienste geleistet, von China aus gesperrte Webseiten wie Amnesty oder Falun Gong aufzurufen, doch haben die chinesischen Behörden jetzt auch den JAP-Zugang gesperrt.“

5 Abschließende Bemerkungen

Anonymität wird oftmals als etwas negatives dargestellt. Dabei ist sie notwendig für eine demokratische Gesellschaft und deren Weiterentwicklung. Ohne anonyme Wahlen und die Chance unerkannt seine Meinung sagen zu können, ist die demokratische Entscheidungsfindung gefährdet, da sich viele schlicht nicht mehr trauen würden, ihre Auffassungen zu vertreten, wenn diese von den allgemein üblichen abweichen. Die Strafverfolgungsbehörden sind für eine erfolgreiche Verbrechensbekämpfung auf anonyme Hinweise aus der Bevölkerung angewiesen.

Viele der „neuen Gefahren“ sind altbekannt (z. B. das Einkaufen mit falschen Angaben) und Lösungen längst verfügbar (was man z. B. daran sieht, daß man beim Pizzalieferservice seine Telefonnummer angeben muß). Andere Gefahren (wie z. B. der „Identitätsklau“) lassen sich gerade mit Anonymisierungstechniken verhindern. Immer mehr Daten zu erfassen und auf unbestimmte Zeit für den Fall der Strafverfolgung zu speichern, ist sicher der falsche Weg. Vielmehr sollte man unter Ausnutzung moderner Technologien wie Verschlüsselung, digitaler Signatur, Anonymität und Pseudonymität dafür sorgen, daß Straftaten im Internet erst gar nicht begangen werden können.

Anonym im Netz – eine neue Gefahr? Nein!

Literatur

[BKA02] *Notwendigkeiten, Möglichkeiten und Perspektiven der Bekämpfung von Internet-Kriminalität. Abschlussbericht zum Projekt der Strategischen Kriminalitätsanalyse (SKA) im Bundeskriminalamt*. überarbeitete Fassung vom Juni 2002, BKA, Wiesbaden

[BrEl03] David Bratzer, Andrew Elkin. *Freedom 2.2 Abuse Issues and Analysis*. http://osiris.978.org/~brianr/crypto-research/anon/www.freedom.net/products/whitepapers/freedom_abuse2-2.pdf, 2003.

[BT 13/7385] *Gesetzesbegründung zu § 4 TDDSG*. BT-Drucks. 13/7385, 09. April 1997, S. 71

[Chau81] David Chaum. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*. Communications of the ACM 24/2 (1981) 84-88.

[EU] *BERICHT über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI))*. EU Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon, Sitzungsdokument A5-0264/2001, Teil 1, 11. Juli 2001.

[GeTi03] Rainer W. Gerling, Marie-Theres Tinnefeld. *Anonymität im Netz. Einige Gedanken zum Heft 3/2003*. DuD Datenschutz und Datensicherheit, Heft 5/2003, S. 305, Vieweg Verlag, Wiesbaden

[Gole03] Claudia Golembiewski. *Das Recht auf Anonymität im Internet*. DuD Datenschutz und Datensicherheit, Heft 3/2003, S. 129, Vieweg Verlag, Wiesbaden

[Heise1] Heise News Ticker. *Erneute Warnung von T-Online an Tauschbörsen-Nutzer*. http://www.heise.de/newsticker/data/hob-23.08.02-001/

[Heise2] Heise News Ticker. *US-Musikindustrie verklagt Studenten wegen Tauschbörsen*. http://www.heise.de/newsticker/data/jk-04.04.03-000/

[Heise3] Heise News Ticker. *Bayern prescht bei der Telefonüberwachung vor*. http://www.heise.de/newsticker/data/jwe-06.05.03-000/

[Heise4] Heise News Ticker. *Telefonüberwachung kommt immer mehr in Schwung*. http://www.heise.de/newsticker/data/anm-03.05.03-000/

[Heise5] Heise News Ticker. *Erste Ergebnisse der Abhörstudie des Justizministeriums*. http://www.heise.de/newsticker/data/jk-02.11.01-000/

[Heise6] Heise News Ticker. *EU will Verbindungsdaten mindestens ein Jahr speichern*. http://www.heise.de/newsticker/data/uma-21.08.02-000/

[Heise7] Heise News Ticker. *Neuer Anlauf in Großbritannien zur Verbindungsdatenspeicherung*. http://www.heise.de/newsticker/data/anw-12.03.03-021/

[TIA] *Homepage des Total Information Awareness (TIA) System*. http://www.darpa.mil/iao/TIASystems.htm