Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes

Stefan Köpsell, Hannes Federrath, Marit Hansen

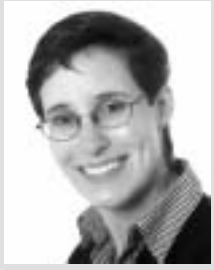
Der folgende Beitrag beschreibt die Erfahrungen bei der Entwicklung und beim Betrieb eines Anonymisierungsdienstes an der TU Dresden. Die dafür entwickelte Client-Software JAP ist seit Januar 2001 öffentlich zugänglich.

Stefan Köpsell

Wiss. Mitarbeiter am Lehrstuhl Datenschutz und Datensicherheit, TU Dresden, Arbeitsschwerpunkte: Anonyme und unbeobachtbare Kommunikation im Internet
E-Mail: sk13@inf.tu-dresden.de

Hannes Federrath

Wiss. Oberassistent am Institut für Informatik der Freien Universität Berlin, Arbeitsschwerpunkte: IT-Sicherheit, Mobilkommunikation, technischer Datenschutz
E-Mail: feder@inf.fu-berlin.de



Marit Hansen

Dipl.-Inform; Referatsleiterin „PET – Privacy-Enhancing Technologies“ im ULD Schleswig-Holstein; Arbeitsschwerpunkt: Identitätsmanagement, PET
E-Mail: hansen@datenschutzzentrum.de

Einleitung

An der TU Dresden wird seit September 2000 ein Anonymisierungsdienst betrieben, der ein weitgehend unbeobachtbares Surfen im Internet erlaubt. Mit bis zu 4000 Nutzern täglich erfreut sich dieser Dienst wachsender Beliebtheit und zählt inzwischen zu den fünf meistgenutzten Anonymisierungsdiensten dieser Art weltweit.

Die für die Nutzung des Dienstes benötigte Client-Software JAP ist entstanden im Rahmen der Zusammenarbeit der Projekte „AN.ON – Anonymität.Online“, gefördert vom BMWi, und „Effiziente und skalierbare Realisierung von unbeobachtbarer und anonymer Kommunikation im Internet“, gefördert im DFG-Schwerpunktprogramm Sicherheit.

Neben dem gesellschaftlichen Spannungsfeld, das beim Betrieb unseres Anonymisierungsdienstes zu Tage tritt, geht es in diesem Beitrag um „technische“ Erfahrung, die sich für den Betrieb von Internet-basierten Diensten verallgemeinern lassen.

1 Anonymisierer

Einführend werden zunächst einige bekannte Anonymisierungsdienste[1] sowie unser System kurz vorgestellt.

1.1 Proxies

Die Klasse der anonymisierenden Proxies gehört zu den bekanntesten Tools für anonymes Surfen. Der einfache Einsatz eines Proxy hat jedoch Schwächen. Dem verwendeten Proxy muss vertraut werden, da er das Surfverhalten des Nutzers beobachten kann. Außerdem schützt das Verfahren nicht gegen einen Beobachter, der zwischen Nutzer-Rechner und Proxy mitlesen kann.

Rewebber[2] bzw. *Anonymizer*[3] gehören zu den auf Web-Formularen basierenden 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 werden auch die vom Web-Server gesendete Antwort gefiltert und z.B. aktive Inhalte entfernt. Weiterhin werden die in der Seite enthaltenen Verweise (Links) so geändert, dass damit verbundene Anfragen automatisch wieder über den Proxy geleitet werden. Manche Proxies unterstützen zusätzlich eine Verschlüsselung der Verbindung zum Proxy mittels SSL (Secure Socket Layer).

Daneben existieren Tools wie z.B. *Steganos Internet Anonymität*[4] oder *Anon4Proxy*[5], die die Anfragen des Browsers über offene Proxies leiten. Diese Proxies werden zusätzlich gewechselt (z.B. 1x/min). Dadurch kann ein einzelner Proxy nicht mehr das gesamte Surfverhalten beobachten, und eine Rückverfolgung der Kommunikation wird erschwert.

Nachdem die kanadische Firma *ZeroKnowledge* im letzten Jahr ihren starken Anonymitätsdienst *Freedom* eingestellt hat, bietet sie als neues Anonymisierungsprodukt *Freedom WebSecure*[6] an. Dabei handelt es sich um einen einfachen Proxy, mit dem verschlüsselt kommuniziert wird.

1.2 Mixe

David Chaum schlug 1981 ein Verfahren für anonyme E-Mail[7] vor, deren Kernkompo-

[1] Eine ausführlichere Analyse verschiedener Anonymisierungsverfahren findet man in Oliver Berthold/Hannes Federrath/Marit Köhntopp: Project „Anonymity and Unobservability in the Internet“; Proc. Workshop on Freedom and Privacy by Design / CFP 2000, Toronto/Canada, April 4-7, 2000, ACM, 2000, 57-65. Siehe auch die Beiträge von Roessler, DuD 11/1998, S. 619-621 und Federrath/Pfitzmann, DuD 11/1998, S. 623-627.

[2] http://www.rewebber.de/
[3] http://www.anonymizer.com/
[4] http://www.steganos.de/
[5] http://www.inetprivacy.com/
[6] http://www.freedom.net/
[7] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84–88.

nenten sog. Mixe[8] sind. Um Mixe wirklich sicher betreiben zu können, müssen einige Maßnahmen durchgeführt werden, die zu Lasten der Effizienz gehen.

Das oben bereits erwähnte System *Freedom* löste das Problem, indem nur Funktionen eines Mixes implementiert wurden, die der Verzögerung von Nachrichten wenig schaden. Bei der Konzeption wurde also bewusst auf Sicherheit zu Gunsten von Benutzbarkeit verzichtet. *Freedom* wurde im Oktober 2002 aus ökonomischen Gründen eingestellt. Einen ähnlichen Ansatz verfolgte auch das Projekt *Onion Routing*[9], das den Testbetrieb seit Januar 2000 eingestellt hat. Auch unser Dienst basiert auf Mixen.

1.3 Peer-To-Peer

In letzter Zeit gibt es verstärkt Entwicklungen auf dem Gebiet der Peer-To-Peer-basierten Systeme. Ein bekanntes System, das nach diesem Prinzip arbeitet, ist *Crowds*[10]. Dabei werden die Webzugriffe über zufällig ausgewählte Teilnehmer des Systems geleitet, bevor sie den Webserver erreichen.

Die Kommunikationsinhalte werden bei *Crowds* im Gegensatz zum *Anonymizer* verschlüsselt. Eine Verkettung über die Länge der Nachrichten und damit die Beobachtung ist jedoch nach wie vor möglich, wenn der Angreifer Verkehrsanalysen durchführt. Gegen Angriffe über die zeitliche Verkettung von eingehenden Nachrichten eines Knotens und deren Ausgabe wurden keine Schutzmaßnahmen vorgesehen.

Zu den neueren Peer-To-Peer-basierten Systemen zählen *Tarzan*[11] und *GNUnet*[12]. Bei beiden Systemen unterhält ein Teilnehmer verschlüsselte Verbindungen zu anderen Teilnehmern des Peer-To-Peer-Netzes. Die Daten werden dann über eine zufällig gewählte Route durch das Peer-To-Peer-Netz gesendet. Die Sicherheitsannahme dieser System ist, dass jeder Beteiligte abstreiten kann, Urheber eines Requests zu sein. Jedoch ergibt sich als Problem, dass Teilnehmer Daten im Namen von anderen abrufen, wobei es sich dabei auch um strafrechtlich relevante Abfragen handeln kann. Während professionelle Betreiber von Anonymisierungsdiensten analog einem Internetzugangsprovider juristisch nicht für die Inhalte weitergeleiteter Pakete verantwortlich sind, gilt dieses Privileg für Privatpersonen normalerweise nicht.

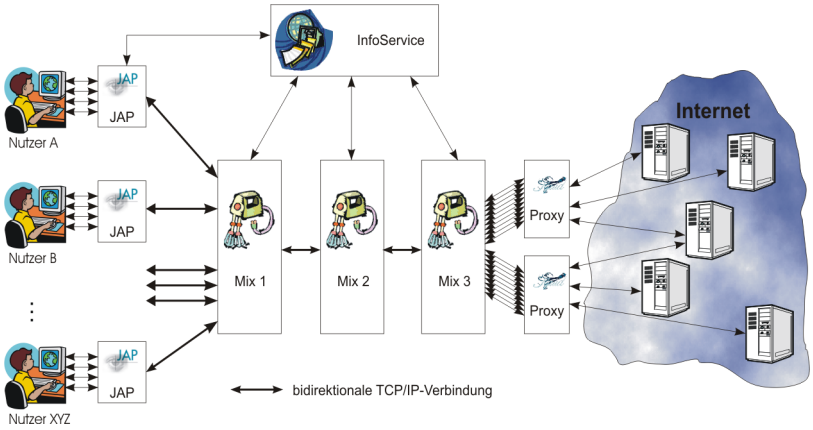


Abbildung 1: Architektur des Anonymisierungsdienstes JAP

2 Unser Dienst

Die Basis des von uns entwickelten Systems[13] bilden die Mixe. Mehrere Mixe werden in einer festen, nicht vom Nutzer bestimmbaren Reihenfolge zusammengeschaltet – der Nutzer kann nur zwischen diesen Mixkaskaden wählen. Um die Vertrauenswürdigkeit einer Kaskade zu erhöhen, werden die einzelnen Mixe von unterschiedlichen Betreibern betrieben, da zur Deanonymisierung von Teilnehmern alle Mixe zusammenarbeiten müssten.

Das Anonymisierungssystem besteht aus drei Komponenten: einer Client-Software (JAP), mehreren Anonymisierstationen (Mixe) und dem InfoService (s. Abb. 1).

Über unseren Anonymisierungsdienst lassen sich proxy-fähige Dienste nutzen, d.h. die beim Benutzer zu installierende Software JAP implementiert eine Proxy-Schnittstelle, während hinter dem letzten Mix das entsprechende Gegenstück existiert. JAP sorgt für die Verschlüsselung der anonym zu übertragenden Daten und bereitet diese gemäß dem Protokoll des zugrundeliegenden Anonymisierungsdienstes auf. Ein Vorteil standardisierter Proxy-Schnittstellen ist, dass die Verarbeitung des Proxy-Protokolls auf erprobte und ausgereifte Komponenten ausgelagert werden kann, die oft noch zusätzliche Funktionalität (Zugriffskontrolle, Ressourcenbegrenzung, Caching etc.) bieten.

Um die Benutzung des Anonymisierungsdienstes zu erleichtern und dem Nutzer eine Rückmeldung über sein aktuelles Schutzniveau zu geben, wurde ein dritter Bestandteil in das Gesamtsystem aufgenommen – der sogenannte „InfoService“. Dieser ist mit einer Datenbank vergleichbar und hält Informationen über die aktuell verfügbaren Mixkaskaden, deren Auslastung etc. bereit. JAP kann mit Hilfe der beim InfoService vorliegenden Daten dem Nutzer eine Vorstellung über den momentanen „Grad der Anonymität“ vermitteln.

Ziel war es, möglichst vielen Menschen den Zugang zu ermöglichen. Daher wurde die Client-Komponente in der (weitgehend) plattformunabhängigen Programmiersprache Java entwickelt.[14] Die Mixe sind für den Betrieb auf Unix-artigen Betriebssystemen konzipiert und aus Performancegründen in C++ geschrieben.

3 Erfahrungen

3.1 Betrieb und Nutzung

Wir haben unseren Dienst erstmals im September 2000 der Öffentlichkeit zur kostenlosen Nutzung bereit gestellt. Mit

[8] Siehe „Gateway“ in diesem Heft.
[9] http://www.onion-router.net/.
[10] http://www.research.att.com/projects/crowds/.
[11] http://pdos.lcs.mit.edu/tarzan/.
[12] http://www.gnu.org/software/GNUnet/.
[13] http://anon.inf.tu-dresden.de/.
[14] Die Vor- und Nachteile der Programmiersprache Java für JAP haben sich im Umfeld von Installation und Konfiguration deutlich gezeigt. Positiv ist, dass Nutzer von Nicht-Windows-Plattformen so in der Lage sind, unseren Dienst zu benutzen. Dies bedingte aber gleichzeitig, dass nur eine Version der Java-Ausführungsumgebung verwendet werden konnte, die auf möglichst vielen Plattformen vorinstalliert bzw. verfügbar ist. Die Wahl fiel auf Java 1.1, da diese Version z.B. in Microsoft Windows integriert und für MacOS 9 keine aktuellere Version verfügbar ist. Java 1.1 kann jedoch mittlerweile als veraltet angesehen werden (aktuell ist Version 1.4). Neuere Versionen besitzen einen wesentlich größeren Umfang an mitgelieferten Bibliotheken z.B. kryptographischen Funktionen. Der eingeschränkte Funktionsumfang von Java 1.1 erzeugte letztlich größeren Implementierungsaufwand, da eigene Entwicklungen benötigter Funktionen notwendig waren.

einer Meldung auf dem Heise-News-Ticker[15] vom Januar 2001 weckte der Dienst erstes öffentliches Interesse. In den folgenden Wochen stieg die Nutzerzahl auf durchschnittlich 200–300 Nutzer, die gleichzeitig über den Dienst surften. Im September 2001 benutzten durchschnittlich 500–600 Nutzer gleichzeitig den Anonymisierungsdienst. Ein Speicherausbau im Januar 2002 führte zu einer deutlichen Performancesteigerung des Dienstes, was wiederum zu einem Anstieg der Nutzerzahlen auf durchschnittlich 800–1.000 Nutzer führte. Momentan sind bis zu 2.000 Nutzer gleichzeitig online. Es werden ca. 4.000 Web-Requests pro Minute abgewickelt. Dabei wird täglich ein Datenvolumen von ca. 90–100 GByte verarbeitet.[16] Die Client-Software JAP wurde über 100.000mal von unserem Web-Server heruntergeladen, unsere Einstiegsseite mehr als 1 Millionen Mal besucht. Auf Grund der Art des Dienstes ist es schwierig, eine Aussage darüber zu treffen, wie viele Menschen unseren Dienst regelmäßig nutzen. Wir schätzen, dass dies ca. 20.000 sind.

Momentan sind drei Mixkaskaden im Betrieb. Zwei davon werden von uns vollständig kontrolliert. Bei der einen handelt es sich um eine „lokale“ Kaskade, die aus zwei Mixen auf einem Rechner in Dresden besteht. Die andere besteht aus zwei Mixen, die über das Internet verbunden sind – einer steht in Lübeck, einer in Dresden. Die dritte Kaskade wird in Kooperation mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) betrieben. Dabei soll herausgefunden werden, welche Probleme auftreten, wenn die Mixe einer Kaskade unabhängig betrieben werden.

Was die abgefragten Inhalte betrifft, so haben wir einige stichprobenartige Analysen durchgeführt. Dabei stellte sich heraus, dass es sich überwiegend um Seiten mit erotischem Inhalt handelte, insbesondere zu Beginn des Betriebes. Dies legt die Vermutung nahe, dass ein Anonymisierungsdienst zunächst von Menschen benutzt wird, die eine konkrete Vorstellung davon haben, wogegen sie sich schützen wollen. Mittlerweile zeichnet sich eine Veränderung dahingehend ab, dass „normale“ Internetseiten, die generell häufig abgerufen werden, auch über unseren Dienst angefragt werden. Sehr häufig werden Magazine wie heise.de, spiegel.de oder chip.de abgerufen. Dies legt nahe, dass die JAP-Benutzer ihre Unbeobachtbarkeit beim Offline-Lesen von Zeitungen auch online erhalten wollen. Besonders häufig sind auch Seiten von eBay, Yahoo oder Google vertreten. Seiten aus .com-Domainen, werden wesentlich häufiger abgefragt (ca. 50%) als Seiten aus .de- (ca. 25%) und .net-Domainen (ca. 8%).

Bei den meisten Anfragen handelt es sich um HTTP-Requests. FTP-Anfragen machen weniger als 0,05% aus. Anders sieht dies bei den übertragenen Datenmengen aus, da FTP speziell zum Übertragen von (großen) Dateien benutzt wird. Der Anteil des FTP-Datenverkehrs beträgt ca. 5-10% am gesamten Übertragungsvolumen.

Die Anzahl der Anfragen sinkt in den Morgenstunden und ist tagsüber nahezu gleichverteilt. Da der Dienst hauptsächlich im deutschsprachigen Raum beworben wurde, vermuten wir, dass unsere Nutzer hauptsächlich von dort kommen.

Obwohl wir den Dienst kostenlos und unverbindlich anbieten, entsteht bei den Nutzern eine große Erwartungshaltung bzgl. der Verfügbarkeit des Systems. Daher waren Veränderungen an dem stark genutzten Testsystem (z.B. Update der Mixsoftware) nur eingeschränkt durchführbar. Als eine Lösung weisen wir auf unseren Web-Seiten auf „Service-Zeiten“ hin (montags und mittwochs 14.00-16.00), in denen wir solche Wartungsarbeiten durchführen. Generell erzeugt die Gewährleistung einer hohen Verfügbarkeit einen nicht zu unterschätzenden Aufwand. Fehler im System müssen umgehend beseitigt werden. Außerdem muss die zu Grunde liegende Betriebssystemsoftware stets auf dem aktuellen Stand gehalten werden (Einspielen von Sicherheitspatches, Updates etc.) – was natürlich insbesondere für einen Internet-Dienst wichtig ist.

Problematisch gestalten sich auch Änderungen an dem zugrundeliegenden Anonymisierungsprotokoll. Anonymität bedingt, dass sich möglichst viele Menschen gleich verhalten, so dass ein einzelner innerhalb der Gruppe nicht zu identifizieren ist. Dies bedeutet, dass alle Benutzer einer Kaskade dasselbe Protokoll verwenden, da sie sonst anhand der verwendeten Protokollversion unterscheidbar wären. Veränderungen am Mixprotokoll bedingen also, dass die JAP-Software aller Nutzer auf denselben Stand gebracht werden muss. Wir haben deshalb einen halbautomatischen Updatemechanismus implementiert: Verbindet sich JAP zu einer Kaskade mit neuerem Protokoll, so wird dem Nutzer nahegelegt, ein Update von JAP – automatisch oder manuell – durchzuführen. Andernfalls ist eine Nutzung der betreffenden Kaskade nicht möglich.

3.2 JAP – Entwicklung, Installation, Konfiguration

Ziel war es, dass auch der Internet-Laie, der keine umfangreichen Kenntnisse auf dem Gebiet der Sicherheit hat, unseren Dienst nutzen kann. Installation und Konfiguration sollten daher so einfach wie möglich sein. Wir haben versucht, durch eine umfangreiche Frage-Antwort-Liste (FAQ) auf unseren Webseiten für möglichst viele Probleme dem Nutzer eine Lösung zu geben. Außerdem haben wir unter jap@inf.tu-dresden.de eine Support-Mailaddresse eingerichtet. Dabei wuchs der Aufwand für diesen Support mit der ständigen Zunahme der Nutzergruppe beträchtlich.

Im betrieblichen Umfeld bzw. in Ländern mit restriktivem Internet-Zugang existieren häufig Firewalls, auf deren Konfiguration der Nutzer keinen Einfluss hat. Meistens müssen zusätzlich „Zwangsproxies“ verwendet werden, z.B. ein HTTP-Proxy, um ins Internet zu gelangen.[17]

[15] „TU-Software schützt vor Datenschnüfflern“; http://www.heise.de/newsticker/data/wst-10.01.01-000/default.shtml.

[16] Zum Vergleich: Das Onion-Routing-Projekt gibt auf seinen Webseiten eine Zahl von täglich etwa 50.000 Web-Zugriffen an.

[17] Um auch diesen Menschen den Zugang zum Dienst zu ermöglichen, wurden eine Reihe von Strategien verfolgt:

1. InfoService und Mixe lauschen auf einer Reihe von Ports, bei denen die Chance groß ist, dass sie nicht durch eine Firewall geblockt sind z.B. 80 (HTTP), 443 (HTTPS) oder 22 (SSH).
2. Die Kommunikation zwischen JAP und InfoService erfolgt mittels HTTP, da in den allermeisten Fällen des kontrollierten Internetzugangs zumindest der Web-Zugriff möglich ist. Für den Zugang zum Mix war diese Strategie nicht möglich, da dass HTTP-Protokoll nicht die dafür notwendigen Eigenschaften besitzt (permanente Vollduplex-Verbindung).
3. JAP unterstützt den Zugriff auf das Internet über SOCKS- und HTTP-Proxies. Beim HTTP-Proxy-Protokoll wird insb. der CONNECT-Befehl verwendet, der den Aufbau einer „normalen“ TCP/IP-Verbindung ermöglicht.

Dadurch kann ein Großteil der zuvor ausgeschlossenen Personen unseren Dienst nutzen. Generell lässt sich ableiten, dass man Systeme so entwickeln sollte, dass möglichst wenige Verbindungen zu externen Servern benötigt werden (in unserem Fall zwei: eine zum InfoService und eine zum Mix). Eingehende Verbindungen sollten

3.3 Mixe – Entwicklung, Installation, Konfiguration

Beim Design der Mixe sind wir zunächst davon ausgegangen, dass Installation und Betrieb nur durch professionelle Administratoren erfolgen. Anfangs war die Konfiguration recht kompliziert, wodurch potenzielle Mixbetreiber abgeschreckt wurden, die uns zunächst entsprechende Bereitschaft signalisiert hatten. Daher entschlossen wir uns zur Entwicklung eines Konfigurationsprogramms. Es befindet sich momentan in der Entwicklung; erste Erfahrungen wurden bei der ULD-Mixinstallation gesammelt.

3.4 Open-Source

Alle von uns entwickelten Quelltexte stehen unter einer BSD-artigen Lizenz und können als Open-Source aus dem Internet heruntergeladen werden. Gleichzeitig haben wir bei SourceForge[18] ein Projekt eingerichtet. Wir haben nur wenig Hilfe von externen Entwicklern erhalten, jedoch auch nicht viel Werbung für das Mitentwickeln gemacht. Da es sich bei dem Anonymisierungsdienst um ein Forschungsvorhaben handelt, ist allerdings auch entsprechendes Spezialwissen notwendig, um die zu implementierenden Algorithmen und Komponenten erst einmal zu verstehen.

3.5 Missbrauch

Leider wird solch ein Anonymisierungsdienst auch missbraucht.[19] Daher haben wir von Anfang an versucht, das Missbrauchspotenzial unseres Dienstes zu minimieren. So ist die Möglichkeit der Anonymisierung einer allgemeinen TCP/IP-Verbindung zwar implementiert, aber nicht aktiviert, da wir darin ein zu großes Risiko für Hacking bzw. Denial-of-Service-Angriffe sehen. Der Dienst unterstützt momentan nur das Abrufen von Informationen aus dem Web.

Trotzdem kam es zu einer Reihe von Missbrauchsfällen.[20] In Auskunftsersuchen der Polizei wird etwa 1-2 Mal pro Monat darum gebeten, alle Informationen bezüglich der IP-Adressen 141.76.1.121 bzw. 141.76.1.122[21] zu dem Zeitpunkt *x* herauszugeben. Der Zeitpunkt liegt meist Monate vor dem Eingang des Schreibens.[22] Da keine Informationen mitgeloggt werden, können wir keine sachdienlichen Hinweise geben. Da der Betrieb unseres Dienstes gesetzeskonform[23] ist, wurden unsere Antworten seitens der Strafverfolgungsbehörden akzeptiert. Weiterführende Maßnahmen, wie etwa Durchsuchungen oder Beschlagnahme von Geräten, gab es nicht.

Wie könnte man in berechtigten Fällen (richterliche Anordnung etc.) eine Deanonymisierung durchführen, ohne das Risiko einer Massenüberwachung oder Vorratsdatenspeicherung? Eine Möglichkeit wäre eine Art „Online"-Überwachung, bei der ähnlich der Telefonüberwachung nur der im Moment ausgeführte Zugriff zurückverfolgbar ist, jedoch nicht rückwirkend deanonymisiert werden kann.

In persönlichen Gesprächen mit Ermittlern wurde jedoch signalisiert, dass solche Online-Ermittlungsmöglichkeiten im Bereich Internet nichts bringen würden, weil ja mit den Ermittlungen erst begonnen werde, „wenn alles längst vorbei ist". Obwohl im Polizeibereich JAP sogar bei Planspielen zur Bekämpfung von Internetkriminalität vorkommt, zeigen sich die Behörden sehr zögerlich bei der Definition ihrer Anforderungen.[24]

3.6 „Positiv"-Missbrauch

Unser Dienst wird auch für Zwecke benutzt, für die er nicht unmittelbar entwickelt wurde. Dazu zählt die Umgehung von Internet-Zensurmaßnahmen. Menschen aus Ländern mit restriktivem Internetzugang benutzen unseren Dienst, um darüber auf das gesamte Netz zugreifen zu können. Aus Saudi-Arabien wurde uns berichtet, dass der Zugriff aufs Netz nur über einen staatlich kontrollierten Proxy möglich ist.

Da momentan nur einige wenige Zugangspunkte existieren, ist eine Sperre unseres 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."

Diese Erfahrungen führten zu Überlegungen, wie ein Sperren des Dienstes erschwert werden kann. Beispielsweise könnten JAP-Nutzer es anderen Menschen ermöglichen, über ihre Rechner Zugriff auf den Anonymisierungsdienst zu erlangen. In diesem Fall müssten die Sperrlisten ständig angepasst werden. Die Information, welche Zugangspunkte zum Anonymisierungsdienst existieren, könnte über zensurresistente Publikationssysteme (z.B. Peer-To-Peer-Netze) verteilt werden.

Fazit

Am Schluss sollen kurz einige unserer Erfahrungen zusammengefasst werden:

- Java als Programmiersprache ist gut für die Verfügbarkeit auf vielen Plattformen, sofern man sich auf den Sprachumfang älterer Versionen beschränkt. Dies ist jedoch problematisch bei der Implementierung von Sicherheitsfunktionen. Java besitzt Schwächen in Benutzbarkeit, Installation und Konfiguration.
- Firewalls sind ein Problem beim Anbieten bestimmter Dienste, so dass das Design notgedrungen auf wenigen, tunnelfähigen Verbindungen beruhen wird.
- Missbrauch von Anonymisierungsdiensten findet statt. Allerdings ist die Missbrauchshäufigkeit wesentlich geringer, als allgemein befürchtet.

clientseitig nicht notwendig sein. Außerdem sollten die Protokolle so gewählt werden, dass sie sich über vorhandene Proxies tunneln lassen.

Nicht verschwiegen werden soll, dass diese Art der Umgehung von „Zwangsproxies" insb. im betrieblichen Umfeld nur erfolgen sollte, wenn entsprechende Betriebsvereinbarung etc. dies nicht explizit verbieten. Gerade wenn der Proxy nicht nur die reine Weiterleitung von Daten übernimmt, sondern auch noch potenziell gefährliche Inhalte filtert. Da die Kommunikation zwischen JAP und Anonymisierungsdienst verschlüsselt erfolgt, greifen diese Schutzmaßnahmen nicht mehr.

[18] http://www.sourceforge.net, ein bekannter Server für Open-Source-Projekte, der die zur Durchführung und Betreuung notwendige Infrastruktur wie Diskussionsforen, Mailinglisten, Quelltext-Versionsverwaltung etc. anbietet.

[19] S.a. die Missbrauchsanalyse, die die Betreiber des „Freedom"-Dienstes veröffentlicht haben (David Bratzer/Andrew Elkin: „Freedom 2.2 Abuse Issues and Analysis", ZKS Inc., davidb@zeroknowledge.com, June 14, 2001). Unsere Erfahrungen bestätigen dies.

[20] S.a. Beitrag Golembiewski in diesem Heft.

[21] Dies sind die nach außen sichtbaren IP-Adressen des Anonymisierungsdienstes.

[22] So traf beispielsweise die erste Anfrage bei uns am 24. Juli 2001 ein, bei dem es um den Missbrauchszeitpunkt 25. April 2001 ging.

[23] Basierend auf § 4 Abs. 6 TDDSG.

[24] Im Abschlussbericht zum Projekt Strategische Kriminalitätsanalyse im Bundeskriminalamt (Juni 2002) wird dies kritisch angemerkt: „... 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...".