

# Anonymität – Die Kehrseite der Medaille

Germano Caronni

*Das Internet ist bei weitem nicht so anonym, wie es auf den ersten Blick erscheint. Ein Großteil der Aktivitäten eines Benutzers lassen sich zu diesem zurückverfolgen. Das ist in der Regel auch kein Problem; unter bestimmten Umständen kann es jedoch von Vorteil sein, sich anonym äußern zu können, ohne Konsequenzen oder Repressalien befürchten zu müssen. Dafür wurden anonymisierende Dienste geschaffen.*

*Der vorliegende Beitrag untersucht die Mißbrauchsmöglichkeiten, die anonymisierende Dienste erlauben. Dazu wurde der Verkehr eines „Mixmaster“-Remailers beobachtet und ausgewertet. Schließlich wird dargestellt, wie sich Benutzer und Betreiber vor solchem Mißbrauch schützen können.*



Germano Caronni

Internet Commerce and Security Group,  
Sun Microsystems Inc., Palo Alto

E-Mail: gec@acm.org

## Einleitung

Die Möglichkeit, im Internet anonym Dienste zu nutzen, insbesondere anonym elektronische Briefe (E-Mails) zu verschicken, ist im Sinne des Datenschutzes sehr zu begrüßen.<sup>1</sup> Redefreiheit und freie Meinungsäußerung werden gefördert, da niemand direkt eine Nachricht einer Person zuordnen und diese ungerechtfertigterweise benachteiligen oder anderweitig zur Rechenschaft ziehen kann. Dies kann zum Beispiel für Mitglieder verfolgter Minderheiten wichtig sein, die miteinander kommunizieren wollen, oder auch für Menschen, die bestehende Mißstände in ihrer Firma oder andernorts aufdecken oder ein Verbrechen aufklären wollen.

Anonymität kann auch für den „gewöhnlichen“ Internet-Benutzer von Vorteil sein, wenn er zum Beispiel verhindern möchte, als Reaktion auf seine Usenet Postings (öffentliche Nachrichten an eine Newsgroup) seinen privaten Briefkasten mit Werbung und Spam gefüllt zu sehen, oder, wie tatsächlich vorgekommen, von einem Arbeitgeber mit anderen persönlichen Ansichten aufgrund eines Usenet Postings plötzlich am Arbeitsplatz diskriminiert zu werden.

## Formen des Mißbrauchs

Der vorliegende Beitrag setzt sich im Kontext elektronische Post und News mit der Kehrseite der Medaille „Anonymität“ auseinander. Der Mißbrauch dieser Dienste ist ein bedauerliches aber unumstößliches Faktum, das schon verschiedentlich beobachtet wurde [1] und hier näher untersucht werden soll.

Um dazu hinlänglich aussagekräftiges Zahlenmaterial zu gewinnen, wurde ein

anonymer Remailer vom Typ „Mixmaster“ [2] ausgewählt und der ausgehende Verkehr beobachtet.

Ein Mixmaster<sup>2</sup> erlaubt die Weiterleitung von Nachrichten entweder direkt an eine Person oder an eine Newsgroup, wo sie dann allgemein öffentlich zugänglich sind und auch in News-Archiven gespeichert werden können. Im Verlaufe einiger Monate sind etliche Mißbräuche sichtbar geworden, und die Verkehrsdaten und Inhalte für zehn Tage im September 1998 wurden detailliert untersucht (siehe auch weiter unten). Generell können zwei Sorten von „Mißbrauch“ unterschieden werden:

- ◆ Manche Personen nutzen den Schutz der Anonymität, um illegitime oder anstößige Handlungen begehen.
- ◆ Gewissen Kreisen und Organisationen ist die Existenz anonymer Remailer ein Dorn im Auge, und sie setzen alles daran, deren Betreiber unter Druck zu setzen und die Schließung des Dienstes zu erreichen.<sup>3</sup>

Zum ersten Punkt ist anzumerken, daß dabei der Unterschied zwischen illegitim und illegal wesentlich ist. Nicht alle Kulturen und Staaten haben das gleiche Rechtsverständnis, und Menschen nehmen ethische und moralische Verpflichtungen in unterschiedlichem Maße wahr. Markante Beispiele sind z. B. der Sicherheitsbeamte einer Großbank, der trotz Schweigepflicht gewisse Akten vor der Vernichtung bewahrt und sie der Presse zugänglich macht, oder ein Behördenmitarbeiter, der Mißstände trotz Schweigepflicht anprangert. Die Unterscheidung zwischen „richtig“ und „falsch“ ist sehr schwierig [4] und in letzter Konsequenz wohl jedem selber überlassen.

Während der zweite Punkt auf den ersten Blick nichts mit dem Mißbrauch eines Remailers zu tun hat, läßt sich doch ein Zusammenhang erkennen. Der Mißbrauch eines Remailers verärgert üblicherweise die

<sup>1</sup> Siehe auch „Datenschutzfreundliche Technologien“, AK Technik der Datenschutzbeauftragten, DuD 12/1997, S. 709 ff.

<sup>2</sup> Siehe dazu auch den Artikel „Anonymität im Internet“ von T. Roessler in diesem Heft.

<sup>3</sup> Dies wurde bspw. beim anonymen Remailer „anon.penet.fi“ erreicht.

Empfänger der anonymen E-Mails: Sie belegen Bandbreite, Zeit und verursachen Kosten. Menschen, deren Interessen durch anonymisierende Dienste behindert werden, mißbrauchen diese möglicherweise zum Zweck der Diffamierung und um sie unbeliebt zu machen.

## Verkehrsdaten

Wie oben erwähnt wurde der Verkehr eines „Mixmaster“-Remailers für elf Tage im September 1998 ausgewertet. Nachfolgend wird das eigentliche Verkehrsaufkommen dargestellt, und für einen Teil des lesbaren Verkehrs eine Inhaltsklassifizierung vorgenommen.

Mixmaster erhalten für sie verschlüsselte Nachrichten als Eingang und entschlüsseln diese. Das Resultat ist entweder für einen anderen Mixmaster bestimmt und wird an diesen weitergeleitet, oder es wird an eine Person oder eine Newsgroup ausgeliefert. Nur der Verkehr, der im Klartext ausgeliefert wird, kann weiter betrachtet werden.

Deshalb ist die vorliegende Aufstellung nicht vollständig. Sie ergibt einen guten Querschnitt durch das tatsächliche Verkehrsaufkommen und die verschiedenen Verwendungszwecke.

Abbildung 1 gibt einen Überblick über den Verkehrsverlauf für elf Tage im September dieses Jahres. Hierbei entspricht der Verkehr jedes Tages einem Balken. Am Tag werden 100 bis 600 Nachrichten in Empfang genommen, die entweder von anderen Remailern stammen, oder direkt von Benutzern eingespeist werden. Sie sind verschlüsselt und durch die „Eingang“-Balken dargestellt. Der größte Teil dieses Eingangs wird als verschlüsselte Nachricht an andere Mixmaster weitergereicht, und nur der als „Ausgang“ bezeichnete Teil (ca. 50-100 Nachrichten) ist für Endbenutzer oder

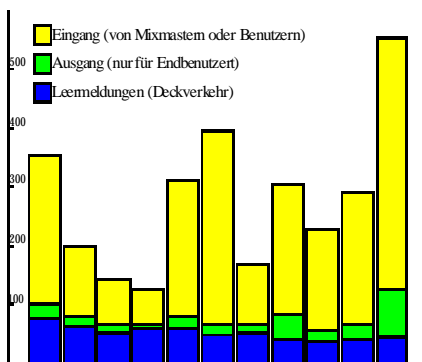


Abb. 1: Verkehrsverlauf

oder Newsgroups bestimmt. Davon ist ein großer Teil „Leermeldungen“, und nur der Mittelstreifen stellt die von diesem Mixmaster ausgehenden interessanten Nutznachrichten dar.

Der beobachtete Mixmaster kommuniziert mit zwei Dutzend gleichberechtigten System, die zusammen einen Verbund bilden. Der anonyme Gesamtverkehr ist also wesentlich größer als der hier beobachtete Ausschnitt<sup>4</sup>. Die im Klartext verfügbaren Nachrichten wurden nun weiter betrachtet. Verblüffenderweise waren bei weitem nicht alle Daten auf dem Pfad vom Mixmaster zum Benutzer verschlüsselt – dies hätte z. B. unter Verwendung von PGP mit Hilfe des öffentlichen Schlüssels des Empfängers geschehen können.

Mißbräuche mit dem klaren Ziel, den Remailer-Dienst oder seinen Betreiber zu diskreditieren, waren kaum zu beobachten. Der eigentliche Mißbrauch von Anonymität an und für sich wiegt hingegen sehr stark. Tabelle 1 zeigt eine Unterteilung der lesbaren Nachrichten in verschiedene Klassen.

Tabelle 1: Klassifiziertes Verkehrsaufkommen

	Sa	So	Mo	Di	Mi	Do	Fr	Sa	So	Mo	Di
<b>T-1</b>	-	4	-	5	10	2	6	4	1	2	6
<b>PGP</b>	-	4	7	1	2	-	-	1	-	1	7
<b>Test</b>	1	1	-	-	1	6	4	5	7	4	9
<b>Spam</b>	-	1	-	-	3	1	6	6	2	3	21
<b>Order</b>	-	-	2	-	-	-	1	-	1	-	2
<b>Insult</b>	3	1	-	-	-	4	2	2	2	2	8
<b>News</b>	1	5	7	1	5	1	5	8	2	3	12
<b>Total</b>	25	19	14	8	21	18	14	42	18	25	81

Klassen.

- ◆ T-1: Verschlüsselte Meldungen, die an anonyme Remailer vom Typ „1“ weitergeleitet werden.
- ◆ PGP: Verschlüsselte Meldungen, die an Benutzer oder Usenet Newsgroups weitergeleitet werden.
- ◆ Test: Testmeldungen von Benutzern.
- ◆ Spam: Werbung für Erotik, Multilevel-Marketing und andere Dienste und Produkte.
- ◆ Order: Bestellungen von Material übers Internet.

<sup>4</sup> Aufgrund der unterschiedlichen Verkettungslänge anonymer Nachrichten kann das vollständige Verkehrsaufkommen nur vermutet werden, es dürfte aber mindestens das Zehnfache betragen.

- ◆ Insult: Persönliche Beschimpfungen, Drohungen oder Beleidigungen.
- ◆ News: Nachrichten, die in Newsgroups eingespeist werden (nicht notwendigerweise mißbräuchlich).
- ◆ Total: Die Gesamtzahl an beobachteten Nachrichten. Dies schließt auch die sinnvollen Nachrichten ein, auf die im vorliegenden Beitrag nicht weiter eingegangen wird.

Die stärksten während der Untersuchung beobachteten Formen von Mißbrauch bestanden aus: Morddrohungen und Beschimpfungen, sexuellen und persönlichen Belästigungen in verschiedenster Stärke<sup>5</sup>, Steuerbetrug und Anleitungen zum Erhalt und Aufbewahren von Kinderpornographie. Des weiteren tauchten politisch und religiös extrem radikale Meinungsäußerungen, Verschwörungstheorien, sowie drogen- und waffenbezogene Nachrichten auf. Daneben war auch das Verschicken von Werbetrieben für Erotikprodukte und -dienste und Multilevel-Marketing, Kettenbriefen, Software-Piraterie und Haßbriefen zu beobachten.

beobachten.

## Gegenmaßnahmen

Ein kategorisches Filtern, oder um präziser zu sein, Zensieren von Nachrichten, die durch den Mixmaster gehen, ist wegen des damit verbundenen Aufwands weder vertretbar noch ist es technisch leicht durchführbar. Zudem widerspricht es der Idee des unkontrollierten und freien Meinungsaustausches und ist somit für die meisten Betreiber von Remailern unakzeptabel. Genausowenig können Nachrichten zum Absender zurückverfolgt werden, um im Be-

<sup>5</sup> Die Umstände eines Extremfalls, der während der Untersuchung auftauchte sind in [3] ausführlich dargelegt.

werden, um im Bedarfsfalle weitergehende Sanktionen ergreifen zu können. Unabhängig davon, ob eine Nachricht legitim ist oder nicht, sind doch alle Benutzer gleich stark geschützt.

Zudem muß man sich bewußt sein, daß es sehr einfach möglich ist, temporär Zugang zum Internet zu erhalten, um „anonym“ Nachrichten verschicken zu können. Es reicht, z. B. ein AOL-Konto mit einer Handvoll Freistunden zu eröffnen oder einen Proxy (wie *www.hotmail.com*) zu verwenden, oder auch nur von einem lokalen Provider ein „Testkonto“ zu erbiten, und dieses dann zum Verschicken der offensiven Nachrichten zu verwenden. Bevor Regreß geübt werden kann, werden dann das Konto abgemeldet und die Spuren verwischt. Mixmaster machen den Mißbrauch von Anonymität also nicht an und für sich erst möglich, sondern können wie andere Dienste auch in diesem Sinne zweckfremdet werden.

Stereotyper Spam und Junkmail wird von den meisten Remailern einfach und automatisch abgefangen, da sie gewissen gebräuchlichen Mustern folgen. So werden z. B. alle Nachrichten, die an mehr als zwei oder drei Newsgroups zugleich ausgeliefert werden sollen, blockiert, oder solche, die an übermäßig viele Benutzer gleichzeitig adressiert sind.

Benutzer, die sich durch Nachrichten angegriffen oder belästigt fühlen, die durch den Mixmaster weitergeleitet werden, können den Betreiber dazu auffordern, ihnen keine anonymen Nachrichten mehr zuzustellen. Dies ist eine sehr wirksame Maßnahme, die durchaus vertretbar ist, da sie auf Aufforderung des Empfängers ausgeführt wird. Die Methode hat sich bewährt und wird gern genutzt.

Eine mögliche zukünftige Lösung könnte darin bestehen, keine Nachrichten auszuliefern, die nicht verschlüsselt sind. Zum einen muß dann der Sender die Meldung speziell für den Empfänger vorbereiten, und somit auch gewissen Aufwand treiben – Mißbrauch wird so erschwert. Zum anderen kann der Mixmaster-Betreiber dann nicht mehr mitlesen, filtern oder zensurieren.

## Fazit

In diesem Beitrag wurden die Schattenseiten anonymer Remailer betrachtet. Bei all dem mit Mißbrauch verbundenen Ärgernis fällt es manchmal schwer, die sinnvollen Nutzungen nicht aus dem Blick zu verlieren. Dennoch: Im Zeitraum der Untersuchung wurden viele wertvolle Nachrichten von Menschen befördert, die sich sonst kaum hätten unerkant oder frei aussprechen können. Darunter fallen folgende ganz

Darunter fallen folgende ganz konkreten Beispiele:

- ◆ Aufdecken von Mißständen in der Wirtschaft, in Behörden und Sekten (z. B. Scientology)
- ◆ Aussprachemöglichkeit für mißhandelte Ehepartner und Kinder
- ◆ Foren für verfolgte Minderheiten (politische, religiöse und andere)

Diese und andere ähnliche Nutzungen sind es wert, die Nachteile, wie sie hier beleuchtet wurden, in Kauf zu nehmen – als Preis für unser aller Freiheit.

## Literatur

- [1] D. Mazières, M. F. Kaashoek, *The Design, Implementation and Operation of an Email Pseudonym Server*, Proceedings of the 5th ACM Conference on Computer and Communication Security, 1998.
- [2] L. Cottrell, *Frequently Asked Questions about Mixmaster Remailers*, 1996. (See also: <http://www.obscura.com/~loki/remailer/mixmaster-faq.html>)
- [3] C. L. Armistead, *Harrassed*, 1998. (See <http://www.technomom.com/harrassed/>)
- [4] G. B. Lee, *Addressing Anonymous Messages in Cyberspace*, Journal of Computer-Mediated Communication, vol. 2, no. 1, 1996. (See also: <http://www.usc.edu/dept/annenbergl/vol2/issue1/anon.html>)