F A C H H O C H S C H U L E W E D E L

S E M I N A R A R B E I T

in der Fachrichtung
IT-Sicherheit
Wintersemester 2015/2016

Seminar: IT-Sicherheit

Thema:

Anonymität im frühen Internet – anon.penet.fi und co.

Eingereicht von: Jana Lübkemann (Matrikelnr. winf100191)
E-Mail: winf100191@fh-wedel.de

Erarbeitet im: 7. Semester

Abgegeben am: 17.11.2015.

Betreuer: Prof. Dr. Gerd Beuster
Fachhochschule Wedel
Feldstraße 143
22880 Wedel

Gliederung

Inhaltsverzeichnis

1 Einführung

1.1 Problemstellung

Die Sicherheit im Internet spielt in der heutigen Zeit eine zunehmend wichtige Rolle. Ein Großteil der deutschen Bevölkerung ist beispielsweise täglich mehrere Stunden im Internet.

Diese Arbeit befasst sich mit den Ursprüngen des Internets, sowie das Entstehen der ersten Sicherheitsgedanken in den zur damaligen Zeit innovativen Netzwerken. Es entstanden nach und nach verschiedene Verschlüsselungsverfahren. Im Folgenden wird deren Entstehung und Entwicklung betrachtet.

1.2 Gang der Untersuchung

Diese Seminararbeit soll einen Überblick über die Entstehung des Internets und die zu der Zeit verwendeten Verschlüsselungs- und Anonymisierungstechniken geben. Begonnen hat alles mit dem ARPANET und dem Wunsch, untereinander auch über weite Entfernungen Informationen auszutauschen. Aus dem gleichen Wunsch heraus entstanden einige Jahre später das Usenet und die sogenannten Bulletin Board Systems (Mailboxen). Eines der ersten Verschlüsselungsverfahren war der Data Encryption Standard, welcher ein symmetrisches Verschlüsselungsverfahren verwendete. Bereits kurze Zeit später entstand die sogenannte Public Key Verschlüsselung, die auf asymmetrische Verschlüsselungsverfahren zurückgreifen konnte. In diesem Zeitraum entstand auch das bekannte Pretty Good Privercy Verfahren von Phil Zimmermann. Darüber hinaus entwickelte sich der erste Remailer (Typ 0). Mit dem anan.penet.fi Remailer war es nun möglich, anonymisierte Nachrichten zu verschicken.

2 Theoretische Grundlagen

2.1 Das ARPANET

Die Anfänge des Internets wurden von dem Forscher J.C.R. Licklider geprägt. Er entwickelte in den späten 1950er Jahren, zusammen mit einer Gruppe von Forschern, das erste Time-Sharing-System. Licklider wollte die Kommunikation zwischen Computern voranbringen. Im Jahr 1962 wurde er Leiter des Information Processing Techniques Office (IPTO), einer Abteilung der Advanced Research Projects Agency (ARPA). Ziel dieser Forschungsabteilung war es, eine Möglichkeit zu finden, wie Rechenzeit zwischen unterschiedlichen Computerzentren der ARPA geteilt werden kann.[1]

Am 29.10.1969 wurde die erste Nachricht von der University of California in Los Angeles an einen Computer im Stanford Research Institut verschickt. Die Nachricht sollte „log“ heißen, nach dem „o“ brach jedoch der Computer am SRI zusammen. Noch am gleichen Tag wurde ein erneuter Versuch durchgeführt und dieses Mal kam das gesamte Wort an. Sechs Wochen später wurden die University of California (Santa Babara) und die University of Utah in das Netzwerk integriert.[2]

Für die Übertragung der Daten wurde erstmals die Paketvermittlung als Übertragungstechnologie verwendet. Die Paketvermittlung wurde unabhängig voneinander von Paul Baran und Donald Davies erfunden. Paul Baran schickte seine Entwicklung an das Verteidigungsministerium mit dem Hintergedanken ein Kommunikationsnetzwerk zu schaffen, dass selbst einen Atomangriff überstehen könnte.

Ungefähr zur selben Zeit entwickelte Steve Crocker den ersten Request for Comments (RFC), der die technischen Standards des Internets spezifizieren sollte. Aus diesem RFC ging später das Network Control Protocol (NCP), das erste ARPANET Protokoll hervor.

1972 wurde das ARPANET auf der International Conference on Computer Communications in Washington zum ersten Mal öffentlich vorgestellt. Das nächste Problem, welches es zu lösen galt, war die Kommunikation von Computernetzwerken. Bereits ein Jahr später hatte ein Team von internationalen Forschern die Lösung in Form des Transmission Control Protocols (TCP) gefunden. 1978 wurde das TCP zum TCP/IP-Protokoll weiterentwickelt.

[1] Castells, Die Internet-Galaxie (S. 20)
[2] (Kluy, 2007)

1983 wurde das ARPANET aus Sicherheitsgründen in das ARPA-Internet, welches für die Forschung gedacht war und das MILNET, welches ausschließlich für die militärische Nutzung gedacht war, aufgeteilt. 1990 wurde das ARPANET in seiner ursprünglichen Form aufgegeben. Dafür errichteten eine Reihe von privaten Providern eigene Netzwerke für die kommerzielle Nutzung.

2.2 Das Usenet

Die Geschichte des Usenet

Das Usenet entstand durch den Wunsch der drei Studenten „Tom Truscott“, „Jim Ellis“ und „Steve Bellowin“, über ein Netzwerk zu kommunizieren.[3] Da das ARPANET nur für Wissenschaftler, die an einem Projekt für das Verteidigungsministerium teilnahmen zugänglich war, entwickelten sie ein eigenes Netzwerk, worüber sie Informationen austauschen konnten. Zur Umsetzung verwendeten sie das UUCP-Softwarepaket, welches bei UNIX-Systemen mitgeliefert wurde. Erst durch die Anbindung ans ARPANET und die Umstellung auf das TCP/IP Protokoll konnte das Usenet auch von anderen Betriebssystemen als Unix verwendet werden.

Um eine gewisse Struktur in das Usenet zu bekommen, unterteilte man die Diskussionsräume in die drei Namensbereiche:

- net → für Usenet Gruppen
- fa → als Abkürzung für „from ARPANET“
- mod → für moderierte Gruppen.[4]

Doch diese Unterteilung reichte nicht. Durch das stetige Wachstum des Usenet und der steigenden Anzahl der Artikel wurde das Usenet immer undurchsichtiger. 1986 entstand die Top-Level-Hierarchie. Diese 7 Themenbereiche werden auch die „Big Seven“ genannt und werden wie folgt abgekürzt:

- comp → Themen rund um den Computer
- sci → wissenschaftliche Themen
- soc → Gesellschaftliche (soziale) Themen
- talk → Gespräche über allgemeine Themen

[3] Boris-A.Piwinger, 1997 (S.41 ff.)
[4] Boris-A.Piwinger, 1997 (S.203 ff.)

- rec → Freizeit-Themen
- news → Technik und z.B. das Usenet selbst
- misc → alles, was nirgendwo sonst zugeordnet werden kann.

Brian Reid erschuf 1989 einen weiteren Themenbereich (alt → alternativ), der bis heute jedoch noch kein offizieller Teil des Usenet ist. Dieser Themenbereich entstand, als eine Reaktion darauf, dass die Einrichtung der Newsgroups soc.sex und soc.drugs verweigert wurde. 1995 wurden die „Big Seven" um den Themenbereich humanities → Kultur und Geisteswissenschaften zu den „Big Eight" erweitert. Diese 8 Themenbereiche werden international auf allen News-Servern bereitgestellt.[5]

Die Netiquette

Die Netiquette ist ein Dokument, welches im Usenet entstanden ist und das gewünschte Verhalten im Usenet beschreibt. Es legt Regeln fest, wie im Usenet diskutiert werden soll. Einer der Hauptaspekte der Netiquette ist der Hinweis, dass man mit einen anderen Menschen diskutiert und nicht mit einen Computer. Gerade Neueinsteiger werden öfter auf die Netiquette hingewiesen. Zu finden ist die deutschsprachige Netiquette im Usenet unter: de.newusers.infos[6]

Anonymität im Usenet

Durch die dezentrale Verbindung der News-Server ist eine starke Anonymität für die User entstanden. Die Folge der dezentralen Struktur ist, dass heute keiner mehr weiß, wie viele Server, User oder Artikel es zurzeit im Usenet gibt. Die durchschnittliche, tägliche Uploadrate beträgt 16 Terabyte. Allein aufgrund dieser gewaltigen Menge an Informationen die täglich ins Usenet geladen werden, fällt es selbst Bundesbehörden schwer einen Überblick zu behalten. Die einzige Methode, die auch die Film-und Musikunternehmen verwenden, ist nach Schlüsselworten zu suchen. Für den Fall das ein Schlüsselwort gefunden wird, wird der Beitrag mit einer Originaldatei verglichen (denn es kann ja auch sein, dass z.B. nur über einen Film diskutiert wird). Wird jedoch eine Übereinstimmung zurückgemeldet, so muss der Ursprungs-News-Server den Beitrag wieder aus dem Usenet entfernen. Bei dem ganzen Vorgang macht sich jedoch keiner

[5] Boris-A.Piwinger, 1997 (S.204 ff.)
[6] Boris-A.Piwinger, 1997 (S.240 ff.)

die Mühe herauszufinden, wer den Beitrag gepostet hat. Der Download von Daten aus dem Usenet wird von keinem News-Server protokolliert und ist somit anonym.

2.3 Bulletin Board Systems (BBS)

Ein Bulletin Board System zu Deutsch Mailbox genannt, ist ein Rechnersystem, welches gerade Anfang der 1990er Jahre meistens in privater Hand lag. Seine Struktur bildete die Grundlage für das später entstandene Internet. In einer Mailbox besaß jeder Benutzer einen eigenen Bereich, wo Nachrichten empfangen und gespeichert werden konnten. Des Weiteren gab es eine große Anzahl an Foren, die genutzt werden konnten, um Informationen auszutauschen. In den meisten Mailboxen gab es zusätzlich einen Bereich, wo Software und andere Dateien heruntergeladen werden konnten. Durch diesen Bereich war es nun möglich, Updates oder Hilfsprogramme von zuhause aus runterzuladen und zu installieren, anstatt zum nächsten Händler zu gehen. Viele Mailboxen tauschten die Informationen auch untereinander aus, so dass schnell ein großes Netzwerk entstand. Im Folgenden werden einige Mailboxen etwas genauer betrachtet.

Das FidoNet

Das Fidonet war das weltweit größte Mailbox-Netz. Es wurde 1984 von Tom Jennings in den USA gegründet und nach seinem Hund „Fido“ benannt. Das Fidonet hatte eigene Protokolle, die das Kommunizieren auf zwei Weisen ermöglichte. Zum einen die direkte Kommunikation über sogenannte „Netmails“, die ähnlich, wie E-Mails funktionierten und zum anderen die Kommunikation über Echomails, die ähnlich wie das Usenet funktionierten.

Fast jedes Echo besitzt einen Moderator, der aufpasst, dass die Beiträge nicht zu stark vom eigentlichen Thema abweichen und dass die Regeln eingehalten werden. Die Regeln werden vom Moderator erstellt und einmal im Monat in das Echo geschrieben. Werden die Regeln nicht befolgt, gibt es zunächst eine Verwarnung. Bei weiteren Verstößen kann es dazu führen, dass der Benutzer zeitweise von dem Echo ausgeschlossen wird.

In diesem Zusammenhang entsteht immer wieder die Diskussion über den Klarnamenzwang. Im Fidonet, ähnlich wie im Usenet, ist das Schreiben unter einen Pseudonym nicht gerne gesehen. Es wird allgemein als unhöflich angesehen. Auf der anderen Seite der Diskussion steht der Glaube an die freie Äußerung der eigenen Meinung, die gerade bei prekären Themen nicht immer mit der eigenen Person in Verbindung gebracht werden soll.

Das Z-Netz

Das Z-Netz oder auch Zerberus-Netz war eines der ersten deutschsprachigen Mailboxnetze. Es umfasste Themen aus allen Bereichen, die oftmals auch nichts mit Computern zu tun hatten. Aus einzelnen Themenbereichen des Z-Netzes entstanden später neue Mailboxnetze, die sich auf die einzelnen Themen spezialisiert hatten, wie z.B. das CL-Netz. Darüber hinaus war das Z-Netz demokratisch organisiert. Das zeigte sich auch in der Wahl des Protokolls (ZConnect) zum Verschicken und Empfanden von E-Mails und News.

Das CL-Netz

Das CL-Netz entstand aus dem Z-Netz und wurde von Journalisten gegründet. Es befasste sich vorwiegend mit politischen Themen wie Menschenrecht und Umweltschutz, aber auch viele Friedensorganisationen tauschten sich über das CL-Netz aus. In Deutschland gestartet, verbreitete es sich schnell in anderen Ländern und schloss sich mit deren Netzen zusammen.

3 Sicherheit im frühen Internet

3.1 Anon.penet.fi und der Nym Remailer

Ein Remailer ist ein Computer, der eine E-Mail annimmt, sie so modifiziert, dass keine Rückschlüsse auf den wirklichen Absender gezogen werden können und die E-Mail danach an die ursprünglich vorgesehene Adresse weiterleitet. Der Nym Remailer oder auch Remailer vom Typ 0 genannt, war die erste Möglichkeit anonym Nachrichten mit dem Computer zu versenden. Der erste Nym Remailer war anon.penet.fi und wurde von Johan Helsingius erstellt.

Die Entstehung von anon.penet.fi war eine Reaktion auf eine Diskussion in einem Universitätsnetzwerk, wo es darum ging, dass jeder grundsätzlich seine echten Namen angeben soll, damit jeder für die Informationen, die geschrieben wurden greifbar sein konnte. Johan Helsingius, welcher ein starker Befürworter des freien Meinungsaustausches war, argumentierte dagegen. Zur Festigung seines Standpunktes entwickelte er innerhalb von zwei Tagen den anon.penet.fi Remailer.[7]

Funktionsweise:

Erreichte eine E-Mail den anon.penet.fi Remailer, so wurden alle Informationen über die Herkunft bzw. den Absender der E-Mail gelöscht und die E-Mailadresse durch anNNNN@anon.penet.fi ersetzt. Hierbei wurden die N jeweils durch Zahlen ersetzt. Die Zuordnung der anonymen E-Mailadresse und der echten E-Mailadresse wurde in einer Datenbank abgespeichert. Dies hatte den Vorteil, dass man auf die anonymen E-Mails antworten konnte, ohne dafür die wahre Identität des Absenders zu kennen. Der Nachteil ist jedoch, dass anhand der Datenbank die anonymen E-Mailadressen wieder den wahren Identitäten zugewiesen werden können. Genau diese Eigenschaft wurde Johan Helsingius letzten Endes zum Verhängnis.

Im Februar 1995 forderte Scientology Johan Helsingius auf einen Benutzer zu identifizieren und an Scientology weiterzuleiten. Der Benutzer sollte eine Datei vom internen Scientology-Computer gestohlen haben und in die Usenet Newsgroup alt.religion.scientology gestellt haben. Erst unter dem Zwang eines Durchsuchungsbefehls willigte Johan Helsingius ein, die wahre E-Mailadresse der anonymisierten E-Mailadresse an144108@anon.penet.fi herauszugeben. Es stellte sich heraus, dass die E-Mailadresse (tc@alumni.caltech.edu) von dem California Institut of Technology (Caltech)in Pasadena (Kalifornien) gehörte.

[7] Boris-A.Piwinger, 1997 (S.302 f.)

Der zweite Angriff von Scientology fand im Frühjahr 1996 statt. Scientology forderte Johan Helsingius auf zwei weitere Namen preiszugeben, die Daten von Scientology in der Usenet Newsgroup alt.religion.scientology gepostet hatten. Nachdem Helsingius um eine Vertagung der Gerichtsverhandlung gebeten hatte, wurde am 22.August 1996 das Urteil zu Gunsten von Scientology gefällt. Ein paar Tage später erschienen Artikel in der Zeitung „The Observer“ in denen es hieß, dass Helsingius es zugelassen hätte, dass durch anon.penet.fi anonym Kinder-pornographien verteilt worden sind. Johan Helsingius konnte diese Anschuldigungen schnell wiederlegen, da der Remailer nicht dazu in der Lage war Dateien in einer solchen Größe zu verwalten. Dennoch stellte Helsingius am 30. August 1996 die Dienste von anaon.penet.fi ein.

4 Fazit und Ausblick

Die Menschen haben sich schon in den Anfängen des Internets Gedanken über Ihre Anonymität und Sicherheit in den Netzwerken gemacht. Viele der damals entstandenen Verfahren werden noch heute verwendet. Auch die Frage des Verhaltens in den Netzwerken wird zu heutigen Zeiten immer wieder diskutiert. So hat z.B. Facebook die Diskussion um den Klarnamenzwang wieder aufleben lassen, die schon im Usenet und in den Mailboxen ein stark diskutiertes Thema war.

Literaturverzeichnis:

Boris-A.Piwinger, E. K. (1997). *Newsgroups: Weltweit diskutieren.* Bonn: International Thomas Publishing Company.

Castells, M. (2005). *Die Internet-Galaxie: Internet, Wirtschaft und Gesellschaft.* Berlin: VS Verlag für Sozialwissenschaften.

Kluy, A. (29. Oktober 2007). *Der 29. Oktober ist Internet-Tag.* Von www.welt.de: http://www.welt.de/welt_print/article1308095/Der-29-Oktober-ist-Internet-Tag.html abgerufen