Das Internet
Eine kurze Abhandlung über Vergangenheit, Gegenwart und Zukunft

Niels Provos

1 Einleitung

Der Begriff Internet bezeichnet das Netz zwischen den Netzen, das heute weltweit über zwei Millionen Computer miteinander verbindet. Es erlaubt einer noch viel größeren Anzahl von Menschen miteinander zu kommunizieren.

1.1 Entstehung des Internet

Das Internet entstand vor über 20 Jahren als ein Versuch, das Rechnernetz des Amerikanischen Verteidigungsministeriums mit verschiedenen anderen Funk- und Satellitennetzen zu verbinden. Das sogenannte ARPAnet war insbesondere darauf ausgelegt, teilweisen Ausfällen durch Bombenschäden zu widerstehen und trotzdem noch funktionsfähig zu sein, also auch dann, wenn ganze Teile des Netzes versagen [4]. Die Computer kennen nur ihre eigene Adresse und die des Ziels, so daß die zurückgelegten Wege sich jederzeit ändern können. Das Netz stellt nicht sicher, daß alle Pakete korrekt übermittelt werden. Diese Aufgabe übernimmt das Transmisson Control Protocol (TCP) [8]. Ungefähr zur selben Zeit enstanden auch lokale Netze (LAN) auf Ethernet Basis. Das von Berkley ausgelieferte `UNIX` enthielt bereits Internet Protocol (IP) Netz Software. Im Rahmen der National Science Foundation (NSF) und deren Netzen konnten sich akademische Einrichtungen am Internet beteiligen. Im Rahmen des Deutschen Forschungsnetzes e.V. (DFN) wurden 1991 auch Deutsche Universitäten und Forschungseinrichtungen angeschlossen. Heute kann jeder, der einen Computer und ein Telephon besitzt, am weltweiten Datennetz teilhaben.

1.2 Dienste

Eine Vielzahl von Protokollen, die alle auf TCP/IP aufbauen, regeln den Datenaustausch im Internet:

- SMTP - E-Mail wird durch das Simple Mail Transfer Protocol übertragen.
- FTP - Das File Transfer Protocol dient der Übertragung von Dateien, z.B. von großen Meßdaten aus einem Teilchendetektor auf einen Auswertungscomputer
- NNTP - Über das Network News Transfer Protocol werden die Artikel aus den ca. 16000 Diskussionsforen, zusammengefaßt im `USENET`, verteilt.
- HTTP - Das Hyper Text Transfer Protocol steckt hinter dem Modebegriff World Wide Web (WWW).

2 Cyberspace heute

In der Vergangenheit nahmen am Internet nur eine kleine Zahl von Akademikern teil. Die Gesetzgeber nahmen keine Kenntnis von dem Netz, das auch nicht auf eine große Masse von Teilnehmern ausgelegt war. An Systemsicherheit oder Privatsphäre wurde zunächst nicht gedacht [1]. Es herrschte Anarchie, für Hacker die goldenen Jahre. Heute tummeln sich immer mehr Menschen im Cyberspace[1], führen dort ein zweites Leben, das nicht durch Äußerlichkeiten wie Aussehen oder Herkunft beeinflußt ist. Trotzdem entsteht eine Gesellschaft, die mit Problemen zu kämpfen hat, wie es sie in der "Wirklichkeit" auch gibt [6]. Die unglaublichen Datenmengen, nicht zuletzt vervielfacht durch das WWW, in Insiderkreisen auch "World Wide Waste" genannt, bieten aber auch für die Nachrichtendienste eine wahre Fundgrube. E-Mail und Artikel aus dem `USENET` werden automatisch nach Schlagworten wie "CASTOR" oder "Kokain" durchsucht und bei Relevanz für spätere Bearbeitung archiviert. Für die verdachtslose Rasterfahndung könnten Möglichkeiten entstehen, die Orwells "1984" vergleichsweise harmlos erscheinen lassen.
Im Gegensatz dazu herrschte im Internet bisher

[1] William Gibson erfand den Begriff `cyberspace` als Synonym für die durch Computer- und Telekommunikationsnetze geschaffene Welt [3].

absolute Meinungsfreiheit. So lange der Beitrag im Rahmen der Netiquette (Leitfaden für das Benehmen im Netz) war, konnte jeder seine Meinung mitteilen, egal wie kontrovers sie war. Um auch über Themen wie "sexuellen Mißbrauch", "Sucht" oder "politische Verfolgung" sprechen zu können, wurden von den "Cypherpunks[2]" sogenannte "Anonyme Remailer" entwickelt, die mit Hilfe von starker Kryptographie[3] anonyme Mitteilungen erlauben. Einer der bekanntesten anonymen Remailer mußte vor kurzem schliessen, da auf Drängen von Scientology die finnische Polizei den Rechner fast beschlagnahmt hätte und der Betreiber auf eine klarere Rechtslage in Finnland warten will. Mit Verschlüsselungsprogrammen wie PGP (Pretty Good Privacy) können Internet Teilnehmer ohne Furcht vor Bespitzelung miteinander reden. Eine Kombination von beiden Methoden eröffnet noch viel mehr Möglichkeiten [9, 5]. Gerade diese Art der Kommunikation bereitet manchen Politikern immer mehr Sorge. Eine einfache Kontrolle des Bürgers und seiner Gedanken ist dadurch nicht mehr möglich. In Deutschland wurde durch das Telekommunikationsgesetz allerdings schon vorgebeugt. Leider ist Deutschland mittlerweile in der Welt für seine Zensurmaßnahmen bekannt. Vor einem Jahr hat Compuserve in Deutschland den Zugriff auf sämtlichen Newsgruppen, in deren Namen "sex" oder "gay" enthalten war, auf Anraten eines bayerischen Staatsanwalts gesperrt. Bei den meisten dieser Gruppen handelte es sich um Diskussionsforen, die sich mit den Problemen von Homosexuellen oder sexuell mißbrauchten Menschen beschäftigten. In Singapur und China müssen sich Teilnehmer anmelden und erhalten nur von einem zentralen Filter bearbeitete Informationen; vor allem unerwünschte Nachrichten aus dem westlichen Kulturkreis sollen aufgehalten werden. Man ist nur an "commerce" und "business" interessiert [2]. Die Filter sind jedoch noch nicht so weit entwickelt, daß sie den Möglichkeiten des Internets gewachsen wären: Ein bekanntes Beispiel ist die propagandistische Seite des kanadischen Neonazis Zündel. Er verbreitet die Meinung, daß Hitler nichts von der Massenvernichtung der Juden in Konzentrationslagern wußte. Ein für Deutschland wegen der noch fehlenden Vergangenheitsbewältigung besonders heikles Thema. In Deutschland wurde daraufhin der Zugriff auf den Rechner mit diesen Seiten sofort gesperrt, was zur Folge hatte, daß auf circa 3000 andere Angebote auch nicht mehr zugegriffen werden konnte. Passend zu dem Zitat

> Das Internet betrachtet Zensur als Störung und routet[4] um sie herum.

wuchsen Mirrorseiten[5] wie Pilze aus dem Boden. Innerhalb von Tagen war Zündels Gedankengut, auf der ganzen Welt verstreut, von unzähligen Rechnern erhältlich. Heute redet keiner mehr darüber. Um so erstaunlicher ist der neueste Zensurversuch durch die Internet Content Task Force (ICTF), einer Vereinigung von deutschen kommerziellen Internetprovidern, die dem Hinweis der Bundesanwaltschaft folgend den Zugriff auf den Rechner `xs4all.nl` zu sperren versuchte. `xs4all` ist im Internet vor allem durch den Prozeß gegen Scientology bekannt. Die neueste Ausgabe einer in Deutschland verbotenen linksextremistischen Zeitung war dort zu finden. Obwohl die Blockade dieses Rechners vier Wochen lang versucht wurde, gelang sie noch nicht einmal ansatzweise, da `xs4all` prompt durch Rotation ihrer Rechnernummern antwortete und innerhalb von wenigen Tagen, die Zeitung auch über vierzig andere Computer im Internet zu erhalten war.

3 Aussicht

Das Internet wird sich zwischen zwei Extremen einpendeln

- Informationen werden kontrolliert und reguliert. Nur regierungskonforme Firmen können Informationen anbieten, der Bürger wird wahrscheinlich ein dem heutigen Fernsehen ähnliches Angebot konsumieren.
- Jeder kann alles sagen. Der Informationsfluß wird überhaupt nicht gefiltert, Gedankengut wird frei ausgetauscht. Methoden zur Kryptographie oder Steganographie[6] sind frei erhältlich.

Um die erste Möglichkeit zu verhindern, muß die Gesellschaft sich damit anfreunden, daß die Welt zu einem globalen Dorf geworden ist. Der

[2] `Cypherpunks` sind Menschen, die sich der Kryptographie widmen. Sie schreiben Programme zum Schutz ihrer Privatsspähre[5]: *Cypherpunks write code.*

[3] Verschlüsselung, siehe Anhang

[4] Routen bezeichnet den Prozeß der Wegfindung im Internet, Störungen werden einfach umgangen.

[5] Mirrorseiten spiegeln den Inhalt anderer Seiten im WWW, häufig um das Netz zu entlasten.

[6] Steganographie bedeutet verstecktes Schreiben. Ein Dritter erkennt nicht, daß Mitteilungen versand werden.

Austausch zwischen den Bewohnern verschiedener Nationen führt auch zu einer kritischen Reflektion und Auseinandersetzung mit den jeweils vorherrschenden Ideologien. Dieses Umdenken ist nicht einfach, da vor allem auch der westliche Kulturkreis seine Kultur und Moralvorstellungen als universell ansieht. Andererseits bedarf es, um eine Kontrolle zu ermöglichen, internationaler Verträge, die jedes am Internet beteiligte Land anerkennen muß, oder einer Abschottung und Isolation des eigenen Landes, die heute schon nicht mehr möglich ist. Die USA versucht gerade, mit den G-7 Staaten ein Gesetz zur Kontrolle des Imports und Exports von kryptographischen Produkten durchzusetzen. Die Idee ist schon seit Jahren bekannt und jedes "Clipper"-Gesetz ist bisher in den Staaten gescheitert. Eine Infrastruktur zur "Keyrecovery" soll den Nachrichtendiensten das Entschlüsseln von Nachrichten ermöglichen. Die Möglichkeit, anonym ohne Angst vor Repressalien zu kommunizieren, wäre genommen. Damit ein solches Gesetz gelingen kann, muß schon vorhandene Kryptographiesoftware verboten werden und darf nicht mehr zugänglich sein.

Da im neuen Internet Protokol (IPng) potentiell für jedes Haushaltsgerät eine eigene Nummer vorgesehen ist und langfristig wohl fast alle Haushalte in irgendeiner Form angeschlossen werden, ergeben sich auch ganz neue Möglichkeiten für die Praxis einer Demokratie. Im Netz wird bereits heute über die Einrichtung von Newsgruppen und deren Charta abgestimmt. Dabei darf jeder teilnehmen, der sich für die Thematik dieser Newsgruppe interessiert. Im `USENET` stellt sich bei Diskussionen recht schnell ein gewisser Grundkonsens ein. Gegensätzliche Meinungen werden von allen Seiten beleuchtet und das Für und Wider erörtert. An einer Diskussion kann jeder teilnehmen. Je nachdem, wie qualifiziert die Äußerungen sind, wird auch mehr oder weniger auf einen Beitrag eingegangen. Ähnlich könnte man dieses Prinzip auch in der Politik umsetzen: Es wird erkannt, ob ein Problem besteht. Über dieses Problem wird diskutiert und ein Konsens gefunden. Der Konsens kann per Gesetz umgesetzt werden. Die Politikverdrossenheit und Entfremdung des Bürgers vom Staat entfällt durch die viel direktere Teilnahme an Entscheidungen. Voraussetzung dafür ist auf jeden Fall die freie Meinungsäußerung und die Privatssphäre jedes einzelnen. In Deutschland wird gerade an einem Gesetz zur Regulierung der Kryptographie gearbeitet. Auf Anfrage nach den bisherigen Ergebnissen, erhält man aber nur die Antwort, daß noch keine zur Öffentlichkeitsarbeit geeigneten Papiere vorhanden seien. Noch ist allerdings keine Entscheidug getroffen, und Dänemark hat vor kurzem ein Gesetz verabschiedet, das die uneingeschränkte Benutzung von Kryptographie gewährt.

A Kryptographie

Kryptographie ist die Wissenschaft der Verschlüsselung von Nachrichten. Sie ist die zentrale Methode, um vertrauliche Kommunikation, Anonymität und auch die Identifizierung von Benutzern zu gewährleisten. Mit starker Kryptographie bezeichnet man die Verfahren, die nach öffentlichen Wissen auch nicht mehr von Nachrichtendiensten in einer akzeptablen Zeit entschlüsselt werden können [7].

Literatur

[1] William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security Repelling the Willy Hacker*. Addison-Wesley Publishing Company, 1994.

[2] CUD. Computer Underground Digest, Jan, Oct 1996.

[3] William Gibson. *Neuromancer*. Victor Gollancz Ltd, 1984.

[4] E. Krol and E. Hoffman. FYI on "What is the Internet?", May 1993.

[5] Timothy May. Cyphernomicon. Gedanken über den Einsatz von Kryptographie bis zur Idee der Crypto-Anarchie.

[6] Elizabeth M. Reid. Electropolis: Communication and Community on Internet Relay Chat. Master's thesis, University of Melbourne Department of History, 1991.

[7] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, Inc., 2nd edition, 1995.

[8] W. Richard Stevens. *TCP/IP Illustrated*. Addison-Wesley Publishing Company, 1994.

[9] Peter Wayner. *Disappearing Cryptography*. Academic Press, Inc., 1996.