Zeitschrift für Urheber- und Medienrecht ZUM 43/3 (1998) 177-180

# Zur Kontrollierbarkeit des Internet

Hannes Federrath

TU Dresden, Fakultät Informatik, 01062 Dresden
E-Mail: federrath@inf.tu-dresden.de

## 1 Einführung

Technisch gesehen ist das Internet ein stark vermaschter Graph von einzelnen kleineren Computernetzen. Das Internet ist international und organisationsübergreifend, nicht nur bezüglich der abrufbaren Daten, sondern ebenfalls bezüglich der Kommunikationsprotokolle, die weltweit standardisiert sind. Im Internet sind eine Vielzahl von Diensten realisierbar; die wichtigsten (z.B. E-Mail-Transfer, World Wide Web, File Transfer) sind ebenfalls standardisiert. Es gibt im wesentlichen Client-, Server- und Vermittlungsrechner. Der Client nutzt einen vom Server angebotenen Dienst, während die Vermittlungsrechner an den Knotenpunkten der Kommunikationswege lediglich Datenpakete (siehe Abbildung 1) durch das Netz transportieren, ohne deren eigentlichen Inhalt näher zu untersuchen. Ein Rechner kann gleichzeitig Client- und Serverfunktionen übernehmen und auch Kommunikationspakete vermitteln. Man muß also jeweils für jeden Dienst unterscheiden, welche Rolle ein Rechner im Kommunikationsgeschehen einnimmt.


*Abbildung 1. Alle Inhalte werden in Pakete verpackt*

Ursprünglich wurde das Internet für Hochverfügbarkeit entwickelt. Das bedeutet, daß ein unterbrochener Kommunikationsweg nicht zwangsläufig zur Unterbrechung der Kommunikation führen muß, da die Vermittlungsrechner in der Lage sind, alternative Kommunikationswege zu finden (siehe Abbildung 2).

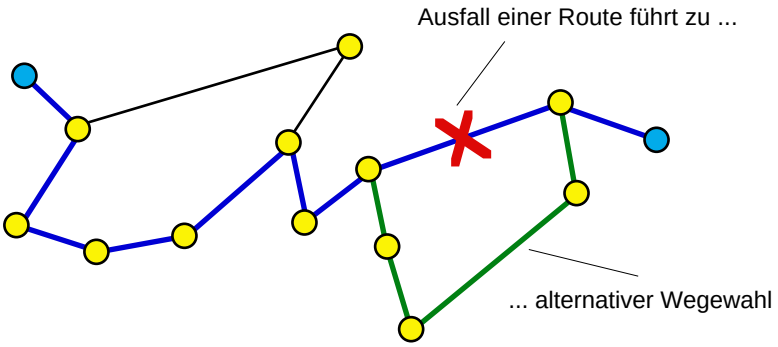


*Abbildung 2. Ausfall einer Route führt zu alternativer Wegewahl*

Das Internet ist ein verteiltes System. Das bedeutet, daß die Ressourcen (z.B. Speicher, Rechenleistung) nicht zentral angeordnet sind, sondern über das Netz verteilt sein können. Beispielsweise kann der Aufruf einer Webseite dazu führen, daß viele, weltweit verteilte Kommunikationsverbindungen vom Client (hier also dem Browserprogramm auf dem PC) angefordert werden. Am Ende entsteht die Webseite als Ganzes, obwohl die auf ihr dargestellten Bilder oder Texte im Internet verteilt gespeichert waren.

# 2 Rollen im Internet

Wie bereits angedeutet, kann der Betreiber eines Rechners, der an das Internet angeschlossen ist, mehrere Rollen einnehmen. Er kann gleichzeitig Dienste anbieten, also Server sein, Vermittlungsfunktionen bereitstellen, aber auch selbst als Client die Dienste anderer Server nutzen.
Im folgenden sollen die Rollen von Anbietern exemplarisch für die Dienste des World Wide Web diskutiert werden. Bezogen auf die im Internet bereitgestellten Inhalte und Angebote und die bei ihrer Vermittlung und Verbreitung Beteiligten kann man die folgenden Rollen unterscheiden, die jeweils kurz diskutiert werden.

## 2.1 Inhaltsanbieter (Content Provider)

Der Inhaltsanbieter fertigt Inhalte an und stellt sie anderen zur Verfügung. In diesem Sinn ist er auch verantwortlich für die Inhalte. Gemäß § 5 (1) Teledienstegesetz ist der Content Provider nach den allgemeinen Gesetzen voll verantwortlich für die Inhalte.
Im Internet existieren Verfahren, mit denen es möglich ist, Daten so bereitzustellen und auszutauschen, daß Sender und/oder Empfänger anonym sind und auch Dritte (inkl. Netzbetreiber) nicht nachvollziehen können, wer mit wem kommuniziert (Unbeobachtbarkeit). Diese Verfahren (z.B. Remailer und

Mixmaster, siehe www.obscura.com/~loki) sind auch einsetzbar, um Inhalte z.B. in Newsgruppen zu verbreiten, ohne daß der Urheber der Nachricht ist rückverfolgbar ist.

## 2.2 Anbieter verweist auf fremde Inhalte

Verweise eines Anbieters auf die Inhalte fremder Inhaltsanbieter sind z.B. Hotlists, d.h. Empfehlungen und Sammlungen von Verweisen. Neben den reinen Inhaltsangeboten (gemäß 2.1) ist dies die häufigste Form des Angebots. Im Normalfall wird ein Anbieter vor dem Verweis auf einen fremden Inhalt dessen Qualität prüfen. Allerdings hat er keinen Einfluß auf Änderungen des Inhaltes seitens des fremden Inhaltsanbieters. Wollte er die dauerhafte Qualität seiner Verweise sicherstellen, müßte er ständig alle Links überprüfen. Noch extremer gilt dies für dynamische Inhaltsangebote (Kataloge, Zeitungen, News), da sich hinter einer festen Adresse (URL) auch ein wechselnder Inhalt verbergen kann. So ist es sogar möglich, in Abhängigkeit vom Abfrager (genauer: dessen Internetadresse oder anderer Erkennungsmerkmale, wie z.B. Coockies oder einer ausgewählten bevorzugten Sprache) verschiedene Inhalte anzubieten.
Es ist einem Anbieter damit praktisch nicht möglich, einen Verweis auf fremde Inhalte vollständig zu überprüfen, um dessen dauerhafte Qualität zu garantieren.

## 2.3 Provider stellt Speicherplatz für fremde Inhalte zur Verfügung

Bei dieser Form der Dienstleistung besitzt ein Provider einen Server (z.B. www.provider.com), auf dem er für einen Kunden Speicherplatz zur Verfügung stellt, damit dieser Inhalte anbieten kann (www.provider.com/kunde). Gemäß § 5 (2) Teledienstegesetz ist der Provider nur dann für die Inhalte verantwortlich, wenn dieser Kenntnis davon hat und es ihm technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Einem Provider sollte es im Normalfall technisch möglich sein, die gespeicherten Inhalte eines Kunden zu sperren, sobald er von deren Rechtswidrigkeit weiß.
Bei einigen Diensten (z.B. E-Mail, News), für die der Provider Speicherplatz zur Verfügung stellt, werden die Inhalte über einen längeren Zeitraum (bei News einige Tage, bei E-Mail bis zur Abholung durch den Kunden) zwischengespeichert. Diese Speicherung geschieht aufgrund der technischen Umsetzung des Dienstes. Sobald dem Provider die Rechtswidrigkeit bestimmter Inhalte bekannt wird, ist er zumindest bei News in der Lage, diese zu sperren. Da es sich bei E-Mail im Normalfall um eine Punkt-zu-Punkt-

Kommunikation zwischen dem Sender und dem Empfänger einer Nachricht handelt, ist eine Überprüfung auf die Rechtswidrigkeit nicht möglich, es sei denn, die Kommunikation wird gezielt überwacht. Dies dürfte im Normalfall und im großen Stil jedoch weder nützlich noch sinnvoll sein, da die Kommunikationspartner die Nachrichten auch verschlüsseln können und somit jeder Zugriff unmöglich ist. Diese Aussage gilt generell, sobald die Speicherung und Übermittlung von Inhalten nur in einer geschlossenen Gruppe von Nutzern stattfindet. Hier ist jede Form der Kontrolle von außen wirkungslos.

## 2.4 Provider stellt speziell zugeschnittene Standarddienste zur Verfügung

Häufig stellen Internet Service Provider ihren Kunden speziell zugeschnittene Standarddienste zur Verfügung, bei denen eine grobe Vorauswahl der Inhalte und auch eine Sperrung bereits bekannter kritischer Inhalte erfolgt. Dies kann z.B. sinnvoll sein, wenn Eltern ihren Kindern den Zugang zum Internet ermöglichen wollen. So kann der Provider z.B. einen Filter für Spam-E-Mails, Werbe-E-Mails oder spezielle Webadressen (URLs) vorsehen, um seine Kunden nach ihren Wünschen zu schützen. Leider gibt es für den Kunden keinerlei Garantien, daß das Filtern erfolgreich verläuft und zwar in zweierlei Hinsicht. Einerseits kann ein eigentlich zu filternder Inhalt „durchs Netz gehen“, andererseits kann ein völlig unkritischer Inhalt falsch eingestuft sein und gefiltert werden.
Die speziell zugeschnittenen Standarddienste sollen den Nutzer schützen. Der Nutzer kann sich jedoch leicht über die Filterung hinwegsetzen, wenn er kein Filtern wünscht, was die Wirkung solcher gefilterter Dienstangebote teilweise in Frage stellt. Der Nutzer muß hierzu z.B. auf ungefilterte News-Server ausweichen, oder er benutzt sogenannte Proxy-Dienste (siehe auch Abschnitt 4).

## 2.5 Zugang zum Netz (Access Provider)

Der Access Provider stellt die technische Infrastruktur bereit, um Internetdienste zu nutzen. Er kennt zunächst nur die Dienste (E-Mail, World Wide Web, News etc.) und vermittelt Datenpakete. Für ihn ist es weder zumutbar noch technisch realisierbar, die ein- und ausgehenden Datenpakete zu kontrollieren. Dies hat mindestens drei Gründe. Erstens müßte für den Access Provider die Semantik der Daten, die ausgetauscht werden, erkennbar sein. Computer allein sind jedoch nicht in der Lage, semantische Analysen durchzuführen. Folglich müßte zumindest ein Teil der zu vermittelnden Daten ma-

nuell durch Menschen kontrolliert werden. Zweitens ist die zu verarbeitende und damit zu analysierende Datenmenge eines Providers derart enorm, daß selbst eine teilweise manuelle Kontrolle praktisch unmöglich ist. Drittens ist eine Kontrolle völlig unmöglich und damit wirkungslos, sobald die zu vermittelnden Daten verschlüsselt sind. Häufig begegnet man der Formulierung, einem Access Provider sei es „nicht zumutbar“, Inhalte zu kontrollieren. Da Daten jedoch verschlüsselt sein können, ist diese Formulierung nicht allgemeingültig, da es dem Access Provider in diesem Fall selbst beim besten Willen *nicht möglich* ist, die Inhalte zu kontrollieren.
Viele Access Provider speichern die vermittelten Daten ausgewählter Dienste (z.B. World Wide Web) temporär in einem speziellen Speicher (Cache). Dieses Caching dient ausschließlich der Leistungssteigerung des Systems und der Entlastung des Internets, da erneut angeforderte Daten direkt aus dem Cache entnommen werden. Dies geschieht für den Endbenutzer meist unbemerkt und kommt sehr häufig vor. Ein Proxy, der häufig mit einem Cache kombiniert ist, vermittelt nur Datenpakete.
Gemäß § 5 (3) Teledienstegesetz ist der Access Provider nicht für die Inhalte verantwortlich, da er lediglich den Zugang zur Nutzung vermittelt.

# 3 Filtern und Sperren von Inhalten

Die automatisierte Kontrolle von Inhalten erfordert eine semantische Analyse von Daten. Computer sind jedoch bestenfalls in der Lage, syntaktische Auswertungen vorzunehmen. Folglich ist eine vollautomatische Filterung von Inhalten unmöglich. Halbautomatische Verfahren, d.h. eine Kombination von automatischer und manueller Bewertung sind jedoch möglich. Das Filtern von Inhalten ist selbstverständlich nur bei unverschlüsselter Nachrichtenübermittlung möglich.
Eine weitaus ausführlichere Diskussion zu den Folgen und der Wirkung von Sperrungen im Internet ist z.B. in „Kristian Köhntopp, Marit Köhntopp, Martin Seeger: Sperrungen im Internet. Datenschutz und Datensicherheit DuD 21/11 (1997), S. 626-631“ zu finden.

## 3.1 Automatische Bewertung aufgrund formaler Kriterien

Die einfachste und einleuchtendste Art der Bewertung ist das Überprüfen der Inhalte nach vorgegebenen Schlüsselworten. Dies eignet sich natürlich nur für Texte. Für Bilder und andere Medien bietet sich eine Überprüfung mit Hilfe von Checksummen an. Allerdings werden hier nur Inhalte erkannt, die bereits vollständig dem Bewerter bekannt sind und vom Sender nicht, d.h. nicht einmal in einem Bit, verändert wurden.

Ein Ansatz zu einer intelligenteren Bewertung von Inhalten ist das content based database retrieving (siehe z.B. wwwqbic.almaden.ibm.com), bei dem über die Angabe bestimmter Bildkriterien (z.B. Vorhandensein bestimmter Texturen, Farbzusammensetzung etc.) eine Bewertung möglich ist.
Trotz der Fortschritte, die im Bereich der automatisierten Bewertung noch zu erwarten sind, können Fehleinschätzungen bei der automatisierten Bewertung in beide Richtungen auftreten: Einerseits können zu filternde Inhalte als einwandfrei erkannt werden, andererseits könnten auch Inhalte ohne Relevanz geblockt werden. Beispiele hierfür sind Diskussionsforen, die sich mit den Auswirkungen rechtswidriger, krimineller oder pornographischer Handlungen und Inhalte beschäftigen, ohne die Inhalte selber zum Gegenstand des Austauschs zu machen.

### 3.2 Manuelle Bewertung durch Dritte

Zunächst besteht natürlich die Möglichkeit, daß der Content Provider selbst seine Inhalte mit einer Bewertung versieht. Dies ist in Bereichen, in denen die Selbstregulierung greift, durchaus sinnvoll und hat in Systemen wie PICS (Plattform for Internet Content Selection) seine Berechtigung. Die Kombination mit dem unabhängigen Rating der Angebote durch unabhängige Dritte kann so eine qualitative Steigerung des Internetangebots nach sich ziehen, wie dies bei PICS der Fall ist. Infolge der Bewertung entstehen Sperrlisten, die entweder beim Provider oder auf dem lokalen Rechner des Benutzers vorhanden sind. Bei der Anforderung gesperrter Inhalte werden diese gar nicht erst vom Server angefordert.
Filterkriterien, aus denen die Listen aufgebaut werden, können Rechneradressen (IP-Adressen), Webadressen (URLs), Namen von Newsgruppen, aber auch Message-IDs (besonders bei E-Mail und News-Beiträgen) sein.
Aufgrund der riesigen Datenmenge, die das Internet heute aufweist, ist eine vollständige Bewertung aller Inhalte aussichtslos. Die hinzukommende Dynamik der Inhalte macht eine dauerhafte und nachhaltige Bewertung unmöglich.

## 4 Umgehen einer Sperre – ein Beispiel

Das Sperren von Internetangeboten dient hauptsächlich dem Schutz des Endbenutzers. Wünscht er diesen Schutz nicht, aber sein Provider hat entsprechende Vorkehrungen getroffen, kann er sich über eine lokale Sperre leicht hinwegsetzen. Abbildung 3 zeigt die Umgehung einer Sperre durch den Client-Rechner, indem der Client auf einen sogenannten Proxy ausweicht, der innerhalb eines Providers 2 liegt und der den Zugang zu dem Server nicht ge-

sperrt hat. Solange der Provider 1 den Zugang zu Provider 2 nicht ebenfalls sperrt, oder Provider 2 nicht seinerseits den Zugang zu dem Server blockiert, gelingt dieses Ausweichen. Eine Sperre ist damit unwirksam, solange nicht alle Provider (weltweit) ebenfalls den Server blockieren.

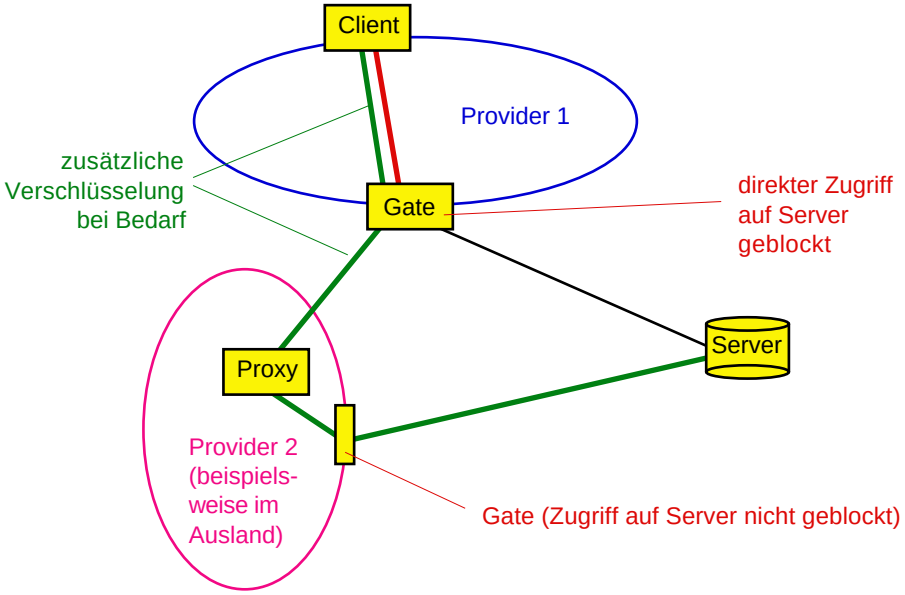


*Abbildung 3. Ausweichen auf einen fremden Provider überbrückt die Sperre*

Auch ein Server ist in der Lage, eine Sperrung zu umgehen, indem er z.B. alle Minuten seine IP-Adresse ändert. Bei Inhalten in Newsgruppen wird einfach ein Inhalt in andere, bisher unverdächtige und einwandfreie Newsgruppen „gepostet“. Auch ein Namenswechsel der Newsgruppe bewirkt für einige (kurze) Zeit die ungefilterte Verbreitung von Inhalten.
Generell ist es dem Content Provider möglich, falls er sich über eine Sperre hinwegsetzen möchte, sich dynamisch an die Filterkriterien anzupassen. Somit gelingt das Filtern und Sperren von Inhalten bestenfalls auf Zeit.

## Zusammenfassung

Eine reaktive Sperrung von Inhalten im Internet ist möglich und in vielen Fällen auch zumutbar. Eine proaktive Suche nach rechtswidrigen Inhalten kommt einer Massenüberwachung aller Kommunikation gleich und versagt, falls die Daten verschlüsselt werden. Dies gilt ebenso für Individualkommunikation (z.B. E-Mail) wie für geschlossene Benutzergruppen, die rechtswidrige Inhalte verschlüsselt austauschen.
Eine Sperre äußert sich als „technischer Defekt“. In einem verteilten System wie dem Internet, in dem niemand eine globale Übersicht über den Netzstatus

hat, ist für einen Administrator die Einschätzung der Fehlerursache sehr schwer, möglicherweise gar unmöglich. So wird es häufiger zu Fehleinschätzungen (Fehler oder Sperre?) kommen, die eine Administration des Netzes unmöglich machen. Folglich ist eine globale Übersicht über die Sperren notwendig.
Die manuelle Kontrolle aller Inhalte des Internet ist unzumutbar. Hat man ein Angebot als kritisch erkannt und möchte es sperren, beginnt der Wettlauf zwischen Anbieter und Filter, da der Anbieter sich an die Filterkriteren anpassen wird, um die Sperre zu umgehen.
Solange ein Anbieter mit seinen rechtswidrigen Inhalten ins Ausland abwandern kann, sind lokale Sperrungen nur ein wenig wirkungsvolles Mittel; internationale Regelungen jedoch greifen, da sie das Abwandern verhindern können.