Erschienen in: Fox, D.; Horster, P.: Datenschutz und Datensicherheit (DuD). Vieweg-Verlag, Wiesbaden 1999, S. 113-126.

Inhaltsfilterung und Jugendschutz im Internet

Marit Köhntopp

Der Landesbeauftragte für den Datenschutz Schleswig-Holstein
marit@koehntopp.de

Dörte Neundorf

Secorvo Security Consulting GmbH
neundorf@secorvo.de

Zusammenfassung

Wie alle anderen Medien auch wird das Internet zur Verbreitung von Daten beispielsweise jugendgefährdenden oder kriminellen Inhalts genutzt. Daher wurden verschiedenen Techniken der Sperrung und Inhaltsfilterung entwickelt und in Form von Programmen angeboten. Keine dieser Methoden kann eine vollständig korrekte Filterung und damit einen sicheren Jugendschutz garantieren. Die Verfahren sind jedoch unter bestimmten Randbedingungen ein nützliches Hilfsmittel im Rahmen einer umfassenden Medienerziehung.

1 Einführung

Wie alle anderen Medien auch wird das Internet zur Verbreitung von Daten beispielsweise jugendgefährdenden oder kriminellen Inhalts genutzt. Dies hat den Ruf nach staatlichen Eingriffen und technischen Verfahren laut werden lassen, um die Verbreitung dieser Inhalte zu verhindern oder zumindest das Abrufen dieser Inhalte durch Jugendliche und Kinder.

Die technischen Verfahren können zum einen auf der Netzwerkebene ansetzen und den Weg vom Anbieter der Information zum Endbenutzer unterbrechen. Zum anderen können sie auf dem lokalen Rechner filternd eingreifen.

Bevor man die technischen Maßnahmen zur Sperrung von Inhalten im Internet und die Wege ihrer Realisierung diskutieren kann, muß man sich darüber klar werden, welche Ziele man mit einer solchen Sperrung erreichen möchte. Mögliche Ziele sind:

- *Law Enforcement*: Man möchte verhindern, daß nach den Kriterien einer nationalen oder regionalen Rechtsordnung strafrechtlich relevantes Material für die Subjekte dieser Rechtsordnung erreichbar ist bzw. von ihnen veröffentlicht werden kann, und zwar auch dann, wenn die Veröffentlichung außerhalb des Durchsetzungsbereiches dieser Rechtsordnung erfolgt. Angestrebtes Ziel wäre, das Begehen solcher Straftaten technisch unmöglich zu machen.
- *Indecency*: In den USA wurde mit dem *communication decency act* (CDA) versucht, eine

noch weitergehende Regelung zu etablieren: Es sollte verboten werden, Material über Datennetze zugänglich zu machen, das *indecent* ist, d.h. nach den Grundsätzen der jeweils herrschenden Moraldefinition ungehörig, obszön oder in anderer Weise störend.[1]

- *Jugendschutz*: Nur Minderjährigen soll der Zugang zu bestimmten Materialien verwehrt werden, während Volljährigen weiterhin die gesamten Inhalte des Internet zugänglich bleiben sollen.
- *Rating*: Für jeden Teilnehmer im Netz soll weiterhin frei definierbar sein, welches Material empfangen/nicht empfangen werden soll, aber es soll eine Bewertungsstruktur geschaffen werden, die es jedem Konsumenten in eigener Verantwortung ermöglicht, seine Präferenzen anzugeben (z.B. „kein Sex“/“viel Sex“, „keine Gewalt“/“Blood and Splatter“, „politisch links“/“politisch rechts“) und nur noch den Ausschnitt aus dem Internet wahrzunehmen, der diesen selbstgewählten Filter passieren kann.
- *Nichtregulierung*: Jeder Netzteilnehmer soll freien Zugriff auf alle angebotene Information haben. Sogar die Existenz von Bewertungskriterien Dritter wird als schädlich angesehen und die Bildung einer Bewertungsinfrastruktur abgelehnt.

2 Betroffene Dienste

Unter der Bezeichnung „Inhalte im Internet“ wird eine ganze Reihe von Diensten verstanden, die technisch vollkommen unterschiedlich realisiert werden und administrativ zu großen Teilen disjunkte Strukturen aufweisen. Allen Diensten ist lediglich gemeinsam, daß ihnen das Datenübertragungsprotokoll TCP/IP zugrunde liegt.

Man muß mindestens die beiden Dienste World Wide Web und USENET News betrachten. Weitere Dienste sollen hier im Interesse einer kompakten Darstellung nicht diskutiert werden. Die folgenden Argumente gelten aber in ähnlicher Form auch dort.

2.1 World Wide Web

Das World Wide Web (WWW) ist der graphisch ansprechendste Dienst des Internet. Es handelt sich um Server, die auf die Anfrage eines Benutzers „Seiten“ beliebigen Inhaltes an das Darstellungsprogramm („*Browser*“) auf dessen Rechner ausliefern. Der Zugriff auf diese Seiten erfolgt in der Regel mit Hilfe des *HyperText Transport Protocol* (HTTP). Dieses Protokoll erfordert keine Identifizierung oder Authentisierung des Abrufers und des Anbieters.

Größere Server erzeugen die Seiten oftmals dynamisch in Abhängigkeit von der Identität des Abrufers, seiner Netzadresse, seiner bevorzugten Landessprache (im Browser konfigurierbar), dem vom Abrufer verwendeten Browsertyp, der Uhrzeit des Abrufs oder anderen Kriterien, die frei progammierbar sind. Es ist also nicht sichergestellt, daß zwei aufeinanderfolgende Abfragen derselben Seite identische Antworten ergeben.

Falls die Seiten aus einer Datenbank dynamisch erzeugt werden, kann sich der Datenbestand des Webservers durch die Updates der Datenbank ständig ändern. Dies ist zum Beispiel der Fall bei Katalogsystemen für Onlinehandel (Preis- und Produktupdates, Änderungen im Lagerbestand mit Auswirkungen auf die Lieferbarkeit usw.), bei Nachrichtenagenturen mit

[1] Zu „Free Speech“ siehe z.B. The Electronic Frontier Foundation (EFF), http://www.eff.org/

Anschluß an Presse- und Tickerdienste und bei Webverzeichnissen und Suchmaschinen, die einen Volltextindex für Seiten generieren und eine Recherche nach Inhalten erlauben.

Grundsätzlich ist der Datenbestand im Web also höchst dynamisch: Neue Versionen von Seiten lassen sich zu sehr geringen Kosten erzeugen und in Verkehr bringen. Dadurch ist eine hohe Auflagenfrequenz möglich.

2.2 USENET News

Das USENET ist ein verteiltes System von Diskussionsforen („*Newsgroups*“). Es handelt sich um ein teilweise zusammenhängendes Netz von Servern, von denen jeder eine Auswahl von Artikeln zum Abruf bereithält. Die Artikel sind in der Regel in thematisch gegliederten Diskussionsforen in der Reihenfolge des Eingangs abgelegt. Leser können eine Verbindung zum netztopologisch am günstigsten gelegenen Server aufbauen, Artikel nach Diskussionsforen und Eingangsdatum selektiert abrufen und grundsätzlich auf jeden gelesenen Artikel antworten oder unabhängig eigene Artikel auf dem Server ablegen. Der Server wird dann seine Nachbarserver darüber informieren, daß er einen neuen Artikel vorrätig hat, und den Artikel ggf. an seine Nachbarserver replizieren. Diese verbreiten den Artikel dann wieder an ihre Nachbarn usw. Nach einigen Stunden existieren Hunderttausende von Kopien dieses Artikels auf der gesamten Welt.

Die Zeitspanne bis zur Löschung eines Artikels hängt von der individuellen Konfiguration des Servers und seiner Platzsituation ab, liegt aber in der Regel nicht über 14 Tagen. Es gibt jedoch auch einige Newsarchive, die Diskussionen über mehrere Jahre hinweg abspeichern und diesen Datenbestand durch weitgehende Recherchemöglichkeiten erschließen.[2]

Die Kommunikation zwischen Leser und Server sowie die Kommunikation zwischen den Servern erfolgt in der Regel unverschlüsselt und ohne Identifizierung und Authentisierung der Leser oder der Autoren von Artikeln. Die Fälschung von Absenderadresse oder Herkunftspfad eines Artikels ist trivial und in einigen Diskussionsforen sogar üblich. Es existieren Umsetzungsdienste von E-Mail nach USENET News und Anonymisierungs- sowie Pseudonymisierungs-Server, die zum Teil mit kryptographisch starken Methoden [3] die Identität des Absenders zu verschleiern suchen. Einige Newsserver lassen Lese- und Schreibzugriff von jedermann und ohne Authentisierung zu; es ist Sache des Veröffentlichenden, seine Identität in einem Artikel offenzulegen oder nicht.

3 Sperrungstechniken im Netzwerk

Der erste Ansatz zur Sperrung von Servern oder Seiten ist die Unterbrechung der Netzwerkverbindung oder zumindest der Übertragungswege auf dem physikalischen Netzwerk.

3.1 Vorgehen

Sperrungen können dabei auf unterschiedlichen Ebenen der Kommunikation ansetzen. Nicht

[2] Z.B. http://www.dejanews.com, http://www.altavista.digital.com im Newsmodus

[3] Insbesondere Mixmaster-Remailer
FAQ von Lance Cottrell unter http://www.obscura.com/~loki/remailer/mixmaster-faq.html,
Liste existierender Mixmaster-Remailer unter http://kiwi.cs. berkeley.edu/mixmaster-list.html

praktikabel ist es, die physikalische Kommunikation zu unterbinden, indem man etwa einen Telefonanschluß sperrt oder bestimmte Telefonnummern nicht erreichbar schaltet, Standleitungen unterbricht oder Störsender in Richtfunkstrecken einbringt.

Im Internet wird meist keine homogene physikalische Verbindung verwendet, sondern diese Verbindung wird aus Teilstücken unterschiedlicher Technologie zusammengestückelt. An den Übergangspunkten zwischen den Teilstücken befindet sich ein Router, der IP-Pakete von einem Teilstück zum nächsten weiterreicht. In Routingtabellen ist eingetragen, in welche Richtung der Router Pakete mit einer gegebenen Zieladresse weiterzuleiten hat. Sperrungen können hier über Eingriffe in die Routingtabellen vorgenommen werden. Es ist beispielsweise leicht möglich, alle Pakete an bestimmte Zieladressen am Router verwerfen zu lassen („*eine Route zu erden*"). Mit diesem Verfahren werden ganze Rechner unerreichbar: Bei der durch den DFN-Verein 1997 kurzzeitig praktizierten Sperrung des Rechners mit dem Namen *www.xs4all.com* waren auf diese Weise die Webseiten von mehr als 6000 Anbietern nicht mehr abrufbar, es konnte keine Mail auf der Maschine *www.xs4all.com* eingeliefert werden, und auch jede andere Kommunikation des DFN-Vereins mit dieser Maschine wurde unterbunden.

Die Auswahl eines Dienstes erfolgt im TCP/IP-Protokoll in der Regel durch die Angabe einer TCP-Portnummer. Mit Hilfe dieser Portnummer könnte eine selektivere Sperrung eines Dienstes erfolgen. Beispielsweise sind einige Router in der Lage, nach entsprechender Konfiguration TCP-Verkehr für den Port 80 (HTTP) zu einer Zieladresse zu sperren, Verkehr auf Port 25 (*Mail*) zur selben Adresse jedoch zu gestatten.

Mit Hilfe eines Vermittlungsrechners („*Proxy*") oder einer geeigneten Firewall, denen die Ebene der Anwendungsprotokolle zugänglich ist, kann eine selektive Sperrung von Dienstelementen (einzelne Seiten, einzelne Nachrichten) erreicht werden. Eine Firewall muß hierbei jedoch für jeden Dienst (WWW, News, Mail, IRC etc.) angepaßt werden. Solche Systeme sind in der Regel sehr aufwendig im Betrieb, da sie für die nutzenden Clients die volle Leistung aller durch den Client in Anspruch genommenen Dienste simulieren müssen.[4]

Sperrungen von IP-Adressen und der Einsatz von Firewalls sind unter bestimmten Voraussetzungen kombinierbar. Diese Lösung ist je nach Art der zu sperrenden und zu simulierenden Dienste sehr aufwendig zu konfigurieren und zu warten. Zum einen setzt sie einen zentralen Übergangspunkt zwischen dem zu kontrollierenden Netz und dem Rest der Welt voraus. Zum anderen handelt es sich bei diesem Verfahren um einen klassischen „Man in the middle"-Angriff. Daher versagt der Ansatz bei verschlüsselter Kommunikation, die unempfindlich gegen solche Angriffe ist.

Grundsätzlich sind die Auswirkungen von Filtermechanismen auf die Systemleistung desto höher, je feiner die Granularität der Sperrungen und je größer die Liste der zu sperrenden Informationsquellen ist.[5]

Alle bisher diskutierten Sperrungsverfahren setzen auf dritten Maschinen zwischen dem Anbieter der zu sperrenden Information und dem Abrufer an. Denkbar wäre auch eine

[4] Trotzdem setzen einige totalitäre Staaten auf dieses System, um das Eindringen mißliebiger Inhalte in das Land zu erschweren: In China läuft sämtliche Kommunikation mit dem Ausland durch staatlich betriebene Firewalls (Nachricht von Li Gong vom 14.06.97 in comp.risks, RISKS DIGEST 19.23).

[5] Systeme wie PICS lassen sich nicht effizient an zentralen Stellen im Netz etablieren, sondern können nur dezentral funktionieren.

freiwillige Sperrung beim Anbieter oder beim Abrufer der Information.

Eine Sperrung beim Anbieter würde bedeuten, daß der Anbieter die zu sperrenden Inhalte entweder niemandem anbietet oder daß er sie nur bestimmten Personen nicht anbietet.

Ein personenselektives Anbieten von Inhalten setzt selbst bei Kooperation des Anbieters voraus, daß der Anbieter den Abrufer einer Information zweifelsfrei identifizieren kann und daß ihm genaue Entscheidungstabellen vorgelegt werden, die es ihm erlauben, automatisch zu entscheiden, wem er welche Inhalte ausliefern darf. Ein Identifikationsmechanismus, der das Geforderte leistet, existiert derzeit nicht und ist auch nicht in absehbarer Zeit realisierbar. Insbesondere kann im allgemeinen nicht aus der IP-Adresse oder dem Rechnernamen eines Absenders auf seine Identität oder seinen physikalischen Aufenthalt geschlossen werden: Deutsche Kunden von amerikanischen Online-Diensten erscheinen im Netz als aus den Vereinigten Staaten kommend. Ähnliches gilt für Mitarbeiter multinationaler Konzerne. Zudem ist es möglich, eine falsche IP-Adresse einzustellen.

Eine Sperrung beim Abrufer würde bedeuten, daß dieser selber eine Inhaltsfilterung vornimmt; z.B. anhand in den Seiten enthaltener Bewertungen oder automatisierter Bewertungsverfahren. Die hierfür existierenden Ansätze werden in Abschnitt 4 diskutiert.

3.2 Möglichkeiten zum Unterlaufen von Sperrungen

Für den Nutzer stellt sich eine Sperrung von Inhalten als Betriebsstörung dar. Er wird nach Wegen suchen, die ordnungsgemäße Funktion des Netzes wiederherzustellen, d.h. die Sperrung zu unterlaufen. Diese Motivation ist um so größer, je stärker sich der Benutzer durch die Sperrung behindert fühlt.

Bei einer Sperrung der physikalischen Kommunikation ist dies nur durch einen Wechsel des Mediums möglich: Wenn etwa ein Störsender in Betrieb genommen wird, wird man versuchen, auf das Telefonnetz auszuweichen.

Bei einer Sperrung von bestimmten IP-Adressen stehen dem Benutzer mehrere Möglichkeiten offen, die Störung zu umgehen. Alle laufen darauf hinaus, den sperrenden Router vollständig zu umgehen.[6]

Der Benutzer wechselt den Internet-Anbieter, notfalls wird er Kunde bei einem ausländischen Provider. Er baut eine Telefonverbindung oder Standleitung zu diesem Provider auf und wickelt seine Kommunikation über diesen nichtsperrenden Provider ab. Der sperrende Router des lokalen Providers wird nicht mehr verwendet, die Sperre ist wirkungslos.[7]

Der Anbieter der gesperrten Information kann Abrufer unterstützen, indem er ebenfalls versucht, die Sperre zu unterlaufen.

So hat beispielsweise im Falle der Sperrung des Rechners *www.xs4all.nl* der gesperrte Anbieter die Internet-Adresse seines Rechners alle zwanzig Minuten verändert. Sperrungen einer einzelnen Adresse wurden dadurch wirkungslos, statt dessen mußten ganze Teilnetze gesperrt werden; die Sperrung wurde noch unspezifischer, es wurden als Nebenwirkung noch mehr unbeteiligte Anbieter mitgesperrt.

---

[6] Siehe auch Ulf Möller: „Internet-Zensur: Routingsperren umgehen“, http://www.fitug.de/ulf/zensur/

[7] Diese Situation tritt automatisch ein, wenn der Nutzer Mitarbeiter eines (multinationalen) Konzerns mit einem eigenen Konzernverbundnetz ist, das an mehreren Stellen (im Ausland) mit dem Internet verbunden ist.

Nicht nur vom Standpunkt der Kontrolle der Bewerter, sondern auch vom Standpunkt des technischen Netzbetriebes ist außerdem eine Offenlegung aller Sperrungen unumgänglich. Wenn Sperrungen von Rechnern oder einzelnen Angeboten massenhaft umgesetzt werden, ist für den einzelnen Systembetreiber ebenso wie für den einzelnen Anwender nämlich nicht mehr entscheidbar, ob eine technische Störung vorliegt, die zu beheben ist, oder ob eine inhaltlich begründete Sperrung vorgenommen wurde. Andererseits können offengelegte Sperrlisten natürlich leicht als Kataloge für pornographische oder gewalttätige Angebote genutzt werden. Wie gezeigt wurde, sind offengelegte Sperrungen zudem mit entsprechend modifizierten Programmen automatisiert umgehbar.

Die bisher diskutierten Möglichkeiten des Unterlaufens von Sperrungen waren unabhängig vom gesperrten Dienst. Die im folgenden dargestellten Möglichkeiten sind dienstspezifisch.

3.2.1 World Wide Web

Ähnlich der erwähnten Veränderung der IP-Nummer eines Serverrechners kann auch die Adresse eines Angebotes auf einem Server automatisch verändert werden. Eine automatische Sperrung einzelner Angebote würde dadurch unterlaufen, und man müßte wieder den gesamten Rechner pauschal sperren.

Wenn zu einem Angebot eine Suchmaschine existiert, mit der alle Seiten eines Angebotes nach bestimmten Begriffen durchsucht werden können, ist eine einzelne Seite unter nicht vorhersagbaren Adressen zu finden (nämlich allen Begriffen, die den Text in der Suchmaschine finden). Eine Sperrung müßte hier zusätzlich den Zugriff auf die Suchmaschine verhindern.

Das Verfahren des indirekten Zugriffs, wie es unter „Mobile-IP“ diskutiert wurde, läßt sich mit Veränderungen auch für WWW einsetzen: Mit Hilfe eines entfernten Webservers, der Zugriffe im Auftrag Dritter abwickelt („*Proxy*“-Server), ist ein indirekter Abruf der Seite möglich. Da Proxy-Server mit Zwischenspeicher zur Beschleunigung von Zugriffen üblich sind, ist es in der Regel kein Problem, einen solchen dritten Server zu finden. Während der Diskussion der letzten Monate sind mittlerweile im In- und Ausland auch schon Proxy-Server ausschließlich für solche Umgehungen eingerichtet worden – etwa am MIT für chinesische Staatsbürger, die die Zensur im eigenen Land unterlaufen möchten.

Bei verschlüsselter Kommunikation [8] entsteht ein nicht mehr in Echtzeit einsehbarer und nicht einfach verfälschbarer Kanal zwischen Server und Client. Für Dritte ist nicht erkennbar, welche Seiten abgerufen werden und welche Informationen sie enthalten. Damit scheitert eine Sperrung nach einzelnen Seiten oder nach Stichworten.

3.2.2 USENET News

Artikel in den USENET News liegen in zahlreichen Kopien auf Tausenden von Servern überall auf der Welt vor. Löschungen werden von vielen dieser Server nicht mehr ausgeführt, nachdem es seit einigen Jahren immer wieder zu gefälschten Löschaufforderungen von Saboteuren kam. Die großen Archive für USENET News (DejaNews und AltaVista) führen grundsätzlich keine Löschungen aus. Über Archivanfragen ist es daher in der Regel möglich, auch auf ältere und lokal nicht mehr verfügbare Texte zuzugreifen. Dabei gilt wie bei Suchmaschinen für Webseiten (siehe oben): Artikel sind nicht nur unter einer festen

[8] Etwa mit dem in allen gängigen Browsern eingebauten SSL-Support (Secure Sockets Layer), siehe Esslinger/Müller, DuD 12/1997.

Bezeichnung abrufbar, sondern werden auch zu beliebigen im Artikel enthaltenen Stichworten gefunden.

Im Rahmen einer Untersuchung der bayrischen Staatsanwaltschaft wurde der Betreiber Compuserve aufgefordert, einige Newsgroups grundsätzlich nicht mehr bereitzustellen, da bei ihnen davon auszugehen sei, daß diese in Deutschland strafrechtlich relevante Inhalte enthielten. Die Leser dieser Gruppen beziehen diese jetzt direkt von anderen, nicht gesperrten Newsservern. Außerdem gehen die Autoren von Artikeln für solche schlecht verbreiteten Newsgroups immer mehr dazu über, ihre Artikel zusätzlich in andere, thematisch unpassende, aber besser verbreitete Gruppen zu setzen. So kam es zum Beispiel anläßlich der Sperrung des Servers *www.xs4all.nl* wegen des Angebotes der verbotenen Zeitschrift „Radikal, Ausgabe 154“ zweimal zu je einem Posting der Komplettausgabe der Radikal in den Diskussionsforen „de.soc.zensur“ (Diskussion über Zensur und Inhaltskontrolle) und „de.org.politik.spd“ (Forum des virtuellen Ortsverbandes der SPD).

Da die Neueinrichtung von Newsgroups technisch automatisiert werden kann, kommt es vielfach zur Neueinrichtung lokal gesperrter Gruppen unter neuem Namen oder zum Angebot bekannter Gruppen unter Aliasnamen.[9]

4 Inhaltliche Filterung

Soll es dem Endnutzer ermöglicht werden, sich selber (oder im Falle des Jugendschutzes die den Internetzugang mitbenutzenden Kindern oder Schülern) nur den Zugang zu einem Teil des Internetangebotes zu gestatten – Sperrung beim Abrufer –, benötigt er dafür ein technisches Instrumentarium zur Inhaltsfilterung.

Die Durchführung der dazu notwendigen Sortierung (Filterung) wiederum erfordert, daß die Inhalte *bewertet*, *gekennzeichnet* und *ausgewählt* werden. Jeder dieser Vorgänge kann sich dabei auf ganze Server beziehen, auf Unterverzeichnisse oder einzelne Seiten, Dokumente oder Dateien. Dabei können sie auf verschiedenen Wegen und von verschiedenen Personen bzw. Instanzen mit jeweils spezifischen Vor- und Nachteilen durchgeführt werden.

4.1 Bewertung der Inhalte

Inhalte im Internet – und auch in anderen Medien – können zunächst sehr einfach in „kriminell“ und „nicht kriminell“ unterschieden werden, wobei die zugrunde liegenden Maßstäbe z.B. den gesetzlichen Grundlagen entnommen werden können. Im Sinne einer sinnvollen Nutzung ist jedoch eine feinere Unterteilung hilfreich, z.B. nach Eignung für verschiedene Altersklassen (wie z.B. die Kategorien für die freiwillige Selbstkontrolle von Spielfilmen) für den Jugendschutz, aber auch nach der Art des Inhalts (Unterhaltung, Naturwissenschaft, Suchmaschine, ...) zur Erleichterung einer persönlichen Auswahl. Eine solche Bewertung erlaubt eine spezifische Einstellung der verwendeten Filtersoftware nach den strafrechtlichen, inhaltlichen, pädagogischen oder sozialen Anforderungen.

In beiden Fällen stellt sich jedoch das Problem, den jeweiligen Inhalt den Kategorien zuzuweisen. Da dort Text, Bilder, Audio-Sequenzen etc. zusammenspielen, ist eine solche Be-

[9] So wurde die Gruppe de.talk.sex (Diskussionsforum über Sexualität) an einer deutschen Universität mehrere Jahre lang unter dem Namen de.talk.verkehr geführt, nachdem dort entschieden worden war, keine Gruppen mehr anzubieten, deren Bezeichnung den Begriff „sex“ enthält.

wertung nur sehr selten automatisiert möglich. Daher ist eine Einzelbetrachtung und Einordnung durch einen Menschen notwendig.

Um eine Einheitlichkeit der durchgeführten Bewertungen zu gewährleisten, ist weiterhin eine detaillierte und eindeutige Festlegung der Bewertungsmaßstäbe erforderlich. Dies ist um so wichtiger, je mehr Personen an der Bewertung beteiligt sind.

Im Grundsatz besteht ein solches Bewertungssystem aus einer Liste von Inhaltsgruppen und einer mehr oder weniger detaillierten Beschreibung, was zu jeder dieser Gruppen gehört. Ein großer Teil der existierenden Schemata beschränkt sich auf eine Eingruppierung der Eignung für Kinder und Jugendliche in verschiedene Kategorien wie „Sexualität“, „Gewalt“, „Drogen“. Nur wenige sehen zusätzliche Inhaltsbeschreibungen vor wie „Politik“, „Einkaufen“ o.ä.

Diese Systeme können öffentlich zugänglich sein, z.B. wenn die Bewertung einer Seite vom Autor selbst vorgenommen wird.[10] Kommerzielle Hersteller werden ihre Schemata eher nicht veröffentlichen; insbesondere die Bewertungen einzelner Seiten werden in diesen Fällen nicht preisgegeben, da in ihrer Erstellung ein wesentlicher Teil der Leistung liegt. Oft unterbleibt eine Veröffentlichung des Bewertungssystems auch aus der (nicht unberechtigten) Befürchtung, Anbieter jugendgefährdender Seiten könnten das Wissen um die Kategorisierungskriterien zur Umgehung der technischen Filterlösungen mißbrauchen. Um als Endbenutzer eine geeignete Auswahl treffen zu können ist allerdings eine Transparenz der Bewertung unabdingbar. Auch Fehlbewertungen können nur identifiziert werden, wenn Kontrollen möglich sind.

Für die konkrete Durchführung der Bewertung in technischer Hinsicht ist zu unterscheiden, wo und durch wen diese Bewertung vorgenommen wird. Daraus ergeben sich unterschiedliche Konsequenzen für Aufwand, Verwaltung, Verwendbarkeit und Aktualisierung des Verfahrens.

4.1.1 Bewertung durch Verfasser

Die einfachste, dem Umgang mit Videos, Spielen etc. nachempfundene Variante ist eine Eigenbewertung durch die Verfasser einer WWW-Seite oder Dokuments. Der zusätzliche Aufwand bei der Erstellung der Seite ist gering.

Voraussetzung für diese Vorgehen ist ein Bewertungsschema, das möglichst objektive und präzise Einstufungen ermöglicht und außerdem weit verbreitet ist.

Die Gefahr bei diesem Ansatz ist, daß gerade bei jugendgefährdenden Inhalten die Verfasser ihre eigenen Inhalte harmloser einschätzen werden als z.B. Eltern. Eine Kontrolle der Bewertungen ist also erforderlich – durch die Öffentlichkeit oder auch durch eine dafür zu schaffende Kontrollinstanz. Außerdem wird es immer Seiten ohne eine solche Bewertung geben – und sei es nur durch technische Fehler bei der Übertragung. Es muß also immer zusätzlich eine Verfahrensvorschrift für solche Fälle geben.

4.1.2 Bewertung durch Dritte

Eine einheitlichere Vorgehensweise ist die Durchführung der Bewertung durch eine dritte – von der die Seite verfassenden und lesenden Person verschiedene – Instanz. Der Aufwand ist bei der großen Anzahl von Internetseiten beträchtlich. Daher verfolgen die Anbieter solcher

[10] Dies sind z.B. SafeSurf, RSACi, ESRB, evaluWEB.

Bewertungen meist spezifische Interessen. Diese können politisch sein (z.B. Elterninitiativen, politische Verbände, Initiativen für bestimmte politische Ziele etc.) – daraus resultierende Bewertungen sind meist frei verfügbar – oder auch kommerziell.

In der Bewertung schlagen sich die unterschiedlichen Interessen der Bewertenden nieder. Dies ist bei der Auswahl eines Filtersystems zu beachten, da sonst eine ungewollte und im Falle von nicht offengelegten Filterregeln auch unerkannte Einschränkung des Angebotes in Kauf genommen wird.[11] Gerade hier ist also die Einsicht in die Bewertungskriterien eine wesentliche Voraussetzung für deren Nutzbarkeit.

4.1.3 Bewertung durch die Allgemeinheit

Eine weitere, dem Charakter des Internets besonders entsprechende Variante ist eine Bewertung durch alle Netzteilnehmenden. Generell könnte dann jeder und jede eine Bewertung einer Seite an eine verwaltende Instanz schicken. Je nach Charakter des Systems würden die Bewertungen dort überprüft oder direkt in eine Liste eingefügt, die dann – eventuell unter Verwendung bestimmter Software – abrufbar gehalten werden könnte.

Die Verwaltung muß allerdings dafür sorgen, daß die Bewertungen ein gewisses Grundmaß an Einheitlichkeit aufweisen. Es wird dabei mit großer Wahrscheinlichkeit zu Mehrfachbewertungen mit unterschiedlichen Resultaten kommen. Daher muß es ein Konzept geben, wie mit solchen Widersprüchen umzugehen ist. Außerdem sollte es nicht möglich sein, durch mehrfache Bewertung einer Seite als „pornographisch“ diese für das Internet praktisch zu sperren, wenn sie z.B. politisch unangenehme Aussagen enthält.

Andererseits kann mit dieser Methode eine sehr große Zahl von Seiten ohne hohen (zentralen) Aufwand bewertet werden.

4.1.4 Bewertung durch Endnutzer

Das aus Benutzungssicht zuverlässigste Vorgehen ist eine Bewertung am Endrechner selber. So könnte z.B. ein Lehrer oder eine Lehrerin eine genaue Liste aller für eine bestimmte Klasse verfügbaren Seiten definieren; und nur diese sind dann zugänglich.

Der Konfigurationsaufwand dafür ist allerdings sehr groß, da jede Seite (oder wenigstens jeder Server oder jede Domäne) explizit eingegeben werden muß. Der im Vergleich zum Angebot im Internet geringe Umfang solcher Listen schränkt die Möglichkeiten des Internets drastisch ein. Daher ist eine solche Möglichkeit in vielen Produkten häufig nur als Ergänzung zu einem der anderen Verfahren integriert und wird kaum als Einzellösung angeboten.

4.2 Kennzeichnung der Inhalte

Eine Bewertung ist nur dann für eine technische Unterstützung des Jugendschutzes verwertbar, wenn sie für das lokale Endsystem verfügbar ist. Dazu wird sie entweder direkt auf einer Webseite vermerkt und kann beim Abruf ausgewertet werden oder in getrennten Listen gesammelt, die dann für den abrufenden Computer verfügbar sein müssen, so daß dieser einen Abgleich durchführen kann.

[11] Auf www.peacefire.org finden sich viele Fälle, in denen nach Kriterien des Jugendschutzes unproblematische Server in den Sperrlisten kommerzieller Programme auftauchten.

4.2.1 Markierung der Seite

In einer WWW-Seite enthaltene Bewertung können nur praktikabel von den verfassenden Personen durchgeführt werden, da sie im Quelltext der Seite enthalten sein müssen. Sie eigenen sich daher nur für die Selbstbewertung. Aktualisierungen sind ebenfalls nur vom Autor durchzuführen, wenn er oder sie den Inhalt der Seite ändert; für den filternden lokalen Rechner besteht also kein Aktualisierungsbedarf.

Um eine allgemeine Verwertbarkeit dieser Angaben zu gewährleisten, sind formale Regeln für die Integration und die Übertragung erforderlich (z.B. PICS [12]). Diese müssen eine Markierung jeder Seite ermöglichen, auch wenn sie nur aus einem Bild oder einer Audio-Sequenz besteht und keine expliziten html-Befehle enthält.

Ist ein solches System weit verbreitet, steigt die Motivation, Bewertungsmerkmale in eigene Webseiten einzufügen, da diese einerseits eine Blockade wegen fehlender Kategorisierung verhindern und andererseits die Anzahl der erwünschten Zugriffe steigern können.[13]

4.2.2 Bewertungslisten

Bewertungen können statt auf der WWW-Seite selbst auch separat gesammelt und verwaltet werden. Dies geschieht im allgemeinen dann, wenn die Bewertung von Dritten (also Institutionen oder der Öffentlichkeit) durchgeführt werden.

Für die Verwaltungsinstanzen solcher Listen gelten ähnliche Anmerkungen wie die oben für die Bewertungsinstanzen gemachten: Es stehen meist politische oder kommerzielle Interessen dahinter, die bei der Auswahl einer Filterlösung beachtet werden sollten.

Für die konkrete Filterung muß eine solche Liste für den Endrechner verfügbar sein: entweder als lokal gespeicherte Kopie – die dann immer wieder durch aktuelle Versionen ersetzt werden muß – oder online auf einem aktiv arbeitenden Server, der vor dem Laden einer Seite jeweils über deren Zulässigkeit befragt wird (dann entfällt die Übertragung der neuen Versionen, der Server muß allerdings dauernd und schnell verfügbar sein). In beiden Fällen ist die Aktualität einer solchen Liste der kritische Parameter für die Wirksamkeit und Korrektheit einer darauf aufbauenden Filterung: Im Internet entstehen ständig neue Seiten und werden bestehende verändert, so daß die Bewertung entsprechend schnell aktualisiert werden muß.

4.3 Auswahl

Die eigentliche Aufgabe eines Werkzeugs zur technischen Unterstützung des Jugendschutzes im Internet ist die Auswahl geeigneter bzw. die Sperrung ungeeigneter Seiten. Die Durchführung dieser Auswahl erfolgt entweder direkt auf dem Client-Rechner oder auf den vorgeschalteten Netzwerkkomponenten (Server eines Internetproviders, Proxy).

Dies kann aufgrund eines oder mehrerer der genannten Bewertungsschemata oder durch automatisierte Filterung geschehen; am effektivsten sind Kombinationen.

---

[12] Platform for Internet Content Selection, www.w3c.org/pics, eine Initiative des WorldWideWebConsortiums (W3C), die Regeln zur Angabe und Übertragung von Bewertungen im Internet spezifiziert. Auf diese Spezifikation basieren die verbreitetsten Labeling-Systeme SafeSurf und RSACi.

[13] Einige Systeme sehen neben der Angabe der Eignung für Kinder auch eine Inhaltsbeschreibung vor, die die Resultate von Suchvorgängen verbessern soll. Auch haben viele Anbieter von kostenpflichtigen Angeboten für Erwachsene kaum Interesse an jugendlichen Besuchern, da sie Kosten für die Internetnutzung verursachen, aber nicht zu den zahlenden Kunden gehören.

4.3.1 Inhaltsbewertung

Geschieht die Auswahl nach Inhaltsbewertung, so ist es für den Systemadministrator möglich, in Abhängigkeit vom Bewertungssystem genaue Richtlinien für die Auswahl vorzugeben. So kann definiert werden, welche Inhalte angezeigt werden (z.B. jede Seite mit dem Label „für Kinder unter 10“ oder „Grundschule“, wenn ein Kind am Computer sitzt) und welche Seiten verborgen bleiben (z.B. „nur für Erwachsene“ oder auch „Politik“ oder „Werbung“).

Entsprechend spricht man von Positivauswahl – die anzuzeigenden Seiten werden charakterisiert – oder Negativauswahl, wenn die zu sperrenden Seiten benannt werden. Dabei ist eine Positivauswahl immer restriktiver, da damit alle Seiten ohne die geforderte Eigenschaft ausgeschlossen werden; hingegen erlaubt eine Negativauswahl weiterhin einen Zugriff auf fast alle Internet-Angebote, sofern sie nicht die ausgewählte Bewertung besitzen.

Eine Inhaltsbewertung in Reinform sperrt alle nicht bewerteten Seiten oder Server. Damit wird ein großer Teil des Internets von vornherein ausgeschlossen, solange sich nicht weltweit Bewertungssysteme verbreitet haben. Als alleiniger Mechanismus eignet sich eine Filterung nach Inhaltsbewertung also erst dann, wenn ein Großteil der Angebote bewertet ist.

4.3.2 Automatisierte Filterung

Um auch unbewertete Seiten oder Server oder auch einzelne Nachrichten in Diskussionsforen beurteilen zu können, werden automatische Filtersysteme eingesetzt. Sie blockieren Seiten, auf denen bestimmte Schlüsselwörter oder Sätze enthalten sind oder zeigen zumindest diese Ausschnitte nicht an. Einige Systeme setzen auch kontextsensitive Verfahren ein.

Obwohl dieser Ansatz allein nicht zuverlässig filtern kann,[14] ist er als Ergänzung zu den oben genannten Filterungen nach Bewertungen hilfreich und kann gerade bei Negativlisten die Zuverlässigkeit erhöhen. Seine Leistungsfähigkeit hängt wesentlich von der „Intelligenz“ der Filterung ab.

5 Anwendung: Jugendschutz im Internet

Eine der häufigsten Anwendungen für Filtertechnologien im Internet ist der Jugendschutz. Hier wird die Technologie von Lehren, Eltern oder auch Internetserviceprovidern verwendet, um für Kinder und Jugendliche den Zugang zu jugendgefährdendem und anderem als ungeeignet eingeschätztem Material möglichst zu untersagen und das Internet auch zusätzlich im Rahmen einer umfassenden Medienerziehung zu nutzen. Dabei erfolgt die Bewertung und Auswahl unter der Zielsetzung „Jugendschutz“ und unterscheidet sich damit z.B. von dem in der Diskussion um die Verbreitung von kriminellen Inhalten einzunehmenden Standpunkt. Insbesondere ist hier die Beschränkung pädagogisch gewollt und somit in Hinblick auf einen Zensurverdacht unproblematisch. Allerdings ist bei der konkreten Auswahl und Bewertung von Inhalten die Gefahr einer ungewollten Anpassung an fremde Bewertungsmaßstäbe zu beachten.

[14] Ein gängiges Beispiel für eine unbeabsichtigte Sperrung ist das Internetangebot der University of sussex auf www.sussex.ac.uk, das durch die Filterung nach dem Wort Sex u.U. gesperrt wird. Andererseits werden Bilder oder Audio-Sequenzen mit harmlosen Namen, aber rassistischem Inhalt durch Schlüsselwortfilterung nicht gesperrt.

Die technischen Umsetzungen lassen sich in zwei Typen unterteilen:[15]

- Einzelplatz-Filterprogramme werden zusätzlich zu den Kommunikationsprogrammen lokal – auf einem Client, Proxy oder Netzwerkserver – installiert; sie beobachten dann die transportierten Daten und beeinflussen die Abrufe gemäß ihrer Einstellung.

  In einem solchen Fall wird die gesamte Konfiguration lokal vorgenommen, bleibt daher vertraulich und kann optimal an die individuellen Bedürfnisse und Vorstellungen angepaßt werden. Bei vielen Nutzern und einem feinen Bewertungsschema kann die Konfiguration und Pflege allerdings einigen Aufwand erfordern.

- Ein solches Programm kann alternativ in das Angebot eines Internetserviceproviders eingebunden sein (z.B. bei AOL und Compuserve); dann entfällt die lokale Haltung des Programms. Zusätzlich erfolgt die Pflege der Filterkriterien und -listen an zentraler Stelle – mit weniger Aufwand bei der Verwendung, aber auch weniger Einfluß auf die Filterung.

  Auch eventuelle Probleme im Zusammenspiel zwischen Filtersoftware und Internetprogramm reduzieren sich. Andererseits ist der Filtervorgang weniger transparent. Auch müssen bei der Konfiguration immer Daten an den Provider übergeben werden (z.B. das Vorhandensein minderjähriger Kinder oder Informationen über politische und/oder pädagogische Präferenzen), die sich in den Einstellungen der Filterung niederschlagen. Der Filtervorgang findet ebenfalls beim Provider statt und kann dort protokolliert werden.

Außerdem gibt es eine Vielzahl von Speziallösungen. Diese führen z.T. neben der Filterung auch die Netzwerkadministration oder das Internet Access Mangement durch – dann eher mit einer Zielrichtung für große Netze und kommerzielle Anwendungen. Andere haben neben einfachen Filteransätzen ein eigenes Angebot für Kinder entwickelt, das als pädagogisches Hilfsmittel zur Medienerziehung dienen kann und damit ein zum strengen Filtern paralleles Jugendschutzkonzept verfolgt.

Eine besonders gute Umsetzung der technischen Unterstützung des Jugendschutzes ist dann möglich, wenn die Programme möglichst viele der folgenden Kriterien erfüllen:

- ein großer Funktionsumfang (mindestens Positiv- und Negativlisten und Schlüsselwörter, möglichst auch PICS und kontextsensitive Verfahren)
- offene Bewertungskriterien für die mitgelieferten Listen, möglichst Listen im Klartext oder Werkzeuge zur Überprüfung
- Anpassungsmöglichkeiten an den konkreten Bedarf (Sicherheit, Altersgruppe, Wertvorstellungen), Möglichkeit zur Einrichtung mehrerer Benutzer mit unterschiedlichen Anforderungen
- einfache Verwendbarkeit (sowohl in der Konfiguration als auch im Gebrauch)

Je mehr dieser Kriterien erfüllt sind, desto zuverlässiger wird das Programm die eingestellten Funktionen realisieren können. Allerdings wird ein vollständiger Jugendschutz nie durch technische Maßnahmen allein auf dem Rechner des Endbenutzers gewährleistet werden können.

[15] Auflistungen von einzelnen Produkten und deren Tests finden sich z.B. in [Cranor98], [Schmidt97], [Tomorrow99]

6 Fazit und Konsequenz

Eine zentrale Sperre von Inhalten im Internet läßt sich technisch auf Neztwerkebene noch nicht paßgenau vornehmen. Es sind immer Umgehungen der Sperrungen möglich; gleichzeitig besteht die Gefahr einer zu weit gefaßten Sperrung.

Daher sind zentrale Maßnahmen von staatlicher Seite nicht erfolgversprechend. Die „Ohnmachtserfahrung“ des Staates bedeutet jedoch nicht gleichzeitig eine Kapitulation vor den neuen Gefahren, sondern die modernen Informationstechnologien bergen vielfältige Möglichkeiten, mit denen der Bürger sich selbst schützen kann.

Hier bietet also die dezentrale Kontrolle und Filterung durch den Benutzer selbst nach dessen eigenen Kriterien einen Lösungsansatz. Dazu müssen jedoch die Bewertungen durch Dritte (etwa nach dem PICS-System) nachvollziehbar sein. Beispielhafte Filterkonfigurationen können von einer Vielzahl von Interessengruppen vorgeschlagen werden; der Benutzer muß jedoch die Möglichkeit haben, seine eigene Konfiguration individuell vorzunehmen oder anzupassen.

Ein universelles Rating wie PICS ist mit erhöhtem Zeitaufwand und zusätzlichen Kosten verbunden. Eine Reihe von Anbietern wird daher darauf verzichten, wenn das System nicht einfach zu realisieren und nicht sehr weit verbreitet ist. Den Rating-Organisationen kommt ein hohes Maß an Verantwortung zu, da jede Vorbewertung bereits zur Meinungsbildung der potentiellen Abrufer beiträgt und da absichtliche oder unabsichtliche Fehlbewertungen großen Schaden anrichten können. Es ist daher unbedingt zu verhindern, daß die Definition moralischer und gesellschaftlicher Werte in den Aufgabenbereich privater Organisationen übertragen wird. Durch eine Offenlegung der Bewertungsmaßstäbe und aller Bewertungen kann diese Gefahr des Mißbrauchs reduziert werden.

Sind die organisatorischen Randbedingungen so, daß diese Bedingungen gewährleistet werden können, kann die Inhaltsfilterung ein wirksames Hilfsmittel im Jugendschutz und im pädagogischen Einsatz des Internets sein, das seine Wirkung im Kontext einer umfassenden Medienpädagogik hat. Das Ziel der weiteren Überlegungen muß daher die Herstellung der genannten Randbedingungen sein, also die Definition geeigneter Rating-Systeme und Organisationen und die Schaffung von Anreizen zu deren Verwendung.

Literatur

[Froomkin96] Froomkin, A. Michael: *The Internet As A Source Of Regulatory Arbitrage.* Kahin / Nesson (Hg.): Borders in Cyberspace, MIT Press 1996. http://www.law.miami. edu/˜froomkin/articles/arbitr.htm

[Kossel96] Kossel, Axel: *Kindersicherung: Jugendfreies Internet*. c’t 9/96, S. 120-121.

[Möcke96] Möcke, Frank; Heinson, Dennis: *Ein Krampf: Extremismus im Internet und Zensurversuche*. c’t 11/96, S. 118-125.

[Ponnath96] Ponnath, Heimo: *Pornographie im Internet? Dichtung und Wahrheit.* in‘side online 2/3 1996. http://www.bda.de/bda/jp/home/heimo.ponnath/articles/SiN.html

[Wuermeling96] Wuermeling, Ulrich: *Ordnungshüter im Netz: Anbieter suchen nach Alternativen zum starken Staat*. c’t 9/96, S. 122-125.

[Cranor98] Lorrie Faith Cranor et al: *Technology Inventory – A Catalog of Tools that Support Parents' Ability to Choose Online Content Appropriate for their Children*, http://www.research.att.com/projects/tech4kids/t4k.html

[Schmidt97] Schmidt , Jürgen: *Kindersicheres Netz*, c't 15/97.

[Tomorrow99] *So schützen Sie Ihre Kinder*, Tomorrow, 2/99.