

Andreas Gleis

Technischer Schutz vor Internetschmutz

Filterprogramme: die effektive Lösung für den Jugendschutz im Internet?

Einführung

Gewaltdarstellungen im Internet sind mittlerweile zu einem Thema von gesamtgesellschaftlichem Interesse geworden. Eltern und pädagogische Fachkräfte stehen vor der Frage wie sie mit dem Medium zukünftig umgehen sollen: Den Computer wegschließen oder Passwortschützen ist keine Lösung, denn früher oder später werden Kinder mit dem Medium konfrontiert. Vielmehr ist Internetkompetenz heute eine wichtige Schlüsselqualifikation in Beruf und Privatleben. Schließlich bietet die Internetindustrie technische Schutzmöglichkeiten an, die Minderjährige vor Gewalt- und Pornographiedarstellungen schützen und die „jugendfreien“ Internetinhalte offen lassen soll.

Am 08.05.2002 wurde vom Bundeskabinett die Neuregelung des Jugendschutzgesetzes (JuSchG) beschlossen. Kinder und Jugendliche sollen stärker vor Gewaltdarstellungen, vor allem in den neuen Medien geschützt werden. Voraussichtlich am 12. Juli wird die Vorlage nach den anstehenden Beratungen im Bundestag abschließend vom Bundesrat behandelt werden. Nach dem Kabinettsbeschluss sollen analog zur Alterskennzeichnung von Kinofilmen auch Computerspiele gekennzeichnet werden. Kindern und Jugendlichen wird der Zugriff auf schwer jugendgefährdende Medien, insbesondere mit Gewaltdarstellungen, verboten (diese Regelung ist keine Neuerung, wurde aber in der Pressemitteilung des Familienministeriums neben den „echten“ Neuregelungen hervorgehoben).

Darstellungen in allen herkömmlichen und neuen Medien kann die künftige „Bundesprüfstelle für jugendgefährdende Medien“ (bisher statt „Medien“: „Schriften“) auf die Indizierungssliste setzen. Damit dürfen diese Inhalte Kindern und Jugendlichen nicht mehr zugänglich gemacht werden. Dies gilt auch für Internet-Seiten, allerdings hat diese Indizierung de facto nur Auswirkungen gegenüber deutschen Anbietern. Ob dies ausreichenden Schutz gewährt, ist jedoch eher zweifelhaft, schließlich hört das Internet nicht an den Landesgrenzen auf. Zur freiwilligen Selbstkontrolle haben sich mehr als 400 deutsche Provider¹ verpflichtet, aber die Mehrheit der Gewaltdarstellungen im Internet stammt von Anbietern aus Osteuropa, USA und Asien. Auch indizierte Computerspiele können aus dem Internet, über verschlüsselte Tauschbörsen-Programme (z.B. Filetopia etc.) unmerkelt heruntergeladen werden.

Auch das Verfahren der Indizierung wird neu geregelt: Künftig kann die Bundesprüfstelle ausnahmsweise bereits ohne Antrag gegen jugendgefährdende Darstellungen tätig werden; insbesondere ist das der Fall, wenn eine nicht antragsberechtigte Behörde oder ein anerkannter Träger der freien Jugendhilfe dies anregt. Schon ohne Indizierung sind (wie bisher) kriegsverherrlichende oder die Menschenwürde verletzende Medien wegen ihrer schweren Jugendgefährdung den indizierten Medien gleichgestellt und unterliegen daher weitreichenden Abgabe-, Vertriebs- und Werbeverboten. Im Zuständigkeitsbereich der Länder sollen parallel zum neuen JuSchG in einem Jugendmedienschutz-Staatsvertrag der Länder begleitende Regelungen getroffen werden, die zwischen Jugendgefährdung und Jugendbeeinträchtigung unterscheiden. Der JMStV soll eine größere Transparenz im Jugendschutzrecht schaffen.

¹ Internet Service Provider sind Firmen, die den Zugang zum Internet zur Verfügung stellen.

In diesem Beitrag werden Funktionsweisen dieser Filtersoftware², ihre Vor- und Nachteile sowie pädagogische Strategien aufgezeigt. Der Artikel hat allerdings nicht den Anspruch, das Thema Jugendschutz im Internet vollständig abzudecken. So konnten wichtige Akteure (Bundesprüfstelle für jugendgefährdende Schriften - BPjS, Freiwillige Selbstkontrolle Multimedia - FSM) nicht berücksichtigt sowie weitere Möglichkeiten des Internet-Jugendschutzes (Rating-Verfahren, Meldestellen etc.) nicht behandelt werden.

Immer mehr Kinder verbringen immer mehr Zeit im Internet. Bei Eltern, Pädagoginnen und Pädagogen gibt es gleichermaßen Unsicherheit und ein Bedürfnis nach Schutz. Mit diesen Bedürfnissen in Familien und in der Jugendhilfe lässt sich hervorragend Geld verdienen. Das beweist die Existenz zahlreicher Softwareprodukte, mit denen es möglich ist, Webseiten³ mit jugendgefährdenden Inhalten automatisch herauszufiltern. Den Erziehenden soll durch den Kauf eines solchen Computerprogramms das zeitaufwendige Aufsichtführen oder das Wegschließen des Computers erspart bleiben. Außerdem werden die Kinder laut Werbeaussagen damit nicht aus der Informationswelt des Internet ausgeschlossen, sondern das Internetsurfen⁴ für sie nur sicherer gemacht.

Die Filterprogramme schützen vor potentiellen Missständen im Internet und wehren unerwünschte, gefährliche und illegale Informationen ab. Kuhlen (2000) vergleicht die Phantasien, die in die Filtersoftware hereingeprojiziert werden einerseits mit dem 'Schutzengel', der den Nutzer vor den Bedrohungen des Internets schützt sowie andererseits mit dem 'Gespenst', das durch das Internet zieht und Seiten zensiert: "Die emphatisch Zustimmenden sehen in diesen Verfahren die Chance, die Kontrolle über Internetinformationen zu behalten. Die kategorisch Ablehnenden sehen die Einschränkung des freien Zugriffs auf Information, wittern sogar die Gefahr des Einstiegs in eine umfassende Internet-Zensur und sei es nur eine Selbstzensur".

Begriffsdefinitionen Filtern & Abblocken

Filtern ist die Leistung, gewünschte Informationen von Ungewünschten zu unterscheiden und nur die gewünschten bereitzustellen. Dagegen ist das Abblocken die umgekehrte Leistung der Filterung: Die unerwünschten Informationen werden von dem Benutzer ferngehalten. Weiterhin unterscheidet man nach aktivem Abblocken und passivem Abblocken. Beim passiven Abblocken hat der Nutzer selber keinen Einfluss darauf, welche Informationen blockiert werden. Vielmehr entscheiden andere darüber, welche Informationen dem Nutzer zur Verfügung stehen. Beim aktiven Abblocken kann dies der Nutzer selber bestimmen.

Funktionsweisen der Filtersoftware

Filterprogramme regulieren den Zugriff auf Informationen und Dienste des Internets nach wählbaren Kriterien. Installieren lassen sich die hier vorgestellten Programme entweder auf dem Rechner des Nutzers oder auf einem Proxy⁵. Es gibt außerdem Filterprogramme, die direkt auf dem Server des Zugangsproviders liegen. So gliedert der Provider AOL verschiedene Bereiche des Internets z.B. nach Altersgruppen und schränkt die Zahl der erreichbaren Seiten für Kinder z.T. erheblich ein.

² Software ist der Sammelbegriff für alle Arten von Computerprogrammen.

³ Als Webseiten werden Internetangebote aus dem World Wide Web (www, weltweites Netz) bezeichnet. Das www ist der jüngste Dienst im Internet, der sich durch hohe Benutzerfreundlichkeit sowie multimediale Elemente auszeichnet.

⁴ Surfen ist der umgangssprachliche Ausdruck für das Bewegen im Internet.

⁵ Ein Proxy ist ein zwischengeschalteter Rechner einer Institution, der den Zugang mehrerer Nutzer in Internet verwaltet.

Die Programme bieten verschiedene technische Lösungsansätze, um eine Filterung zu gewährleisten. Die empfangenen Datenpakete werden nach der Absende-URL⁶ untersucht und dann inhaltlich ausgewertet. Daraus ergeben sich dann Aktivitäten wie Protokollierung, Warnmeldungen, die Blockierung von inkriminierten Webseiten, die Trennung vom Internet, bis hin zum Abschalten des Computers. Je nach Softwareprogramm werden die folgenden Funktionen einzeln oder kombiniert eingesetzt:

- **Zum Protokoll, bitte...**

Jede aufgerufene Webseite wird protokolliert. Bei einigen Programmen ist es daher später ohne weiteres für Eltern oder Pädagogen möglich, die Internetseiten "nachzusehen". Programme sind sogar in der Lage, den Erziehenden die Protokolldatei per E-Mail zuzuschicken und bieten damit eine Fernüberwachungsfunktion.

- **Disney ja - Pro Familia nein (site blocking)**

Viele Filterprogramme arbeiten mit Sperrlisten, also mit gesammelten Adressen von Webseiten, die blockiert werden sollen. Diese Listen enthalten sowohl positive als auch negative Internetseiten. Während die Positivlisten Seiten enthalten, die für Kinder unbedenklich und geeignet zu sein scheinen (z.B. Walt Disney), sind die Internetseiten auf den Negativlisten ('schwarze Listen') für den minderjährigen Nutzer überhaupt nicht mehr aufrufbar.

In diesen Listen sind die Inhalte der Seiten mit bestimmten Kriterien aufgelistet. Das Programm Cyberpatrol unterscheidet beispielsweise nach Kategorien wie Gewalt, teilweise und komplette Nacktheit, Satanischem/Kulthaften und vielem mehr. Hier kann der Nutzer sogar Seiten zur Sexualaufklärung/AIDS oder Tabak/Alkohol abstellen. Bei vielen Programmen ist es für den Nutzer zudem möglich, den Sperrlisten neue Einträge hinzuzufügen. Eine Beschränkung der Internetnutzung auf die Positivliste ist bei vielen Programmen möglich, aber nicht anzuraten, denn dadurch wird die Internetnutzung auf einen minimalen Teil des Internets reduziert, der zum größten Teil auch noch englischsprachig ist. Schlechte Programme sperren bisweilen ganze Topleveldomains (Hauptadressen mit allen darunter liegenden Dokumenten, z.B. den Fernsehsender www.SWR.de), so dass der Nutzer an Inhalte des ganzen Servers nicht mehr herankommt (z.B. das empfehlenswerte SWR-Kindernetz).

Diese umfangreichen Listen werden von Mitarbeitern der Softwarefirmen gepflegt und klassifiziert und können als Update aus dem Internet herunter geladen werden. Die Updates dieser Listen sind entweder im Kaufpreis enthalten, oder werden nach Ablauf einer gewissen Periode kostenpflichtig.

- **Schlüsselwörter (keyword blocking)**

Hierbei handelt es sich um ein simples Sprachanalyseverfahren. Bevor die aufzurufende Internetseite angezeigt wird, untersucht das Programm sie auf Schlüssel- oder Stoppwörter. Falls keine anstößigen Begriffe oder "bösen Wörter" in dieser Seite vorkommen, erscheint sie auf dem Bildschirm, ansonsten wird sie gesperrt. Für die Softwarefirmen haben diese Schlüsselwortlisten den Vorteil, dass sie kaum der Pflege und Aktualisierung bedürfen und damit kostengünstig sind. Es gibt immer noch Programme, die ausschließlich mit Schlüsselwortanalyse arbeiten.

- **Inhaltsbewertung (page labeling)**

Filtersoftware ist in der Lage, in den Internetseiten versteckt gespeicherte Texte auszulesen, nach denen die Anbieter den Inhalt dieser Seiten selber klassifiziert haben. Je nach Einstellung wehrt die Filtersoftware dann die angewählte Seite ab oder stellt sie dar. Allerdings benötigt der Internetnutzer für diese Inhaltsbewertung nicht unbedingt ein Filterprogramm, denn aktuelle Versionen der Internet-

⁶ Eine URL entspricht der Adresse eines Internet-Angebotes (z.B. www.lwl.org/jugendamtsverzeichnis)

browser⁷ haben solche Ratingsysteme bereits integriert. So enthält der MS Internet-Explorer z.B. den „Inhaltsratgeber“.

- **Andere Internetdienste**
Neben dem www gibt es noch weitere Internetdienste, die unerwünschte Inhalte transportieren können. Dazu gehören z.B. E-Mails oder Chatprogramme⁸ (mIRC, AIM, ICQ, Netmeeting etc.) über die auch Dateien ausgetauscht werden können. Einige Filterprogramme ermöglichen es, diese unterschiedlichen Dienste zu sperren oder zu regulieren. Über das Internet hinaus ist es bei einigen Programmen auch möglich, einzelne auf der Festplatte abgespeicherte Programme oder Spiele, zu sperren.
- **Benutzerprofile**
Ein PC wird vielfach von unterschiedlichen Personen genutzt, daher haben Filterprogramme in der Regel mehrere Benutzerprofile, bei denen Konten für die verfügbare Onlinezeit detailliert eingerichtet sowie unterschiedliche 'Freiheitsgrade' für die einzelnen Benutzer bestimmt werden können. Manche Programme (z.B. Contentbarrier) gehen sogar so weit, dass man den „Reifegrad“ des Benutzers angeben muss.
- **Programmsicherheit**
Die Programme müssen vor der Aushebelung durch nicht autorisierte Benutzer geschützt sein. Völlig nutzlos wären die Programme wenn sie jeder Nutzer einfach wieder deinstallieren könnte, daher sollten sich die Programme nur mit Passwordeingabe wieder vom Computer entfernen lassen.

Probleme

Filterprogramme sind bereits zum Politikum geworden. So haben sich die US-Präsidentschaftskandidaten im Jahr 2000 ein Rededuell geliefert, in dem Einigkeit darüber herrschte, dass jungen Menschen Sexseiten im Internet per Filtersoftware zu verschließen seien. Nicht strittig war die Tatsache an sich, sondern nur mit *welchem* Softwareprogramm die Seiten blockiert werden sollen

Wirksamkeit der Filterung

Die Werbung der Herstellerfirmen suggeriert Filterquoten von bis zu 97% (z.B. cybersitter.com). Die Programme laufen Werbeaussagen zufolge also nahezu perfekt: sie filtern den 'Schmutz' heraus und lassen pädagogisch Wertvolles durch. Bei näherer Betrachtung wird allerdings deutlich, dass dieses Versprechen einer hochgradig wirksamen Filterung praktisch nicht einlösbar ist.

Unbegrenztheit des Netzes

Das Internet ist ein "unerschöpfliches" Medium. Es ist über Sperrlisten de facto unmöglich, das Internet so zu kategorisieren, dass alle anstößigen Inhalte ausgesperrt werden können. Auch die Filtersoftwareanbieter erstellen ihre Negativ-/Positivlisten nur mit Suchmaschinen und/oder Beschwerden, die Ihnen von Nutzern angetragen werden. Bei dem exponentiellen Wachstum von Webseiten ist es auch mit hohem Personalaufwand nicht durchführbar, die rechtswidrigen Seiten lückenlos zu blockieren. Filterprogramme sind dazu verdammt, der Entwicklung des Internets nachzuhinken.

⁷ Browser sind Programme mit denen Webseiten betrachtet werden können (z.B. Internet Explorer, Netscape Navigator, Opera). Abgeleitet vom Englischen "to browse" (durchblättern, schmökern, sich umsehen)

⁸ Chat ist die Bezeichnung für "Unterhalten" oder "Plaudern" in Online-Diensten.

Regeln für die Filter

Wenn die Filterprogramme noch sehr viele unerwünschte Internetseiten anzeigen, dann liegt das an der Schwierigkeit, Regeln für die Filterung zu erstellen. Die Frage welche Seiten angezeigt werden dürfen und welche nicht, ist sehr komplex. Schließlich soll der Nutzer so wenig wie möglich in seinem sonstigen Surfverhalten beschränkt werden.

Filterprogramme 'scannen' die Internetseiten bisher rein lexikalisch und verstehen nicht, dass Worte verschiedene Bedeutungsebenen haben. Kommt das Wort 'Sex' auf einer Seite vor, so wird diese Seite gesperrt, egal ob es sich um eine pornografische oder aber eine Seite über Sexualaufklärung handelt. Wenn Filter derart eng geschnürt sind, kommt es also dazu, dass alle Seiten, die „Sextant“ enthalten, gesperrt werden. Der Wortbestandteil „sex“ wird immer eindeutig negativ interpretiert. Ebenso ist es dieser Schlüsselwortsuche nicht möglich, historische Berichte über das Dritte Reich von rechtsradikaler Hetze zu unterscheiden.

Wird die Leine dagegen zu locker gelassen, erhöht sich die Durchlassquote der Seiten, die eigentlich blockiert werden sollten.

Filterquote und US-Lastigkeit

In seiner Diplomarbeit für die Universität Koblenz testete Tröndle 1999 einige Filterprogramme systematisch und stellte fest, "daß 75% der (...) gefundenen Web-Sites fälschlicherweise als anstößig bzw. als unangemessen deklariert und damit abgeblockt wurden und 41% der im Prinzip nach den Vorgaben eigentlich anstößigen bzw. unangemessenen Websites nicht als solche identifiziert wurden und damit frei zugänglich blieben. (...) Zum einen wird (...) offensichtlich viel zu viel abgeblockt, zum anderen kann man sich nicht darauf verlassen, dass nichts durchschlüpft, was unerwünscht ist." Andere Testberichte sprechen von 10% blockierten Positivseiten (c't 23/2000), bis hin zu 35% (TIFAP 1997). Die Filterquoten der Programme differieren stark von Testbericht zu Testbericht. Während im Magazin 'Chip' ein Programm eine Erfolgsquote von 80% hatte, erreichte dasselbe Programm in der Zeitschrift 'c't' eine Quote von nur 60%.

Englischsprachige .com-Pornoseiten werden von sämtlichen Softwareprogrammen sehr gut gefiltert, die deutschen Gegenstücke wesentlich schlechter. Verallgemeinernd kann behauptet werden, dass die Filterquote umso höher ist, je mehr englischsprachige Internetseiten mit dem Schwerpunkt Pornographie zum Testsample gehören. Die Filterquote wird geringer, je mehr deutschsprachige und/oder politisch radikale Seiten zum Testumfang gehören. Somit wird deutlich, dass die Programme alle für den amerikanischen Markt ausgelegt sind. Der Schwerpunkt der Programme liegt eindeutig auf der Filterung von Pornographie und nicht auf politisch extremen Inhalten.

Bild-, Video- und Audioanalyse

Aktuelle Filtersoftware versagt bei unkommentierten Bildern und Videos. Zwar sind auf manchen Internetseiten Graphiken im Seitenaufbau mit beschreibenden Texten hinterlegt, die von Filtersoftware erkannt werden. Auch können einige wenige Programme aus (nicht sichtbaren) Meta-Informationen, die in Grafiken/Fotos gespeichert sind, erkennen, dass diese Dateien blockiert werden müssen. Trotzdem ist Filtersoftware bisher noch nicht in der Lage, eine Bildanalyse durchzuführen. Es gibt im Bereich der Digitalphotoarchivierung bereits erste Forschungsansätze, die sich mit dem Vergleichen von Bildmustern und -strukturen beschäftigen, um beispielsweise ähnliche Bildmotive herauszufinden. Diese Programme befinden sich allerdings momentan noch in der Versuchs- bzw. Entwicklungsphase und sind noch nicht in bereits erhältliche Filtersoftware integriert. Sie können daher noch kein jugendgefährdendes Bildmaterial erkennen.

Es gibt allerdings mittlerweile Programme, die nach Werbeaussagen bereits "Hass- und Gewaltsymbole", "Rassistische Bilder und Symbole" und "sexuell explizite Bilder" finden können. Die Firma gibt keinerlei Auskünfte über die Funktionsweise ihres Programms.

Falls sich solche "Visual Intelligence Plattformen" durchsetzen, werden sie mit ähnlichen Problemen wie die o.g. textbasierten Filter zu kämpfen haben. Deren Probleme lassen sich auch auf Grafik- und Videoanalyse übertragen. Auch Bilder können viele Bedeutungen haben. Wie will man Regeln für historische Fotos oder neutrale Aufklärungsbilder erstellen? Welche Filter werden Karikaturen erkennen und Satire durchlassen? Auf der technischen Seite ist ein erheblich höherer Aufwand erforderlich, denn Bilder und Videos verbrauchen wesentlich mehr Speicherplatz als eine Textdatei und müssen zuerst dekomprimiert und entschlüsselt werden.

Es wird wohl nur eine Frage der Zeit sein, bis Entwickler von Spracherkennungssoftware Wortfilter für das gesprochene Wort z.B. bei Internetkonferenzen und Sprachchats oder für die "explicit lyrics" in Liedtexten entwickeln werden. Vorstellbar ist jedenfalls jetzt schon, was mit visuellen und tonalen Filterprogrammen möglich sein könnte: Werden zukünftig in jedem Tatort, der per Video on Demand ins Haus kommt, automatisch Schimanskis Flüche herausgepiept? Werden Eltern Videoclips nach dem Grad der Bauchfreiheit der Sängerin sperren können?

Sicherheit der Programme

Eine 1999 vom Bundesministerium für Wirtschaft aufgegebenen Studie besagt: "Technische Lösungen zur Filterung der Inhalte bieten bisher keinen adäquaten Schutz, und können prinzipiell keinen absoluten Schutz bieten."

- **Entfernbarkeit:**
Alle Filterprogramme können ausgehebelt werden. Das Programm 'Netnanny' funktioniert schon nicht mehr, wenn nur der Dateiname des Browsers geändert wird. Das Programm SOS KidProof kann sogar ganz regulär ohne Passwortschutz entfernt werden.
In der Regel greifen die Programme zwar wesentlich tiefer in das jeweilige Betriebssystem ein, können aber von versierten Benutzern - zu denen Kinder und Jugendliche oftmals eher gehören als ihre Eltern - wieder entfernt werden.
- **Hackanleitung:**
Detaillierte Anleitungen oder sogar von Hackern bereitgestellte Entfernungsprogramme (zur Deinstallation) finden sich für nahezu alle Filterprogramme im Internet. Noch raffinierter sind Programme, die eine aktive Filtersoftware vortäuschen und kostenlos im Internet herunterladbar sind. So lassen sich beispielsweise SurfWatch, Cyber Patrol, CYBERSitter, NetNanny, X-Stop, PureSight und Cyber Snoop durch das Mini-Programm Peacefire.exe einfach austricksen.
- **Zusatz-Kick:**
Das Blockierprogramm wird minderjährigen Surfern von ihren Eltern und Erziehern aufoktroiert. Der Anreiz für den Benutzer, diese Programme zu umgehen ist um so größer, je stärker er sich durch die Sperrung behindert fühlt. Durch das Knacken des Programms erweitern sie ihre Bewegungsfreiheit. Kinder und Jugendliche kommen schnell darauf, dass Sperrlisten löscher, Systemdateien austauschbar oder parallele Betriebssysteminstallationen machbar sind. Es hat für sie einen großen Reiz, die Sicherheitslücken der Software herauszufinden, schließlich empfinden sie sich bei erfolgreicher Aushebelung cleverer als die Programmierer und die Erwachsenen, die das Programm installiert haben. Außerdem macht es Spaß, die Funktionsweise der Programme abzuklopfen und logische oder technische Mängel herauszufinden. Provozierend könnte man behaupten, dass ein installiertes Filterprogramm Kinder und Jugendliche sogar dazu animieren kann, jugendgefährdende Seiten zu besuchen, um herauszufinden, wovor die Eltern/Pädagogen sie da eigentlich beschützen wollen. Bei den o.g. niedrigen Filterquoten ist ohnehin davon auszugehen, dass die Kinder und Jugendlichen schon nach wenigen Versuchen erfolgreich auf „verbotene“ Seiten gelangen.

Wertvorstellungen und Betriebsgeheimnisse der Softwareproduzenten

Auch die Philosophie der Hersteller von Filterprogrammen spielt eine große Rolle. So wird z.B. die Software CyberSitter von einer US-Organisation "Focus on the Family" (www.family.org) entwickelt. Die Organisation hat sich damit ein Instrument geschaffen, um gezielt ihre pruden Moralvorstellungen durchzusetzen. Dieses Programm filtert neben sexuellen Aufklärungsseiten auch Begriffe wie "homosexuality", "bullshit" oder "lovestory" (vgl. www.jugendschutz.net) heraus. Themen wie Schwangerschaftsverhütung, Homosexualität oder die künstlerische Darstellung von Nacktheit sind nicht im Interesse des Herstellers und werden ausgesiebt.

Der Nutzer hat aus geschäftspolitischen Gründen keine Einsicht in die verschlüsselten Sperrlisten - andere Firmen könnten die mühevoll Handarbeit ja übernehmen. Die Hersteller argumentieren damit, dass offen gelegte Sperrlisten die Gefahr beherbergen Surfer über diese Listen direkt zu den anstößigen Seiten zu bringen. (Trotzdem bin ich bei der Internetrecherche zu diesem Artikel auf geknackte und offen gelegte Linklisten der Programme CyberSitter und NetNanny gestoßen).

Wird ein Seitenanbieter in eine Negativliste aufgenommen oder wird seine Seite durch 'keyword blocking' nicht angezeigt, so erhält er darüber keine Information und kann darauf auch nicht reagieren. Die Listen nehmen keinerlei Einfluss auf das Internetangebot an sich, sondern blenden nur die vermeintlich negativen Teile aus. Dadurch ist natürlich auch kein „pädagogischer Effekt“ für den Anbieter der (eventuell) anstößigen Information möglich. Er kann sich nicht rechtfertigen oder seine Seiten so verändern, dass er in Zukunft nicht mehr blockiert wird. Und wenn eine Seite erstmal blockiert ist, bedarf es große Anstrengungen sie wieder freigeschaltet zu bekommen (vgl. www.blinde-kuh.de).

Die Firmen legen allerdings nicht einmal ihre Kategorisierungskriterien offen. Es existiert auch keine übergeordnete Kontrollinstanz, die die Listen bewertet oder mit der zusammen Kriterien für Sperrlisten entwickelt werden. Zensur ist damit nicht kontrollierbar, sondern namens- und gesichtslos.

Wenn eine Institution oder Eltern Filtersoftware einsetzen wollen, sollten sie sich also über die Wertvorstellungen und politischen Anschauungen der Softwarefirma (oder den dahinter stehenden Organisationen) genauer informieren. Nutze ich ein solches Programm, unterwerfe ich mich (und die Kinder und Jugendlichen) einer Firma, die entscheidet, welche Informationen gut oder schlecht für mich sind. Die Filterprogramme werden daher von Gegnern als „Censorware“ bezeichnet.

Global unterschiedliche Wertvorstellungen

Es gibt weltweit kein einheitliches Wertesystem, vielmehr ist das Internet „ein globaler Kulturraum, in dem viele Auffassungen zusammenkommen. Amerikaner definieren das Recht auf Meinungsfreiheit anders als etwa Asiaten. Und dann unterscheiden sich nationale Empfindlichkeiten von globalen" (Müller-Manguhn 2000).

Es ist nicht möglich, für jeden Kulturkreis mit Zugang zum Internet die passenden moralischen und normativen Filterkriterien herauszufinden. Für die Softwarehersteller ist es überhaupt nicht machbar, einen allgemeingültigen Standard hierfür zu definieren, denn die Vorstellungen sind immer von kulturellen, religiösen und politischen Vorstellungen und individuellen Sozialisationsgeschichten geprägt. Während in Deutschland einerseits die Darstellung eines nackten Erwachsenenkörpers für liberale Eltern und Pädagogen kein Thema ist, kann dies beispielsweise in den USA zu Problemen führen. Andererseits fällt in den USA, die Leugnung des Holocausts unter das Recht auf freie Meinungsäußerung – ein Umstand, der in Deutschland wiederum undenkbar ist. Diesen extrem unterschiedlichen Wertvorstellungen schenkt die für den amerikanischen Markt produzierte Software kaum Rechnung, nicht einmal in regionalisierten deutschen Versionen der Programme: "Die puritanische Sex-Einstellung in den USA drückt in den Abblockverfahren

der Welt ihren Stempel auf" (Kuhlen 2000). Es ist sehr unwahrscheinlich, dass jemals ein für alle Kulturen gemeingültiger Standard gefunden werden kann.

Entwicklung

Die Nachfrage nach diesen Filterprogrammen steigt rasant. Die darauf spezialisierte Firma SurfControl vermeldete für das zweite Halbjahr 2001 einen Umsatzwachstum von 72 Prozent auf 24,4 Millionen US\$ gegenüber dem gleichen Vorjahreszeitraum. Zurzeit gibt es auf dem Markt etwa 60 Programme. Die Preise liegen zwischen 10,- und 80,- Euro. Zwar gibt es einige Softwareprodukte, die für Eltern umsonst sind. Für Schulen, Jugendzentren, Bibliotheken und andere Institutionen gilt aber bei nahezu allen Filterprogrammen, dass diese kostenpflichtig sind. In den USA wird momentan mit dem „Children's Internet Protection Act“ ein Gesetzesentwurf vor Gericht verhandelt, der es vorsieht, öffentlichen Einrichtungen, die den Zugang zum Internet nicht durch solche Programme filtern, die staatlichen Zuschüsse zu entziehen.

Fazit und Handlungsvorschläge

Weder „Schutzengel“ noch „Gespenst“

Eltern und pädagogische Fachkräfte können sich keinesfalls auf diese technischen Ansätze verlassen. Die Filtersoftware ist auf dem heutigen Stand der Technik absolut ungenügend. Als alleinige Schutzmaßnahmen sind diese Programme substanzlos und untauglich. Der lexikalische Ansatz dieser Programme ist von atemberaubender Schlichtheit, die Programme sind bisher noch nicht in der Lage, kontextorientiert zu arbeiten und damit die Mehrdeutigkeit von Worten in den Angeboten zu erkennen.

Filterquoten von 40 bis 80 Prozent der jugendgefährdenden Seiten sind eindeutig zu wenig. Außerdem ist die Software i.d.R. nur auf dem Rechner vor Ort installiert. Kinder und Jugendliche können bei Freunden oder im kommerziellen Internetcafé frei und ohne Softwareblockaden surfen. Darüber hinaus ist die Software leicht zu entfernen oder auszuhebeln.

Als einigermaßen sinnvoll könnte man die Überwachungsfunktion der Programme anführen, denn sie erlaubt zumindest das Festhalten der besuchten Internetseiten. Anhand dieser Protokolle können Eltern und Pädagogen fallweise den Kindern „nachsurfen“, damit Sie zumindest einen Überblick gewinnen können, wohin deren Reise gegangen ist. Ob das dem Vertrauensverhältnis zwischen Erwachsenen und Kindern förderlich ist, kann bezweifelt werden. Außerdem können diese Protokolle von geschickten Benutzern gelöscht werden.

Es ist deutlich geworden, dass diese technischen Möglichkeiten höchstens als flankierende Maßnahmen genutzt werden können. Wo das Individuum und seine Selbstbestimmung einen hohen Stellenwert genießen, kann es keine einfachen und automatisierbaren Erziehungsschemata geben.

Was können pädagogische Fachkräfte und Eltern tun?

Mit diesem Beitrag sollen die vorhandenen Jugendgefährdungen nicht abgeschwächt werden: Kinderpornographie, sexuelle Anmache, extreme Darstellungen von Gewalt und Verletzungen der Menschenwürde, Kriegsverherrlichungen, Nazi-Propaganda u.v.m. gefährden Kinder und Jugendliche im Internet und sind nicht zu tolerieren. Aber: Erziehende kämen auch nicht auf die Idee, ihre Kinder und Jugendlichen nur in Begleitung eines Leibwächters in die Fußgängerzone zu lassen, in der viele reale Gefahren existieren. Kinder und Jugendliche wollen nicht beschützt, sondern ernstgenommen werden. Sie lernen in und aus Beziehungen mit den Erwachsenen:

- Kindern und Jugendlichen im Internet sollte immer eine erwachsene Begleitung zur Verfügung stehen. Und zwar nicht als Aufsicht, sondern als Berater und Ansprechpartner.
- Die Auseinandersetzung der Erziehenden mit Kindern und Jugendlichen ist von zentraler Bedeutung. Sie sollten gemeinsam das Internet erkunden, es verstehen lernen und unbequemen Fragen nicht ausweichen. Eltern und pädagogische Fachkräfte sollten gemeinsam mit den Kindern surfen, über das Internet sprechen und dabei Sexualität, Gewalt und politische Ideologien nicht tabuisieren.
- Kinder benötigen zudem klare Anweisungen, wo sie sich im weltweiten Netz bewegen dürfen.
- Kindern muss die Gelegenheit gegeben werden, sich selbständig im Internet zu bewegen. Eltern, Jugendhilfe, Schule und andere öffentliche Institutionen müssen sie dabei unterstützen und ihnen Medienkompetenzen vermitteln. Unabdingbar ist es, ihnen die Fähigkeit mitzugeben, zwischen wertvollen und unnützen Informationen unterscheiden zu können.
- Eltern und Fachkräfte sollten den Kindern und Jugendlichen Tipps mitgeben, die sowohl in der realen, als auch in der virtuellen Öffentlichkeit sinnvoll sind: "Sprich nicht mit Fremden" und "Gib keine Informationen über Dich und Deine Familie nur weil Du danach gefragt wurdest.", "Gib niemandem, den Du nicht kennst Deine (E-Mail-) Adresse." (siehe Kasten „Sicherheitsregeln im Internet“)
- Für Fachkräfte in Jugendhilfe und Schule ist es besonders wichtig, sich intensiv mit dem Medium auseinanderzusetzen. Sie müssen beispielsweise wissen, welche Sprache und Strategien Pädophile im Internet benutzen, um Kinder zu locken.
- Eltern und Einrichtungen können auch strukturelle soziale Kontrolle schaffen: Der Computer kann so platziert werden, dass es für Kinder nicht möglich ist, alleine den Bildschirm zu betrachten. Einige öffentliche Bibliotheken gehen sogar so weit, einen zusätzlichen Monitor mit gleichem Bildschirminhalt, der für alle Bibliotheksbesucher einsehbar ist, über dem Internetarbeitsplatz aufzuhängen. Aus fachlicher Sicht ist es nicht notwendig, Kindern und Jugendlichen ständig über die Schulter zu gucken. Viel wichtiger ist es, dass den Kindern und Jugendlichen kontinuierlich ein Berater und Ansprechpartner für das Medium zur Verfügung steht.
- Es gibt auch kleine, ganz pragmatische Möglichkeiten für Kinder, die Begegnung mit dem Internet sicherer zu gestalten: So kann die Startseite des Internetbrowsers auf eine kinderfreundliche Suchmaschine gelegt werden (z.B. www.blindekuh.de).

Neben den direkten Erziehungspartnern von Kindern und Jugendlichen (Eltern, Schule und Jugendhilfe) sind andere Instanzen gefragt:

Die Internet-Wirtschaft muss sich stärker selber in die Verantwortung nehmen. Sie macht es sich zu einfach, wenn sie nur auf Softwarelösungen verweist und damit die Verantwortung an Eltern und pädagogische Fachkräfte abtritt. Die Freiwillige Selbstkontrolle Multimedia hat zwar einen eigenen Verhaltenskodex aufgestellt. Sanktionen gegenüber Mitgliedern der FSM finden aber de Facto nicht statt. Nur die wenigsten Internetangebote werden inhaltlich gekennzeichnet (labeling).

Politik muss die Rahmenbedingungen dafür setzen, dass Bildung und Erziehung den Rang erhalten, den sie verdienen. Die Erziehungsverantwortung der Eltern muss durch eine strukturelle Familienpolitik unterstrichen werden und nicht durch eine Erhöhung des Kindergeldes. Neben diesen finanziellen Aspekten benötigen Kinder, Jugendliche und die Erwachsenen, die sie erziehen, vor allem eines: gesellschaftliche Anerkennung.

Aus der aktuellen Diskussion (Stichwort: Erfurt) sollte nicht der Schluss gezogen werden, dass Computer und Internetanschlüsse aus Jugendeinrichtungen verbannt gehören. In der Studie "Internet - außerschulische Lernangebote für Kinder und Jugendliche bis zum 14. Lebensjahr" (2001) fordert das Deutsche Jugendinstitut (DJI) vielmehr die Einrichtung von weiteren Internetplätzen in außerschulischen Einrichtungen (Horten, Jugendhäusern etc.), denn dem Großteil der Kinder und Jugendlichen fehlen Zugänge zum Internet.

Sicherheitsregeln im Internet

Du solltest misstrauisch werden und mit einer Vertrauensperson sprechen:

- wenn Dich jemand zu irgendetwas überreden oder zwingen will ...
- wenn Dich jemand erpressen will oder Dir droht ...
- wenn jemand "schweinische" Wörter benutzt ...
- wenn Dich jemand locken oder kaufen will ...
- wenn jemand Dir großzügige Geschenke anbietet ...
- wenn Dir jemand Angebote macht, die sich einfach zu gut anhören wie z.B. in einem Film mitspielen, als Model arbeiten, ganz billig Super-Turnschuhe besorgen oder ähnliches ...
- wenn jemand hauptsächlich über Dein Aussehen und Deinen Körper reden will ...
- wenn jemand über Sex spricht, Dir sexuelle Dinge von sich erzählt oder nach Deinen sexuellen Erfahrungen fragt ...
- wenn jemand Fotos von Dir machen will ...
- wenn Dich jemand gegen Deine Eltern oder andere Menschen aufhetzen will ...
- wenn Dir jemand Geheimnisse erzählt oder verlangt, dass Du niemand etwas weitersagen darfst.

Weitere Sicherheitsregeln

- Gib niemand im Internet Deine Adresse, Deine Telefonnummer oder die Adresse Deiner Schule, ehe Du mit Deinen Eltern oder einer anderen Vertrauensperson darüber gesprochen hast.
- Schicke niemand Dein Bild.
- Gib keine Informationen über andere Menschen, z.B. Deine Eltern, Deine Geschwister oder Freunde weiter, ehe Du sie gefragt hast, ob es okay ist.
- Gib keine Kreditkartennummern weiter und erzähle nichts über Geld.
- Triff Dich nie allein mit jemandem, den Du im Internet kennengelernt hast. Sprich vorher mit Deinen Eltern oder einer anderen Vertrauensperson.
- Wenn Du Dich mit jemandem triffst, tu das immer an einem öffentlichen Ort z.B. einem Café oder dem Jugendzentrum. Es reicht nicht, wenn Du einen Freund oder eine Freundin mitnimmst. Beim ersten Treff sollte unbedingt ein Erwachsener dabei sein.
- Bleib nicht in Chat-Rooms, in denen über Dinge gesprochen wird, die Dir seltsam vorkommen, Dir unangenehm oder peinlich sind, Dir Angst machen. Wenn Du ein komisches Gefühl hast, traue diesem Gefühl und erzähle jemandem davon.

Quelle: mit freundlicher Genehmigung der Arbeitsgemeinschaft Kinder- und Jugendschutz, Landesstelle NRW

Weiterführende Links:

Übersicht über Filtersoftwareprogramme
<http://fsm.de/info/software/index2.shtml>

Jugendschutz.net, die Zentralstelle der Länder für Jugendschutz in Mediendiensten
<http://www.jugendschutz.net>

Aktion Kinder- und Jugendschutz, Fach- und Landesstellen
<http://www.jugendschutz.de/>

Bundesprüfstelle für jugendgefährdende Schriften (BPjS)
<http://bpjs.bmfsfj.de/>

Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM)
<http://www.fsm.de/>

INHOPE (Internet Hotline Providers in Europe Association)
<http://www.inhope.org/>

DJI-Studie Kinder im Internet: Medienpädagogische Informationen für Erwachsene & Internetseiten für Kinder
<http://www.dji.de/www-kinderseiten/default.htm>

LWL-Landesjugendamt
<http://www.lja-wl.de>

Literatur:

Bundesministerium für Wirtschaft und Technologie - BMWi (1999): Jugendschutz und Filtertechnologien im Internet,
<http://www.secorvo.de/projekt/jugendschutz.htm>, Stand: 11.05.2002, Berlin

Deutsches Jugendinstitut - DJI / Feil, Christine (Hrsg.)(2001): Internet für Kinder. Hilfen für Eltern, Erzieher und Lehrer. Opladen

Kühlen, Rainer (2000): Gespenst oder Schutzengel - Ambivalenz von Filter-, Abblock- und Rating-Verfahren,
URL: http://www.inf-wiss.uni-konstanz.de/People/RK/Texte/tk_jb00.html/,
Stand: 11.05.2002, Konstanz

Tröndle, M. (1999): Experimentelle Bewertung von Blocking- und Filtersystemen im Internet. Ein Vergleich der Systeme von Net Nanny, Cyber Patrol, Cyber Sitter und Surf Watch. Diplomarbeit im Fach Informationswissenschaft an der Universität Konstanz. Konstanz August 1999

Andreas Gleis

Diplom-Sozialarbeiter, Fachberater Jugendarbeit, verantwortlich für den Internetauftritt des Landesjugendamtes Westfalen-Lippe