Friedemann Schindler

Rating und Filtering

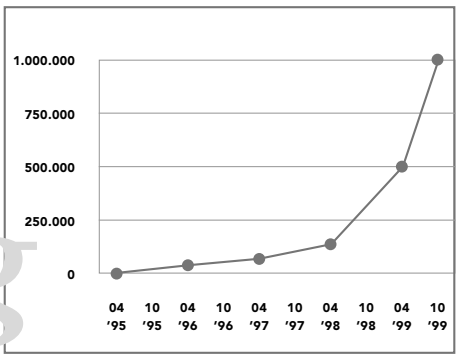
Zukunftstechnologien im Jugendschutz?!?

Das Internet war lange Jahre ein Medium für junge, gebildete Männer, die schnelle innovative Kommunikationsformen mit wissenschaftlichen Inhalten bevorzugten. Seit Mitte der neunziger Jahre hat sich das Netz der Netze aber sehr schnell zu einem Massenmedium entwickelt, in dem kommerzielle Inhalte dominieren und das zunehmend auch von Kindern und Jugendlichen genutzt wird. Das Internet bietet zwar immer noch jedem Nutzer die Möglichkeit, seine Ideen und Vorstellungen in der Öffentlichkeit zu präsentieren, sich zu vernetzen und kulturelle Schranken zu überwinden, es hat sich inzwischen aber auch zu einem jugendgefährdenden Ort entwickelt, in dem ohne Rücksicht auf Kinder und Jugendliche alles angeboten wird, was sich vermarkten lässt. Da die einst wirksame Selbstregulierung der Online-Gemeinde (Netiquette) ihre Wirksamkeit weitgehend verloren hat, wird jetzt nach geeigneten Schutzmaßnahmen gerufen, die Kindern und Jugendlichen einen sicheren Zugang zum Netz ermöglichen sollen.

Neue Dimensionen des Jugendschutzes

Wie in jedem anderen Medium stößt man auch im Internet auf altbekannte problematische Inhalte: Gewaltverherrlichung, rassistische Propaganda, Angst einflößende Darstellungen von satanistischen und okkulten Gruppierungen, Pornographie.

Tabelle: Entwicklung der Zahl der Webseiten, die bei der deutschen Registrierungsstelle Denic angemeldet wurden (Quelle: nic.de)



Neu sind jedoch die Dimensionen, mit denen das Internet den Jugendschutz konfrontiert:

— Neu ist die Geschwindigkeit, mit der sich das Internet vergrößert. Zur Zeit verdoppelt sich die Zahl der Webseiten jedes halbe Jahr. Man geht davon aus, dass das World Wide Web inzwischen auf eine Größe von etwa einer Milliarde Seiten angewachsen ist.
— Neu ist die Vielfalt der Anbieter. Jeder Nutzer ist auch ein potentieller Sender, schon mit 100 DM pro Monat lässt sich eine funktionierende „Sendeanlage" betreiben.
— Neu ist die allgemeine Zugänglichkeit von Internet-Angeboten. Es gibt keine Zugangsbeschränkungen oder Vorprüfungen mehr, nationalstaatliche Schutzregelungen werden zunehmend obsolet – ausländische Angebote sind immer nur einen Mausklick entfernt.
— Neu ist die große Bedeutung pornographischer Angebote im Internet. Pornographie ist integraler Anteil der Internet-Ökonomie.[1]
— Neu ist die Aggressivität, mit der Porno-Anbieter im Internet agieren. Im Kampf um die Aufmerksamkeit der Nutzer wer-

den ihnen unliebsame Angebote regelrecht aufgedrängt. Auch wer nicht nach Pornographie sucht, wird damit behelligt.[2]

— Neu ist auch die Aggressivität in Bezug auf die Inhalte. Es werden zunehmend „bizarre" und „bestialische" Sexualpraktiken präsentiert. Dabei werden gesellschaftliche Tabus massenhaft durchbrochen.[3]

Angesichts dieser neuen Dimensionen erweisen sich viele traditionelle Konzepte des Jugendschutzes als stumpf: Das Internet ist zu schnell, zu vielfältig, und viele ausländische Anbieter sind für die deutsche Strafverfolgung schlicht nicht erreichbar. Die Hoffnung ist deshalb groß, Filtersysteme könnten das Dilemma lösen und den Internetzugang für Minderjährige angemessen regulieren. Seit 1995 entwickeln deshalb Firmen in den USA die unterschiedlichsten Software-Systeme, die alle von sich behaupten, sie könnten problematische Inhalte automatisch und zuverlässig ausfiltern.

Technische Schutz-Konzepte

Filtersysteme sind Anwendungen, die den Zugriff auf Informationen oder Dienste des Internet nach vorgegebenen Kriterien regulieren. Diese Filtersysteme können auf dem Rechner des Nutzers, auf dem zentralen Netzzugang einer Institution (z. B. auf einem Proxy-Server einer Schule) oder auf den Rechnern eines Providers (z.B. AOL oder t-online) installiert sein und unterschiedliche Aktivitäten auslösen: vor problematischen Seiten warnen, die Adressen der besuchten Seiten aufzeichnen, inkriminierte Seiten blockieren oder einen Rechner ausschalten. Sie basieren im Wesentlichen auf drei Konzepten:

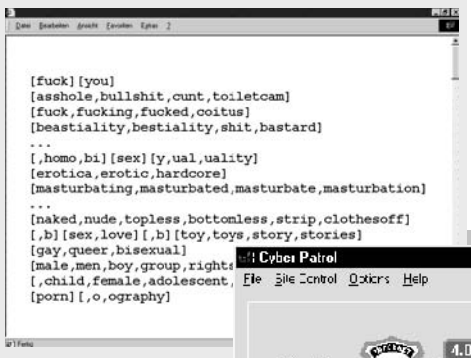
— Das „keyword-blocking" basiert auf Listen mit „forbidden words", die auf einer Seite nicht vorkommen dürften;
— das „site-blocking" nutzt zum Filtern eine Liste mit handverlesenen, unerlaubten Netzadressen;
— beim "page-labeling" klassifiziert jeder Anbieter seine Seiten selbst – die Rating-Information ist im „unsichtbaren" Header jeder Webseite untergebracht.

keyword-blocking

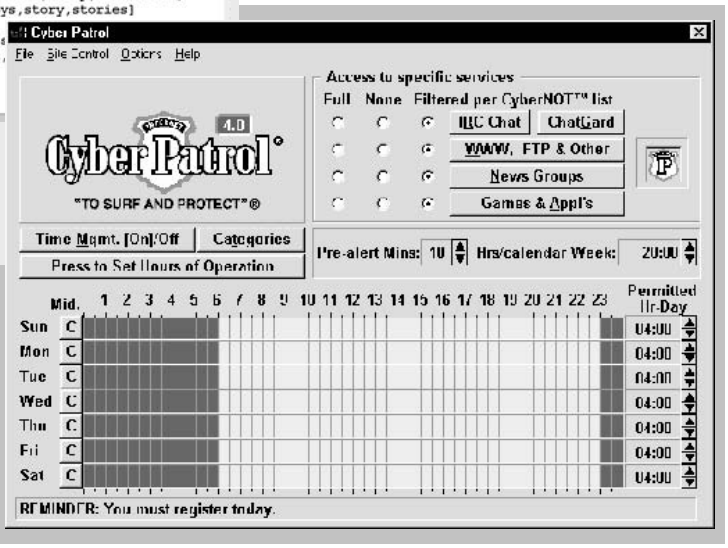
Auf dem Konzept des „keyword-blocking" basieren Programme wie CyberSitter und NetNanny. „Keyword-blocking"-Programme sind in der Herstellung relativ billig und auch einfach zu pflegen, da im Wesentlichen nur eine Liste mit „verbotenen" Worten zusammengestellt und ergänzt werden muss. Diese Programme können auch Seiten blockieren, die neu ins Netz gestellt werden, sofern sie inkriminierte Keywords enthalten. Sie versagen aber komplett bei Bildern, Sounds oder Videos ohne erläuternden Text.

Das größte Problem all' dieser Lösungen ist aber die Mehrdeutigkeit von Begriffen. Bisher gibt es keine Software-Lösung, die Wörter in ihrem Kontext zu analysieren vermag. Stoßen NetNanny und Co. auf das Wort „Pornography", schlägt der Filter gnadenlos zu, egal ob es sich um ein pornographisches Angebot handelt oder um dessen Kritik.[4]

CyberSitter und NetNanny beschränken sich ausschließlich auf englische Begriffe. In der Liste der „forbidden words" taucht kein einziger deutscher Begriff auf, selbst Standardbegriffe wie „Pornographie" können in deutscher Schreibweise[5] ohne Beanstandung den Filter passieren, von deutschen „Fachausdrücken" wie „ficken", „bumsen", „blasen" ganz zu schweigen.



Auszüge aus der Liste der forbidden-words von Cybersitter – sexuality, boygroup, gay, lovestory werden gesperrt.



CyberPatrol Headquarter – Zeitbeschränkungen und Einstellungen der zu filternden Dienste.

Unbrauchbar sind die beiden „keyword-blocking"-Lösungen aber auch aus ideologischen Gründen, weil sie mehr als nur die unzulässigen Inhalte zensieren. Hinter CyberSitter steht die christlich-konservative US-Organisation „Focus on the Family", die ihre prüden Moralvorstellungen auch über Filter durchzusetzen versucht. Es werden jegliche Informationen über Verhütung, Abtreibung und Minderheiten ausgesperrt, Begriffe wie „homosexuality" oder Schimpfwörter wie „bullshit" werden gnadenlos unterdrückt, selbst „nude", „topless" oder „lovestory" führen zur Sperrung. So ist es kein Wunder, dass eine Untersuchung von amerikanischen Bibliotheken zum Ergebnis kam, dass dank CyberSitter mehr als 30% der Internet-Seiten eines Testsamples nicht mehr erreichbar waren.

site-blocking

Eine größere Treffsicherheit weisen Filtersysteme auf, die mit „site-blocking" arbeiten. Jede Webseite wird von Menschen gesichtet, bevor sie in die schwarze Liste eingetragen wird. Der große Nachteil dieser Lösungen besteht darin, dass das Angebot im Netz nicht annähernd erfasst werden kann und dass die Sichtung immer der rasanten Entwicklung im Internet hinterherhinkt. Problematisch ist aber auch, dass die relevanten schwarzen Listen verschlüsselt sind und als Betriebsgeheimnis streng gehütet werden. Würde es gelingen, die Verschlüsselung einer solchen Liste zu knacken, könnten Konkurrenten sie ohne Probleme übernehmen. Wenn ein Angebot auf einer solchen Liste landet, wird der Anbieter nicht benachrichtigt – er kann sich also nicht

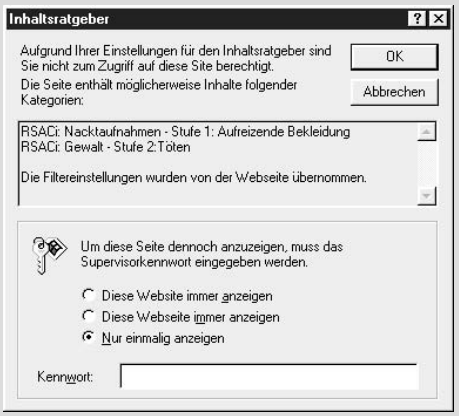
rechtfertigen oder sein Angebot entsprechend verändern. Es gibt auch keine unabhängige Kontrollinstanz, die die Korrektheit der Liste überprüft bzw. an der Kriterienbildung beteiligt ist.[6]

Marktführer im Bereich der Filtersysteme ist das Programm CyberPatrol, das hauptsächlich auf dem „site-blocking"-Konzept basiert. Die Kosten sind relativ hoch. Inklusive der vierteljährlichen Update-Gebühren kostet der Schutz vor problematischen Inhalten etwa so viel wie der Internetzugang selbst. Über die Größe und Zusammensetzung der aktuellen Cyber-Not-Liste findet man keine genauen Angaben, es sollen bisher 150.000 Web-Adressen[7] aufgelistet worden sein.

page-labeling

Führende Firmen der Internet-Industrie setzen inzwischen ganz auf das „page-labeling", um Kinder im weltweiten Datennetz vor „Schmuddelangeboten" zu schützen. Microsoft, AOL/Bertelsmann, t-online und andere Global Player haben im Mai1999 in London die Vereinigung Internet Content Rating Association (ICRA) gegründet, um eine Filtermöglichkeit für Inhalte des World Wide Web zu entwickeln, die „auf der Selbstregulation von Anbietern basiert, die Meinungsfreiheit und den Wettbewerb nicht behindert sowie die kulturelle Vielfalt in Europa berücksichtigt".

Das „page-labeling"-System basiert auf PICS (Platform of Internet Content Selection), das vom MIT entwickelt wurde. PICS sieht vor, dass jeder Anbieter seine Seiten mit einem Label versieht, das den Inhalt einer Seite treffend kennzeichnet. Die Vorteile des „page-labeling" liegen vor allem in der Transparenz – man kann auf jeder Seite sehen, wie sie klassifiziert wurde – und in der Offenheit. PICS ist nur eine leere Hülle, die mit unterschiedlichen Kennzeichnungssystemen inhaltlich gefüllt werden kann. Durch den Einsatz unterschiedlicher Bewertungssysteme können verschiedene moralische, politische und religiöse Vorstellungen weltweit berücksichtigt werden. Theoretisch könnte sich jeder Nutzer eine Labeling-Plattform auswählen, die seinen ideologischen und moralischen Vorstellungen am ehesten entspricht.

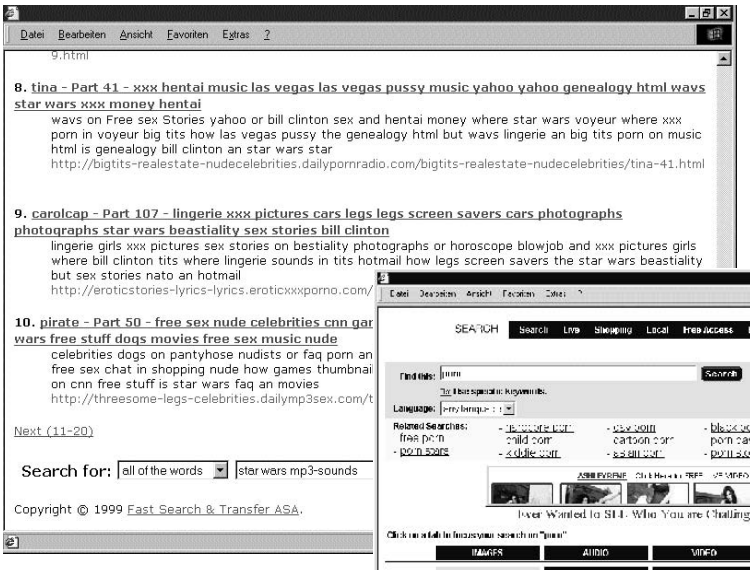


Warnmeldung des Internet Explorers, wenn eine Seite angezeigt werden soll, die den Filterkriterien nicht entspricht.

Es gibt bisher aber nur zwei relevante Bewertungssysteme. Sie stammen vom Recreational Software Advisory Council (RSACi), einer amerikanischen Institution, die in der Vergangenheit hauptsächlich Computerspiele klassifizierte, und von SafeSurf, der Plattform einer amerikanischen Elterninitiative. Dem Nutzer entstehen beim Filtern keine zusätzlichen Kosten. Er braucht auch kein zusätzliches Schutzprogramm, da Internet Explorer oder Netscape PICS bereits unterstützen. Je nach Filterkonfiguration werden nur die Seiten vom Browser gesperrt, deren Label auf problematische Inhalte hinweisen, oder zusätzlich auch alle Seiten, die kein Label besitzen.

Problematisch an diesem Ansatz ist vor allem die Beliebigkeit eines Self-Ratings. Warum sollten Porno-Anbieter plötzlich ein Interesse haben, ihre Seiten korrekt zu labeln? Um von Suchmaschinen überhaupt gefunden zu werden und in den Trefferlisten möglichst weit vorne zu rangieren, „klassifizieren" Porno-Anbieter ihre Seiten massenhaft falsch. Sie versuchen Suchmaschinen mit allen erlaubten und unerlaubten Mitteln auszutricksen, indem sie z. B. mit aktuellen Keywords (z. B. Kosovo, Star Wars, Lara Croft) möglichst viele Surfer auf ihre Seiten locken, die mit dem Angebot nicht das Geringste zu tun haben.

Krasse Beispiele für falsches Labeling liefern aber auch seriöse Anbieter wie die Suchmaschine Altavista, die sich selbst mit null Gewalt, null Nacktheit, null Sex und null Kraftausdrücken klassifiziert hat. Bei Eingabe des Suchbegriffs „porn" präsentiert die Suchmaschine nicht nur pornographische Werbebanner, sondern sie gibt dem Suchenden auch Hinweise, wie er angesichts der Fülle an Treffern seine Suche präzisieren kann. Im Bereich der „related searches" „empfiehlt" Altavista, es doch mal mit den Suchbegriffen „kiddie-" bzw. „kiddy porn" zu versuchen – wohlgemerkt alles unter dem selbst gewählten Label: null Sex, null Gewalt.



Falsch deklarierte Seiten – die Suche nach Sound-Tracks von Star Wars listet auf den ersten Plätzen nur Porno-Angebote auf.

Eine „gewaltlose" und „sexfreie" Suchmaschine empfiehlt – Suchbegriffe aus dem Kinderpornographischen Spektrum.

Gerade der PICS-Ansatz, der eigentlich der Zensur im Internet vorbeugen soll, birgt zudem die Gefahr flächendeckender Zensurmaßnahmen in sich. Es gibt nicht nur in vielen Firmen, sondern auch in vielen Staaten Bemühungen, unliebsame Web-Inhalte im eigenen Einflussbereich zu unterdrücken. Ein Seitenlabel kann nicht nur auf dem heimischen Computer ausgewertet werden, sondern prinzipiell auf jedem Rechner, über den diese Webseite geroutet wird. PICS eröffnet die Möglichkeit für eine flächendeckende Blockade unliebsamer Inhalte, es besteht damit die Gefahr einer drastischen Einschränkung der Meinungsfreiheit. Ein flächendeckendes Labeling von Webseiten würde es z. B. Staaten wie China wesentlich erleichtern, oppositionelle Inhalte auszuschalten.

Amerikanische Moralvorstellungen

Allen Systemen ist gemeinsam, dass sie entweder überhaupt keine oder zu wenig Informationen über ihre ideologische Grundausrichtung liefern. Es gibt bisher keinerlei vereinheitlichte Filter-Kriterien. Die meisten Filter transportieren amerikanische Moralvorstellungen, die mit den Verhältnissen in der BRD nicht kompatibel sind. Alle Filtersysteme bieten relativ feine Einstellungsmöglichkeiten im Bereich von Nacktheit und Sexualdarstellung. PICS/RSACi arbeitet im Bereich Nacktheit beispielsweise mit fünf Filterstufen: „keine Nacktheit, aufreizende Bekleidung, unvollständige Bekleidung, frontale Nacktheit, provokative frontale Nacktheit"[8]. Für unsere Arbeit bei *jugendschutz.net* beginnen aber die Probleme erst bei der letzten Filterstufe namens „provokative frontale Nacktheit". Erst dann ist unsere Entscheidung gefragt, ob es sich um beeinträchtigende, gefährdende oder um unzulässige Angebote handelt. Ob sich Personen „leidenschaftlich küssen" oder „milde Kraftausdrücke" nutzen, ist unter dem Aspekt der Beeinträchtigung oder Gefährdung von Jugendlichen völlig irrelevant.

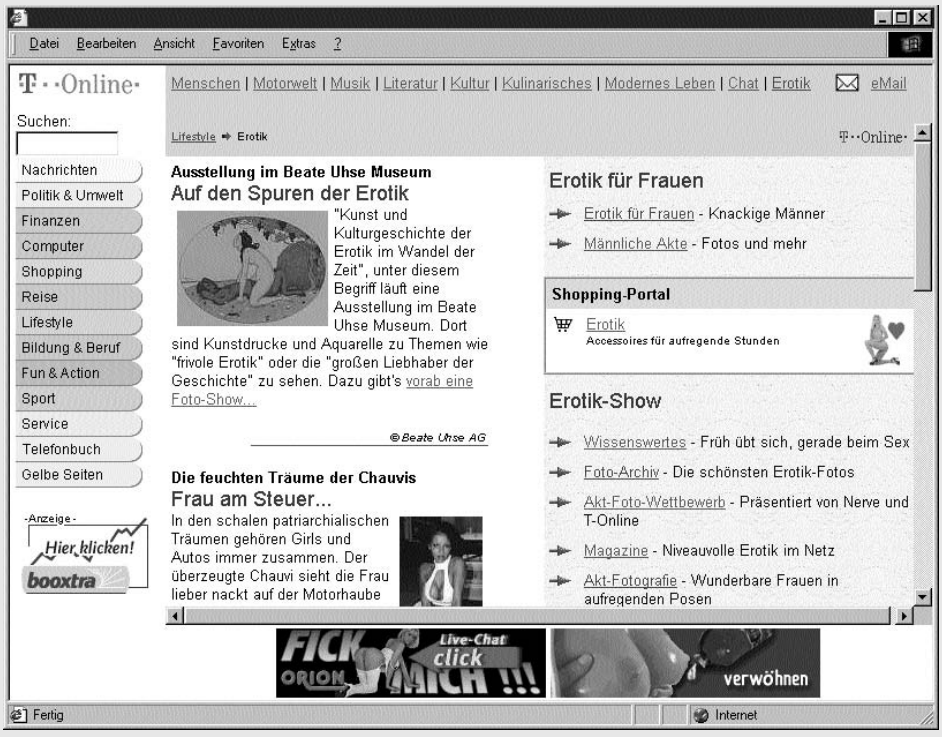
Wirksamkeit

Wir sind gerade dabei, die Wirksamkeit der vorgestellten Schutzlösungen einmal etwas genauer zu überprüfen. Die Untersuchung ist noch nicht abgeschlossen, aber eine erste Auswertung zeigt, dass CyberPatrol und Netnanny im Bereich der pornographischen Angebote etwa die Hälfte der Webseiten filtern können, sobald man aber nach deutschen Begriffen sucht (z. B. „faustfick" statt „fistfuck") sinkt die Erkennungsquote auf etwa ein Drittel. Vor allem Sites mit eindeutigen Titeln wie „sex" oder „porn" werden relativ zuverlässig erkannt, Sites mit deutschen Titeln wie „schlampen", „sittenstrolch" oder „geile weiber" kennen die Filterlösungen aber in der Regel nicht.[9] Während in den USA ein großes Problem darin besteht, dass die Filter auch viele empfehlenswerte Seiten sperren, weil sie für moralisch bedenklich gehalten werden oder weil Begrifflichkeiten der Stop-Wort-Liste doppeldeutig sind, scheint dieses Problem für deutsche Verhältnisse weniger relevant zu sein – die entsprechenden Programme kennen keine deutschen Begriffe und lassen deshalb fast alles passieren.

Völlig unwirksam ist bisher das PICS-System. Nach unseren bisherigen Erkenntnissen sind nur etwa 2% der Seiten entsprechend klassifiziert. Das PICS-System ist aber nur dann richtig wirksam, wenn alle Webseiten ein korrektes Label haben. Der Browser weist den Surfer bei 98 von 100 Seiten darauf hin, dass die Seite nicht klassifiziert ist, und fragt nach, ob die Seite trotzdem angezeigt werden soll. Besser kann man sich das Surfen nicht verleiden, denn bei jeder Nachfrage muss das Passwort neu eingegeben werden.

Allen Verlautbarungen zum Trotz scheinen aber selbst die Global Player, die dieses - Rating-System forcieren wollen, an PICS zu glauben. Nicht einmal die Hälfte der ICRA-Mitglieder hat das eigene Web-Angebot überhaupt klassifiziert, nur Microsoft hat sich die Mühe gemacht, jede einzelne Seite differenziert zu labeln. Bei t-online beispielsweise gibt es nur ein globales Label für das gesamte Angebot: „aufreizende Bekleidung" (Nacktheit Stufe 1) und „töten" (Gewalt Stufe 2). Dieses globale Label wird dem Angebot aber in keiner Weise gerecht. Die Telefonauskunft von t-online ist weder „aufreizend" noch gewalthaltig, das Erotikangebot von t-online bietet dagegen Bilder, das nach dem PICS-Schema korrekterweise als „provokative frontale Nacktheit" (Nacktheit Stufe 4) klassifiziert werden müsste. Welche Einstellung Eltern auch wählen – entweder wird für Kinder auch die Telefonauskunft gesperrt, oder die Beate-Uhse-Seiten sind frei für sie zugänglich.

Beispiel für falsches Labeling – „leicht bekleidete" Models und Links zu Beate Uhse.

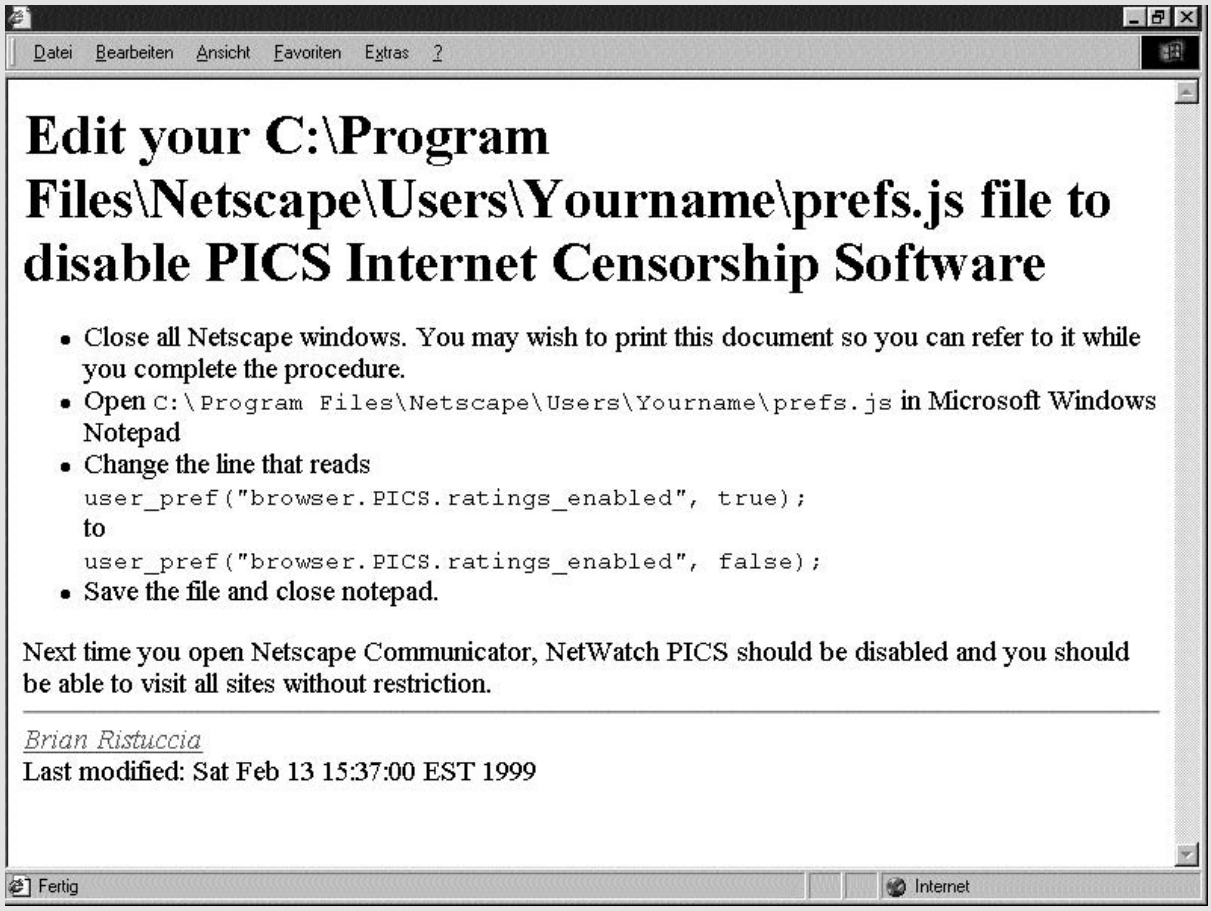


HackZ und CrackZ

Filterprogramme sind kompliziert und alles andere als einfach in der Handhabung. Da Kinder in der Regel technisch versierter sind als ihre Eltern, werden sie ein solches Schutzsystem schneller durchschauen als ihre Erziehungsberechtigten. Alle Systeme, sofern sie auf einem lokalen Rechner installiert sind, können sehr einfach ausgehebelt werden. Das fängt beim Löschen der Sperrlisten an, reicht über das Austauschen der Systemdateien, die den Schutz realisieren, bis hin zur Installation eines neuen oder zum Betrieb eines parallelen Systems/Browsers auf dem geschützten Rechner. Wem selbst nicht einfällt, wie er die Sperren umgehen kann, der muss nur im Internet danach suchen.

„Where Do We Not Want You To Go Today" – CyberSitter

```
To disable CYBERsitter 97:
Rename the file c:\windows\system\wsock32.dll to wsock32.bak
Rename the file c:\windows\system\wsockc97.dll to wsock32.dll
```



„PICS Censorware Disable" – Schalter in den Netscape-Preferences.

Um zu überprüfen, wie fit Kinder und Jugendliche beim Umgehen von Schutzlösungen wirklich sind, haben wir in Kooperation mit dem Offihaus in Bad Freienwalde einen Workshop mit Kindern im Alter von 12 bis 14 Jahren durchgeführt – es waren keine Experten, sondern „normale" Spiele-Kids ohne tiefer gehende Computerkenntnisse. Aufgabe der Kinder war es, NetNanny, CyberPatrol und PICS zu „knacken". NetNanny war nach 20 Minuten geknackt,[10] bei CyberPatrol dauerte es ein wenig länger[11] – am längsten bissen sie sich an PICS die Zähne aus, obwohl die Lösung dort am einfachsten ist.[12] Auf die Idee, im Internet zu gucken, sind die Kinder zwar in der Vorbesprechung gekommen, es waren aber die erwachsenen Betreuer, die diesen Weg eingeschlagen haben – nach einer halben Stunde hatten sie Crack-Hinweise für alle drei Schutzlösungen.

Workshop mit Jugendlichen im Bad Freienwalde.

Ein kinderfreundliches Netz

Als alleiniger Schutz sind alle technischen Schutzlösungen untauglich. Eine Begleitung von Kindern und Jugendlichen im Internet ist immer nötig, was nicht heißen soll, dass man ihnen ständig über die Schulter gucken muss. Es ist aber wichtig, dass Eltern und Pädagogen als Begleiter und Berater zur Verfügung stehen. Eine pädagogische Begleitung ist Blockaden immer vorzuziehen, weil sie am ehesten zur Erziehung junger Menschen und zur Herausbildung von Medienkompetenz beiträgt.

Die Forderung nach mehr Medienkompetenz ist modern geworden. Abgesehen davon, dass kaum Mittel für die Förderung eines medienkompetenten Umgangs mit den neuen Medien bereitgestellt werden, wird diese Debatte viel zu undifferenziert geführt. Es gibt Inhalte im Internet, die sind unzulässig und haben dort generell nichts zu suchen (z. B. Kinderpornographie, Nazi-Propaganda). Es gibt jugendgefährdende Inhalte (z. B. Pornographie), die Kindern und Jugendlichen nicht zugänglich gemacht werden dürfen. Sie gehören in geschlossene Benutzergruppen mit einem funktionierenden Altersprüfungssystem. Und es gibt den Bereich von jugendbeeinträchtigenden Angeboten, in dem Filtersoftware und die Förderung von Medienkompetenz sinnvollerweise zum Tragen kommen könnten. Es lässt sich trefflich darüber streiten, wo Gefährdung aufhört und Beeinträchtigung beginnt, aber es ist unverantwortlich, die gesamte Last problematischer Inhalte auf den Schultern von Kindern und Jugendlichen bzw. Eltern und Pädagogen abzuladen.

Um das Netz kinderfreundlicher zu gestalten, bedarf es gemeinsamer und koordinierter Anstrengungen, auch und gerade auf internationaler Ebene. Man braucht eine aufmerksame Nutzergemeinde, die problematische Inhalte an Hotlines meldet. Es bedarf einer Internet-Industrie, die auch soziale Verantwortung für die Gestaltung ihres Angebots übernimmt. Und man braucht effektive Kontrollen und eine schnelle Strafverfolgung, wenn unzulässige Angebote im Netz auftauchen. In diesem Rahmen können Rating und Filtering unter Umständen eine sinnvolle flankierende Maßnahme sein – mehr nicht!

Friedemann Schindler ist Sozialpädagoge, Medienpädagoge und Mediendesigner mit dem Schwerpunkt „Interaktive Medien". Seit 1999 ist er pädagogischer Mitarbeiter von jugendschutz.net, *der Zentralstelle der Länder mit Sitz in Mainz, die für die Beachtung des Jugendschutzes in den neuen Informations- und Kommunikationsdiensten sorgen soll.*

Anmerkungen:

1
Seriöse Schätzungen gehen davon aus, dass zurzeit 20% des Umsatzes im Internet mit Pornographie erzielt werden. Auch die Anzahl pornographischer Seiten lässt sich nur schätzen. Die Internet-Industrie geht von einem Anteil von nur 1% aus, meint damit aber in erster Linie Kinderpornographie. Wenn man in die großen Suchmaschinen einschlägige pornographische Suchbegriffe eingibt, dann lässt die gemeldete Trefferzahl vermuten, dass der Pornographie-Anteil eher im Bereich von 5 bis 15% liegen dürfte.

2
Suchmaschinen werden massenhaft mit falschen Keywords ausgetrickst, Fake-Seiten werden ins Internet gestellt, um potentielle Nutzer einzufangen, oder die pornographischen „Appetizer" kommen gleich ungefragt per E-Mail direkt ins Haus, egal ob es sich dabei um einen Account eines Kindes oder einer pädagogischen Institution handelt.

3
Die Suchmaschine Altavista meldet bis zu einer Million Webseiten, die mit kinderpornographischen Keywords um das Interesse der Online-Kunden werben.

4
Das gilt für alle gebräuchlichen pornographischen Suchbegriffe wie „anal" oder „oral", „teen" oder „pre-teen", „tier" oder „zoo".

5
Geblockt wird nur „pornography", nicht einmal „Pornographie" mit „ie" am Ende oder „Pornografie" nach neuer Rechtschreibung werden erkannt.

6
Hochgradig sensibel sind diese Listen aber auch, weil sie „Hitlisten" sind, die optimal darüber informieren, wo es im Internet Sex-Angebote zu finden gibt. Während die meisten Firmen diese Listen deshalb auch verschlüsseln, ist die schwarze Liste bei NetNanny offen zugänglich (etwa 10.000 Adressen).

7
Wenn man CyberPatrol über das Internet bezieht, ist standardmäßig noch die Filterliste vom April 1999 aktiv. Erst ein Update der Filterliste, auf dessen Notwendigkeit an keiner Stelle hingewiesen wird, bringt die Liste auf den neuesten Stand.

8
Bezeichnung der Ratingstufen aus der deutschen Version des Internet Explorers, es gibt aber zum Teil erhebliche Definitionsunterschiede. Beispielsweise Gewalt Stufe 2 wird im Internet Explorer als „Töten – Verletzen oder Töten von Menschen oder Tieren" definiert, bei RSACi als „destruction of realistic objects", was auch Gewalt gegen Sachen einschließt.

9
Die Erkennungsquote bei rechtsextremistischen Seiten liegt bei CyberPatrol bei etwa 25% – es sind vor allem die bekannten Seiten wie die des Klu-Klux-Klan, die gesperrt werden. Die Erkennungsleistung von Net-Nanny haben wir in diesem Bereich noch nicht getestet.

10
Das NetNanny-Verzeichnis wurde einfach umbenannt.

11
CyberPatrol „merkt", wenn das Verzeichnis umbenannt wird. Die Kinder kamen aber schnell darauf, dass man ja auch die CyberNot-Liste durch eine leere Liste ersetzen kann.

12
Man muss nur einen anderen Browser installieren.