DuD
Datenschutz und Datensicherheit

Technische Systeme zur Gewährleistung von Jugendschutz im Internet

Dirk Fox

Über Filtersysteme zur Gewährleistung von Jugendschutz im Internet wird seit Mitte der 90er Jahre intensiv gestritten. Vor allem der Versuch, mit der jüngsten Gesetzgebung und auf der Grundlage bestehender Rechtsvorschriften die Internet-Zugangsanbieter in die Verantwortung für Inhalte im Internet zu nehmen, hat zu heftigen fachöffentlichen Diskussionen geführt.[1] Vor diesem Hintergrund wurde die Secorvo Security Consulting GmbH mit der Erstellung einer Studie zu technischen, rechtlichen und soziologischen Aspekten des Jugendschutzes im Internet beauftragt, die Ende des Jahres 1999 vorgelegt wurde.[2] Die Ergebnisse sind aktueller denn je. Sie werden im folgenden in vier zentralen Thesen zusammengefasst.[3]

Dipl.-Inform.
Dirk Fox

Security Consultant und Geschäftsführer der Secorvo Security Consulting GmbH.
Arbeitsschwerpunkt: Public Key Infrastrukturen, Digitale Signaturen, Sicherheit in Netzen.
E-Mail: fox@secorvo.de

These 1

Die Durchsetzung von Jugendschutz im Internet ist eine gänzlich neue Herausforderung für die moderne Informationsgesellschaft.

Die neue Dimension dieser Aufgabe macht sich vor allem an zwei Kernpunkten fest:

- der neuen Qualität des Mediums „Internet“ und
- der neuen Quantität des Inhaltsangebots im Internet.

Worin diese beiden Charakteristika bestehen und warum sich aus ihnen eine gänzlich neue Herausforderung für den Jugendschutz im Internet ergibt, wird im folgenden ausführlicher diskutiert.

1.1 Neue Qualität des Mediums

Das Internet besitzt gegenüber herkömmlichen Medien, in denen Maßnahmen zur Durchsetzung des Jugendschutzes angewendet werden, wie dem Fernsehen, Rundfunk, Videos oder Printmedien, eine Reihe von Eigenschaften, die es zu einem Medium mit einer bisher nicht gekannter Qualität machen.

Zu diesen speziellen Eigenschaften zählen die folgenden, die im Hinblick auf Maßnahmen zur Umsetzung von Jugendschutz von Bedeutung sind:

- **Zugang und Verfügbarkeit**: Im Unterschied zu anderen Medien unterliegen die Inhalte des Internet keinen Verfügbarkeitseinschränkungen.

Hingegen sind Zeitschriften nur am Kiosk zu den üblichen Öffnungszeiten oder über ein Abonnement zu erwerben, ein Video in einer Videothek, ein spezieller Fernsehfilm oder eine Rundfunksendung nur zu einer definierten Sendezeit, ein Buch im Buchhandel oder in einer Bibliothek.

Die Zugangsbeschränkungen dieser herkömmlichen Medien enthalten einen definierten Zugriffspunkt, über den die Verfügbarkeit bestimmter Inhalte kontrolliert werden kann (Verkäufer, Verleiher, Eltern, ...). Natürlich können Kontrollmaßnahmen an diesen Zugriffspunkten nicht verhindern, dass Jugendliche diese umgehen. Die Umgehung ist jedoch in der Regel nicht einfach und mit einem hohen Entdeckungsrisiko behaftet, so dass sie die Ausnahme und nicht die Regel darstellt.

- **Uneinheitlicher Rechtsrahmen**: Der den im Internet bereitgestellten Inhalten zugrundeliegende Rechtsrahmen kann bei einem Inhaltsanbieter (genauer: demjenigen, der bestimmte Inhalte zum Abruf bereitstellt) und einem Nutzer des Internet sehr verschieden sein.

Das ist anders bei herkömmlichen Medien: Da die Verbreitung orts- oder landesgebunden ist, greifen hier für das „Bereitstellen“ und die Nutzung von Inhalten dieselben Rechtsnormen. Im Internet machen die unterschiedlichen Rechtssysteme zudem auch die Verfolgung von Verstößen schwierig, schließen sie häufig sogar praktisch aus.[4]

- **Hohe Unmittelbarkeit**: Zwischen Erstellungs- und Bereitstellungszeitpunkt von Inhalten im Internet liegen oft nur Sekunden.

Anders als bei anderen Medien sind die Erzeugung und Verbreitung von Inhalten im Internet keinem Prozess (Freigabe, Druck, Verteilung, Ausstrahlung etc.) unterworfen, in dessen Verlauf eine Überprüfung, ggf. Überarbeitung und explizite Freigabe der Inhalte erfolgen könnte.

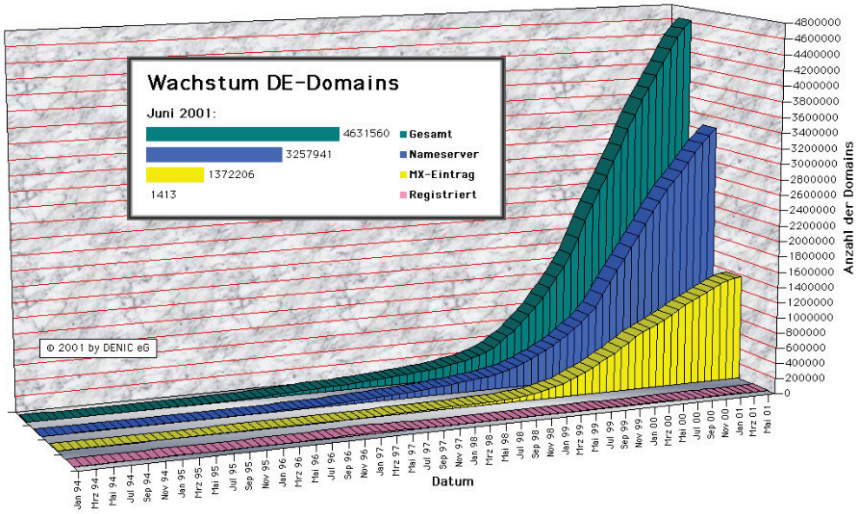
- **Inhaltsfreigabe nach subjektiven Kriterien**: Die Inhalte werden – nicht zuletzt wahrscheinlich dank der niedrigen Eintrittsschwelle (s.u.) – zu sehr großen Teilen von Privatpersonen, meist Einzelpersonen bereitgestellt.

[1] Siehe z.B. Schwerpunktheft „Inhaltskontrolle“, DuD 11/1997.

[2] Die Studie findet sich im Internet unter http://www.secorvo.de/projekt/jugendschutz.htm

[3] Die Darstellung basiert auf einem Vortrag des Autors auf der Stiftungstagung der Alcatel SEL Stiftung für Kommunikationsforschung am 10. Mai 2001.

[4] Beispielsweise stehen in den USA rechtsextremistisches Gedankengut und nationalsozialistische Symbole, deren Verwendung in Deutschland strafbewehrt ist, unter dem Schutz des verfassungsmäßig garantierten „Freedom of Speech“.



Graphik 1: Entwicklung der .de-Domainen bis Juni 2001 [Quelle: denic eG, www.denic.de]

Sie unterliegen daher in der Regel nicht einmal einem informellen Prüf- oder Freigabeprozess; über ihre Bereitstellung wird oft auf der Grundlage einer individuellen, subjektiven Bewertung entschieden.

- **Niedrige Eintrittsschwelle**: Die finanzielle Schwelle für die Bereitstellung von Inhalten ist sehr niedrig. Schon für weniger als 6 Euro jährlich können mehrere hundert zusammenhängende Webseiten mit Inhalten im Internet zugänglich gemacht werden.[5]

Kosten für Vervielfältigung, Verbreitung oder Erstellung (Druck, Film) der Inhalte entstehen im Unterschied zu herkömmlichen Medien dabei nicht. Auch die für die Bereitstellung erforderlichen Kenntnisse werden dank der Entwicklung und oft kostenlosen Verbreitung sehr leistungsfähiger Hilfsprogramme immer geringer: Wer mit einem Textverarbeitungsprogramm umgehen kann, kann heute nach sehr kurzer Einarbeitung auch Webseiten erstellen.

- **Hohe Dynamik**: Die niedrige Eintrittsschwelle, das Fehlen eines Freigabeprozesses und die hohe Unmittelbarkeit sorgen für eine sehr große Dynamik.

Das Inhaltsangebot im Internet unterliegt einer ständigen Veränderung und Erweiterung. Dies erschwert unter anderem auch die Feststellung und Verfolgung von Rechtsverstößen.

- **„Flüchtigkeit" der Inhalte**: Da elektronische Daten anders als herkömmliche Medien „flüchtig" sind, ist die Bereitstellung z.B. jugendgefährdender oder gar rechtswidriger Inhalte nur sehr eingeschränkt nachweisbar.
- **Hocheffiziente Recherchemöglichkeiten**: Anders als bei herkömmlichen Medien erlauben Suchmaschinen eine Volltextsuche über im Internet bereitgestellte Inhalte.

Sehr effiziente Recherche- und Registrierungsmechanismen (Robots, „Meta-Tags", Tools für die Suchmaschinenanmeldung) haben dazu geführt, dass der überwiegende Teil der im Internet erreichbaren Webseiten auch über „elektronische Index-Verzeichnisse" gefunden werden kann. Bei guter Wahl der Suchbegriffe liefern Suchmaschinen trotz der immensen Inhaltsmenge (siehe folgender Abschnitt) innerhalb von Sekunden Verweise auf Webseiten mit den gesuchten Inhalten.

1.2 Neue Quantität des Inhaltsangebots

Wie viele Inhaltsseiten tatsächlich im Internet angeboten werden, lässt sich nicht exakt bestimmen, da es keine zentrale Registratur gibt und ständig neue Seiten hinzugefügt, Seiten geändert oder gelöscht werden. Die Zahl kann daher nur grob geschätzt werden: Zum Beispiel durch eine Zählung der Domain-Namen, die in Top-Level-Domainen (wie z.B. „.de") vergeben wurden; diese können bei Annahme einer durchschnittlichen Anzahl von (Inhalts-) Seiten je Domaine einen Anhaltspunkt für die Anzahl der im Internet erreichbaren Web-Seiten geben.

Zwar sind für den Jugendschutz keineswegs nur Inhalte auf deutschen Webseiten von Bedeutung – ganz im Gegenteil: viele jugendgefährdende Inhalte werden auf ausländischen Webservern bereitgestellt –, die Betrachtung der deutschen Domainen vermag dennoch einen guten Eindruck von der Entwicklung des Inhaltsangebots im Internet vermitteln.

Graphik 1 zeigt die Entwicklung der Domain-Namen mit der Endung „.de", die für Deutschland einheitlich von der Denic e.G. in Frankfurt registriert und verwaltet werden. Die Grafik gibt den Stand von Ende Juni 2001 wieder. Zu diesem Zeitpunkt (30.06.2001) waren über 4,63 Mio. Domainen registriert.

Die Kurve zeigt eine fast exponentielle Entwicklung. Die Zahl der registrierten Domainnamen hat sich demnach innerhalb von 12 Monaten mehr als verdoppelt (April 2000: 2,2 Mio.), innerhalb der vergangenen 24 Monate verzehnfacht (März 1999: 0,44 Mio.) und in den letzten drei Jahren verdreißigfacht (April 1998: 0,14 Mio.).

Hinter jeder dort gezählten, registrierten Domaine können sich eine Vielzahl von Unter-Domainen verbergen (beispielsweise „bmi.bund.de" als Unterdomaine von „bund.de"), und jede Domaine und Unter-Domaine kann wiederum viele Tausend Webseiten umfassen.[6] Grob geschätzt dürfte die Zahl der allein auf deutschen Domainen im Internet bereitgestellten Webseiten mindestens im einstelligen Milliardenbereich liegen.

Bei dieser Schätzung sind andere nationale Top-Level-Domainen – auch deutschsprachige wie die der Schweiz („.ch") und Österreichs („.at") – sowie die internationalen wie „.com", „.org", „.net", „.info" und „.biz" nicht berücksichtigt. Sie dürften in der Summe die Zahl der deutschen Domainen um ein Vielfaches übersteigen.

Die Zahl der weltweit erreichbaren Internet-Seiten wird, ebenfalls grob geschätzt, mindestens um den Faktor zehn über der Zahl der deutschprachigen Webseiten liegen, also sicher im mehrstelligen Milliardenbereich.

[5] Oft wird von Internet-Zugangsprovidern (ISP) heute „Webspace" für eigene Webseiten gleich im Paket mit Internet-Zugang und E-Mail-Postfach bereitgestellt.

[6] Etwas relativiert wird diese Zahl durch die Tatsache, dass z.T. mehrere reservierte Domainnamen auf dieselben Webseiten oder einzelne Unterdomainen zeigen.

Dass diese Informationsmenge die der herkömmlichen Medien um mehrere Größenordnungen übersteigt, macht eine einfache Überschlagsrechnung für Printmedien deutlich: Angenommen,

- in Deutschland habe ein jugendlicher Leser über Kioske Zugriff auf 1.000 verschiedene (einschließlich internationaler) Zeitungen, Zeitschriften und Journale,
- jede dieser Zeitschriften enthielte ca. 500 Inhaltsseiten,
- jede Inhaltsseite einer dieser Zeitschriften entspräche dem Informationsgehalt von etwa 10 Webseiten.

Unter diesen Annahmen[7] hätte ein Jugendlicher damit heute bei herkömmlichen Printmedien täglich Zugriff auf eine Informationsmenge im Umfang von bis zu 0,5 Mio. Inhaltsseiten, die etwa 5 Mio. Internet-Seiten entspräche.

Im Internet hat er hingegen – mit wesentlich effizienteren Suchmöglichkeiten und ohne Verfügbarkeitseinschränkungen – jederzeit Zugriff auf wenigstens die 1.000-fache Informationsmenge, und damit wahrscheinlich auch auf mindestens dasselbe Vielfache an jugendgefärdendem Material.[8]

Der Vergleich zwischen herkömmlichen Medien und dem Internet fällt für Bücher und Filme (Videos) heute vermutlich deutlich weniger eindrucksvoll aus. Es muss aber davon ausgegangen werden, dass sich dies schon in wenigen Jahren dramatisch ändern kann: Die Entwicklung der vergangenen 12 Monate in der Musikindustrie – wie der Online-Tausch von Musiktiteln im MP3-Format mit mehreren Milliarden Abrufen pro Monat – lässt erwarten, dass auch für andere digitale Inhalte der Unterhaltungsindustrie eine sehr große Nachfrage besteht.

These 2

Technik allein ist für Inhaltsfilterung systematisch ungeeignet

Ein zentraler Aspekt im Zusammenhang mit der Filterung von Inhalten gerät bei der Diskussion der Vor-, Nachteile und Alternativen technischer Lösungen oft aus dem Blick: Technische Systeme allein sind nämlich aus systematischen Gründen für die Filterung jedweder Art von Inhalten prinzipiell ungeeignet.

Jedes technische Filtersystem erfordert in einem ersten Schritt eine eindeutige Erkennung und Bewertung von Inhalten, um eine Filterentscheidung treffen zu können. Die Erkennung kann allerdings bei digitalen Daten ausschließlich **syntaktisch**, d.h. auf maschinenlesbare Eigenschaften eines Dokuments bezogen erfolgen: Durch die Suche nach eindeutig vordefinierten Merkmalen. Diese Merkmale können sein:

- der Name eines Dokuments (Webseite, Bild),
- ein aus bestimmten digitalen Inhaltsdaten berechneter Hashwert,
- eine charakteristische Binärfolge (in einem Bild) oder ein bestimmtes Stichwort (in einem Text).

Im Unterschied zu technischen Filtersystemen ist eine Inhaltsfilterung aus Jugendschutzgründen jedoch notwendig **semantisch**, d.h. auf die Bedeutung eines Inhalts bezogen. Semantische Filterung erfordert jedoch Interpretation und Transferleistung:

- Je nach Kontext kann ein bestimmter Begriff auf jugendgefährdende Inhalte hindeuten – oder eben gerade nicht (z.B. in einem Text, der sich in einem pädagogischen Zusammenhang mit der Problematik der Jugendgefährdung auseinandersetzt).
- Auch verändert sich das Gefährdungspotential eines Bildes beispielsweise nicht dadurch, dass es statt im JPEG-Format als GIF- oder TIF-Datei gespeichert, verkleinert oder einfach nur umbenannt wird – wohl aber die syntaktische Ken-

[7] Realistisch dürften diese Werte erheblich zu hoch angesetzt sein, der Unterschied zwischen Print-Medien und Internet also noch extremer ausfallen.

[8] Wahrscheinlich deutlich mehr, da die im Print-Bereich üblichen Kontrollen im Internet nicht greifen; siehe Abschnitt 1.1.

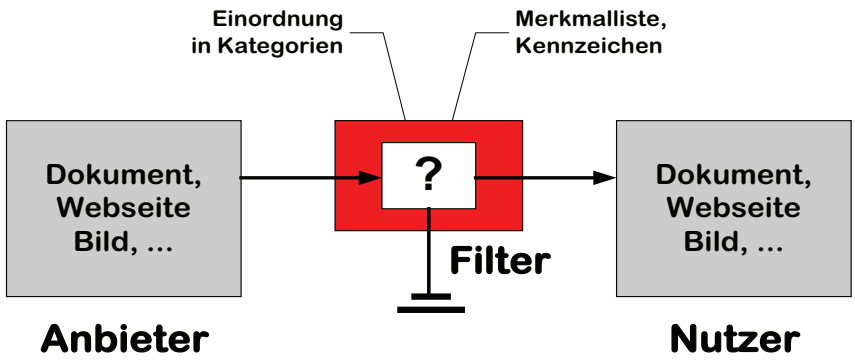


Bild 1: Arbeitsweise eines Filtersystems

nung, die ein Filtersystem zur Erkennung des indizierten Inhalts benötigt.

Damit bleiben alle technischen Systeme zur Unterstützung des Jugendschutzes durch Inhaltsfilterung zwangsläufig lückenhaft und müssen daher immer von nichttechnischen Mechanismen (z.B. sozialer Kontrolle, Aufsicht, Kontrolle durch Erziehungsberechtigte o.ä.) begleitet sein.

These 3

Inhaltsfilterung erfordert die aktive Mitwirkung der Inhaltsanbieter

Ganz prinzipiell lassen sich vier technische Herangehensweisen bei der Realisierung eines Inhaltsfilterungssystems unterscheiden:

- **Sperrung des Internet-Zugangs**: Die Unterbrechnung der Internet-Verbindung ist sicherlich die wirkungsvollste, allerdings auch eine wenig robuste (d.h. von Jugendlichen leicht umgehbare) und in der Regel natürlich wenig sinnvolle Lösung – sie sei hier nur der Vollständigkeit halber erwähnt.
- **Sperrung des Anbieters**: Durch geeignete technische Maßnahmen wird der Zugriff auf die Daten eines bestimmten Inhaltsanbieters gesperrt.[9] Diese Maßnahme schießt allerdings über das angestrebte Ziel der Sperrung ausgewählter Inhalte hinaus: Sie diskriminiert alle auf dem oder den Rechnern eines Anbieters (z.B. Providers) bereitgestellten Informationen.[10] Außerdem ist sie vom Informationsanbieter durch Wechsel der Rechneradresse (oder des Rechners) sehr leicht zu umgehen.
- **Aufbau geschlossener Netze**: Ein wirkungsvoller Weg ist zweifellos der Aufbau geschlossener „jugendfreier" Netze mit einem explizit auf Jugendliche zugeschnittenen Angebot. Dadurch gehen allerdings die Vielfalt des Internet und vor allem die wesentlichen Eigenschaften dieses Mediums verloren – Offenheit, Lebendigkeit und Schnelligkeit. Solche geschlossenen Inhaltsangebote gibt es inzwischen von unterschiedlichen Initiativen und Anbietern.[11]
- **Sperrung von Dokumenten**: Die Sperrung ausgewählter Dokumente ist das eigentliche Ziel einer wirkungsvollen Inhaltskontrolle. Damit ein Filtersystem, das eine gezielte Sperrung erlaubt, robust ist, sind jedoch eine Reihe von Vorkehrungen zu treffen (siehe oben).

Eine geeignete technische Lösung zur Unterstützung des Jugendschutzes im Internet durch Inhaltsfilterung muss dabei folgenden prinzipiellen Anforderungen genügen:

- **Wirksamkeit**: Das gewünschte Filterergebnis muss erreicht werden.
- **Robustheit**: Die Filtermechanismen dürfen weder vom Inhaltsanbieter noch von Jugendlichen leicht umgangen oder deaktiviert werden können.
- **Kontrollierbarkeit**: Die Filtertechnik muss von Verantwortlichen (Pädagogen, Eltern etc.) konfiguriert und in ihrer Wirkung überprüft werden können.
- **Niedrige Kosten**: Die Kosten für die Filterung einschließlich des zeitlichen Aufwands (Installation, Konfiguration, Pflege etc.) müssen sich für Inhaltsanbieter und Nutzer des Filtermechanismus in akzeptablen Grenzen halten.
- **Leichte Administrierbarkeit**: Die Administration der Filtermechanismen muss so gestaltet sein, dass dafür keine vertieften Kenntnisse z.B. der Internet-Technologie erforderlich sind, insbesondere, wenn sie im Client-System erfolgt und auch von technischen Laien durchgeführt werden muss,.

Bild 1 zeigt das Funktionsprinzip eines dokumentenbezogenen Filtersystems: Bevor ein Dokument (WWW-Seite, Bild, Musik-Datei, ...) aus dem Internet auf dem Bildschirm des Abrufers zur Darstellung kommt, erfolgt eine Filterung nach in der Konfiguration eingestellten Merkmalen. Trägt ein Dokument ein Merkmal, das in der Filterkonfiguration als „gesperrt" markiert ist, wird der Inhalt des Dokuments nicht angezeigt.

Zur Erkennung eines zu sperrenden Dokuments können unterschiedliche Merkmale herangezogen werden:

- **Name der Webseite (URL) oder des Dokuments**: Dieses Merkmal erlaubt eine sehr hohe Genauigkeit der Filterung, lässt sich jedoch vom Inhaltsanbieter leicht durch Umbenennung der Webseite umgehen. Außerdem ist die Konfiguration sehr aufwendig, da jede zu sperrende Webseite individuell eingestellt werden muss.
- **Schlüsselworte**: Viele der frühen Filtersysteme arbeiteten mit Schlüsselworten, nach denen im Text einer Webseite gesucht wurde. Ein solcher Schlüsselwort-Filter ist sehr einfach zu konfigurieren, allerdings sind Schlüsselworte nicht kontextbezogen und können daher zu Fehlinterpretationen führen.[12] Schlüsselwort-Filter sind zudem durch Verwendung von Ersatzbegriffen vom Inhaltsanbieter leicht umgehbar. Bei heute verfügbaren Filterprodukten sind die Schlüsselwortlisten daher in der Regel nicht vom Nutzer kontrollierbar, da sie von Herstellern üblicherweise nicht publiziert werden. Schließlich funktionieren Schlüsselworte als Merkmale ausschließlich bei Textdokumenten, nicht aber z.B. bei Bildern.

[9] Technisch wird dabei der Aufbau von Online-Verbindungen mit einem oder mehreren, unter bestimmten Internet-Adressen (IP-Adressen) erreichbaren Rechnern des Anbieters unterbunden.

[10] Ein öffentlich heftig diskutierter Fall war 1997 die Forderung nach einer Sperrung des zentralen Webservers „xs4all.nl", eines niederländischen Internet-Providers, auf dem ein Nutzer extremistische Inhalte zum Abruf bereitgestellt hatte.

[11] Beispielsweise Kidnet.de (www.kidnet.de), das Kindernetz des Südwestfunks (http://www.kindernetz.de/kik) oder GEOlino (http://www.geo.de/geolino)

[12] Beispiel: „breast feeding".

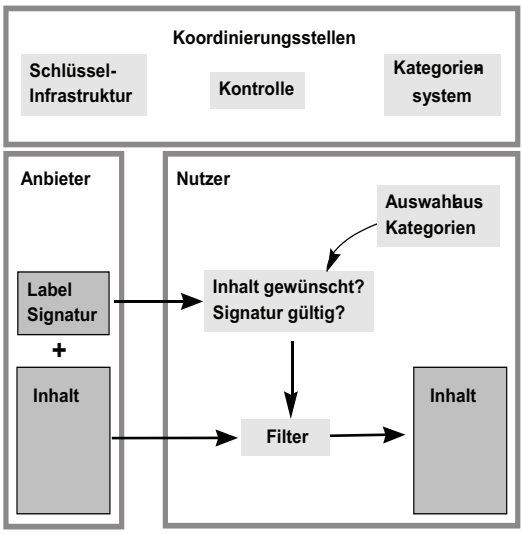


Bild 2: Lösungskonzept für ein wirkungsvolles Filtersystem [Seco_00]

- **„Fingerprints" (Hashwerte)**: Berechnet man aus einem Dokument einen Hashwert, erhält man einen charakteristischen Wert für dieses Dokument, anhand dessen es zweifelsfrei wiedererkannt werden kann. Dieses Merkmal greift prinzipiell bei allen Arten von Dokumenten. Allerdings wird die Filterung durch kleinste Transformationen (Formatänderungen oder kleine Modifikationen) unwirksam. Auch ist die Berechnung der Hashwerte aufwendig.
- **Markierung (Label)**: Schließlich können dem Dokument Markierungen zugeordnet werden, die den Inhalt des Dokuments charakterisieren, z.B. durch die Einordnung in eine Inhalts-Kategorie nach einem vereinheitlichten Kategoriensystem. Diese Zuordnung kann sowohl von unabhängigen Dritten als auch vom Inhaltsanbieter selbst vorgenommen werden. Auch können solche Labels auf einem vom Inhaltsanbieter völlig unabhängigen „Online-Kategorisierungssystem" bereitgehalten werden. Durch eine digitale Signatur kann zusätzlich die Fälschung von Markierungen verhindert werden (siehe unten).

Bei der Bewertung eines technischen Filtersystems ist natürlich nicht nur die Erfüllung der oben angeführten Anforderungen von Bedeutung. Wichtig ist außerdem, welche Instanzen an dem Filtersystem (Betrieb des Filters, Konfiguration des Filters, Überprüfung der Filterung, Auswahl der Merkmale, Auswahl der Kategorien etc.) beteiligt sind – nicht zuletzt, um bei Nutzern und Verantwortlichen Vertrauen für die Realisierung zu gewinnen.

Besonders wichtig ist der Filtermechanismus selbst. Betrieb und Konfiguration des Filters kann dabei an drei unterschiedlichen Stellen erfolgen:

- **Im Client-System**: Der große Vorteil einer nutzerseitigen Konfiguration ist, dass die Auswahl der Kriterien und die Kontrolle der durchgeführten Filterung vollständig in der Hand der Verantwortlichen (Erziehungsberechtigte, Lehrer etc.) liegt. Ein Nachteil ist jedoch, dass Filter mit lokaler Konfigurationsmöglichkeit im Client-System in der Regel wenig robust sind, d.h. entweder von Jugendlichen umkonfiguriert oder sogar deaktiviert bzw. entfernt werden können. Von Nachteil ist weiter, dass es Laien möglich sein muss, die (oft komplexe) Konfiguration durchzuführen. Dadurch steigt nicht zuletzt der Aufwand für den Betrieb des Filtersystems.
- **Beim Internet-Service-Provider**: Die Filterung kann auch als zentrale Dienstleistung angeboten werden.[13] Das entlastet die Betreiber des Client-Systems von Konfiguration und Kontrolle. Nachteilhaft ist allerdings, dass die Filtermechanismen nur sehr eingeschränkt individuell gewählt und vor allem nicht kontrolliert werden können. Diese Lösung erfordert also ein erhebliches Vertrauen in den Dienstleister, dass die Filterung sachgemäß und auch nicht zweckentfremdend (z.B. durch Ausblendung der Webseiten von Mitbewerbern) eingesetzt wird.
- **Durch eine dritte Instanz**: Schließlich ist die Nutzung einer dritten Instanz denkbar, die die Filterung im Auftrag des Betreibers des Client-Systems durchführt. Auch in diesem Fall erfolgt die Filterung als zentrale Dienstleistung, allerdings ist hier in einem gewissen Rahmen die Umsetzung von speziellen Konfigurationswünschen und auch die Kontrolle des Filtermechanismus durch den Nutzer der Dienstleistung möglich. Als problematisch könnte sich die Finanzierung eines solchen Services erweisen.

Bei einer systematischen Gegenüberstellung der Vor- und Nachteile der unterschiedlichen Ansätze zur Realisierung eines geeigneten Filtersystems[14] zeigt sich, dass der folgende technische Lösungsvorschlag den gewünschten Zielen einer Umsetzung der Anforderungen des Jugendschutzes im Internet am nächsten kommt (Bild 2):

- Jeder Inhaltsanbieter ordnet den eigenen Dokumenten nach einem vereinheitlichten Kategoriensystem eine Markierung zu.
- Die Markierung der Dokumente erfolgt durch die Verwendung vereinheitlichter „Labels".[15] Solche Labels können auch von Dritten erstellt und Seiten zugeordnet werden („Labeling-Provider", „Third Party Rating Service").
- Die Filterung erfolgt beim Nutzer und erlaubt durch die Verwendung einheitlicher Kategorien eine einfache, individuelle Konfiguration.
- Die Authentizität von Labels und deren eindeutige (und unfälschbare) Zuordnung zu einem Dokument (Webseite, Bild, Musikdatei etc.) wird durch digitale Signaturen gewährleistet.

Das skizzierte Konzept verfolgt somit im Kern einen **Selbstregulierungsansatz**: Ausgehend von der Annahme, dass jeder Anbieter von Dokumenten ein (nicht notwendig wirtschaftliches) Interesse am Abruf seiner Seiten hat, wird er – die Existenz eines vereinheitlichten Kategoriensystems

[13] Einige große Internet-Service-Provider (ISP) bieten einen eigenen Zugang für Jugendliche an.

[14] Eine solche Untersuchung wurde von der Secorvo Security Consulting GmbH 1999 im Rahmen der im Auftrag des Bundesministeriums für Wirtschaft (BMWi) entwickelten Studie durchgeführt [Seco_00]. Bezugshinweise finden sich im Literaturverzeichnis.

[15] Als technischer Standard hat sich für die Anbringung von Markierungen PICS (Platform for Internet Content Selection), ein vom World-Wide-Web-Konsortium (W3C) entwickeltes Format durchgesetzt (http://w3c.org/PICS/).

und eine verbreitete Nutzung der Filtertechnik vorausgesetzt – den Aufwand einer korrekten Markierung der von ihm angebotenen Informationen nicht scheuen.[16]

Zusätzlich enthält es **Sanktionsmechanismen**: Werden digitale Signaturen zum Schutz der Labels eingesetzt und vom Filtermechanismus geprüft, besteht die Möglichkeit, die erforderlichen Schlüsselzertifikate an einer zentralen Stelle zu erzeugen und bei Feststellung von Verstößen eines Inhaltsanbieters (unzutreffendes Labeling) zu sperren.

Zur Überwachung der korrekten Markierung von Webseiten sollte – analog der Bundesprüfstelle für jugendgefährdende Schriften (BPjS) – eine „Bundesprüfstelle für jugendgefährdende Web-Inhalte" (BPjW) eingerichtet werden, die auf Benachrichtigung tätig wird und erforderlichenfalls durch Zertifikatsrückruf einem Inhaltsanbieter die Berechtigung entzieht, BPjW-gemäße Labels auszustellen.

Zur Realisierung dieses Konzepts fehlt es bislang allerdings an einer zentralen Voraussetzung: Der Verfügbarkeit eines international einheitlichen Kategoriensystems, dass auch verschiedene Sprachen und Mentalitätsunterschiede berücksichtigt.

These 4

Technik darf nicht Medienkompetenz ersetzen

Selbst ein technisch hervorragend entworfenes, etabliertes und allgemein akzeptiertes System zur technischen Inhaltsfilterung darf nicht dazu verleiten, die inhaltliche und didaktische Auseinandersetzung mit dem Medium Internet zu vernachlässigen. Ein Herausfiltern jugendgefährdender Inhalte, gerade wenn es gut gelingt, ersetzt auch keineswegs die Notwendigkeit einer argumentativen Auseinandersetzung mit Jugendlichen im Zusammenhang mit solchen Inhalten – eine wichtige Aufgabe der Erziehung.

Ziel einer jeden Medienpädagogik muss sein, Kindern und Jugendlichen einen souveränen Umgang mit dem Medium Internet zu vermitteln. Daher sollte eine technische Lösung zur Unterstützung des Jugendschutzes im Internet immer eingebettet sein in ein umfassendes und pädagogisch sinnvolles Konzept zur Vermittlung von Medienkompetenz.

Fazit

Die Umsetzung von Anforderungen des Jugendschutzes im Internet stellt sowohl in quantitativer als auch in qualitativer Hinsicht eine völlig neue Herausforderung dar. Die Unterstützung dieser Umsetzung durch technische Systeme stößt dabei an prinzipielle Grenzen: Da eine technische Filterung grundsätzlich nur auf der Basis syntaktischer Merkmale arbeiten kann, wird sie immer fehlerbehaftet sein. Dennoch ist prinzipiell eine hinreichend wirksame Filterung möglich. Sie setzt jedoch drei Punkte voraus:

- die Existenz eines internationalen, vereinheitlichten und anerkannten Kategoriensystems zur einfachen Einordnung von Seiten,
- die Mitwirkung der Inhaltsanbieter (Selbstregulierung durch „self rating") und
- den Aufbau einer Kontroll- und Sanktionierungsinfrastruktur („Bundesprüfstelle für jugendgefährdende Web-Inhalte").

Literatur[17]

[KöKS_97] Köhntopp, Kristian; Köhntopp, Marit; Seeger, Martin: *Sperrungen im Internet*. Studie im Auftrag des Bundesministeriums für Forschung und Technologie, Mai 1997.[18]

[KöKS2_97] Köhntopp, Kristian; Köhntopp, Marit; Seeger, Martin: *Sperrungen im Internet.* Datenschutz und Datensicherheit (DuD), 11/1997, S. 626-631

[KöNe_99] Köhntopp, Marit; Neundorf, Dörte: *Inhaltsfilterung und Jugendschutz im Internet*. In: Fox, D.; Horster, P. (Hrsg.): Datenschutz und Datensicherheit – DuD. Vieweg Verlag, Wiesbaden 1999, S. 113-126.

[Neun_99] Neundorf, Dörte: *Filtertechnologien zur Reduktion der Jugendgefährdung im Internet*. In: Baumgart, R.; Rannenberg, K.; Wähner, D.; Weck, G. (Hrsg.): Verlässliche IT-Systeme, Vieweg, Wiesbaden 1999, S. 357-366.

[Seco_00] Secorvo Security Consulting GmbH: *Jugendschutz und Filtertechnologien im Internet*. Studie im Auftrag des Bundesministeriums für Wirtschaft, BMWi Dok.-Nr. 472, Januar 2000.[19]

[WaMa_00] Waltermann, Jens; Machill, Marcel: *Verantwortung im Internet. Selbstregulierung und Jugendschutz*. Bertelsmann-Stiftung, 2000.[20]

[16] Dieser Aufwand kann durch geeignete Hilfsprogramme und halbautomatische Markierungsmechanismen in Editoren auf eine vernachlässigbare Größe verringert werden.

[17] Online-Referenzen zu weiterführenden Informationen finden sich unter: www.secorvo.de/security-gateway/jugendschutz-links.htm

[18] www.koehntopp.de/kris/artikel/blocking/index.html

[19] www.secorvo.de/projekt/jugendschutz.htm. Kostenlose Bestellung der gedruckten Fassung unter www.bmwi.de/Homepage/Politikfelder/Informationsgesellschaft/Publikationen/Publikationen.jsp

[20] www.stiftung.bertelsmann.de/internetcontent/deutsch/frameset.htm?content/c2000.htm