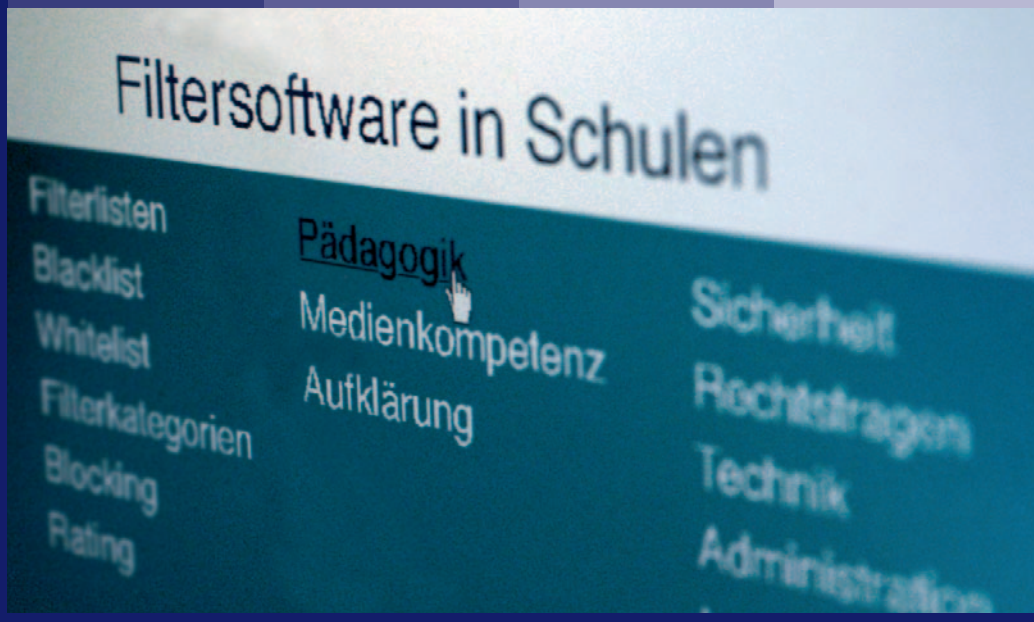
IT works

Jugendmedienschutz



Filterlösungen im schulischen Umfeld

IT works Themenreihe

Schulen ans Netz

Eine Initiative des Bundesministeriums für Bildung und Forschung und der Deutschen Telekom AG

Impressum

Herausgeber
Schulen ans Netz e.V.
IT works
Thomas-Mann-Straße 4
53111 Bonn

Telefon +49 (0)228 91048-261
Telefax +49 (0)228 91048-1261
E-Mail: itworks@schulen-ans-netz.de
Web: http://www.schulen-ans-netz.de/itworks

Gefördert von

Bundesministerium für Bildung und Forschung

Deutsche Telekom

EUROPÄISCHE UNION
Europäischer Sozialfonds

Redaktionsleitung Michael Höllen

Redaktion Daniela Bickler, Andrea Küsel

Gestaltung: eintopf., Wuppertal
Titelfoto: Uwe Schinkel

Stand der zitierten Internetquellen: 02.11.2005

Textbeiträge, Mitarbeit oder inhaltliche Unterstützung
Andreas Gleis, Fachberater Jugendarbeit
Manfred Kasper, Journalist
Dr. Marc Liesching, Vorsitzender Prüfer der Freiwilligen Selbstkontrolle Fernsehen (FSF)
Friedemann Schindler, Leiter jugendschutz.net
Arno Scholten, Schulen ans Netz e.V.

Wir bedanken uns an dieser Stelle bei all jenen, die das Erscheinen dieser Broschüre durch ihre wertvollen Beiträge und hohe Kooperationsbereitschaft tatkräftig unterstützt haben.

Hinweise zur Broschüre

In dieser Broschüre wird ausschließlich aus Gründen der besseren Lesbarkeit die geschlechtsspezifische Differenzierung nicht durchgängig verwendet.

Die Broschüre enthält eine Reihe von Links. Um sie bequem ansteuern zu können, haben wir die Links entsprechend ihrer Reihenfolge, wie sie in der Broschüre angegeben sind, auf der Webseite von IT works aufgeführt. Die Auflistung finden Sie unter http://itworks.schulen-ans-netz.de/publikationen.php

Zum besseren Verständnis von Fachbegriffen aus dem Bereich der Informatik ist am Ende der Broschüre ein **Glossar** mit Erklärungen angefügt.

Vorwort

Bei kontinuierlicher Zunahme der Computerausstattung an bundesdeutschen Schulen wird die Nutzung des Internets zu einem immer wichtigeren Bestandteil der Unterrichtskultur. Dabei rückt das Thema Jugendmedienschutz mehr und mehr in den Fokus der Aufmerksamkeit, denn neben informativen und lehrreichen Angeboten stößt man im Internet früher oder später auch auf fragwürdige, bedenkliche oder sogar verbotene Inhalte.

Schulträger, Schulleitungen und Lehrkräfte stehen daher gemeinsam vor der Herausforderung, die Aufsichtspflicht auch bei der Nutzung des Internets im Unterricht sicherzustellen. In diesem Kontext wird vielfach neben der Stärkung der Medienkompetenz der Schülerinnen und Schüler der Einsatz von Filterprogrammen in Schulen diskutiert. Das Projekt IT works des Vereins Schulen ans Netz greift mit dieser Veröffentlichung den Themenkomplex unter pädagogischen, rechtlichen, technischen sowie praxisbezogenen Aspekten auf und beleuchtet schulspezifische Fragen aus den unterschiedlichen Sichtweisen.

Die verschiedenen zielgruppenspezifischen Angebote von Schulen ans Netz stellen heute eine umfassende integrierte Service- und Inhalteplattform dar, die von Lehrern und Schülern als eine an ihren Bedürfnissen orientierte moderne Arbeitsumgebung genutzt wird. Qualifizierungsangebote und konkrete Beratungsleistungen vor Ort flankieren die internetbasierten Dienstleistungen und runden das Angebotsportfolio ab. Mit der Expertise, komplexe Sachverhalte praxisorientiert für die am schulischen Bildungsprozess Beteiligten aufarbeiten und verfügbar machen zu können, möchte Schulen ans Netz e.V. mit der vorliegenden Publikation für das Gesamtthema „Jugendmedienschutz" sensibilisieren und Schulträger, Schulleitungen sowie administrierende Lehrkräfte bei der Planung und Umsetzung von Schutzmaßnahmen unterstützen.

Wir wünschen Ihnen eine anregende und aufschlussreiche Lektüre und vor allem viel Erfolg bei der Umsetzung in der Schulpraxis.

Dr. Maik Lehmann
Vorstandsvorsitzender
Schulen ans Netz e.V.

Ralf Münchow
Geschäftsführender Vorstand
Schulen ans Netz e.V.

Inhalt

02 **Impressum**
03 **Textbeiträge und Mitarbeit**
04 **Hinweise zur Broschüre**
05 **Vorwort**
07 **Inhalt**

11 **Einleitung: Internetnutzung im schulischen Umfeld**
- Spannungsfeld Jugendmedienschutz -

14 **1. Medienkompetenz als Schlüsselqualifikation**
14 1.1 Potenziale nutzen
15 1.2 Jugendschutzfilter im pädagogischen Fokus
19 1.3 Jugendschutzfilter im ideologischen Fokus

22 **2. Rechtliche Vorgaben des Jugendmedienschutzes**
22 2.1 Rechtliche Kategorisierung der Inhalte
23 2.1.1 Absolut verbotene Inhalte
23 2.1.2 Relativ verbotene Inhalte
24 2.1.3 Entwicklungsbeeinträchtigende Inhalte
25 2.2 Konsequenzen für die schulische Praxis
27 2.3 Umfang und Möglichkeiten der Aufsicht
28 2.4 Grenzen der Kontrolle

31 **3. Einsatz an Schulen**
31 3.1 Funktionsweisen von Filterprogrammen
31 3.1.1 Wortfilter / Worterkennung oder Keyword Blocking
33 3.1.2 Negativlisten / Blacklists
37 3.1.3 Positivlisten / Whitelists
39 3.1.4 Mustererkennung von Grafiken
40 3.1.5 Heuristische Verfahren
40 3.1.6 Self Rating / Site Labelling
42 3.1.7 Kriterien zur Entscheidungsfindung

44 3.2 Technische Grundlagen
44 3.2.1 Lokal installierte Filter (Einzelplatzlösung)
45 3.2.2 Serverbasierte Filter (Netzwerklösung)
46 3.2.3 Einzelplatz- oder Netzwerklösung?
49 3.2.4 Externe Zentrallösung
51 3.3 Filterlösungen in der Schulpraxis
51 3.3.1 Installation
52 3.3.2 Gestaltungsmöglichkeit im Unterricht
52 3.3.3 Aktualisierung der Filterlisten
53 3.3.4 Protokollierung der Zugriffe
55 3.3.5 Manipulationsresistenz
56 3.3.6 Schutz beim Surfen - auch zu Hause?

57 **4. Filtersysteme - ein Überblick**
59 4.1 DansGuardian
61 4.2 FamilyFilter
63 4.3 ICRAplus
67 4.4 LISS security school server
69 4.5 Parents Friend
71 4.6 premioss-cf
73 4.7 SaferSurf School
75 4.8 sBox
77 4.9 SFC - Security for Children / SFE - Security for Education
79 4.10 SmartFilter
81 4.11 SquidGuard
83 4.12 Symantec Parental Control
85 4.13 TIME for kids Schulfilter Plus
87 4.14 T-Online Kinderschutz-Software
89 4.15 webwasher

91 **5. Kommunen und Bundesländer**
91 5.1 Kommunale Initiativen
91 5.1.1 Bremen
91 5.1.2 Hamburg

92 5.1.3 Frankfurt am Main
92 5.1.4 Paderborn
92 5.2 Landesweite Initiativen
92 5.2.1 Baden-Württemberg
93 5.2.2 Bayern
93 5.2.3 Hessen
93 5.2.4 Thüringen

95 **6. Jugendmedienschutz im internationalen Kontext**
95 6.1 Gemeinsam für ein sicheres Internet - Jugendmedienschutz in Europa
97 6.2 Die Situation in Europa und den USA
97 6.2.1 Europa
97 6.2.2 USA
99 6.3 Filtersoftware aus den USA
99 6.3.1 CYBERsitter
99 6.3.2 Net Nanny
100 6.3.3 SurfControl

101 **Zusammenfassung und Ausblick**

104 **Anhang**

104 **Glossar**
108 **Checklisten und Vorlagen**
109 Mustertext Computer-Nutzungsordnung für Schülerinnen und Schüler
125 **Literatur**
130 **Links**
130 Nationale Institutionen / Organisationen / Projekte
134 Internationale Institutionen / Organisationen / Projekte
135 Recht
136 **Feedback zur Broschüre**

Einleitung:
Internetnutzung im schulischen Umfeld
- Spannungsfeld Jugendmedienschutz -

Die angeleitete, regelmäßige Nutzung der neuen Medien und des Internets im Schulunterricht kann zu einem zeitgemäßen Lehren und Lernen beitragen und ist bereits heute zu einem bedeutenden Bestandteil der Unterrichtskultur geworden. Speziell der Einsatz des Internets eröffnet einerseits die Möglichkeit, den Unterricht zu bereichern und zu modernisieren, konfrontiert andererseits Schulträger, Schulleitung und Lehrkräfte aber auch mit neuen Herausforderungen. Hierzu zählt zum Beispiel die Einhaltung der jugendmedienschutzrechtlichen Regelungen. Eine Kontrolle des Internets mit den klassischen Instrumenten der Medienaufsicht wie Altersfreigabe, Festlegung der Sendezeit bei Fernsehprogrammen usw. greift bei der Nutzung des Internets nicht. Schule bewegt sich somit im Spannungsfeld zwischen Jugendmedienschutz und der Vermittlung von Medienkompetenz.

Zahl der Internetangebote nimmt rapide zu

Allein die Tatsache, dass mehr als eine halbe Million Computer in den bundesdeutschen Schulen mit dem Internet verbunden sind,[1] zeigt, wie wichtig der Einsatz dieser sprichwörtlich unbegrenzten Datenbank des Wissens für den Unterricht geworden ist. In der Unbegrenztheit dieses Angebots liegen aber auch gewisse Gefahren für Schülerinnen und Schüler. Die Entwicklung des Internets hat innerhalb kurzer Zeit unvorstellbare Dimensionen erreicht. Das Angebot umfasst heute bereits mehrere Milliarden Webseiten, und täglich kommen unzählige neue Angebote hinzu.[2] Unvermeidbar, dass sich innerhalb dieses gigantischen Pools auch eine Vielzahl von gefährdenden oder gar strafbaren Inhalten ausbreitet. So unerschöpflich der Informationsgehalt des world wide web ist, so unüberschaubar ist aber auch das Gefahrenpotenzial, das von ihm ausgehen kann.

Schulen und Lehrkräfte sind nach den Schulverfassungsgesetzen der einzelnen Bundesländer grundsätzlich verpflichtet, im Rahmen des pädagogischen Auftrags der Aufsichtspflicht gerecht zu werden und die jugendmedienschutzrechtlichen Anforderungen sicherzustellen. Es stellt sich daher beim Einsatz des Internets im

[1] So die Studie des Bundesministeriums für Bildung und Forschung zur „IT-Ausstattung der allgemein bildenden und berufsbildenden Schulen in Deutschland - Bestandsaufnahme 2005 und Entwicklung 2001 bis 2005", Bundesministerium für Bildung und Forschung (BMBF) Referat Publikationen; Internetredaktion http://www.bmbf.de/pub/it-ausstattung_der_schulen_2005.pdf
[2] Allein die Suchmaschine Google kennt im August 2005 über 8 Milliarden Webseiten.

Unterricht die Frage, wie die Schülerinnen und Schüler vor jugendschutzrechtlich fragwürdigen Inhalten geschützt werden können.

Internet abschalten?

Sicher ist es keine Lösung, Kindern „zu ihrem eigenen Schutz" den Zugang zum Internet zu verwehren. Dies wäre auch kaum möglich, denn wie die JIM-Studie 2004 belegt, nutzen 85 Prozent der 12- bis 19-Jährigen regelmäßig das Internet.[3] Den neuesten Untersuchungen[4] zufolge besitzen bereits 57 Prozent der befragten Jugendlichen zwischen 12 und 19 Jahren einen eigenen Computer beziehungsweise ein eigenes Notebook, 35 Prozent der Befragten verfügen über einen Internetzugang zu Hause.

Der kompetente Umgang mit Computer und Internet gilt außerdem zunehmend als Schlüsselqualifikation für den Einstieg ins Berufsleben. Der Versuch, Kinder und Jugendliche vom Internet fernzuhalten, hätte zum einen den Effekt, dass ihre Zukunftschancen erheblich minimiert würden, zum anderen wären die Schülerinnen und Schüler durch mangelnde Medien- und Internetkompetenz den Gefahren beim unbeaufsichtigten Surfen in besonderer Weise schutzlos ausgeliefert.

Internetkompetenz schulen!

Im Umkehrschluss bedeutet dies jedoch nicht, dass Schülerinnen und Schüler unkontrolliert während des Unterrichts im Internet surfen sollen, bis sie irgendwann und irgendwie den eigenverantwortlichen Umgang mit dem Internet erlernt haben. Es erweist sich daher als sinnvoll, in einem geschützten Umfeld medienpädagogisch auf Kinder einwirken zu können. Das Vermitteln von Internetkompetenz ist ein Prozess, der sich über die gesamte Schulzeit erstreckt und im Schulumfeld - sowie im Idealfall auch von den Eltern zu Hause - pädagogisch begleitet und beaufsichtigt werden sollte. Dazu gehört zum einen die aktive Sensibilisierung für problematische Themen, zum anderen die gezielte Einbindung der Eltern in schulische Prozesse. Damit diese aktive Sensibilisierung für alle deutlich in einem klar umrissenen Rahmen erfolgen kann, ist eine verbindliche Regelung zwischen Schule, Schülern und Eltern für die Nutzung von Computer und Internet in der Schule notwendig. Dies gilt sowohl für die Zeiten des Unterrichts als auch für

[3] Als regelmäßige Internetnutzung wird in der Studie bereits die Nutzung des Internets mindestens einmal im Monat bezeichnet. Die vollständige JIM-Studie 2004 finden Sie im Internet unter http://www.mpfs.de/studien/jim/Brosch%FCre%20JIM%2004.pdf

[4] JIM-Studie 2005 (Jugend, Information, (Multi-)Media), mfs medienpädagogischer forschungsverbund südwest, siehe auch http://www.mpfs.de/studien/jim/index_jim.html

weitergehende Zeiträume wie beispielsweise in den Pausen, Freistunden oder während der Nachmittagsbetreuung.

Filter als technische Stütze

Zur Unterstützung der Lehrkräfte wird an vielen Schulen der Einsatz von Filterprodukten diskutiert, mit deren Hilfe der Zugriff auf Internetinhalte gesteuert und kontrolliert werden soll.

Dabei sind stets sowohl die Möglichkeiten als auch die Grenzen von Filterprogrammen zu berücksichtigen.[5] Der Einsatz von Filterprodukten kann dazu beitragen, die Gefährdung der Schülerinnen und Schüler durch bedenkliche Inhalte zu verringern und damit Lehrkräfte und Schulen bei der Erfüllung des pädagogischen Auftrags zu unterstützen.

Bildungsauftrag muss erfüllt werden

Dem Primat der Pädagogik folgend, kann und sollte sich Schule unterschiedlicher Instrumente bedienen, um ihrem Bildungsauftrag gerecht zu werden. Dazu gehört neben der Arbeit mit digitalen Medien im Allgemeinen vor allem die Nutzung des Internets im Besonderen. Die Entscheidung über den Einsatz eines Filterprogramms bei der Erfüllung dieses Bildungsauftrags liegt im Entscheidungsbereich von Schulträgern, Schulleitungen und Lehrkräften.

Die Broschüre enthält keinen vergleichenden Filtertest. Sie soll vielmehr zur vertieften Auseinandersetzung mit dem Thema Jugendmedienschutz und den Einsatzmöglichkeiten von Filterprodukten in Schulen anregen. Sie möchte einen Überblick über schulrelevante Aspekte geben und damit zur Entscheidungsfindung beitragen.

5 Siehe Kapitel 1.2.

1. Medienkompetenz als Schlüsselqualifikation

Medienkompetenz wird durch eine Vielzahl von Fähigkeiten charakterisiert, die den selbstbestimmten, kreativen und sozial verantwortlichen Umgang mit Medien ausmachen. Sie reicht von der selbstständigen Informationssuche und -bewertung über die eigene Gestaltung von Medien und Medieninhalten bis hin zum selbstverständlichen und sicheren Umgang mit neuen Technologien.

Die Vermittlung von Medien- und insbesondere Internetkompetenz ist heute eine der zentralen Aufgaben der Gesellschaft und somit auch der Lehrkräfte und der Eltern. Sie gilt als Schlüsselqualifikation für den eigenverantwortlichen Umgang mit dem Internet, den auch der Jugendmedienschutz mit seinen Maßnahmen fördern möchte. Ein nachhaltiger Schutz vor gefährdenden Inhalten erfolgt am besten über das Wissen der Gefahrenpotenziale und das Einüben von bewussten Handlungsmustern. Damit sich Schülerinnen und Schüler vor Gefahren schützen können, müssen sie wissen, wo diese lauern und wie sie mit ihnen umgehen können. Neugierde und Offenheit im Umgang mit dem Internet sind somit nicht weniger wichtig als die bewusste Vorsicht.

Medienkompetenz und Jugendmedienschutz sind eng miteinander verknüpft und bilden eine Basis, auf der die positiven Möglichkeiten der Mediennutzung im Unterricht voll ausgeschöpft werden können.

1.1 Potenziale nutzen

Individuelle Förderung unterschiedlicher Lerntypen

Die positiven Effekte der Mediennutzung im Unterricht sind zahlreich. Neue Medien - und damit auch das Internet - haben das Potenzial, in hohem Maße selbstbestimmtes Lernen zu fördern. Durch den angeleiteten Einsatz verschiedener Medien und Materialien, eingebunden in ein pädagogisches Gesamtkonzept, werden vielfältige Lernanreize geboten, die den Bedürfnissen unterschiedlicher Lerntypen gerecht werden und zum Entstehen einer neuen Lernkultur beitragen. Eine intensive und nachhaltige Mediennutzung trägt zu einer Differenzierung und Individualisierung des Lernens bei.

Dr. Stefan Aufenanger, Professor für Erziehungswissenschaft und Medienpädagogik an der Universität Mainz, bestätigt die positiven Entwicklungen beim

Umgang mit neuen Medien: „Wenn auch bisher nicht genügend weit reichende empirische Studien dazu vorliegen, machen die berichteten Erfahrungen jedoch deutlich, dass das Arbeiten mit neuen Medien im Grundschulunterricht Kinder zum Lernen motiviert, ihre Aufmerksamkeit und Kooperationsbereitschaft fördert, sie zu vielfältiger Kommunikation anregt [...]."[6]

Zeitgemäße Unterrichtsgestaltung stärkt Schüler

Dies verdeutlicht, dass eine zeitgemäße Unterrichtsgestaltung Schülerinnen und Schüler sowohl motivieren als auch in ihren Fähigkeiten und Kompetenzen stärken kann. Für Lehrerinnen und Lehrer bietet sich in diesem Kontext die Möglichkeit einer attraktiven und zeitgemäßen Unterrichtsgestaltung. Schülerinnen und Schüler haben die Möglichkeit, sich selbstständig, umfassend und multimedial mit allen Themen auseinander zu setzen. Dabei wird die Entwicklung von Problemlösungsstrategien ebenso gestärkt wie die soziale Kompetenz.

1.2 Jugendschutzfilter im pädagogischen Fokus

Bei allem Engagement und pädagogischem Anspruch sind beim Einsatz des Internets zum Erreichen didaktischer Ziele jedoch auch Mechanismen zum Schutz der Kinder und Jugendlichen gefordert. Diese Forderung ergibt sich aus dem Jugendmedienschutz-Staatsvertrag (JMStV):[7]

§ 1 des JMStV

„Zweck des Staatsvertrages ist der einheitliche Schutz der Kinder und Jugendlichen vor Angeboten in elektronischen Informations- und Kommunikationsmedien, die deren Entwicklung oder Erziehung beeinträchtigen oder gefährden, sowie der Schutz vor solchen Angeboten in elektronischen Informations- und Kommunikationsmedien, die die Menschenwürde oder sonstige durch das Strafgesetzbuch geschützte Rechtsgüter verletzen."

Die Richtlinien der Kommission für Jugendmedienschutz der Landesmedienanstalten, KJM[8], führen weiter aus, dass durch „technische oder sonstige Mittel" Kindern und Jugendlichen der betroffenen Altersstufen die „Wahrnehmung" entwicklungsbeeinträchtigender Angebote „unmöglich gemacht" oder „wesentlich erschwert" werden muss.[9]

[6] Aufenanger, Stefan: Neue Medien in der Grundschule. Erweiterung von Lernmöglichkeiten und Umstrukturierung von Schule. In: Grundschulunterricht, 50, 2003, Heft 9, S.2-5.
[7] Den vollständigen Jugendmedienschutz-Staatsvertrag finden Sie im Internet unter http://www.artikel5.de/gesetze/jmstv.html
[8] Kommission für Jugendmedienschutz der Landesmedienanstalten: Die KJM ist die zentrale Aufsichtsstelle für den Jugendschutz im privaten Rundfunk und in den Telemedien (Internet). Mehr unter: http://www.kjm-online.de
[9] Gemeinsame Richtlinien der Landesmedienanstalten zur Gewährleistung des Schutzes der Menschenwürde und des Jugendschutzes (Jugendschutzrichtlinien - JuSchRiL) vom 8./9. März 2005. Die vollständigen Richtlinien der Kommission für Jugendmedienschutz (KJM) finden Sie im Internet unter http://www.kjm-online.de/public/kjm/downloads/JuSchRiL2005_180705.pdf

Filterprogramme als Instrument des Jugendschutzes

Filterprogramme sind ein solches technisches Mittel. Sie können Lehrkräfte dabei unterstützen, zumindest einen Teil der entwicklungsbeeinträchtigenden Angebote des Internets von Schülerinnen und Schülern während des Unterrichts fernzuhalten.

Definition „Filterprogramm/Filtersoftware“
Ein Filterprogramm ist in der Lage, das aufgerufene Internet-Angebot nach vorgegebenen Kriterien zu klassifizieren und dadurch erwünschte Informationen von unerwünschten zu unterscheiden. Ist eine Filtersoftware installiert, erhält der Benutzer nur die Informationen, die der Filter als unbedenklich erkennt und zur Ansicht freigibt.

Altersdifferenzierug gefordert

Sowohl aus pädagogischer als auch aus rechtlicher Sicht ist die Möglichkeit des altersdifferenzierten Zugangs zum Internet von großer Bedeutung. Darauf verweist die KJM in ihren „Kriterien für die Aufsicht im Rundfunk und in den Telemedien“.[10] Der Schutz sollte so modifiziert werden können, dass er „dem Reifezustand und kognitiven Entwicklungsstand“ der Schülerinnen und Schüler entspricht. Unterschiedliche Schulformen stellen somit auch spezifische Anforderungen an ein Filterprogramm.

Kinder im Grundschulalter gehen eher spielerisch mit dem Medium Internet um und brauchen entsprechend mehr Schutz als beispielsweise Achtklässler. In Grundschulen kann es durchaus sinnvoll sein, durch ein Filterprogramm gezielt virtuelle Surf- und Spielräume zur Verfügung zu stellen, in denen sie sich ungefährdet bewegen können. Spezielle Angebote im Internet versuchen zudem, durch die Bereitstellung von kindgerechten Inhalten Kindern einen solchen sicheren Spielraum zu gewähren. Dazu gehört beispielsweise die von Schulen ans Netz angebotene Plattform für Grundschulen „Primolo“.[11] Die Arbeitsgemeinschaft vernetzter Kinderseiten präsentiert unter www.seitenstark.de eine umfassende Übersicht renommierter deutschsprachiger Kinderseiten im Internet.

Für weiterführende und berufsbildende Schulen steht dagegen der selbstständige Umgang mit dem Webangebot im Vordergrund. Im Idealfall sollte es dann darum gehen, das gesamte Webangebot nutzen zu können und dabei die jugend-

[10] Die vollständigen „Kriterien für die Aufsicht im Rundfunk und in den Telemedien“ finden Sie im Internet unter http://www.kjm-online.de/public/kjm/index.php?show_1=136,132,56
[11] www.primolo.de

gefährdenden und entwicklungsbeeinträchtigenden Angebote so weit wie möglich alters- und zielgruppengerecht zu sperren. Schulen in Ballungszentren oder sozialen Brennpunkten benötigen womöglich rigidere Einschränkungen der Filtersoftware, abhängig von der sozialen Reife ihrer Schülerinnen und Schüler.

Die traditionellen Medien verfügen über nationale Kontrollinstrumente, die einen altersabhängigen Schutz - zumindest zu einem großen Teil - gewährleisten können.

Im Internet gibt es alles - zu jeder Zeit

Beim Fernsehen sind dies die Sendezeiten, die sicherstellen sollen, dass beeinträchtigende Angebote von der betroffenen Altersgruppe üblicherweise nicht mehr wahrgenommen werden. Diese zeitliche Barriere fällt im Internet komplett weg. Hier sind alle Angebote rund um die Uhr für jeden verfügbar. Damit ist auch der Zugriff auf jugendschutzrelevante Inhalte jederzeit möglich.

Filme und Computerspiele unterliegen der Kennzeichnung der Freiwilligen Selbstkontrolle der Filmwirtschaft (FSK) und der Unterhaltungssoftware Selbstkontrolle für Computerspiele (USK)[12].

Verbindliche Alterskennzeichnungen der FSK für Filme

Freigegeben ohne Altersbeschränkung gemäß § 14 JuSchG

Freigegeben nach Altersgruppen gemäß § 14 JuSchG

Keine Jugendfreigabe gemäß § 14 JuSchG

[12] Altersfreigaben für Computerspiele sind seit dem 1. April 2003 gesetzlich vorgeschrieben. Sie sollen sicherstellen, dass Kinder und Jugendliche nur Spiele-Software erwerben können, die für ihr jeweiliges Alter unbedenklich ist.

Verbindliche Alterskennzeichnungen der USK für Computerspiele

Freigegeben ohne Altersbeschränkung gemäß § 14 JuSchG

Freigegeben nach Altersgruppen gemäß § 14 JuSchG

Keine Jugendfreigabe gemäß § 14 JuSchG

Für Webseiten hingegen gibt es eine solche Alterskennzeichnung nicht. Sie sind zudem jederzeit für jedermann weltweit zugänglich. Daraus folgt, dass zur Sicherstellung der jugendmedienschutzrechtlichen Anforderungen im Internet andere Mechanismen greifen müssen.

Der Gesetzgeber hat der Kommission für Jugendmedienschutz (KJM) die Aufsicht über privaten Rundfunk und Telemedien[13] übertragen. Sie ist somit als Prüfungs-

[13] Dazu zählt auch das Internet.

instanz für die „Aufsicht über das Internet" zuständig. Die KJM soll laut Gesetzeslage Filterprogramme bewerten und nach einem Prüfverfahren[14] die Anerkennung gemäß den Anforderungen des § 11 JMStV aussprechen. Anbieter von Jugendschutzprogrammen können ihre Produkte der KJM zur Anerkennung vorlegen. Diese hat die Möglichkeit, auch zeitlich befristete Modellversuche zuzulassen, um neue Verfahren, Vorkehrungen oder technische Hilfsmittel - wie beispielsweise Filterprogramme - auf Gewährleistung des Jugendschutzes zu erproben.

KJM prüft Filterprogramme

Die KJM hat bereits mehrere derartige Modellversuche zugelassen. Dabei erfüllte jedoch keines der vorgelegten Jugendschutzprogramme die Anforderungen des § 11 JMStV, so dass die KJM bislang noch keine Anerkennung aussprechen konnte.

Noch keine Anerkennung durch die KJM

Telemedien - hierzu zählen Internetangebote - unterliegen ebenso wie herkömmliche Medien grundsätzlich dem Indizierungsverfahren der Bundesprüfstelle für jugendgefährdende Medien. Nach dem Jugendmedienschutz-Staatsvertrag (§ 16 JMStV) und dem Jugendschutzgesetz[15] (§ 21 JuSchG) ist die KJM in die Indizierungsentscheidungen bei Telemedien durch die Bundesprüfstelle für jugendgefährdende Medien (BPjM) wesentlich eingebunden. Die KJM kann auch selbst Indizierungsanträge bei der BPjM stellen.

Das Indizierungsverfahren bedenklicher Inhalte kann durch einen Antrag beziehungsweise durch eine Anregung zur Indexierung eingeleitet werden. Weitere Informationen zu dem Verfahren sind ausführlich auf den Internetseiten der BPjM beschrieben.[16] Entsprechende Meldungen können auch an die Hotline der Organisation jugendschutz.net weitergeleitet werden.[17]

Bedenkliche Seiten melden

1.3 Jugendschutzfilter im ideologischen Fokus

Filterprogramme funktionieren nach bestimmten Regelwerken, die in den Programmen als so genannte Sperr- beziehungsweise Filterlisten[18] nach genau definierten Bewertungsmaßstäben enthalten sind. Diese können per se nicht objektiv sein. Die auf dem Markt angebotenen Filterprogramme stammen größtenteils von US-amerikanischen Herstellern, die das Angebot im Internet folglich anhand

Filter sind nicht objektiv

14 Mehr zum Prüfverfahren der KJM finden Sie im Internet unter http://www.kjm-online.de/public/kjm/index.php?show_1=137,56
15 Das Jugendschutzgesetz finden Sie im Internet unter http://artikel5.de/gesetze/juschg.html
16 http://www.bundespruefstelle.de
17 Jugendschutz.net wurde 1997 von den Jugendministern aller Bundesländer gegründet, um jugendschutzrelevante Angebote im Internet (so genannte Telemedien) zu überprüfen und auf die Einhaltung von Jugendschutzbestimmungen zu drängen. Ziel ist ein vergleichbarer Jugendschutz wie in den traditionellen Medien. Hinweise auf Verstöße nimmt jugendschutz.net über seine Beschwerdestelle (Hotline) entgegen. Ein entsprechendes Melde-Formular finden Sie unter http://www.jugendschutz.net/hotline/index.html
18 Siehe Kapitel 3.

der in den USA geltenden gesellschaftlichen und kulturellen Werte und Normen kategorisieren. Diese weichen zum Teil erheblich von den kulturellen Wertvorstellungen in Deutschland beziehungsweise Europa ab.

Nach deutschen Maßstäben unproblematische Inhalte, wie beispielsweise Aufklärungsseiten generell zu Sexualität oder speziell zu Homosexualität, werden in den USA häufig als problematisch bewertet und somit durch Filterprogramme geblockt. Andererseits fällt beispielsweise die Leugnung des Holocaust in den USA unter das Recht auf freie Meinungsäußerung. Entsprechende Angebote sind dort also möglicherweise nicht in der Sperrliste enthalten. In Deutschland sind solche Äußerungen jedoch verfassungswidrig und somit strafbar. Sie müssen also nach deutschen Maßstäben durch ein Filterprogramm in jedem Fall geblockt werden.

Filter können nicht denken - aber lenken

Neben der kulturellen Herkunft der Filterhersteller spielt auch deren ideologische Ausrichtung eine große Rolle. Durch die Kategorisierung und Auswahl der gefilterten Inhalte ist eine unerwünschte Manipulation und Beschränkung der Informationsfreiheit denkbar. Insofern ist eine kritische Betrachtung von Filterprogrammen hinsichtlich eines möglichen manipulativen Potenzials durchaus empfehlenswert. Entscheidend ist, dass Filter immer nur das filtern, was „man" sie filtern lässt. Die in anderen Zusammenhängen intensiv diskutierte Zensur-Frage beim Einsatz von Filtern stellt sich an Schulen nur bedingt, da hier Fragen des Jugendschutzes eindeutig im Vordergrund stehen.

Filter sind nicht clever

Damit die optimale Filterleistung eines Programms erreicht werden kann, sollte auch die Sprachspezialisierung der Software berücksichtigt werden. Stammt die eingesetzte Filterliste aus dem englischsprachigen Raum, hat dies Auswirkungen auf die zu erwartende Filterleistung. Das Programm wird möglicherweise Begriffe sperren, die zwar im Englischen problematisch, im Deutschen aber völlig harmlos sind.

Darüber hinaus sind Filterprogramme heute noch nicht hinreichend in der Lage, Begriffe in ihrem Kontext zu erkennen und daraus auf eine potenzielle Jugend-

schutzrelevanz zu schließen. Unter anderem aus diesen Gründen kann es zu einer Überfilterung der Inhalte, auch Overblocking genannt, kommen.

Definition „Überfiltern"
Überfiltern oder Overblocking bedeutet das Filtern beziehungsweise Abblocken von unbedenklichen Inhalten, die aufgrund einer vorliegenden Kategorisierung von der Filtersoftware als unzulässig interpretiert und damit abgeblockt werden.

Im nachfolgenden Beispiel hat der Wortfilter eines Filterprogramms den Wortbestandteil „teenfotos" der Webseite kakteenfotos.de als jugendschutzrelevant klassifiziert und die Seite gesperrt. Obwohl die Inhalte der Seite unbedenklich sind, steht sie für den Biologie- oder Erdkundeunterricht nicht mehr zur Verfügung.

Abbildung 1: Beispiel für Überfilterung
Filtersoftware ist nicht in der Lage, den Wortbestandteil „teenfotos" in „Kakteenfotos" als solchen zu erkennen und blockt diese Seite ab.

2. Rechtliche Vorgaben des Jugendmedienschutzes

Damit Pädagoginnen und Pädagogen ihrer Aufsichtspflicht gerecht werden können, sollten sie sich über die rechtliche Einordnung von problematischen Inhalten informieren. Nur so können sie die konkreten Konsequenzen für den Unterrichtsalltag abschätzen. Zudem gibt die Kenntnis der rechtlichen Zusammenhänge den Lehrkräften mehr Sicherheit, das Internet im Unterricht als selbstverständliches Handwerkszeug einzusetzen.

Tipp
Der Verein Schulen ans Netz unterstützt Lehrerinnen und Lehrer mit einem sehr umfassenden Informationsangebot zu zahlreichen Rechtsfragen aus dem Schulumfeld durch das Online-Angebot unter www.lehrer-online.de/recht

Rechtliche Grundlagen

Der Bereich des Jugendschutzes bei Online-Medien (Telemedien) wird aus Gründen der Gesetzgebungskompetenz nicht im Jugendschutzgesetz, sondern in dem von den Bundesländern verfassten Jugendmedienschutz-Staatsvertrag (JMStV) geregelt.

Der JMStV bestimmt, vor welchen Inhalten Jugendliche und damit auch Schülerinnen und Schüler auf jeden Fall geschützt werden müssen.

2.1 Rechtliche Kategorisierung der Inhalte

Bei der Kategorisierung von Medienangeboten wird aus rechtlicher Sicht zwischen absolut verbotenen, relativ verbotenen sowie entwicklungsbeeinträchtigenden Inhalten unterschieden.

Zugänglichmachen bedeutet aus rechtlicher Sicht, dass Schülerinnen und Schülern die Möglichkeit eröffnet wird, sich durch sinnliche Wahrnehmung Kenntnis vom Inhalt eines jugendschutzrelevanten Angebots zu verschaffen.

2.1.1 Absolut verbotene Inhalte

§ 4 Abs.1 des JMStV legt fest, dass die generelle Verbreitung bestimmter Medienangebote untersagt ist. Diese absolut verbotenen Inhalte sind teilweise durch ihre strafrechtliche Relevanz, immer aber durch eine schwere Jugendgefährdung gekennzeichnet. Dazu zählen:

- **im Bereich Sex/Pornografie**
  frei zugängliche Hardcore-Darstellungen oder die geschlechtsbetonte Darstellung Minderjähriger

- **im Bereich Rassismus/Rechtsextremismus**
  Seiten, die rechtsextreme Propagandamittel verbreiten, verfassungswidrige Kennzeichen nutzen oder Volksverhetzung betreiben

- **im Bereich Tasteless/Gewalt**
  Darstellungen, die die Menschenwürde sterbender oder leidender Personen verletzen (z. B. Bilder von Unfallopfern)

Absolut verbotene Inhalte dürfen den Schülerinnen und Schülern unabhängig vom Alter in keinem Fall zugänglich gemacht werden.

2.1.2 Relativ verbotene Inhalte

Der JMStV untersagt in § 4 Abs. 2 die unbeschränkte Verbreitung bestimmter Medienangebote. Diese Angebote gelten nur dann als legal, wenn der Anbieter die Inhalte einer geschlossenen Benutzergruppe zugänglich macht und sicherstellt, dass Minderjährige keinen Zugriff auf das Angebot haben.
Zu dieser Kategorie zählen:

- Seiten mit pornografischen Inhalten, bei denen die fokussierte Darstellung von Geschlechtsteilen und sexuellen Vorgängen unter Ausklammerung zwischenmenschlicher Beziehungen in den Vordergrund gestellt werden

- wegen Jugendgefährdung durch die BPjM in die Liste aufgenommene Medien wie Splattermovies oder Horrorfilme

- besonders gravierende, so genannte offensichtlich schwer jugendgefährdende Inhalte wie Darstellungen sexueller Erniedrigung unterhalb der Pornografie-Grenze, also SM- oder Bondage-Inhalte

- drogenverherrlichende Inhalte

- Verherrlichung der Selbsttötung oder öffentliches Auffordern zum Suizid (häufig in Foren anzutreffen)

Relativ verbotene Inhalte dürfen minderjährigen Schülerinnen und Schülern nicht zugänglich gemacht werden.

2.1.3 Entwicklungsbeeinträchtigende Inhalte

Laut § 5 Abs. 1 des JMStV müssen Anbieter und Verbreiter von so genannten entwicklungsbeeinträchtigenden Inhalten dafür Sorge tragen, dass diese für Kinder oder Jugendliche **der betreffenden Altersgruppe** nicht zugänglich sind. Zu den entwicklungsbeeinträchtigenden Inhalten zählen:

- alle Inhalte, die geeignet sind, die Entwicklung von Kindern und Jugendlichen zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit zu beeinträchtigen

Entwicklungsbeeinträchtigende Inhalte dürfen minderjährigen Schülerinnen und Schülern nur **entsprechend ihrer Altersgruppe** zugänglich gemacht weden.

2.2 Konsequenzen für die schulische Praxis

Nach dem Jugendmedienschutz-Staatsvertrag dürfen verbotene und jugendgefährdende Inhalte weder durch Lehrkräfte noch durch sonstiges Schulpersonal Kindern und Jugendlichen zugänglich gemacht werden. In der Praxis kann dies Probleme hinsichtlich der Einhaltung der Aufsichtspflicht aufwerfen, die anhand eines Beispiels aus dem Unterrichtsalltag verdeutlicht werden sollen:

> Der Religionslehrer möchte im Unterricht satanische beziehungsweise gewaltverherrlichende Seiten zeigen, um den Schülern die Hintergründe, Zusammenhänge und negativen Auswirkungen transparent zu machen und näher zu bringen. Ist das erlaubt? Die Antwort ist „Nein"! Die pädagogisch betreute Konfrontation der Klasse mit schwer jugendgefährdenden Inhalten - selbst in bester Absicht - ist nicht zulässig.

Kein Elternprivileg für Lehrkräfte

Die straf- und jugendschutzrechtlichen Bestimmungen räumen lediglich den Eltern minderjähriger Personen eine Ausnahme von den jeweiligen Verboten des Zugänglichmachens in einem begrenzten Umfang ein. Dies bedeutet in der Praxis, dass Lehrkräfte auch dann keine schwer jugendgefährdenden Inhalte in den Unterricht einbeziehen dürfen, wenn sie mit Zustimmung der Eltern handeln. Denn selbst das schriftliche Einverständnis der Eltern entbindet Schulleitung und Lehrkräfte nicht von ihrer Verantwortlichkeit, den Zugang zu jugendgefährdenden Inhalten zu verhindern.

Sind Filter für Schulen gesetzlich vorgeschrieben?

Einige der zitierten Gesetze und Vorschriften erwecken möglicherweise den Eindruck, dass der Einsatz von Filtersoftware in Schulen gesetzlich vorgeschrieben sei. Dies ist nach geltender Rechtslage jedoch nicht zwingend. Wie nachfolgend näher ausgeführt wird, greifen aus rechtlicher Sicht unterschiedliche Möglichkeiten zur Erfüllung der Aufsichtspflicht. Filtersoftware oder sonstige technische Schutzmaßnahmen können die Notwendigkeit persönlicher Kontrollen grundsätzlich nicht ersetzen, dürften jedoch in vielen Fällen eine sinnvolle Ergänzung darstellen. Zahlreiche konkrete Praxisbeispiele sowie aktuelle Nachrichten und Informationen zu rechtlichen Aspekten der neuen Medien in Schulen stellt der Verein Schulen ans Netz unter http://www.lehrer-online.de/recht zur Verfügung.

Nach dem **deutschen Strafgesetzbuch** (StGB) ist die Verbreitung beziehungsweise das Zugänglichmachen zahlreicher Internetinhalte bei Strafe untersagt. Dazu zählen insbesondere:

- **Propagandamittel oder Kennzeichen verfassungswidriger Organisationen** (§ 86, 86a StGB),
- **Öffentliche Aufforderung zu Straftaten** (§ 111 StGB),
- **Volksverhetzung und Holocaust-Leugnung** (§ 130 StGB),
- **Unterstützen einer kriminellen oder terroristischen Vereinigung** (§§ 129, 129a StGB),
- **Extreme Gewaltdarstellungen** (§ 131 StGB),
- **Anleitung zu Straftaten** (§130a StGB),
- **Belohnung und Billigung von Straftaten** (§ 140 StGB),
- **Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen** (§ 166 StGB),
- **Pornografie** (§ 184 StGB) („harte" Pornografie [Kinderpornografie, Sex mit Gewalttätigkeiten oder Tieren] sind generell untersagt; „einfache" Pornografie darf Minderjährigen nicht zugänglich gemacht werden),
- **Beleidigung, üble Nachrede, Verleumdung, Verunglimpfung des Andenkens Verstorbener** (§ 185 ff. StGB),
- **Unerlaubtes Glücksspiel** (§ 284 ff. StGB).

Nach dem **Jugendmedienschutz-Staatsvertrag** (JMStV) sind weitere Internetinhalte entweder generell untersagt oder zumindest das Zugänglichmachen gegenüber Minderjährigen. Dazu zählen insbesondere:

- **Kriegsverherrlichende Inhalte** (§ 4 Abs. 1 S. 1 Nr. 7 JMStV),
- **Geschlechtsbetonte Darstellungen Minderjähriger** (§ 4 Abs. 1 S. 1 Nr. 9 JMStV),
- **Die Menschenwürde verletzende Inhalte einschließlich solcher, die real sterbende oder schwer leidende Menschen darstellen** (§ 4 Abs. 1 S. 1 Nr. 8 JMStV),
- **Inhalte, welche von der Bundesprüfstelle für jugendgefährdende Medien (BPjM) indiziert, also auf eine Verbotsliste aufgenommen worden sind** (§§ 15, 18 JuSchG, § 4 Abs. 2 S. 1 Nr. 2 JMStV),
- **Offensichtlich schwer jugendgefährdende Inhalte** (zum Beispiel Anleitung und Aufruf zum Drogenkonsum oder zum Suizid) (§ 4 Abs. 2 S. 1 Nr. 3 JMStV).

2. 3 Umfang und Möglichkeiten der Aufsicht

Sobald das Internet im Unterricht eingesetzt wird, sind die Lehrkräfte diesbezüglich verstärkt zur Einhaltung des Jugendmedienschutzes verpflichtet. Grundsätzlich ist dabei zu beachten, dass die eingesetzten Mittel aufgrund datenschutzrechtlicher Bestimmungen stets verhältnismäßig sein müssen.

Der schulischen Aufsichtspflicht - und damit der Erfüllung des Erziehungs- und Unterrichtsauftrags - ist trotz datenschutzrechtlicher Grenzen eine besondere Bedeutung beizumessen. Nachfolgend sind einige Möglichkeiten der Überwachung und Aufsicht im Schulbetrieb näher erläutert.

Persönliche Kontrolle

Der Umfang der Aufsichtspflicht sollte vom Alter beziehungsweise Reifezustand der Schülerinnen und Schüler, ihrem bisher bekannten Verhalten sowie dem Maß der bestehenden Gefahr abhängig gemacht werden. Dieser sehr theoretisch anmutenden Forderung kann zum Beispiel durch persönliche Kontrolle Rechnung getragen werden. Lehrkräfte können sich während des Unterrichts durch Stichproben davon überzeugen, dass die Schülerinnen und Schüler keine unzulässigen Inhalte aufrufen. Für diese Methode ist eine offene Anordnung der Computertische sinnvoll, bei der die Lehrkraft alle Bildschirme im Blick hat.

Monitoring stellt partielle Kontrolle sicher

Eine weitere Aufsichtsmaßnahme stellt das so genannte Monitoring dar. Es ermöglicht den Lehrkräften, sich den Bildschirminhalt einzelner Schüler auf den eigenen Monitor zu übertragen und so deren Aktivitäten direkt zu kontrollieren. Aus datenschutzrechtlichen Gründen[19] ist beim Monitoring lediglich eine Echtzeitkontrolle ohne Aufzeichnung erlaubt.

Filter können unterstützen

Ergänzend und unterstützend zu den erwähnten Kontrollmöglichkeiten können Filterprogramme eingesetzt werden. Es ist wichtig darauf hinzuweisen, dass die Aufsichtspflicht demnach keinesfalls auf die Filterprogramme alleine übertragen werden kann. [20] Gegenwärtig kann kein Filtersystem einen vollständigen Schutz vor jugendschutzrechtlich fragwürdigen Inhalten bieten. Die schnelle Entwicklung des Internets mit weltweit täglich neu hinzukommenden Angeboten macht es aus heutiger Sicht unmöglich, alle Internetinhalte zeitnah mit einem Filterprogramm zu

19 Siehe Kapitel 2.4.
20 So auch zum Beispiel die Muster-Nutzungsordnung zum Gebrauch von Computereinrichtungen an Schulen des Thüringer Arbeitskreises Schulsoftware. Diese Nutzungsordnung finden Sie im Internet unter http://filter.th.schule.de/menue/hauptseite.php

erfassen und zu bewerten. Gleichwohl bieten Filterprogramme im Rahmen ihrer Möglichkeiten eine wichtige und oftmals auch weitreichende Ergänzung zu den manuellen Kontrollmöglichkeiten. Der Einsatz von Filterprodukten kann Lehrkräften somit eine wertvolle Unterstützung sein und eine höhere Sicherheit bei der Internetnutzung im Unterricht gewährleisten.

2.4 Grenzen der Kontrolle

Datenschutz setzt Grenzen

Die Einhaltung der Aufsichtspflicht erfordert den Einsatz gewisser Überwachungsmaßnahmen und Kontrollmechanismen. Der Datenschutz legt dabei die Grenzen der Überwachung von Schülerinnen und Schülern im Rahmen der Internetnutzung im Unterricht und auf dem Schulgelände fest. Kann nicht ausgeschlossen werden, dass durch die Kontrolle dieser rechtlich geschützte Bereich verletzt wird, muss laut Gesetz von der entsprechenden Kontrolle abgesehen werden. Da ein unkontrollierter Zugriff auf das Internet in der Unterrichtspraxis jedoch nicht vertretbar ist, empfiehlt es sich, vor der Internetnutzung im Unterricht die Schülerinnen und Schüler sowie die Erziehungsberechtigten über die Kontrollmaßnahmen und die Installation technischer Kontrollinstrumente wie Filter oder Monitoring zu informieren. Es hat sich in der Praxis als nützlich erwiesen, hierüber eine schriftliche Vereinbarung zwischen Schule und Schülern beziehungsweise den Erziehungsberechtigten zu fixieren.

Schriftliche Vereinbarung regelt Internetnutzung

Diese Vereinbarung kann auch in Form einer von Schülern, Lehrern und Eltern gleichermaßen akzeptierten Nutzungsordnung[21] erfolgen, die neben festgeschriebenen Regeln zur Nutzung des Computerraums auch den Umgang mit Schulcomputern einschließlich des Surfens im Internet festschreibt. Die Nutzung der Rechner beziehungsweise des Computerraums kann grundsätzlich von der schriftlichen Anerkennung einer solchen Benutzerordnung durch die Schülerinnen und Schüler respektive deren Eltern abhängig gemacht werden.

Aufsichtspflicht auch außerhalb des Klassenraums

Eine solche Vereinbarung ist besonders für die Nutzung des Internets auch außerhalb des Unterrichts von Bedeutung, beispielsweise bei Freistunden im Computerraum, im Internetcafé oder der Schulbibliothek. Durch die verstärkte Nutzung offener Unterrichtsformen im Rahmen Freier Lernorte[22] wird dieser Frage

[21] Schulen ans Netz e.V. stellt den Mustertext einer Nutzungsordnung mit vielen Hinweisen zur Verfügung unter: http://www.lehrer-online.de/url/nutzungsordnung
Eine "Muster-Nutzungsordnung der Computereinrichtungen an Schulen" der Kultusministerkonferenz (KMK) ist unter http://www.bildungsportal.nrw.de/BP/Schule/Multimedia/Internetnutzung/NutzungsordnungComputer.doc abrufbar.

[22] Mehr Informationen finden Sie unter www.freie-lernorte.de

künftig wachsende Bedeutung beizumessen sein. Die Aufsichtspflicht greift grundsätzlich auch in solchen Fällen. In diesem Zusammenhang ist bemerkenswert, dass die Schule auch dann schon einen haftungsrechtlich relevanten Beitrag leistet, wenn sie nur Teile der benötigten Mittel zur Verfügung stellt - beispielsweise nur die Räumlichkeiten -, die Computer und der Internetanschluss aber von den Schülerinnen und Schülern selbst organisiert werden.

Absicherung für Schulleitungen und Lehrkräfte

Doch keine Sorge! Für Schulleitung und Lehrkräfte kann die vorgenannte Nutzungsordnung auch in diesem Fall eine rechtliche Absicherung leisten. So können unter anderem Bestimmungen zur Benutzung der Medien sowie Kontrollen und insbesondere mögliche Sanktionen bei einem Verstoß gegen die Nutzungsordnung festgeschrieben werden. Damit ist aus Sicht der Schule ein verbindlicher rechtlicher Rahmen zur Nutzung von Internet und Medien an der Schule gesteckt, der Schülerinnen und Schülern eine verbindliche Orientierung vorgibt.

In Chatrooms wird nicht nur geplaudert

Auch wenn für Schulen meistens das Filtern von Angeboten des Internets im Vordergrund steht, sind aus jugendschutzrechtlicher Sicht auch weitere Internetdienste wie zum Beispiel der Chat in die Überlegungen einzubeziehen. Kinder und Jugendliche chatten gern und viel. Über die Hälfte aller Jugendlichen besucht mehr oder weniger regelmäßig Chaträume.[23] Der Aufenthalt im Chat kann jedoch unter bestimmten Umständen vom netten Plaudern mit Gleichgesinnten zu einer traumatischen Erfahrung für die Kinder mutieren. Denn durch seine Anonymität und Unverbindlichkeit stellt der Chatraum eine ideale Plattform für sexuelle Übergriffe dar. Recherchen und Befragungen[24] von jugendschutz.net belegen, dass bei einer Vielzahl der Chats problematische Kontakte, zum Beispiel Beleidigungen und Beschimpfungen, und sogar weitergehende Kontakte, wie sexuelle Belästigung und sexueller Missbrauch, an der Tagesordnung sind.

Kinder sind oftmals unbedarft

Ein angebahnter Kontakt kann darüber hinaus im Extremfall auch zu Übergriffen per Telefon oder E-Mail führen, insbesondere dann, wenn die Kinder im Chat ihre Identität namentlich preisgeben.[25] Umfassende Hintergrundinformationen zum Thema gibt die Broschüre „Chatten ohne Risiko“ von jugendschutz.net.[26]

23 JIM-Studie 2003, http://www.mpfs.de/studien/jim/jim03.html
24 Chatten ohne Risiko? Zwischen fettem Grinsen und Cybersex. Jugendschutz.net - Jugendschutz in Telemedien (Hrsg.), 2. Auflage 2005, S.6.
25 Nach der Studie Kinder Online (2004) gibt jedes siebte Kind im Alter von 6 bis 16 Jahren seine Identität im Chat preis. Die Ergebnisse der Studie finden Sie im Internet unter: http://www.neue-digitale.de/deutsch/presse/040908_Ergebnispraesentation_Studie_Kinder_Online_2004.pdf
26 Die Broschüre sowie „Spickzettel“ für Kinder und Jugendliche finden Sie im Internet unter der Adresse: http://www.jugendschutz.net/materialien/chatten_ohne_risiko.html zum Download bereit.

Wie das vorgenannte Beispiel zum Thema Chat ahnen lässt, geht es im Schulumfeld nicht einzig darum, den Zugriff auf die Inhalte des Internets im Auge zu behalten. Auch die Nutzung weiterer, internetspezifischer Dienste wie Mail, News, Tauschbörsen & Co. sind zu berücksichtigen. Manche Filterprodukte bieten auch für diesen Fall entsprechende Einstellungen, um den Zugriff auf Mail, Chat & Co. zu regulieren und bei Bedarf einzuschränken. Fehlen diese Optionen, können ergänzende Maßnahmen, zum Beispiel durch Einbindung einer Firewall, für die gewünschte Sicherheit sorgen.

3. Einsatz an Schulen

3.1 Funktionsweisen von Filterprogrammen

Filterprogramme sind, betrachtet man ihre Entstehungsgeschichte, eigentlich nur Ableger von Entwicklungen mit ursprünglich anderem Hintergrund. So dienten Programme zur inhaltlichen Filterung des Internets zunächst der Downloadoptimierung von grafikintensiven Webseiten. Später wurden die Mechanismen von Filtersoftware verfeinert und in der Industrie zur Einschränkung des privaten Surfens am Arbeitsplatz eingesetzt. Jugendschutzfragen spielten in den frühen Einsatzgebieten der Filterprodukte zunächst kaum eine Rolle.

Bevor in den nachfolgenden Ausführungen der Frage nachgegangen werden kann, welche Anforderungen an einen Jugendschutzfilter im Schulumfeld zu stellen sind, werden die unterschiedlichen Filterverfahren und -systeme kurz erläutert. Die am Markt angebotenen Filterprodukte basieren auf sehr unterschiedlichen Ansätzen. Die Techniken reichen dabei vom simplen Abgleich einfacher Textmuster bis hin zu komplexen Verfahren mit Bildanalyse oder sogar „künstlicher Intelligenz".

3.1.1 Wortfilter / Worterkennung oder Keyword Blocking

Ein auf Wortfilter, Worterkennung oder Keyword Blocking basierender Filter verfügt über eine oder mehrere Listen mit zu sperrenden Schlüsselwörtern. Bevor eine Internetseite angezeigt wird, analysiert die Filtersoftware den Quelltext[27] der Seite und gleicht diesen mit allen Einträgen der Filterliste ab. Falls **keine** Begriffe aus der Liste in dieser Seite vorkommen, erscheint diese auf dem Bildschirm, ansonsten wird sie vom System geblockt und somit nicht angezeigt.

Die Liste kann beliebige Wörter und Begriffe enthalten, wie beispielsweise auf Sexualität zielende Wörter aus der Alltags-, Umgangs- und Vulgärsprache. Üblich sind auch beliebige Kombinationen aus Ziffern und/oder Buchstaben, so genannte Zeichenketten. Der besseren Übersicht wegen verwenden auf Wortfiltern basierende Filterprodukte oftmals mehrere Dateien zum Speichern von Schlüsselwörtern nach Kategorien wie beispielsweise Pornografie, Gewalt oder Rassismus.

[27] Als „Quelltext" bezeichnet man den Inhalt einer Internetseite inklusive den für Internetnutzer unsichtbaren Programmierbefehlen (zum Beispiel für das Layout).

Abbildung 2: Beispiel Wortliste der Kategorie Sexualität

Keine Chance für Essex

Ein systembedingtes und damit grundsätzliches Problem dieser Filtermethode ist, dass bei einer Filterung nach der vorgenannten Beispielliste Seiten über das "Pastoral**sEx**amen" oder „Es**sex**“ ebenso wenig angezeigt werden können wie die Mathematikseite, die sich mit "**Potenz**en" oder „**Anal**ysis“ auseinander setzt. Die Filterprogramme nach diesem Verfahren untersuchen Internetseiten nach den Vorgaben rein lexikalisch und können semantische Unterschiede nicht erkennen. Kommt also beispielsweise das in der Sperrliste aufgeführte Wort „Sex“ auf einer Seite vor, so wird diese Seite gesperrt, egal ob es sich um ein Pornoangebot oder aber eine Seite zur Sexualaufklärung handelt. Aus dem gleichen Grund ist es der Schlüsselwortsuche auch nicht möglich, historische Berichte über den Nationalsozialismus von rechtsradikaler Propaganda zu unterscheiden.

Anbieter finden immer einen Weg

Anbieter einschlägiger Angebote sind zudem erfindungsreich und umgehen die Filter durch immer einfallsreichere Schreibweisen der angebotenen Inhalte, zum Beispiel V!agra oder V1agra.

Sprachspezialisierung beeinflusst Filterleistung

Bei internationalen Seiten gestaltet sich eine Filterung auf Keyword-Basis äußerst uneffektiv, da im Prinzip für jede Sprache eine eigene Filterregel aufgestellt werden müsste. Durch die Sprachspezialisierung der Filtersoftware können sich auch Probleme mit Homonymen[28] ergeben, weil der Filter die Bedeutung gleicher Wörter - für den Computer sind das lediglich Buchstabenfolgen - in verschiedenen

[28] Laut Duden ist von Homonymen in der Sprachwissenschaft die Rede, wenn zwei Wörter eine unterschiedliche Bedeutung haben, dabei jedoch in Aussprache und Schreibung völlig übereinstimmen, z. B. Bauer (= Landwirt/Vogelkäfig), Schauer (= Regenguss/sich aufbauender Schrecken), Heide (= Landschaft/Nichtchrist).

Sprachen nicht erkennen kann. Je detaillierter also die „Sprachkompetenz“ des Filterprogramms, desto niedriger der Faktor der Überfilterung.

Versteckspiel mit Hilfe von Grafiken

Worterkennungsprogramme haben zudem prinzipiell ein Problem mit Internetseiten, die einen sehr hohen Grafikanteil aufweisen oder gar ausschließlich mit Grafik- oder Multimedia-Elementen, zum Beispiel Flash[29], erstellt wurden. Grafiken werden nämlich durch den rein textorientierten Filtermechanismus nicht berücksichtigt und somit auch nicht gefiltert. Texte, die als Grafik im Internet veröffentlicht werden, können daher von diesen Programmen auch nicht als Text erkannt und ausgewertet werden.

Durch weitere Programmoptionen können die Programme in der Wirkung bis zu einem gewissen Grad optimiert werden, zum Beispiel durch Unterscheidung von Groß- und Kleinschreibung oder Analyse von Wortteilen. Die Filterwirkung ist im Vergleich zu anderen Verfahren insgesamt jedoch eher mäßig. So gibt es heute auch nur noch wenige Programme, die ausschließlich mit diesem simplen Verfahren arbeiten.

3.1.2 Negativlisten / Blacklists

Gezielte Sperrung von Internetseiten

Eine Vielzahl von Filterprogrammen basiert auf dem Einsatz von so genannten Negativlisten oder Blacklists. Im Unterschied zum Wortfilter werden in den Listen keine Schlüsselwörter abgelegt, sondern komplette Internetadressen verzeichnet. Dies erfolgt im Idealfall als URL in der Schreibweise „www.domain.de“ nebst der dazugehörigen IP-Adresse[30] in der Schreibweise 195.132.10.xxx. Negativlisten sind häufig in Kategorien unterteilt, wie zum Beispiel Gewalt, teilweise und komplette Nacktheit, Drogen oder Satanisches/Kulthaftes. Diese Kategorien erlauben in den Administrationseinstellungen der Filterprogramme die fein abgestufte Regelung des Internetzugangs nach den gewünschten Kriterien.

Ähnlich der Sprachspezialisierung bei Wortfiltern stellt sich auch bei den Blacklists die Frage nach den enthaltenen Listeneinträgen. Sofern sich die Filterlisten auf bestimmte Internetbereiche beschränken, zum Beispiel jeweils nur auf *.de, *.com, *.net, gilt: nur die in den Listen enthaltenen Einträge werden differenziert

29 Flash bezeichnet eine Technik zur Anzeige „bewegter Grafiken“.
30 Eine IP-Adresse ist eine einmalig vergebene Nummernkombination, die den zugehörigen Rechner im Internet zweifelsfrei identifiziert. Die IP-Adresse besteht immer aus einem Zahlencode von vier Zahlen von 0 bis 255 (zum Beispiel 192.168.0.55).

gefiltert, alle anderen werden entweder gar nicht gefiltert oder aber komplett gesperrt.

Abbildung 3: Beispiel Negativliste der Kategorie Sexualität

Ständige Aktualisierung notwendig

Das Internet unterliegt wie kein anderes Medium permanenten Veränderungen. Allen Negativlisten ist daher das Erfordernis der aufwändigen Aktualisierung, das heißt Hinzufügen neuer Einträge und Überprüfung der Richtigkeit der bestehenden, gemein. Filterprogramme, die auf Negativlisten basieren, müssen ständig an die Veränderungen im Internet angepasst werden, um nachhaltig eine sichere Filterwirkung erzielen zu können. Bei kommerziellen Filterprodukten pflegen und kategorisieren Mitarbeiter der Herstellerfirma diese Sperrlisten. Eine andere Möglichkeit ist die automatisierte Aktualisierung durch Robots.[31] Die Meinung zu Qualitätsunterschieden zwischen manueller oder automatischer Listenpflege geht allerdings sehr weit auseinander. Jedes Verfahren hat seine spezifischen Vor- und Nachteile.

Die mit großem Aufwand aktualisierten Filterlisten stellen für die Anbieter von Filtersoftware ein erhebliches Betriebskapital dar. Die Listen sind daher meist nur gegen Entgelt in verschlüsselter Form zu beziehen. Die aktualisierten Fassungen (Updates) können dann regelmäßig aus dem Internet heruntergeladen werden. Eine gewisse Anzahl von Updates oder eine zeitlich begrenzte Update-Periode sind häufig im Kaufpreis enthalten. Danach wird in der Regel auch das Aktualisieren der

[31] Robots sind Programme, die weitgehend selbstständig und ohne Benutzerinteraktion arbeiten.

Listen kostenpflichtig.[32] Negativlisten sollten aber grundsätzlich auch aus einem anderen Grund nur in verschlüsselter Form vorliegen. Die Inhalte der Listen sind als hochsensibel anzusehen, stellen sie doch das umfassende Inhaltsverzeichnis bedenklicher Inhalte dar.

Auch Negativlisten überfiltern

Bei der Verwendung von Negativlisten muss ein mögliches Überfiltern ebenso einkalkuliert werden wie die Möglichkeit, dass unerwünschte Inhalte nicht komplett vom Filter erfasst werden können. Zu einer Überfilterung kann es insbesondere dann kommen, wenn unter einer IP-Adresse mehrere Webangebote zu erreichen sind. Dies ist ein übliches Verfahren bei Providern, die auf **einer** Server-Hardware **mehrere** so genannte virtuelle Web-Hosts[33] betreiben. In diesem Fall kann die Sperrung der IP-Adresse zu einem jugendgefährdenden Angebot zur gleichzeitigen Sperrung eigentlich unbedenklicher Webangebote unter der gleichen IP-Adresse führen. Filterprodukte, die auf Negativlisten basieren, erlauben daher meist auch die gezielte Freigabe von ungerechtfertigt gesperrten Webseiten.

Negativlisten haben prinzipiell ein Problem mit so genannten dynamischen IP-Diensten.[34] Anbieter von unseriösen Inhalten nutzen immer wieder die von Providern bei jeder Einwahl neu zugewiesenen IP-Adressen, um so die Sperren der statischen IP-Listen zu überwinden.

Aus der Praxis

Die Geschwister Scholl-Schule setzt ein Filterprogramm ein, um den Zugriff auf bedenkliche Internetseiten zu sperren. Trotzdem hat es ein Schüler mit Hilfe eines einfachen Tricks geschafft, eine Erotikseite zu öffnen. Wie kann das passieren? Mit Hilfe einer URL-Blacklist werden im Schulnetz die Adressen unerwünschter Seiten gesperrt. Es wurde jedoch versäumt, auch die dazugehörigen IP-Adressen auf die Blacklist zu setzen. Für den technisch versierten Schüler war es nicht schwierig die IP-Adresse der von ihm gewünschten Internetseite zu ermitteln. Da die IP-Adresse nicht auf dem Index des Filters stand, erhielt er ungehindert Zutritt.

32 Neben den kostenpflichtigen Listen kann bei einigen Programmen auch auf kostenlose Blacklists aus dem Internet zurückgegriffen werden. Kostenlos ist zum Beispiel die Blacklist des Bürgernetzes Pfaffenhofen http://www.bn-paf.de, kostenpflichtig ist zum Beispiel die Liste von www.urlblacklist.com

33 Als virtuelle Hosts bezeichnet man mehrere, voneinander unabhängige Webserverprogramme, die sich gemeinsam einen Hardware-Server teilen.

34 Beschreibung der Funktionsweise: http://de.wikipedia.org/wiki/DynDNS

Um einen umfangreichen Schutz zu gewährleisten, muss darauf geachtet werden, dass nicht nur die URL-Adressen, sondern auch die IP-Adressen in die Blacklist mit aufgenommen werden. Weiterhin kann auch ein komplettes Blocken der IP-Eingabe - also beispielsweise in der Form http://173.123.211.xxx - den unerwünschten Webzugriff auf diesem Umweg verhindern.

Qualität - welche Liste ist die Beste?

Die Werbeaussagen der Filterhersteller geizen nicht mit Superlativen. Dabei stellen Angaben zur Anzahl der Filtereinträge oder Kategorien, Aufzählungen von Funktionen und Einstellmöglichkeiten oder Pauschalaussagen zur Kontrolle oder Aktualisierung der Filterlisten kein aussagekräftiges Qualitätskriterium dar.

So ist zum Beispiel die Anzahl der Filtereinträge zu hinterfragen. Bei Milliarden von bestehenden Webseiten decken die oft beworbenen x-Millionen Seiten des Filters nur einen geringen Teil des gesamten Internets ab. Eine Liste mit sehr vielen Einträgen kann zudem nicht mehr existierende Adressen enthalten und damit jeden Filtervorgang mit veralteten Abfragen unnötig belasten. Ebenso wenig sagt die Anzahl der Kategorien etwas über die Qualität einer Filterliste aus. Verwendet ein Programm zum Beispiel „nur" zehn Kategorien, können in diesen sowohl qualitativ bessere als auch zahlenmäßig höhere Einträge enthalten sein als in einem Filterprogramm mit zwanzig Kategorien, in denen nur wenig aktuelle Einträge eingestellt sind. Zudem kann die Qualität zwischen den einzelnen Kategorien voneinander abweichen. Liefert ein Produkt in der Kategorie Pornografie zufriedenstellende Filterergebnisse, kann der Filter in der Kategorie Rechtsradikalismus womöglich nur ungenügend agieren.

Die Angaben zu den Aktualisierungsintervallen der Filterlisten werden ebenfalls zu Werbezwecken oft herangezogen. Das Intervall alleine ist nicht aussagekräftig, vielmehr sollte man zusätzlich das Augenmerk auf die Angaben zu den jeweils durchsuchten und neu aufgenommenen Einträgen richten und auch die Aussagen zu der eingesetzten Aktualisierungstechnik - manuell durch geschultes Personal oder durch Computerroboter - hinterfragen. Zudem ist der Sprachraum von Bedeutung, der in die Aktualisierung der Listen einbezogen ist, denn es ist schon ein Unter-

schied, ob eine Liste täglich um Einträge im deutschsprachigen Raum ergänzt wird, oder ob sich die wöchentliche Aktualisierung lediglich auf den US-amerikanischen Raum beschränkt.

Eine generelle Aussage zum Qualitätsvergleich der Produkte oder gar eine Empfehlung für „das beste Produkt" ist aus den dargelegten Gründen nicht möglich. Im Einzelfall kann nur eine direkte Nachfrage bei den Herstellern zur Entscheidungsfindung beitragen. Produkte von Herstellern, die diese Angaben nicht oder nur widerwillig zur Verfügung stellen, sollten mit einer gewissen Skepsis betrachtet werden.

3.1.3 Positivlisten / Whitelists

Das genaue Gegenteil zu Negativlisten (Blacklists) sind Positivlisten (Whitelists). In der Funktionsweise grundsätzlich vergleichbar, zielt der Ansatz von Positivlisten jedoch auf eine explizite Freigabe von unbedenklichen Seiten ab, während alle anderen Seiten des Internets einer Vollsperrung unterliegen.

Abbildung 4: Beispiel Positivliste / Whitelist der Kategorie Schule

Gezielte Freigabe von Internetseiten

Eine Whitelist enthält also als Einträge ausschließlich gebilligte Seiten, die als unbedenklich kategorisiert werden. Mit diesem Verfahren kann eine sehr hohe Sicherheit erreicht werden. Wird mit Hilfe einer Whitelist gefiltert, ist der Zugriff auf die in der Liste enthaltenen Einträge beschränkt. Aufgrund dieser starken Restriktion der Internetnutzung ist diese Filterlösung insbesondere für die Bereitstellung von genau definierten Zugangsmöglichkeiten geeignet, den so genannten Walled Gardens. Diese Filtermethode ist im Umfeld von Grundschulen häufiger anzutreffen als in anderen Schularten.

Allerdings ist das Verfahren unter Pädagogen umstritten, da durch die erhebliche Einschränkung des Internetzugriffs die Vermittlung von Medienkompetenz deutlich erschwert wird.

Es gibt Filterprogramme, die ausschließlich auf Positivlisten basieren. Meist sind jedoch Positivlisten als ein optionaler Bestandteil in Filterlösungen integriert. Die Listen enthalten in der Regel bereits einige Beispieleinträge. Sie sind meistens offen und unverschlüsselt, können um weitere Einträge ergänzt und so an die eigenen Bedürfnisse angepasst werden.

Angebotswechsel über Nacht

Der Zeitaufwand zur Pflege einer Whitelist hängt von ihrem Umfang ab. Die in Positivlisten verzeichneten Webseiten müssen regelmäßig auf ihre Unbedenklichkeit überprüft werden. Dies ist erforderlich, da sich so genannte Domaingrabber[35] zunehmend auch auf freigegebene Domainnamen spezialisiert haben. So ist es nicht ausgeschlossen, dass das Angebot unter ein und derselben Adresse von heute auf morgen wechselt. Wo heute noch ein Bildungsportal unbedenkliche Inhalte präsentiert, kann schon morgen unter derselben Adresse ein LiveCam-Portal seine jugendgefährdenden Inhalte im Netz anbieten.

Verantwortung bei Erstellung und Pflege

Auch bei der Verwendung von Positivlisten sollte darauf geachtet werden, wer die Auswahl der Einträge getroffen hat und wer die Liste redaktionell aktualisiert. Die Auswahl kann nämlich sehr stark die subjektive Wahrnehmung und Haltung des Erstellers widerspiegeln. Dies gilt in besonderem Maße, wenn Positivlisten mit verifizierten Einträgen als kostenpflichtiger Bestandteil eines Filterprodukts ange-

[35] Domaingrabber sammeln oder kaufen ohne ein Interesse an der Eigennutzung Domains auf beziehungsweise lassen diese auf ihren Namen registrieren.

boten werden. In diesem Fall besteht jedoch auch die Chance, eine sehr umfassende, aktuelle und für den pädagogischen Bedarf optimierte Liste zu erhalten.

Kombination von Positiv- und Negativlisten

Die Mischung macht's

Manche Filterprodukte erlauben den gleichzeitigen Einsatz von Positiv- und Negativlisten. Diese auf den ersten Blick unsinnig erscheinende Kombination erlaubt über unterschiedliche Priorisierungen der Listen eine sehr feine Abstimmung der Zugriffsmöglichkeiten. Die Negativliste beispielsweise sperrt Webseiten aus dem Bereich der Pornografie, die Positivliste gibt jedoch Aufklärungsseiten explizit frei um zu verhindern, dass diese Seiten aufgrund ähnlicher Kriterien oder identischer Wort- oder Bildbestandteile geblockt werden.

3.1.4 Mustererkennung von Grafiken

Das Internet besteht nicht nur aus reinen Textbeiträgen, sondern mit zunehmender Geschwindigkeit der Internetzugänge zu einem immer größeren Anteil aus Grafik- und Bildelementen sowie aus dynamischen Inhalten, zum Beispiel Flash.[36] Die Inhalte solcher Elemente können von textbasierten Filterlisten weder erkannt noch ausgewertet werden. Zur Bewertung der Grafikanteile einer Webseite sind also andere Mechanismen erforderlich.

Pornografische Bilder erkennen und sperren

Einige Filterprogramme scannen daher die Grafiken der aufgerufenen Internetseiten während des Hochladens nach bestimmten Mustern und Darstellungen. Farben, Formen und Kombinationen in einem bestimmten Bereich können dabei zu einer Bewertung der möglichen Inhalte herangezogen werden. Finden sich zum Beispiel sehr viele „Hautfarben", geht der Filter davon aus, dass es sich um eine Seite mit Nacktheit oder sexuellem Inhalt handeln könnte. Dieser Bewertung fallen allerdings auch wissenschaftliche Seiten, beispielsweise aus dem Bereich der Biologie oder Kunst, zum Opfer, da das Programm nicht in der Lage ist, den Kontext zu erkennen, in den die Bilder eingebettet sind. Eine kontextsensitive Kombination aus Bild- und Textfilter kann die Filterqualität womöglich erhöhen.

Grundsätzlich ist die Erkennung und Auswertung von Grafiken und Bildern sehr komplex. Filterverfahren, die mit einer Mustererkennung arbeiten, gelten auf-

36 Flash bezeichnet eine Technik zur Anzeige „bewegter Grafiken".

grund ihrer hohen Hardwarevoraussetzungen und Entwicklungskosten als verhältnismäßig teuer. Einige aktuelle Filterprodukte kombinieren dennoch die vorgenannten Verfahren zur Optimierung der Filterleistung.

3.1.5 Heuristische Verfahren

Es ist leicht vorstellbar, dass sich die Dimensionen und die Komplexität des Internets in Listen nur schwer erfassen lassen. Aus diesem Grunde entwickeln zum Beispiel die Betreiber von Suchmaschinen die Erkennungsverfahren laufend weiter und optimieren die komplexen Strukturen ihrer Suchalgorithmen.[37]

Intelligente Erkennungsverfahren?

Strategien, die das Suchverfahren beschleunigen können, bezeichnet man als Heuristiken. Sie sind prinzipiell auch für die Entwickler von Filtersoftware sehr interessant. Diese beschäftigen sich daher zunehmend mit so genannten heuristischen Verfahren zur Optimierung der Filterergebnisse. Die Werbung spricht in diesem Zusammenhang auch von „künstlicher Intelligenz".

Heuristische Verfahren versuchen zumeist mit einer Mischung aus Keyword- und Listenauswertung sowie Grafik- und Bilderkennung eine möglichst optimale Filterwirkung zu erreichen. Derzeit setzen Produkte vermehrt auf diese vergleichsweise neue Technik. In diesem Zusammenhang findet oft der Begriff „Echtzeitanalyse" in unterschiedlicher Bedeutung Verwendung. Während manche Hersteller schon bei der gleichzeitigen Suche in verschiedenen Filterkategorien diesen Begriff bemühen, verstehen andere Anbieter unter der Echtzeitanalyse eine externe Anfrage bei einem zentralen Firmenserver. Eine einheitliche Verwendung dieses Begriffs hat sich im Umfeld der Filtersoftware bisher noch nicht etabliert.

3.1.6 Self Rating / Site Labelling

Die bisher beschriebenen Filterverfahren basieren alle auf dem Grundgedanken, die Internetinhalte als gegeben zu akzeptieren und auf Seiten der Internetnutzer für eine Auswahl und Filterung zu sorgen. Einen anderen Ansatz wählt das so genannte Self Rating / Site Labelling.

[37] In der Informatik bezeichnet man als Suchalgorithmus eine Funktion, der eine Frage als Eingabe übergeben wird und die eine Lösung zu der Frage zurückgibt.

Rating-Verfahren basieren auf seriöser Selbsteinschätzung

Das Rating-Verfahren basiert ganz wesentlich auf dem Engagement und der Ehrlichkeit sowie der korrekten Selbsteinschätzung der Anbieter von Webinhalten. Innerhalb dieses Verfahrens können Anbieter von Internetseiten die eigenen Webangebote in einem ersten Schritt selbstständig bewerten (Self Rating). Dies geschieht mit Hilfe eines nach Themen geordneten Fragenkatalogs, anhand dessen der Anbieter seine eigene Webseite hinsichtlich jugendschutzrelevanter Inhalte bewertet und kategorisiert. Diese Bewertung wird von einer unabhängigen Stelle zertifiziert und durch ein Label bestätigt. Ein solches Label besteht in der Regel aus wenigen Zeilen html-Programmcode, der von dem Webseitenbetreiber in die bewertete Webseite eingebunden wird (Site Labelling). Zudem ist eine kleine Steuerdatei (labels.rdf) auf dem Webserver abzulegen.

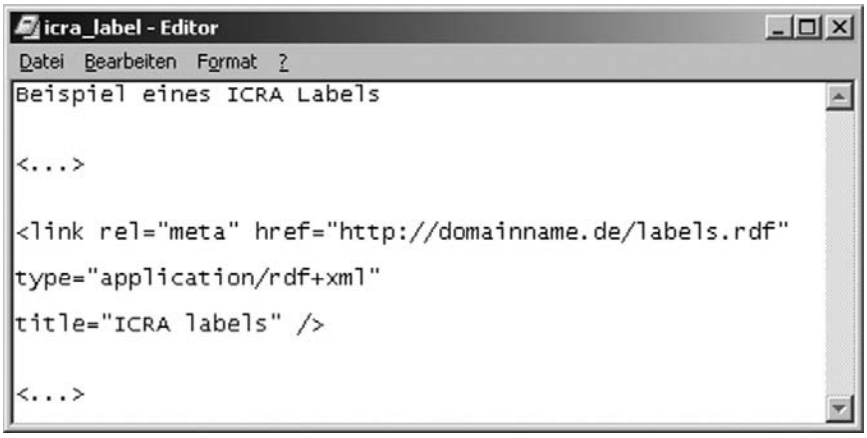


Abbildung 5: Beispiel eines Labels

Rating-Verfahren erfordern eine Software

Wer als Internetnutzer den Zugriff auf das Internet über das Rating-Verfahren filtern möchte, muss eine Software installieren. Diese ist in der Lage, aufgerufene Webseiten nach Labeln zu durchsuchen, Label auszulesen und darüber den Webzugriff zu kontrollieren und zu steuern. Je nach Auswertung des Labels blockt die Filtersoftware die angewählte Seite ab oder stellt sie dar.

Bisher nur wenige Seiten gelabelt

Gegenwärtig ist nur eine geringe Anzahl von Webinhalten mit einem Label versehen. Daher führt eine Verwendung des Systems derzeit noch zu einem

Ausschluss des größten Teils des Internets. Allerdings lassen sich die auf reinem Self Rating und Site Labelling basierenden Ansätze auch mit listenbasierten Produkten kombinieren.

Umgangssprache wird nicht immer akzeptiert

Für das System kann - je nach Kategorisierung von Themen - die Verwendung von Umgangssprache problematisch werden. Gerade in der Drogen- oder AIDS-Aufklärung wird häufig Umgangssprache verwendet, um die Zielgruppen auch in „ihrer Sprache" zu erreichen. Da aber Umgangssprache nach den Ratingkriterien meist als kontroverse Sprache gekennzeichnet werden muss, können solche aufklärenden Seiten unter Umständen nicht erreicht werden.

3.1.7 Kriterien zur Entscheidungsfindung

Die vorgenannten Verfahren versuchen auf unterschiedliche Weise, das Surfen im Internet zu erfassen und so sicher wie möglich zu machen. Das Internet bietet aber neben dem Aufruf von Webseiten im Browser viele weitere Dienste an. Über Datenleitungen werden Mails verschickt, Dateien per Upload oder Download[38] transferiert, Treffen in Chaträumen organisiert, Klingeltöne für Handys getauscht oder Online-Games auf virtuellen Spielplätzen ausgetragen. Die mobile Welt tauscht sich zudem durch SMS und MMS nicht nur über Handys aus. Kurzum, die weiteren Dienste des weltumspannenden Internets sind ebenso zu betrachten und in die Überlegungen zur Sicherstellung des Jugendmedienschutzes einzubeziehen. Sofern das gewählte Filterprogramm diesen Anforderungen nicht gerecht werden kann, müssen zusätzliche Maßnahmen ergriffen werden, die die erforderliche Sicherheit garantieren können, wie zum Beispiel der Einsatz einer Firewall.

Dialog mit Herstellern wünschenswert

Aus pädagogischer Sicht ist ein Austausch zwischen der Schullandschaft und den Anbietern von Filterprogrammen und -listen wünschenswert, gerade hinsichtlich der Prinzipien, die den Kategorien und Sperrmaßnahmen zugrunde liegen. Im Vordergrund sollte die Frage stehen, welche Inhalte im Wirkungsbereich Schule auf welche Weise gefiltert werden (müssen). Da die meisten Filtersysteme nicht spezifisch auf die Zielgruppe Schule ausgerichtet sind, ist es unter pädagogischen Aspekten wichtig, die vorgegebenen Listen editieren oder zumindest

[38] Upload bezeichnet das Senden von Daten von einem Rechner zur Gegenstelle (z. B. Netzrechner, Mailbox, Internet-Server). Der Upload ist somit das Gegenteil vom Download, dem Herunterladen. Up- und Downloads erfolgen über Netzwerkprotokolle, wie zum Beispiel FTP (File Transfer Protocol).

bei Bedarf ergänzen zu können. Die Programme sollten daher die Option bieten, entsprechende Anpassungen mit überschaubarem technischen Aufwand vornehmen zu können.

Sperrt das Programm eine Seite ohne Kommentar, kann bei Anwendern schnell ein Gefühl der Willkür und des Ausgeliefertseins entstehen. Solch eine Situation stünde der pädagogischen Verantwortung der Schule jedoch entgegen. Je klarer ein Programm also seine Filterentscheidung begründet, desto effektiver kann die Sperrliste modifiziert werden.

Die gesellschaftspolitische Diskussion rund um das Thema Jugendmedienschutz hat offensichtlich die Wirtschaft zu aktivem Handeln stimuliert. Einige Anbieter haben den Schulbereich auch als Absatzmarkt erkannt und beteiligen sich auf unterschiedlichen politischen und praktischen Ebenen bereits an den schulspezifischen Diskussionen.

3.2 Technische Grundlagen

Bevor Schulträger oder Schulen das für sie geeignete Filterprodukt auswählen, sollten einige prinzipielle Aspekte in die Überlegungen einbezogen werden. Dies betrifft sowohl die bestehenden oder festzulegenden Rahmenbedingungen im jeweiligen Umfeld als auch die personellen und technischen Voraussetzungen in der vorgesehenen Einsatzumgebung. Eine wesentliche Frage ist beispielsweise, ob die Filtersoftware auf den Einzelrechnern der Schule oder einem zentralen Server installiert werden soll. Die Absicherung kann beispielsweise auch über eine im Netzwerk integrierte Filter-Box[39] oder extern durch die Einbindung eines zentralen Dienstleisters erfolgen.

3.2.1 Lokal installierte Filter (Einzelplatzlösung)

Im Heimbereich werden Filterprogramme häufig auf dem jeweils zu schützenden Computer direkt installiert. Jede Information, die aus dem Internet heruntergeladen wird, muss zunächst diesen internen Filter durchlaufen. Dieser analysiert den angeforderten Inhalt, und je nach Ergebnis der Analyse werden die Inhalte dann entweder abgeblockt oder zur Ansicht im Browser weitergegeben. Auf dem Computer sind also alle Bestandteile des Filterprogramms, wie Filtersoftware, Filterlisten oder Kennwörter, lokal gespeichert.

Keine zentrale Steuerung möglich

Sollen auf diese Art und Weise in Schulen mehrere Computer geschützt werden, muss das Programm auf jedem einzelnen Rechner der Schule gesondert installiert werden. Ebenso sind weitere Ergänzungen, wie Änderungen oder Erweiterung der Filterlisten, auf jedem einzelnen Computer vorzunehmen. Das gilt auch für die Anpassung von Kennwörtern, für die Verwaltung von Nutzergruppen oder für sonstige Administrationstätigkeiten wie das Update der Filterliste. Eine zentrale Administration ist in einer solchen Geräteumgebung nicht angedacht. Die klassenweise Freigabe oder Sperrung von bestimmten Webseiten kann somit nicht zentral mit einem Mausklick aktiviert werden.

[39] Eine Filter-Box ist ein geschlossenes, aus feststehenden Hard- und Softwarekomponenten bestehendes System zur Regelung des Internetzugangs.

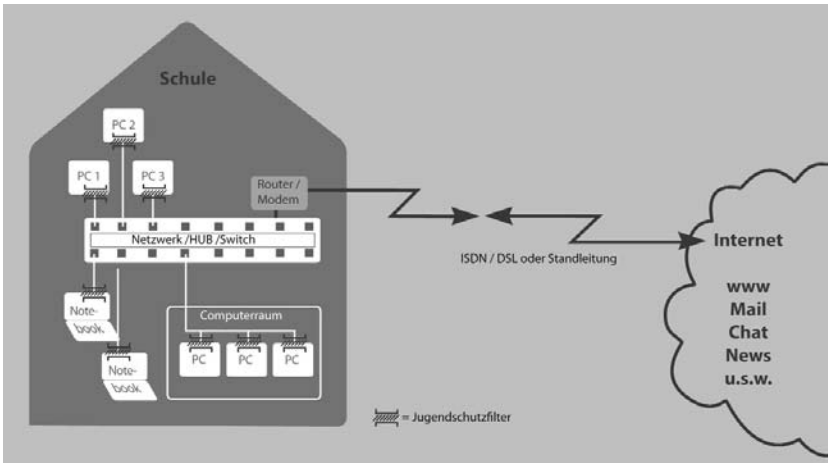


Abbildung 6: Einzelplatzlösung
Auf jedem Computer / Notebook ist jeweils ein Filterprogramm installiert.

3.2.2 Serverbasierte Filter (Netzwerklösung)

In Schulen sind üblicherweise mehrere Rechner zu einem Netzwerk verbunden. Auf jedem Rechner im Netzwerk ein eigenes Filterprogramm zu installieren ist - insbesondere bei größeren Netzwerken - sehr aufwändig, da das Programm immer separat installiert, konfiguriert und laufend aktualisiert werden muss. In Netzwerken wird das Filterprogramm daher oft auf einem zentralen Computer oder Server installiert oder aber durch eine gesonderte Filter-Box realisiert. Die einzelnen Computer greifen über den zentralen Filter im Netzwerk auf das Internet zu und nutzen so die Filterfunktion.

Meist kann eine zentrale Einheit - ganz gleich ob Server oder Filter-Box - auch noch weitere Funktionen für das Netzwerk zur Verfügung stellen. Fungiert ein solcher Rechner beispielsweise als Proxy-Server[40], werden die angeforderten und freigegebenen Seiten in einer Art Zwischenspeicher vorgehalten. Greifen mehrere Computer aus dem Netzwerk auf dieselbe Seite im Internet zu, was im Unterricht häufig der Fall sein dürfte, so wird die Seite nur einmal aus dem Internet geladen und vom Proxy für alle Computer im internen Netzwerk zur Verfügung gestellt.

40 Ein Proxy-Server (oder kurz: Proxy) ist ein Computer, der als Zwischenspeicher für aufgerufene Webseiten dient. Internetnutzer können schneller auf die dort zwischengespeicherten Seiten zugreifen, als wenn diese erneut über das Internet geladen werden müssten.

Dies bedeutet besonders bei langsamen Internetanbindungen einen meist deutlichen Geschwindigkeitsvorteil.

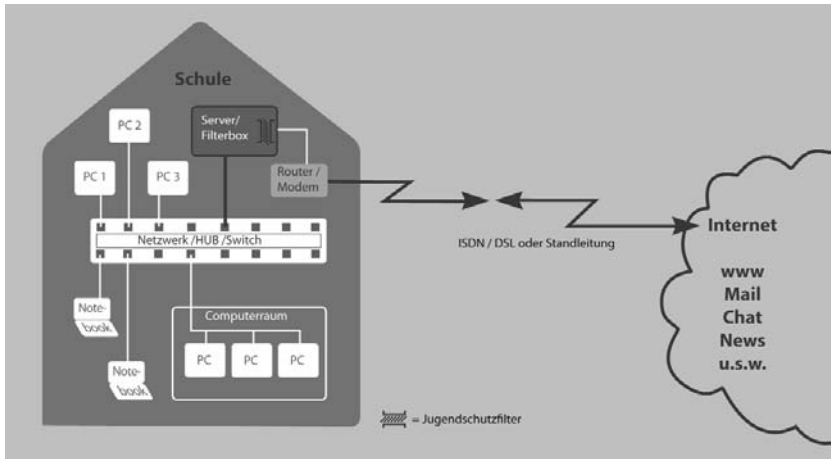


Abbildung 7: Netzwerklösung
Ein zentral installierter Filter sichert alle angebundenen Computer / Notebooks des Netzwerks.

3.2.3 Einzelplatz- oder Netzwerklösung?

Maßgeblich für die Entscheidung zwischen Einzelplatz- oder zentraler Lösung ist insbesondere die Anzahl der an der Schule zu schützenden Computer. Dabei sollte nicht nur der Ist-Zustand entscheidend sein, sondern immer auch die voraussichtliche zukünftige Nutzung neuer Medien im Unterricht berücksichtigt werden. Verfügt eine Schule nur über einige Einzelcomputer in Klassenräumen oder wenige Computer in einer Medienecke, so lohnt unter Umständen der Aufwand zur Realisierung einer zentralen Lösung nicht.

Neben der Kostenfrage für einen zentralen Server sollte bei den Planungen einer zentralen Lösung berücksichtigt werden, ob die infrastrukturellen Voraussetzungen vorhanden sind oder ob für die erforderlichen Vernetzungsarbeiten weitere Kosten einzuplanen sind. Auch ist von Belang, ob das erforderliche Fachwissen, beispielsweise zur Einrichtung eines Proxy-Servers, zur Installation und nachhaltigen Betreuung einer zentralen Lösung sichergestellt werden kann.

Netzwerke können sparen helfen

In Schulen, die über eine größere Anzahl von Rechnern verfügen, ist eher eine zentrale Lösung üblich. Dies ergibt sich meist schon daraus, dass die Computer ohnehin bereits über eine Zentrale im Netzwerk, zum Beispiel über einen Router[41], an das Internet angebunden sind. Auch wenn die Einrichtung einer zentralen Filterlösung im ersten Schritt mit erhöhtem Aufwand verbunden scheint (zum Beispiel durch die Anschaffung von Hardware), dürften sich in größeren Netzwerken im laufenden Betrieb deutliche Einsparpotenziale ergeben. Durch die zentrale und damit einmalige Administration von Kennwörtern, Listeneinstellungen, Zugriffsprotokollen und Filterupdates werden insbesondere wiederkehrende, zeitintensive Wartungsarbeiten erheblich reduziert.

Einige Filterprogramme bringen eigene Nutzerverwaltungen mit, die es gesondert zu pflegen gilt. Andere greifen auf bestehende Nutzerverwaltungen im Netzwerk, wie Active Directory oder LDAP[42], zurück. Dies erlaubt eine sehr differenzierte Steuerung der Zugriffsrechte. So können den Lehrkräften beispielsweise andere Rechte eingeräumt werden als den Schülern. Aber auch die Nutzung zentraler Sicherheitseinstellungen, wie beispielsweise die unveränderbare Vorgabe der Internetverbindung, können hierdurch festgelegt werden. Solche Funktionalitäten bietet ebenfalls nur eine zentrale Lösung.

Das vorstehende Schaubild zeigt eine einfache Darstellung einer zentralen Lösung. Bei der Umsetzung sollte dem Sicherheitsaspekt eine angemessene Bedeutung eingeräumt werden. Es ist insbesondere dann auf die richtige Einbindung in das Netzwerk zu achten, wenn ein Filter-Server nachträglich in das Netzwerk aufgenommen wird.

41 Ein Router ist ein Vermittlungsgerät, welches in einem Netzwerk dafür sorgt, dass bei ihm eintreffende Daten zum vorgesehenen Ziel weitergeleitet werden.

42 Der LDAP-Verzeichnisdienst von Microsoft Windows 2000/2003 Server heißt Active Directory Service (ADS). Bei einem Verzeichnis (engl. Directory) handelt es sich um eine Zuordnungsliste, wie zum Beispiel bei einem Telefonbuch. Es ordnet Telefonnummern den jeweiligen Anschlüssen (Besitzern) zu. Das Active Directory ordnet verschiedenen Netzwerkobjekten, wie Benutzern oder Computern, Eigenschaften zu und verwaltet diese. LDAP ist die Abkürzung für das Lightweight Directory Access Protocol. Dieses Protokoll unterstützt einen Verzeichnisdienst (Directory) zur zentralen Nutzerverwaltung. Mehr dazu im Internet unter http://www.mitlinx.de/ldap

Das nachfolgende Schaubild verdeutlicht, dass Computer (hier: PC 4) bei falscher Konfiguration vorbei an dem Filterschutz alle Seiten im Internet erreichen könnten.

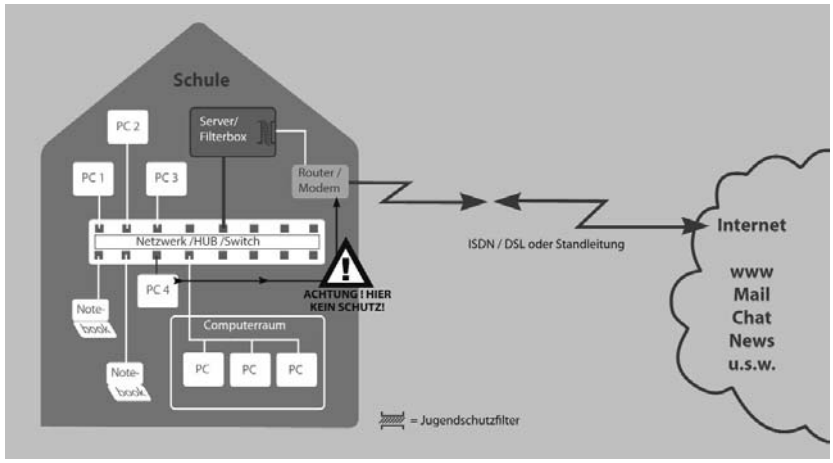


Abbildung 8: Sicherheitshinweis zur Netzwerklösung
In diesem Beispiel könnte PC 4 das Internet ungeschützt ohne Filterfunktion nutzen.

3.2.4 Externe Zentrallösung

Die bisher beschriebenen Szenarien basieren jeweils auf schulinternen Installationen. Sofern Schulträger für alle in ihren Zuständigkeitsbereich fallende Schulen einen übergreifenden Ansatz umsetzen möchten, kann auch eine externe Zentrallösung in Betracht gezogen werden.

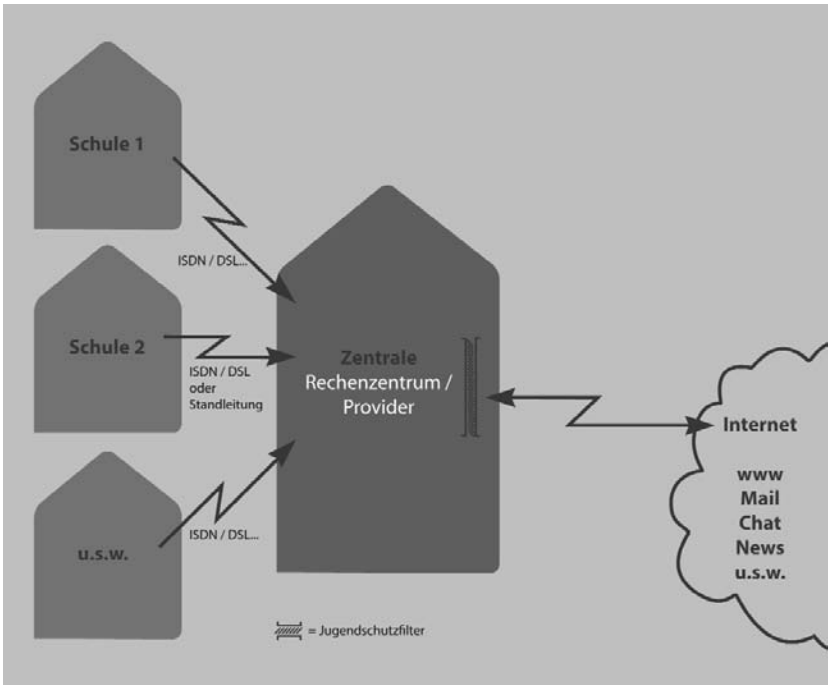


Abbildung 9: Externe Zentrallösung
Mehrere Schulen sind über externe Filterdienste geschützt an das Internet angebunden.

Wie Abbildung 9 zeigt, steht der Zugangsfilter innerhalb einer solchen Lösung extern zur Verfügung. Betreiber kann zum Beispiel ein kommunales Rechenzentrum[43] oder auch ein Internet-Provider[44] sein. In der Schule ist bei diesem Ansatz lediglich der sichere Netzzugang zum zentralen Filter zu gewährleisten. Erst hinter diesem Filter ist dann für die Schule das „gefilterte" Internet erreichbar.

[43] Zum Beispiel www.schulon.org
[44] Zum Beispiel www.belwue.net

Entlastung für Lehrkräfte

Der meist als externe Dienstleistung angebotene zentrale Filterschutz kann die Personalressourcen in der Schule von Administrationsaufgaben entlasten. Möglicherweise sind auch für den Schulträger bei zentraler Lizenzierung günstigere Preise für die Filterprodukte zu erzielen.

Ein möglicher Nachteil dieser Lösung könnte in den zentralen, und damit für die einzelne Schule eventuell unflexiblen oder unabänderbaren Vorgaben der Filtereinstellungen gesehen werden. Hier ist eine genaue Abwägung zwischen Kosten und Nutzen sowie organisatorischen Fragen vorzunehmen. Zudem bestimmen die personellen Kapazitäten und die verfügbaren Fachkenntnisse den Entscheidungsspielraum maßgeblich mit.

3.3 Filterlösungen in der Schulpraxis

Installation, Betrieb und Wartung

Die Einführung und der Betrieb einer Lösung, die den Anforderungen an den Jugendmedienschutz in Schulen gerecht wird, werfen bei Schulträgern, Schulleitungen und Lehrkräften erhebliche Fragen auf. Im Idealfall soll die Filterlösung einfach zu installieren sein, im Schulalltag leicht zu bedienen und dabei unauffällig und sicher funktionieren. Auch sollten die Fragen nach der laufenden Wartung keine Probleme aufwerfen und das Produkt dem Etat des Schulträgers entsprechen.

Die nachfolgenden Hinweise sollen einige häufig gestellte Fragen aus dem Schulumfeld beantworten und darüber hinaus Impulse für die Planung geben.

3.3.1 Installation

Planung ist wichtig

Ein neu installiertes Filterprogramm wird den Anforderungen der Schule in den meisten Fällen nicht automatisch gerecht. Das Programm muss den Gegebenheiten vor Ort[45] angepasst und die Filtereinstellungen exakt vorgenommen werden. Dafür sollte in jedem Fall ein ausreichender zeitlicher Aufwand eingeplant werden. Zudem sind die erforderlichen Netzwerkkenntnisse zur Installation eines zentralen Filters nicht zu unterschätzen.

Neben der Einrichtung und Installation der zentralen Komponente sind auch an allen zu schützenden Computern des Schulnetzwerks die Netzwerkeinstellungen anzupassen. Es müssen beispielsweise an jedem Arbeitsplatz die Proxy-Einstellungen für die Internetverbindung konfiguriert werden, eine Position, die bei der Zeitplanung nicht selten vergessen wird.

Unerwünschte Überraschungen vermeiden

Sofern der Zugriff auf das Internet bisher ohne Einschränkungen erlaubt war, kann es nach der Einführung eines Filtersystems - gerade in der ersten Zeit der Nutzung - zu einigen überraschenden Auswirkungen kommen. Ein Internetangebot, das bisher im Unterricht schon oft genutzt wurde, ist plötzlich nicht zu erreichen, weil der Filter beispielsweise durch Überfilterung den Zugriff darauf sperrt. Für den reibungslosen Interneteinsatz im Unterricht ist es wichtig, dass Lehrkräfte auf solche Situationen vorbereitet sind und entsprechend agieren,

[45] Hierunter fallen auch spezifische Fragen der unterschiedlichen Schulformen.

in diesem Fall also die gesperrte Seite freigeben können. Eine fundierte Einweisung in das System ist daher für alle künftigen Nutzer unumgänglich und fördert darüber hinaus die Akzeptanz des Filterprogramms.

3.3.2 Gestaltungsmöglichkeit im Unterricht

Ein bedeutender Aspekt bei der Auswahl der geeigneten Filtersoftware ist ihre Bandbreite an Gestaltungsmöglichkeiten, die sie den Lehrkräften im Unterricht bietet. Können die Rechner im Computerraum beispielsweise gezielt für eine Recherchearbeit zum Unterrichtsthema „Drittes Reich" freigegeben werden? Kann der Lehrer ohne großen Aufwand vom Lehrer-PC aus diejenigen Seiten gezielt freigeben, die er für seinen Unterricht benötigt? Kann er bestimmte Seiten kurzfristig sperren, deren Aufruf er während der Klassenarbeit verhindern möchte?

Diese Beispiele machen deutlich, dass die Mechanismen von Filterprodukten auch zur Steuerung organisatorischer oder pädagogischer Belange eingesetzt werden können, die oftmals weit über die eigentlichen jugendschutzrechtlichen Fragestellungen hinausgehen.

3.3.3 Aktualisierung der Filterlisten

Ganz gleich ob Wortfilter, Negativ- oder Positivliste - die Filterlisten sollten stets auf dem aktuellsten Stand sein. Insbesondere bei der Nutzung von Sperrlisten ist ein aktueller Datenbestand ganz entscheidend für eine optimale Filterwirkung. Die zur Verfügung gestellten Updates der Filterhersteller müssen auf den zu schützenden Arbeitsstationen, beziehungsweise bei zentralen Ansätzen auf dem Server oder der Filter-Box, installiert werden.

Mit einem Update der Filterlisten auf einem zentralen Server ist eine sehr schnelle Aktualisierung der Filterfunktion für alle Rechner im Netzwerk möglich. Da für die Aktualisierung oft die vollen Administrationsrechte benötigt werden, sind diese genau zu definieren, festzulegen und zu dokumentieren.

Einige Filterprodukte sind auch in der Lage, ein solches Update automatisch durchzuführen. Hersteller von Filter-Boxen bieten darüber hinaus oft ein Update

per Fernwartung an. Von Seiten der Schule sind dann keine Eingriffe mehr zur Aktualisierung erforderlich.

Konfigurationsschutz ausschalten

Beim Einsatz von Einzelplatzcomputern sollte eine in Schulen oft anzutreffende Besonderheit berücksichtigt werden. Diese besteht darin, dass viele Schulen die Konfiguration der Desktops standardisieren und die Einstellungen der Arbeitsplätze durch Hard- oder Software schützen. Eine Hardwarekarte oder eine Software verhindern dauerhafte Veränderungen an den Einstellungen des Computers, indem sie diesen nach jedem Neustart wieder in den vordefinierten Zustand zurückversetzen. Diese Sicherheitsmaßnahme zum Schutz der Konfiguration behindert allerdings die Aktualisierung eines Filterprogramms. Damit diese notwendigen Aktualisierungen dennoch vorgenommen werden können, müssen die Schutzmechanismen für den Zeitraum der Neuinstallation oder Aktualisierung der Jugendschutzsoftware deaktiviert werden.

3.3.4 Protokollierung der Zugriffe

Ähnlich einem Einzelverbindungsnachweis zur Telefonrechnung zeichnet das Filterprogramm alle Benutzeraktivitäten in einem Protokoll, der so genannten Logdatei, auf. Je nach Konfiguration der Filtersoftware werden nur bestimmte Aktivitäten wie zum Beispiel der Aufruf gesperrter Seiten protokolliert oder aber alle Zugriffe auf das Internet festgehalten und dokumentiert.


logfile - Editor

Datei Bearbeiten Format Ansicht ?

<Logfile Grundschule Talweg>

Uhrzeit	PC	aufgerufene Seite	Aktion
11:05	PC_123	www.sexy*****.de	geblockt
11:06	PC_221	www.abschreiben.***	geblockt
11:08	PC_123	www.lizzynet.de	zugelassen
11:09	PC_131	www.pornobil*****.com	geblockt
11:12	PC_221	www.alkoholprobleme.de	zugelassen

u.s.w.

Abbildung 10: Beispiel einer einfachen Logdatei

Da es sich bei Logdateien um die Speicherung von personenbezogenen Daten handeln kann, müssen diese Daten sensibel behandelt werden.[46] Je nach eingesetztem Verfahren geben die Logdateien Auskunft darüber, wer zu welcher Zeit auf welche Webseiten zugegriffen hat. Wenn Schüler A beispielsweise Beratungsseiten für Homosexualität oder Drogenprobleme aufruft, dann tauchen diese Adressen auch in den Logdateien auf.

Datenschutz sicherstellen

Um den datenschutzrechtlichen Vorgaben zu genügen empfehlen Praktiker, zwei voneinander unabhängige Protokolldateien aufzuzeichnen:

1. Anmeldelog
Das Anmeldelog gibt Auskunft über die Person, die zu einer bestimmten Uhrzeit einen bestimmten Rechner genutzt hat. Welche Seiten der Nutzer aufgerufen hat, wird hier nicht festgehalten.

2. Internetlog
In einer zweiten, separaten Datei wird der reine Zugriff auf die Internetseiten protokolliert. Ein direkter Bezug zu Personen ist nicht herstellbar.

Sofern der Zugriff auf beide Dateien lediglich verschiedenen Personen möglich ist, kann nur mit Hilfe eines Zwischenschritts, nämlich der Verknüpfung beider Dateien, nachvollzogen werden, welcher Schüler welche Internetseite besucht hat. Einem möglichen Missbrauch personenbezogener Daten durch Einzelpersonen kann durch dieses Verfahren vorgebeugt werden.

Stichproben sind sinnvoll

Abhängig von den bestehenden Nutzungsvereinbarungen[47] mit den Schülerinnen und Schülern sowie den Erziehungsberechtigten, können aus pädagogischen Gründen auch Stichproben sinnvoll sein. Allein die Ankündigung einer möglichen Kontrolle zeigt oft schon Wirkung. Die Einträge der Logdateien können außerdem auch als Nachweis über Verstöße gegen die bestehenden Nutzungsvereinbarungen herangezogen werden.

Die Auswertung der Logdatei erlaubt aber nicht nur die Kontrolle unberechtigter Zugriffe. Sie eignet sich auch zum Abgleich von unberechtigt geblockten Seiten.

[46] Mehr zum Thema Datenschutz siehe auch Kapitel 2.
[47] Zur Nutzungsordnung siehe auch Kapitel 2.

Werden solche Einträge in der Logdatei gefunden, kann zum Beispiel durch Eintragung in eine Whitelist eine gezielte Freigabe erfolgen. Auf die unberechtigterweise geblockte Webseite kann anschließend wieder zugegriffen werden.

Einen Schritt weiter als die reine Protokollfunktion geht die so genannte Benachrichtigungsmöglichkeit. Dabei sendet das Filterprogramm per E-Mail oder SMS eine Meldung an berechtigte Empfänger, sobald ein versuchter Zugriff auf gesperrte Seiten registriert wird. Dieses Verfahren ist geeignet, um zeitnah bestimmte „Ermittlungen" wegen Missbrauch des Internetzugangs durch Schüler oder Verstöße gegen die bestehenden Nutzungsordnungen zu führen. Ein solches Verfahren ist in jedem Fall datenschutzrechtlich abzustimmen.

Aus der Praxis
Während des Unterrichts gibt es eine einfach Möglichkeit, die zuletzt aufgerufenen Seiten zu kontrollieren, denn Internetbrowser führen eine Liste der zuletzt aufgerufenen Seiten oder speichern gar die Seiten in einem internen Zwischenspeicher (Cache). Die Optionen zu diesen Funktionen sind meist unter den Konfigurationseinstellungen <EXTRAS / Einstellungen> der Browser zu finden.

3.3.5 Manipulationsresistenz

Sicherheitslücken erkennen und schließen

Für alle Schulformen gilt: Der Jugendschutzfilter ist ein Teil der Gesamtsicherheit. Die Arbeitsstationen und auch die übrigen Netzwerkkomponenten müssen so sicher konfiguriert sein, dass sie nicht einfach ausgehebelt oder umgangen werden können. Dies gilt insbesondere für Schulbereiche wie Bibliothek oder Internetcafé, in denen Schüler ohne permanente Aufsicht Zugang zum Internet erhalten.

Kinder und Jugendliche mit guten Computer- und Netzwerkkenntnissen können ansonsten die Schutzmechanismen unterlaufen und am Jugendschutzfilter vorbei im Internet surfen.

Eine mögliche Sicherheitslücke ist ein fehlender BIOS-Schutz[48], so dass die Kinder von einer bootfähigen CD-ROM oder einem USB-Stick ein eigenes, ungeschütztes Betriebssystem starten können. Eine weitere Sicherheitslücke kann das Vorhandensein eines zweiten Netzzugangs sein. Das bedeutet, dass neben dem geschützten Internetzugang über die Filtersoftware eine zweite, ungeschützte Verbindung ins Internet - zum Beispiel über einen Router oder eine ISDN-Karte in einem der Computer - existiert.

Nicht zuletzt ist die Weitergabe von Kennwörtern unter den Schülerinnen und Schülern ein eklatantes Sicherheitsrisiko. Macht das Kennwort zur Entsperrung des Filters auf dem Schulhof erst einmal die Runde, ist jede Filtersoftware machtlos.

Aus der Praxis

Wird eine Seite von dem Filter geblockt, melden dies manche Filterprogramme mit einem markanten Verbot- oder STOPP-Zeichen. Verbote reizen jedoch dazu, übertreten zu werden. Pädagogisch sinnvoller scheint die Weiterleitung an eine neutrale Seite oder aber der Hinweis, sich an den Vertrauenslehrer zu wenden. Dies erfolgt in den meisten Fällen natürlich nicht, wenn der Hinweis das Ergebnis eines verbotenen Versuchs war.

3.3.6 Schutz beim Surfen - auch zu Hause?

Lernen ohne Medienbruch

Die Internetwelt wird zunehmend mobiler. Auch im Schulumfeld gibt es Projekte, die eine Nutzung der neuen Medien zu jeder Zeit an jedem Ort propagieren. Sofern das pädagogische Konzept den Zugriff auf das Internet nicht nur auf dem Schulgelände vorsieht, stellen sich weitere Fragen. Wie können die Schülerinnen und Schüler von zu Hause aus sicher auf das Internet oder den Server in der Schule zugreifen? Die gleiche Frage stellt sich auch für die immer häufiger anzutreffenden Notebookprojekte, die eine Nutzung des Rechners auch außerhalb der Schule erlauben.

Damit diese Fragen in der Praxis nicht unbeantwortet bleiben, sollten stets alle Nutzungsoptionen von Computer und Internet auch außerhalb der Schule in die Planungen und Überlegungen einbezogen werden.

[48] Als BIOS (Basic Input/Output System) bezeichnet man die Funktion, die ein Computer direkt nach dem Einschalten ausführt, um angeschlossene Geräte wie Festplatte, DVD-Laufwerk oder USB-Stick zu suchen.

4. Filtersysteme - ein Überblick

Bei der Auswahl eines Filtersystems für Schulen sind vielfältige wichtige Aspekte zu berücksichtigen, die in den vorhergehenden Kapiteln näher erläutert wurden. Der nachfolgende Überblick liefert Informationen zu Filtersystemen, die stellvertretend für verschiedene Filtertechniken stehen und unterschiedliche Einsatzzwecke verfolgen. Damit kann die in den Schulen anzutreffende Vielfalt an möglichen Anforderungen bestmöglich abgebildet werden.

Die Angaben[49] beruhen auf Informationen der Produkthersteller und -anbieter (Broschüren, Internetpräsentationen, direkte Kontakte). Trotz größter Sorgfalt bei der Zusammenstellung der Daten können Fehler prinzipiell nicht ausgeschlossen werden. Für die Richtigkeit der Angaben kann daher ausdrücklich keine Haftung übernommen werden.

Die Zusammenstellung soll einer ersten Übersicht dienen, kann jedoch - vor dem Hintergrund komplexer Detailfragen - keinesfalls eine eingehende Marktrecherche oder Beratung durch autorisierte Dienstleister oder Vertriebspartner der Anbieter ersetzen. Eine wertende Aussage zur Qualität der einzelnen Produkte ist nicht möglich, da sich für jeden Einsatzzweck unterschiedliche Anforderungen an ein Filterprodukt ergeben.

Erläuterungen zu den Produktinformationen, die in einer Übersicht den Einzelbeschreibungen vorangestellt sind:

Produktinformation	
Produkt	Name des Produkts
Hersteller/Anbieter	Hersteller / Vertriebspartner inklusive Anschrift
Internet	Internetadresse zur Produktbeschreibung
Vertriebsform	Software/Hardware - Freeware, Shareware, kommerzielle Soft- oder Hardware
Demoversion	Sind Testversionen erhältlich?
Bedieneroberfläche	Sprache der Bedieneroberfläche (nicht der Filtertechnik!)
Einzelplatz / Netzwerk	Produkt für Einzel-PC und / oder Netzwerkeinsatz verfügbar?

[49] Stand aller Informationen und Angaben zu den hier beschriebene Filterprodukten: November 2005.

Black- / Whitelist	Kommen Black- und / oder Whitelist zum Einsatz?
Wortfilter ergänzbar	Bearbeitungsmöglichkeiten des Wortfilters
Self Rating / Site Labelling	Basiert das Produkt auf der Technik Self Rating / Site Labelling?
Bildanalyse	Wird von dem Produkt eine Auswertung von Bildmaterial vorgenommen?
Protokollfunktion	Werden aufgerufene / gesperrte Webseiten in einem Protokoll zur Kontrolle erfasst? (Achtung: Datenschutz!)
Update der Filterlisten	Erfolgt ein Update der Filterlisten manuell und / oder automatisch?
Betriebssystem	Welche Betriebssystemplattformen werden unterstützt?
Sonstiges	Weitere Detailinformationen, soweit verfügbar

Hinweis zu den Kosten:
In der nachfolgenden Übersicht stehen Freeware-, Shareware- und Open-Source-Programme neben kommerziellen Software-Produkten und kostenpflichtigen Hardwareangeboten. Die Ermittlung der Gesamtkosten ist von zahlreichen, sehr individuellen Faktoren abhängig. Zu diesen Faktoren zählen:

- Welche Anforderungen werden an die Filterlösung gestellt?
- Anzahl der zu schützenden Computer / Netzwerke
- Kann ein Softwareprodukt auf vorhandener Hardware installiert werden, oder sind Neuanschaffungen erforderlich?
- Ist personeller und technischer Sachverstand vorhanden oder muss dieser als Dienstleistung eingekauft werden?
- Ist ein externer Support oder Fernwartung gewünscht?
- Werden Einzellizenzen erworben, oder kann auf Rahmenverträge zurückgegriffen werden?
- Können Sonder- oder Sponsoringangebote der Filterhersteller genutzt werden?

Zu den zu erwartenden Gesamtkosten können daher im Rahmen dieser Publikation keine allgemein gültigen Angaben gemacht werden.

4.1 DansGuardian

Produktinformation

Produkt	DansGuardian
Hersteller/Anbieter	Open Source (freie Software)
Internet	http://dansguardian.org
Vertriebsform	Software / Open Source optionale Filterlisten wahlweise kostenlos oder kommerziell
Demoversion	ja
Bedieneroberfläche	englisch
Einzelplatz / Netzwerk	nein / ja
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	./.
Bildanalyse	ja
Protokollfunktion	ja
Update der Filterlisten	wahlweise manuell oder automatisch
Betriebssystem	Linux, x-BSD, Mac OS, HP-UX, Solaris
Sonstiges	umfangreiche Konfigurationsmöglichkeiten erfordern umfassende Fachkenntnisse

DansGuardian ist eine Open-Source-Software für Server unter Linux, x-BSD, Mac OS, HP-UX und Solaris, die modular verschiedene Filtermethoden unterstützt und diese zu einer Gesamtlösung kombinieren kann. Die Nutzung der Software ist nach den Copyright-Bestimmungen[50] für Schulen kostenlos. DansGuardian wird häufig von Schulen im englischsprachigen Raum genutzt. Der Filter wird aber ebenso im deutschen Schulumfeld eingesetzt. So existieren zum Einsatz von DansGuardian beispielsweise Beschreibungen zur Musterlösung in Baden-Württemberg[51] sowie auf den Seiten des Schul-Support-Service für Hamburger Schulen (3S)[52]. Weiterhin beschäftigen sich Entwickler im Umfeld der verschiedenen Schul-Server unter Linux mit der Einbindung von DansGuardian in die jeweiligen Serverdistributionen.

50 http://dansguardian.org/?page=copyright2
51 http://www.support-netz.de/faq-lml-dansguardian.html
52 http://3s.hh.schule.de/wissen/filtersoftware.html

Basis des Produktes sind Filterlisten (Produktbeschreibung: „true web content filter"), die sich - technisches Verständnis vorausgesetzt - mit Proxy-Servern wie beispielsweise dem kostenlosen Squid oder dem kostenpflichtigen Smooth-Guardian kombinieren lassen. Dabei kommen Blacklists unterschiedlicher Herkunft zum Einsatz.[53] Es besteht die Möglichkeit, zwischen kostenlosen und kostenpflichtigen Listen zu wählen. Nutzer der freien Listen erhalten dabei Hilfe zur Nutzung von Mailinglisten und Supportforen unter http://dansguardian.org.

Die kostenpflichtigen Listen[54] werden neben einer automatischen Aktualisierung zusätzlich manuell gepflegt und überprüft. Zudem wird für Nutzer der kostenpflichtigen Listen ein professioneller Support angeboten. Der Preis für die Nutzung der kostenpflichtigen Filterlisten wird - je nach Anbieter - nicht pro Arbeitsplatz, sondern pro Schule festgelegt. Dabei sind für Schulen Sonderkonditionen möglich. Die Höhe der Kosten hängt dabei unter anderem vom gewünschten Zugriff auf die Updates der Blacklist ab. Für Schulen würde dies bei einem normalen Nutzervertrag beispielsweise bedeuten, dass ihnen einmal monatlich eine aktualisierte Liste als Download zur Verfügung steht. Wird eine häufigere Aktualisierung der Blacklists gewünscht, so kann diese Option gegen einen Aufpreis erworben werden.

Aktuelle Informationen zu DansGuardian sowie Angaben zu den verfügbaren Filterlisten finden Sie im Internet unter:
http://dansguardian.org

[53] http://dansguardian.org/?page=blacklist
[54] http://urlblacklist.com

4.2 FamilyFilter

Produktinformation

Produkt	FamilyFilter
Hersteller/Anbieter	coolspot AG Am Albertussee 1 D-40549 Düsseldorf
Internet	http://www.familyfilter.de
Vertriebsform	Software, kommerziell
Demoversion	ja, 30 Tage
Bedieneroberfläche	mehrsprachig
Einzelplatz / Netzwerk	ja / k.A.
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	ja, Anmeldung über www.familyfilter.de
Bildanalyse	ja
Protokollfunktion	ja
Update der Filterlisten	wahlweise manuell oder automatisch
Betriebssystem	ab Windows 95
Sonstiges	altersspezifische Einstellungen und Programme sperren möglich, Zeitsteuerung einstellbar

Die coolspot AG ist nach eigenen Angaben eines der ersten Unternehmen, das offiziell den Antrag auf Aufnahme in die Modellphase[55] zur Erprobung der Filtersysteme durch die KJM gestellt hat. Das Produktangebot der Firma coolspot ist auf die Bereiche Jugendschutz, Alters- und Personenverifikation ausgerichtet.

Der FamilyFilter ermöglicht es, auf einzelnen Computern Themenbereiche nach Kategorien unterteilt auszuwählen und gezielt freizugeben oder zu sperren. Auch kann der Zugriff auf Tauschbörsen und Chatsysteme sowie auf lokale Programme - zum Beispiel PC-Spiele und Online-Banking - geregelt werden. Dabei können individuelle Vorgaben eingestellt werden, nach denen die inhaltliche und zeitliche Nutzung geregelt wird.

[55] Verfahren zur Anerkennung durch die KJM siehe Kapitel 1.2., Seite 18-19.

Die Software bietet zudem die Möglichkeit, altersspezifische Nutzereinstellungen vorzunehmen. Neben der generellen Sperrung von Internetseiten nach Kategorien wie beispielsweise Pornografie, illegale oder gewalttätige Inhalte sowie der Sperrung von Programmen und Dateien, ermöglichen vordefinierte Sperrfilter den altersgerechten Schutz der Nutzer. Es können auch eigene Filterregeln konfiguriert und geschlossene Benutzergruppen angelegt werden.

Die Filterlisten werden nach Herstellerangaben in eigenen Datenbanken geführt und mit den Daten und Kategorisierungen anderer Quellen abgeglichen sowie daraus aktualisiert und ergänzt. Die Aktualisierung der Software beim Nutzer erfolgt automatisch, kann aber auch von berechtigten Benutzern manuell geprüft und initiiert werden. Welche Seiten konkret von der Software gesperrt wurden, lässt sich aus einer Logdatei im Administrationsbereich ablesen. Beim Einsatz in Schulen sind dabei die bereits angesprochenen datenschutzrechtlichen Einschränkungen zu beachten.

Unter www.familyfilter.de haben Administratoren und Webmaster von Internetangeboten die Möglichkeit, freiwillig die eigenen Internetangebote mit einem FamilyFilter-Label zu versehen.

Weitere Informationen zum FamilyFilter finden Sie unter:
www.familyfilter.de oder www.coolspot.de

4.3 ICRAplus

Produktinformation

Produkt	ICRAplus
Hersteller/Anbieter	ICRA Deutschland eco Electronic Commerce Forum Verband der deutschen Internetwirtschaft e.V. Arenzhofstraße 10 D-50769 Köln
Internet	http://www.icra.org/_de
Vertriebsform	Software / ICRAplus Freeware
Demoversion	./.
Bedieneroberfläche	mehrsprachig
Einzelplatz / Netzwerk	ja / nein
Black- / Whitelist	optional
Wortfilter ergänzbar	optional
Self Rating / Site Labelling	ja
Bildanalyse	optional
Protokollfunktion	optional
Update der Filterlisten	wahlweise manuell oder automatisch
Betriebssystem	ab Windows 98
Sonstiges	optionale Programmerweiterungen: kostenlos: www.jugendschutzprogramm.de oder kostenpflichtig: Optenet[56], FilterX[57]

Die Abkürzung ICRA steht für „Internet Content Rating Association". Dabei handelt es sich um eine gemeinnützige Organisation, die 1999 von der Bertelsmann-Stiftung und einigen führenden Internet-Firmen gegründet wurde. Hauptziel ist es, ein System der freiwilligen Selbstklassifizierung international zu etablieren und so die für Kinder und Jugendliche bedenklichen Webinhalte zu blockieren. Das Projekt wird von der Europäischen Union unterstützt. Der ICRA-Filter war zudem Teil eines Pilotprojekts bei der KJM zur Umsetzung des deutschen Jugendmedienschutzrechts.

[56] www.optenet.com
[57] www.iit.demokritos.gr

Das Funktionsprinzip scheint einfach: Anbieter und Betreiber von Webseiten kennen die eigenen angebotenen Inhalte sehr genau. Sie können nach objektiven Kriterien über ein Webformular das eigene Internetangebot klassifizieren und diese Informationen zur Steuerung der Filterprogramme bei ICRA hinterlegen. Ist dies erfolgt, so stellt ICRA ein Label zur Einbindung in den entsprechenden Webseiten aus. Die Aktualisierung der Filterfunktion erfolgt also dadurch, dass die Anbieter ihre eigenen Webseiten klassifizieren beziehungsweise die Klassifizierung geänderter Seiten anpassen. Ein möglicher Nachteil des Verfahrens ist allerdings darin zu sehen, dass das System von der aktiven Beteiligung der Seitenbetreiber abhängt. Bislang haben nur recht wenige Betreiber ihre Webseiten mit dem ICRA-Label ausgezeichnet. Dabei könnte auf diese Weise sichergestellt werden, dass nicht Dritte, deren Qualifikation und Weltanschauung für Webmaster und Nutzer in der Regel unbekannt bleiben dürften, darüber entscheiden, welche Inhalte von einem Filter gesperrt und welche freigegeben werden. Das ICRA-System folgt dem Grundgedanken, das Internet in seiner entscheidenden Stärke zu bewahren, nämlich ein unabhängiges und freies Medium zu sein. Die ICRA-Webseite[58] bietet - ebenso wie einige der nachfolgend beschriebenen Zusatzprogramme - die Möglichkeit, über eine einfache Abfrage zu ermitteln, ob eine URL bereits gelabelt ist oder nicht. Das Ergebnis wird sofort - je nach Ergebnis der Prüfung - in rot, gelb oder grün präsentiert.

Auf Seiten der Computeranwender, die ihren Internetzugang schützen möchten, ist die Installation der kostenlosen ICRA-Software[59] erforderlich. Bei Anwendern, die ihren Computer mit dieser Software schützen, werden die von den Betreibern der Webseite hinterlegten Informationen (Label) in der Folge ausgewertet mit dem Ergebnis, dass nur die Seiten angezeigt werden, die gemäß des eingebundenen Labels unbedenkliche Filterkriterien erfüllen. Entspricht eine Seite nicht diesen Parametern oder ist kein ICRA-Label auf der Webseite eingebunden, wird sie nicht geladen und somit gesperrt. Der ICRA-Filter liefert allerdings keine Informationen darüber, warum eine Seite gesperrt wird.
Neben dem reinen Site Labelling werden ergänzend auch keyword- und listenbasierte Filter angeboten. ICRAplus offeriert diesbezüglich mehrere Möglichkeiten zum Download. Kostenlos kann zum Beispiel der Zusatzfilter von

[58] http://www.icra.org/label/tester
[59] http://www.icra.org/icraplus

jugendschutzprogramm.de als Kombi-Tool zusammen mit der ICRAplus-Software von der Webseite www.icra.org/icraplus heruntergeladen werden. Das Setup installiert dabei vollautomatisch sowohl die ICRA-Software als auch den Filter JusProg. Die JusProg-Filterliste wird nachfolgend mit dem Server von jugendschutzprogramm.de abgeglichen und gegebenenfalls aktualisiert. Alternativ können die beiden Komponenten auch einzeln von der Seite heruntergeladen und nacheinander installiert werden. Die beiden genannten Programme stehen als Freeware kostenfrei zur Verfügung.

Mit zwei kostenpflichtigen Angeboten (Optenet und FilterX) stehen zusätzliche Möglichkeiten offen, den ICRAplus-Filter um optionale Filterlisten zu erweitern. FilterX plant aktuell die Erweiterung des Filters um ein deutsches Sprachpaket.

Von Bedeutung für die zukünftige Verbreitung und Akzeptanz von ICRAplus könnten drei aktuelle Entwicklungen sein:

■ **Modellversuch der KJM**
Im November 2004 hat die KJM das System „ICRAdeutschland" sowie das System „jugendschutzprogramm.de" des Vereins JusProg e.V. für einen auf 18 Monate befristeten Modellversuch zugelassen.

■ **Neue Technik**
Im Juli 2005 wurde der ICRA-Filter von der bisherigen Labeltechnologie PICS auf das leistungsfähigere RDF-label-module umgestellt. Das RDF-Modul soll vollständig in das ICRA-Grundmodul integriert werden.

■ **Lizensierung Microsoft**
Zudem hat nach offiziellen Meldungen die Firma Microsoft Ende Oktober 2005 den ICRA-Jugendschutz u.a. für den Internet Explorer, Windows und Frontpage lizenziert. Schon der ICRA-Vorgänger namens RSACi war seit Jahren im Webbrowser aus Redmond integriert.

ICRAplus kann auf allen Windows-Versionen ab Windows 98 eingesetzt werden. Andere Betriebssysteme werden gegenwärtig nicht unterstützt. Auch steht bislang eine Serverversion zum zentralen Einsatz in Netzwerken nicht zur Verfügung.

Weitere Informationen zu ICRAplus und den entsprechenden Zusatzangeboten finden Sie im Internet unter:
http://www.icra.org/icraplus

4.4 LISS security school server

Produktinformation

Produkt	LISS security school server
Hersteller/Anbieter	TELCO TECH GmbH Potsdamer Str. 18a D-14513 Teltow
Internet	http://www.telco-tech.de
Vertriebsform	Hardware, kommerziell
Demoversion	k.A.
Bedieneroberfläche	mehrsprachig
Einzelplatz / Netzwerk	nein / ja
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	optional
Self Rating / Site Labelling	./.
Bildanalyse	ja
Protokollfunktion	ja
Update der Filterlisten	wahlweise manuell oder automatisch
Betriebssystem	./.
Sonstiges	optionale Sicherheitsfeatures wie Firewall und VPN

Mit dem LISS security school server bietet die Firma TELCO TECH als ganzheitliches Sicherheitskonzept eine zentrale Hardwarelösung zum Schutz von Schulnetzwerken an. Diese ermöglicht Schulen, verschiedene Bausteine der IT-Sicherheit im Rahmen einer Gesamtlösung einzusetzen. Das System kann in bestehende Netzwerke integriert werden. Der LISS security school server bietet neben der Filterfunktionalität jugendgefährdender Webseiten u.a. auch eine Firewall, ein Virenschutzprogramm sowie weitere Netzwerkdienste wie DNS- und DHCP-Server.

Die Filterfunktion des LISS security school server basiert auf der URL-Datenbank der Firma Cobion. Wird eine Internetseite aufgerufen, so führt LISS auf direktem Wege eine Anfrage bei Cobion durch, die umgehend die Einstufung in eine der insgesamt 62 Kategorien ermittelt und sofort zurückmeldet.

Diese Abfrage erfolgt über ein spezielles, auf Performance optimiertes Verfahren. Dabei „merkt" sich ein Cache die Einstufung bereits angefragter Seiten. Häufig besuchte Seiten müssen dadurch nicht permanent mit der externen Datenbank abgeglichen werden. Die Konfigurationseinstellungen des LISS security school server erlauben auch die Pflege von Positivlisten und das Anlegen von Benutzergruppen, beispielsweise getrennt für Schüler- und Lehrerarbeitsplätze.

Der LISS security school server steht je nach Anzahl der zu erwartenden Nutzer in zwei Versionen zur Verfügung. Die beiden Hardwarevarianten sind dabei für eine Größenordnung von bis zu 50 in der kleinen sowie mehr als 50 in der großen Ausführung konzipiert.

Die Firma TELCO TECH ist auf Security Systeme für die gewerbliche Wirtschaft spezialisiert. Mit dem LISS security school server bietet das Unternehmen ein speziell auf den Schulmarkt ausgerichtetes Produkt an. Eine zentrale Hotline rundet das Angebot ab. In einer Pressemeldung wirbt das Unternehmen im Sommer 2005 mit der Installation des Systems an mehr als 250 Brandenburger Schulen.

Weitere Informationen zum LISS security school server finden Sie im Internet unter der Adresse:
http://www.liss.de/produkte/securityschoolserver.php

4.5 Parents Friend

Produktinformation

Produkt	Parents Friend
Hersteller/Anbieter	Michael Müller Neetzer Kirchweg 3 D-21354 Bleckede
Internet	http://www.parents-friend.de
Vertriebsform	Freeware / lizenzpflichtige Bonusversion, optional kostenpflichtiger Mailsupport für registrierte Nutzer
Demoversion	Freeware ohne Support
Bedieneroberfläche	deutsch
Einzelplatz / Netzwerk	ja / Monitorfunktion für Netzwerk
Black- / Whitelist	ja (manuell) / ja (manuell)
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	./.
Bildanalyse	k.A.
Protokollfunktion	ja
Update der Filterlisten	manuell
Betriebssystem	Windows
Sonstiges	Programm-, Verzeichnis- und Dateisperre, Zeitsteuerung

Parents Friend ist ein Freeware-Produkt, das die Internetnutzung an einzelnen Rechnern sowohl benutzerabhängig als auch programmbezogen regeln kann. Es handelt sich nicht um eine klassische Filtersoftware, sondern vielmehr um ein Programm mit mannigfaltigen Einstellungsmöglichkeiten, das Kinder und Jugendliche an einen behutsamen Umgang mit dem Rechner heranführen soll und auch für die private Nutzung angeboten wird.

Das Programm ist nach der Installation „unsichtbar“ und kann erst mit der Tastenkombination Strg+Shift+F7 sowie dem zugehörigen Kennwort auf dem

Desktop aufgerufen werden. Der erscheinende Bildschirm offenbart dann die gesamte Vielfalt an Einstellmöglichkeiten. Hierzu zählen neben der programmeigenen Benutzerverwaltung auch die Einrichtung und Pflege von Filterlisten, die Definition und Regelung des Zugriffs auf Programme, Verzeichnisse, Dateien und Systemeingriffe, das Einrichten von Zeitlimits sowie die Ansicht von Protokolldateien. Das Programm arbeitet nach dem bereits beschriebenen Wortfilter-Verfahren.[60] Eine Beispielliste mit Sperrwörtern zum Thema Pornografie wird vom Autor mitgeliefert. Darin befinden sich knapp über 100 Begriffe aus der pornografischen Begriffswelt. Diese Liste ist manuell erweiterbar. Listen zu weiteren schutzwürdigen Themen sind manuell anzulegen und für jeden Arbeitsplatz zu pflegen. Bei der Listenpflege besteht jeweils die Möglichkeit, für einzelne Begriffe Kennwörter und Programmfunktionen festzulegen, zum Beispiel Browser beenden oder aber auch Begriffe explizit zu erlauben (Whitelist).

Die vielfältigen Kontroll- und Konfigurationsmöglichkeiten bergen ein gewisses Risiko. In mehreren Veröffentlichungen zum Programm findet sich der Hinweis, dass widersprüchliche Konfigurationseinstellungen oder vergessene Kennwörter zu einer Aussperrung aus dem eigenen Computersystem führen können.

Das Programm Parents Friend findet in vielen Veröffentlichungen der vergangenen Jahre Beachtung und wird im Schulumfeld mehrfach zum Schutz von Schulcomputern zitiert, zum Beispiel von der Stiftung Partner für Schule NRW.[61] Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist auf das Programm hin.[62]

Supportanfragen können per Mail gegen Entrichtung einer Gebühr gestellt werden. Zur Nutzung der uneingeschränkten Protokollfunktion - in der Freewareversion wird jeweils der vierte Buchstabe durch einen Punkt ersetzt - kann ein Bonus-Key erworben werden. Für Schulen ist es zudem möglich, gegen eine einmalige Pauschalgebühr eine uneingeschränkte Protokollfreischaltung zu erwerben. Darüber hinaus ist optional als Shareware ein Netzwerkmonitor zur Betrachtung aller Parents Friend Logdateien des Netzwerks erhältlich.
Weitere Informationen zu Parents Friend finden Sie im Internet unter der Adresse: www.parents-friend.de

60 Siehe Kapitel 3.1.
61 http://www.partner-fuer-schule.nrw.de/news_complete.php?id=2591
62 http://www.bsi-fuer-buerger.de/toolbox/tb10.htm

4.6 premioss-cf

Produktinformation

Produkt	premioss-cf
Hersteller/Anbieter	IP VALUE GmbH Stockholmer Allee 24 D-44269 Dortmund
Internet	http://www.ip-value.de/www/de
Vertriebsform	lizenzpflichtige Software
Demoversion	k.A.
Bedieneroberfläche	mehrsprachig
Einzelplatz / Netzwerk	ja / ja
Black- / Whitelist	. / .
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	k.A.
Bildanalyse	k.A.
Protokollfunktion	ja
Update der Filterlisten	manuell
Betriebssystem	Linux
Sonstiges	Filterwirkung durch ACR (Artificial Content Recognition-Technologie)

Bei der Filtersoftware premioss-cf handelt es sich um eine serverbasierte Softwarelösung zur Contentfilterung für Linux in Verbindung mit dem Proxy-Server Squid. Vertrieben wird premioss-cf in Deutschland von IP VALUE, das auch eine spezielle School-Edition anbietet. Nach Herstellerangaben wird das System an zahlreichen französischen Schulen eingesetzt. Im Jahr 2002 stellte IP VALUE die Software einigen hessischen Schulen für eine Testphase zur Verfügung. Eine Beschreibung der Testphase ist auf den Seiten des hessischen Bildungsservers http://medien.bildung.hessen.de/jugendschutz/IP-VALUE verfügbar.

Im Gegensatz zu anderen Filterprogrammen arbeitet premioss-cf weder mit einem Datenbanksystem noch mit Positiv- oder Negativlisten. Die Internetseiten werden vielmehr aufgrund „künstlicher Intelligenz" in Echtzeit nach verdächtigen Inhalten durchsucht, die dann entsprechend gefiltert werden können. Das Produkt basiert auf der Artificial Content Recognition-Technologie (ACR). Diese nutzt nach Angaben von IP VALUE hoch entwickelte Algorithmen, um Webseiten nach Inhalten zu „verstehen" und entsprechend zu kategorisieren. Große Datenbanken sind aufgrund der ACR-Technologie bei diesem Verfahren nicht notwendig. Die Aktualität des Programms ist auch ohne regelmäßige Updates sichergestellt, denn die Erkennung per „künstlicher Intelligenz" bezieht stets auch neue Seiten des Internets mit ein. Das Programm erlaubt ergänzend die Pflege eines Wortfilters, der sich zur manuellen Freigabe oder Sperrung von Internetseiten individuell konfigurieren lässt.

Der Anbieter offeriert für Schulen preisreduzierte Lizenzformen. Weitere Informationen zu premioss-cf finden Sie im Internet unter:
http://www.ip-value.de/www/de/produkte/premioss-cf/premioss-cf.html

Zusätzliche Informationen zur „School-Edition" unter:
http://www.ip-value.de/www/de/produkte/premioss-cf/school-edition/premioss-cfSchoolEdition.html

4.7 SaferSurf School

Produktinformation

Produkt	SaferSurf School
Hersteller/Anbieter	SaferSurf School Distribution Pfeffingerstraße 25 D-04277 Leipzig
Internet	www.safersurfschool.de
Vertriebsform	Soft- oder Hardwareversion, kommerziell
Demoversion:	ja, kostenloser Onlinezugang
Bedieneroberfläche	deutsch
Einzelplatz / Netzwerk	nein / ja
Black- / Whitelist	optional / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	./.
Bildanalyse	k.A.
Protokollfunktion	ja
Update der Filterlisten	ja, automatisch
Betriebssystem	Linux
Sonstiges	optionale Pakete (Virensoftware, Softwaresupport u.a.), Installationspauschale für die Softwareversion

Die Linux basierte Filterlösung SaferSurf School wurde vom Leipziger Internetunternehmen Nutzwerk GmbH entwickelt und wird derzeit von der SaferSurf School Distribution, Leipzig, vertrieben. Es handelt sich um ein zentrales Zugangstool, das - je nach Konfiguration - auch die Funktionen Proxy-Server, Firewall und Router ermöglicht. Optional kann auch ein Paket zum Virenschutz eingebunden werden. Das Produkt wird in einer Hardware Version (SaferSurf School in-a-box) oder als Software (SaferSurf School CD-ROM) angeboten. Für Schulen im Bundesland Sachsen gelten für die Basis-Pakete Sonderkonditionen.

SaferSurf School ist auf Grundlage eines Positivfilters konstruiert, der es den Lehrenden ermöglicht, nur solche Internetadressen für den Unterricht freizugeben, die als relevant und zuverlässig in die entsprechenden Listen eingetragen werden. Alle anderen Inhalte bleiben in der Grundfunktionalität zunächst gesperrt. Die Freigabe gewünschter Seiten erfolgt durch den Einsatz von Regelsätzen, in denen - nach Themengebieten sortiert - die für den Unterricht benötigten Adressen gespeichert werden können. Die Nutzung der Positivlisten wurde so gestaltet, dass sie von jedem Lehrer angewendet werden können. Dabei lassen sich verschiedene Klassenräume wahlweise gleichzeitig oder nach individuellen Regeln getrennt managen. Unter der Internetadresse www.schlauesweb.de initiiert SaferSurf School zudem einen Austausch von individuell erstellten Regelsätzen.

Optional verfügt die Lösung auch über die Möglichkeit eines Grundschutzes durch den Einsatz einer Blacklist. Dabei wird prinzipiell ein freier Zugang ins Internet gewährt. Die zugeschaltete Blacklistfunktion regelt nachfolgend den Abgleich der aufgerufenen Seiten mit den Einträgen in der Filterliste (URL, Domainnamen und IP-Adressen). Die Blacklist wird monatlich automatisch aktualisiert.

Zusätzlich zu den genannten Funktionen bietet SaferSurf School unter anderem auch einen konfigurierbaren Dateitypenfilter, der das Aufrufen bestimmter Dateitypen unterbindet, beispielsweise von Videos oder MP3-Dateien.

Weitere Informationen zu SaferSurf School finden Sie im Internet unter:
www.safersurfschool.de

4.8 sBox

Produktinformation

Produkt	sBox
Hersteller/Anbieter	D.O.M. Datenverarbeitung GmbH Bahnhofstrasse 41 D-90402 Nürnberg
Internet	http://sbox.domdv.de
Vertriebsform	Hardware, kommerziell
Demoversion:	k.A.
Bedieneroberfläche	deutsch
Einzelplatz / Netzwerk	nein / ja
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	./.
Bildanalyse	k.A.
Protokollfunktion	ja
Update der Filterlisten	ja, automatisch
Betriebssystem	./.
Sonstiges	Schnittstelle zu Benutzerverwaltungen, Funktionen: „Raumsperren“, Zeitsteuerung und mehr, optional: Virenscanner

Die sBox der D.O.M. Datenverarbeitung GmbH ist ein in sich geschlossenes, aus feststehenden Hard- und Softwarekomponenten bestehendes System zur Regelung des Internetzugangs. Das Konzept des Produkts verfolgt den Grundgedanken, dass die sBox als zentrale Einheit direkt zwischen den ISDN- oder DSL-Anschluss auf der einen und das schulische Netzwerk auf der anderen Seite positioniert wird. Dabei sollen sich die Funktionalitäten der sBox einzig auf die Regelung und Steuerung des Internetzugangs beschränken. Neben der Filterfunktion kann die Box sowohl als Router und Firewall sowie Anmelde- und Proxy-Server fungieren.

Die sBox wird in einer Schulversion angeboten, mit deren Hilfe Schulen den Zugriff auf das Internet nach festen Regeln gestalten können. Für größere Umgebungen wird mit der Version sBox 2D die Möglichkeit geboten, zwei DSL-Anschlüsse mit dynamischer Proxy-Lastverteilung zu nutzen.

Die Filterfunktionen der sBox umfassen sowohl das Einrichten und Definieren von Positiv- und Negativlisten als auch die Zuweisung von Gruppen und die Vergabe von individuellen Rechten für Lehrer, Schüler sowie Computerräume oder PC-Gruppierungen. Das System erlaubt es, berechtigte Personen, zum Beispiel Lehrkräfte, als Gruppenadministratoren einzusetzen, die das System dann für den jeweils zugewiesenen Bereich selbst verwalten. Auch kann das Herunterladen von Dateien, beispielsweise mp3- oder Videodateien, gesteuert und eingeschränkt werden.

Die Indexlisten werden nach Angaben der D.O.M. Datenverarbeitung GmbH täglich aktualisiert und - ebenso wie Software-Updates der sBox - von D.O.M. zur automatischen Aktualisierung angeboten.

Weitere Informationen zur sBox finden Sie im Internet unter:
http://sbox.domdv.de

4.9 SFC - Security for Children / SFE - Security for Education

Produktinformation

Produkt	Security for Children (SFC) / Security for Education (SFE)
Hersteller/Anbieter	Security for Children AG Passauer Strasse 35 D-81369 München
Internet	www.sfcag.de
Vertriebsform	SFC - Software download / SFE Software-CD, Freeware für private Nutzung / CD für Server kostenpflichtig
Demoversion:	ja, kostenloser Download
Bedieneroberfläche	deutsch u. englisch
Einzelplatz / Netzwerk	SFC für Einzelplatz / SFE für Netzwerk
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	eigenes Label (kostenpflichtig)
Bildanalyse	k.A.
Protokollfunktion	ja
Update der Filterlisten	./.
Betriebssystem	Windows
Sonstiges	Zeitsteuerung, Dialerschutz, Programm-Filter für Mail, Chat und mehr.

Die SFC AG hat nach eigenen Angaben mit SFC (Security for Children) ein Projekt zum individuellen Schutz im Internet initiiert. Die Lösung SFC zielt auf den Schutz von Einzelrechnern ab. Eine Installation ist auf allen üblichen Windowsplattformen möglich, die gängigen Browser werden unterstützt. Mit der verfügbaren Erweiterung SFE (Security for Education) richtet sich die Initiative auch an Schulen und Institutionen im Bildungsumfeld, die den Schutzmechanismus in

einem Netzwerk installieren und dort Anwender zentral administrieren möchten. Die SFE-Variante steht auf einer kostenpflichtigen Installations-CD zur Verfügung.

Die Software arbeitet auf der Grundlage eines „wortbasierenden online Monitoring und einer intelligenten Seitenselektion".[63] Das Verfahren wird durch voreingestellte Sperrlisten und Kategorien ergänzt, die sich durch manuelle Ergänzungen in URL-Listen an die individuellen Bedürfnisse anpassen lassen.

Das Programm erlaubt in den Filtereinstellungen eine Einstufung nach Altersklassen (SFC 6, SFC 12 und SFC 16). Nach jedem Neustart ist - aus Sicherheitsgründen - die Altersklasse SFC 6 aktiviert. Bei der Liste für die bis zu Sechsjährigen handelt es sich um eine vom Programm vorgegebene Positivliste. Bei SFC 12 und SFC 16 vergrößert sich die Zahl der frei zugänglichen Seiten entsprechend der jeweiligen Altersgruppe, auch hier arbeitet das Programm mit Positivlisten. Die Programmstufen für 12- beziehungsweise 16-Jährige sind durch Kennwörter geschützt.

Das gesamte Programm bietet durch Eingabe des Administrator-Kennworts die Wahl zwischen den grundlegenden Optionen FilterON und FilterOFF. Weitere Funktionalitäten sind Dialer-Schutz sowie für registrierte Kunden Mail-, News- und Chat-Filter und Einschränkungen für die Systemumgebung, zum Beispiel Desktop, Registry. Über eine zusätzliche Konfigurationsbox (Location) können Ländereinstellungen vorgenommen werden. Dabei lassen sich bestimmte Ländergruppen (beispielsweise DEUTSCH für .de, .at, .ch oder INTERNATIONAL für .com, .org, .info, .net) per Mausklick kombinieren.

Die SFC AG bietet Industriepartnern die Möglichkeit, sich mit einem SFC-eigenen „Trusted Site"-Siegel dem Engagement zum Kinder- und Jugendschutz anzuschließen.

Weitere Informationen zu den Angeboten der SFC AG finden Sie im Internet unter: www.sfcag.de

[63] http://www.sfcag.de/sfcag/de/index.html

4.10 SmartFilter

Produktinformation

Produkt	SmartFilter
Hersteller/Anbieter	Secure Computing GmbH Central European Regional Office Ohmstrasse 4 / Haus C D-85716 Unterschleißheim
Internet	www.securecomputing.de
Vertriebsform	Software, kommerziell
Demoversion:	ja, 30-Tage-Testversion erhältlich
Bedieneroberfläche	mehrsprachig
Einzelplatz / Netzwerk	nein / ja
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	./.
Bildanalyse	ja
Protokollfunktion	ja
Update der Filterlisten	täglich
Betriebssystem	Windows, Linux, Solaris
Sonstiges	umfassende Reportfunktionalität der Log-Files,Melde-verfahren für zu sperrende oder überfilterte Seiten[64]

Das Produkt SmartFilter der Secure Computing GmbH ist auf den Einsatz in größeren Netzwerkumgebungen ausgerichtet. Der Filter wird als so genannte „On-Box" als Plugin auf Firewall-, Proxy- und Cacheservern unter Windows, Linux oder Solaris installiert. Das Produkt ist damit auf den Einsatz in Netzwerkumgebungen ausgerichtet und als Einzelplatzversion nicht verfügbar.

Das Prinzip des SmartFilters funktioniert wie folgt: Alle Zugriffe der einzelnen Arbeitsplätze auf das Internet durchlaufen zunächst den Proxy-Filter und werden anhand der Kontrolllisten der „On-Box" gecheckt. Je nach Ergebnis der Prüfung

64 http://www.securecomputing.com/sfwhere/?lang=en

werden die Anforderungen zugelassen oder blockiert und mit einer individuell anzupassenden Meldung an den Arbeitsplatz zurückgemeldet, zum Beispiel mit der Meldung „Zugriff nicht gestattet".

In der Hauptdatenbank des Filters werden täglich neue Einträge zu den URL- oder IP-Listen hinzugefügt. Die aktualisierten Listen stehen regelmäßig zur Aktualisierung des eigenen Systems in hoch komprimierter Form auf der Homepage von Secure Computing zum Download bereit.

Auch wenn der SmartFilter mit einer zentralen Konfiguration arbeitet, können optional individuelle Einstellungen vorgenommen werden. So können beispielsweise einzelne Webseiten zu Kategorien hinzugefügt oder aus Kategorien entfernt werden. Darüber hinaus kann der Nutzer selbst dynamische Regeln für ein abgestimmtes, benutzerdefiniertes Filtern bestimmen sowie zusätzliche Kategorien einrichten. Diese Einstellungen können per Browser direkt von jedem Arbeitsplatz des Netzwerks aus verwaltet und konfiguriert werden. In Abhängigkeit von den Gegebenheiten vor Ort ist es beispielsweise möglich, für den Schulunterricht individuelle Einstellungen vorzunehmen.

Weiterhin lassen sich durch zentrale Einstellungen Benutzergruppen[65] definieren oder die Möglichkeiten für den Download bestimmter Dateien, zum Beispiel mp3 oder Video, regulieren. Eine Zeitsteuerung erlaubt zudem die automatische Ausführung von festgelegten Aktionen. Auch kann das System den Inhalt der lokalen Festplatte oder des Speichers nach bedenklichen Inhalten durchsuchen. Im Einsatz von übergreifenden Umgebungen wie beispielsweise www.belwue.net[66] gelten diesbezüglich zentrale Vorgaben.

Der Bezug von SmartFilter kann in kostenpflichtigen Abonnements für ein oder zwei Jahre abgeschlossen werden. Software, Supportleistungen sowie ein unbeschränkter Zugriff auf die Download-Seite sind dabei jeweils eingeschlossen.

Weitere Informationen zum SmartFilter finden Sie im Internet unter:
http://www.securecomputing.com

[65] Alle gängigen Authentifizierungsverfahren wie AD, LDAP und andere werden unterstützt.
[66] http://www.belwue.de/services/wwwproxy.html

4.11 SquidGuard

Produktinformation

Produkt	SquidGuard
Hersteller/Anbieter	Open Source (freie Software)
Internet	www.squidguard.com
Vertriebsform	Open Source
Demoversion:	./.
Bedieneroberfläche	englisch
Einzelplatz / Netzwerk	nein / ja
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	./.
Bildanalyse	nein
Protokollfunktion	ja
Update der Filterlisten	ja
Betriebssystem	Linux mit installiertem Proxy Squid
Sonstiges	häufig Bestandteil von Schulservern unter Linux

SquidGuard ergänzt als Systemerweiterung den Proxy-Server Squid um erheblich erweiterte Filtermöglichkeiten. Es handelt sich um ein Open-Source-Paket unter Linux für den zentralen Einsatz in Netzwerken. Für die Software stehen Blacklists aus verschiedenen Quellen[67] als Listen oder kompilierte Datenbanken zur Verfügung. Die freien Blacklists werden nicht kommerziell gepflegt und stehen in eher unregelmäßigen Aktualisierungsintervallen zum Download unter www.squidguard.com zur Verfügung. In der Praxis werden dabei oftmals Filterlisten aus unterschiedlichen Quellen kombiniert, um eine möglichst hohe Filterwirkung zu erreichen. Eine Beschreibung zum Abgleich der unterschiedlichen Filterlisten steht auf der Webseite www.linux-schulserver.de[68] zur Verfügung.

[67] http://www.bn-paf.de/filter/index_de.html
[68] http://www.linux-schulserver.de/Sections-article33-p1.phtml

Die offene Architektur des Systems erlaubt zudem die Möglichkeit des kombinierten Einsatzes von Filterlisten für SquidGuard und kommerziellen Produkten wie beispielsweise DansGuardian.

Für die Installation und den Einsatz von SquidGuard als Plugin zum Squid-Proxy auf den verschiedenen Linux-Schulservern existieren vielfältige Anleitungen und Hilfestellungen im Internet.[69]

Ein Blick in die genannten Hilfestellungen zeigt, dass das System vor allem für solche Schulen geeignet sein dürfte, die über ausreichendes Know-how verfügen, ein solches System selbst zu installieren, konfigurieren und zu betreiben. SquidGuard setzt administrative Fähigkeiten voraus, da manuelle Installations- und Anpassungsarbeiten vorgenommen werden müssen.

SquidGuard bietet neben der reinen Filterfunktionalität eine Reihe weiterer Optionen und Konfigurationsmöglichkeiten an. Der Internet-Zugang kann beispielsweise nach Zeit, IP-Adresse, Negativ- oder Positivliste blockiert beziehungsweise freigegeben werden. Es können auch einzelne Nutzer von der Filterung ausgenommen werden oder das Internet nur für bestimmte Nutzer / Rechner blockiert werden. Das System bietet zudem umfangreiche Protokolldateien. Die geblockten Seiten werden einschließlich der Userkennung mitgeloggt.[70]

Der Einsatz von SquidGuard im schulischen Umfeld wird bundesweit unter verschiedenen Gesichtspunkten diskutiert und getestet, beispielsweise im Projekt des Thüringer Arbeitskreises Schulsoftware[71] oder beim Schul-Support-Service in Hamburg[72]. Das Programm findet zudem auch in so genannten Black-Boxes[73] Anwendung.

Weitere Informationen zu SquidGuard gibt es im Internet unter:
http://www.squidguard.com

69 Zum Beispiel unter http://www.linux-schulserver.de/Sections-article2-p1.phtml
70 Siehe auch die Hinweise zum Datenschutz in Kapitel 2.4.
71 http://www.th.schule.de/th/schulsoftware/newsletter.php?datei=nl1.php
72 http://3s.hh.schule.de/wissen/handouts/Filtersoftware.pdf
73 Als Black-Box werden geschlossene Gesamtsysteme bezeichnet, deren Soft- und Hardware unveränderbar vorgegeben ist.

4.12 Symantec Parental Control

Produktinformation

Produkt	Parental Control
Hersteller/Anbieter	Symantec Deutschland GmbH
	Lise-Meitner-Str. 9
	D-85737 Ismaning
Internet	http://www.symantec.com/region/de

Vertriebsform	Software, kommerziell
Demoversion:	ja
Bedieneroberfläche	deutsch
Einzelplatz / Netzwerk	ja / nein
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	k.A.
Bildanalyse	k.A.
Protokollfunktion	ja
Update der Filterlisten	ja
Betriebssystem	Windows
Sonstiges	im Security-Paket sind weitere Funktionen enthalten

Das Filtersystem Symantec Parental Control ist Teil des Norton Internet Security 2005 Pakets der Firma Symantec. Dieses richtet sich an Verbraucher, die ihren Computer unter Windows mit einem umfassenden Sicherheitspaket gegen Viren und Spam schützen sowie mit einer Firewall absichern möchten. Das Programm ist für den Einsatz auf Einzelcomputern ausgelegt. Eine Serverversion wird nicht angeboten.

Das Schutzprogramm basiert auf Filterlisten, die sich in zirka 30 Kategorien unterteilen. Kategorisiert wird allgemein nach grundsätzlichen Lebensbereichen und im Besonderen nach Kategorien, die auf Jugendschutz abzielen, wie Sex, Gewalt, Hass, Drogen und Waffen. Eine manuelle Ergänzung der Listen ist möglich.

Der Schutzmechanismus lässt sich in zwei Arbeitsschritten für einzelne Nutzer des Systems aktivieren. In einem ersten Schritt werden übergreifende Gruppenkonten angelegt, denen gewisse Rechte zur Internetnutzung zugewiesen werden können. Auf Grundlage der Konten können dann gesonderte Benutzerprofile angelegt werden. Auf diese Weise können Zugriffsrechte und Einschränkungen individuell festgelegt werden. Eine gesonderte Zuweisung von Rechten für Schüler und Lehrer ist somit möglich.

Die Sprachausrichtung von Symantec Parental Control erfasst deutschsprachige Seiten, der inhaltliche Schwerpunkt des Programms liegt aber eindeutig im englischsprachigen Bereich.

Weitere Informationen finden Sie im Internet unter:
http://www.symantec.com/region/de/product

4.13 TIME for kids Schulfilter Plus

Produktinformation

Produkt	Schulfilter Plus
Hersteller/Anbieter	TIME for kids Informationstechnologien GmbH Gubener Straße 47 D-10243 Berlin
Internet	www.schulfilterplus.de
Vertriebsform	Software, kommerziell
Demoversion:	ja
Bedieneroberfläche	deutsch / englisch
Einzelplatz / Netzwerk	ja / ja
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	k.A.
Bildanalyse	ja
Protokollfunktion	ja
Update der Filterlisten	ja
Betriebssystem	Windows, Linux, IPCop
Sonstiges	Zusatzangebote für Schulen, Hotline für Schulen Angebot auch zur privaten Nutzung

Der von der TIME for kids Informationstechnologien GmbH in Berlin angebotene Jugendschutzfilter „Schulfilter Plus“ basiert ursprünglich auf dem Produkt „Orange Box“ der Cobion AG, die seit Januar 2004 zur Internet Security Systems Inc. (ISS) gehört. Das von ISS als Proventia Webfilter weitergeführte Produkt wird von der TIME for kids GmbH als Basis-Technik zu dem angebotenen Produkt „Schulfilter Plus“ eingesetzt. Darin sind speziell für den Einsatz in Schulen entwickelte Zusatzleistungen enthalten. Das System kann auf einzelnen Computern installiert werden, zielt aber klar auf den Einsatz auf einem zentralen Server unter Windows oder Linux ab. Das Produkt kann mit allen gängigen Proxy-Servern kombiniert werden und bietet auch die Möglichkeit, unter IPCop[74] integriert zu wer-

[74] IPCop ist eine freie Linux Router- / Firewall-Kombination. Infos unter http://de.wikipedia.org/wiki/IPCop

den. Zudem stehen umfassende Schnittstellen zur Einbindung in bestehende Benutzerstrukturen - zum Beispiel Windows-Domänen oder Verzeichnisdienste wie beispielsweise Active Directory, OpenLDAP oder Novell NDS - zur Verfügung.[75]

Der Schulfilter Plus arbeitet mit einer auf Positiv- und Negativlisten basierenden Textanalyse sowie mit einer Bild- und Symbolerkennung. Dabei wird auch eine semantische Textanalyse durchgeführt, die durch eine Texterkennung in Grafiken durch OCR[76] ergänzt wird. Die Filterlisten sind in derzeit 60 individuell einstellbare Kategorien unterteilt, zu denen beispielsweise die Bereiche Sex, Erotik, Pornografie, Gewaltverherrlichung, Hass, politischer sowie religiöser Extremismus und Fanatismus gehören. Die tägliche Überprüfung von zahlreichen Webangeboten fließt regelmäßig in eine Aktualisierung der Filterlisten ein.

TIME for kids bietet zur einfachen Nutzung des Inhaltsfilters mit der Lernbox eine deutschsprachige Benutzeroberfläche an. Die Lernbox ermöglicht es den Lehrkräften, das Filtersystem vom jeweiligen Lehrerarbeitsplatz aus zu administrieren oder zu steuern. So können Grundeinstellungen angepasst, Filter-Kategorien oder Linklisten gepflegt und Einstellungen zu Klassenraumfunktionen und Zeitsteuerungen vorgenommen werden. Die Lernbox ist fester Bestandteil des Produkts Schulfilter Plus und steht für Windows- und Linux-Systeme zur Verfügung. Ebenfalls in dem Gesamtpaket Schulfilter Plus enthalten ist der Webkatalog. Der Webkatalog wird von der TIME for kids Foundation gemeinnützige GmbH weiterentwickelt und gepflegt. Er fungiert mit derzeit über 12.000 kategorisierten, geprüften und bewerteten Unterrichtsinhalten als Positivliste für den Einsatz in der Schule.

TIME for kids bietet Schulen eine Hotline für technischen Support oder pädagogische Fragen sowie Installationshilfen für mehrere Plattformen an. Das Produkt wird je nach Laufzeit oder Anzahl der zu schützenden Computer in mehreren schulspezifischen Lizenzmodellen angeboten. Zum Schutz von Heimcomputern wird das Paket „Internetfilter Plus“ angeboten.

Weitere Informationen zu dem Schulfilter Plus erhalten Sie im Internet unter:
www.time-for-kids.de oder www.schulfilterplus.de

[75] Der LDAP-Verzeichnisdienst von Microsoft Windows 2000/2003 Server heißt Active Directory Service (ADS). Bei einem Verzeichnis (engl. Directory) handelt es sich um eine Zuordnungsliste, wie zum Beispiel bei einem Telefonbuch. Es ordnet Telefonnummern den jeweiligen Anschlüssen (Besitzern) zu. Das Active Directory ordnet verschiedenen Netzwerkobjekten, wie Benutzern oder Computern, Eigenschaften zu und verwaltet diese. LDAP ist die Abkürzung für das Lightweight Directory Access Protocol. Dieses Protokoll unterstützt einen Verzeichnisdienst (Directory) zur zentralen Nutzerverwaltung. Mehr dazu im Internet unter http://www.mitlinx.de/ldap

[76] OCR bedeutet Optical Character Recognition und beschreibt die Umwandlung von einer eingescannten Grafik mit Text in ein reines Textformat.

4.14 T-Online Kinderschutz-Software

Produktinformation

Produkt	Kinderschutz-Software
Hersteller/Anbieter	T-Online International AG D-64306 Darmstadt
Internet	www.t-online.de[77]
Vertriebsform	Freeware (für Kunden von T-Online)
Demoversion:	./.
Bedieneroberfläche	deutsch
Einzelplatz / Netzwerk	ja / nein
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	ja
Bildanalyse	k.A.
Protokollfunktion	ja
Update der Filterlisten	ja
Betriebssystem	Windows
Sonstiges	Nutzung nur mit T-Online Zugang möglich (auch T@School)

Mit dem Produkt „Kinderschutz-Software" bietet T-Online eine kostenlose Schutzsoftware für Einzelplatz-Computer unter Windows an. Die Software kann im Download bezogen werden und steht nur Kunden von T-Online, also auch für die kostenfreien T@School Anschlüsse in Schulen, zur Verfügung.

Die Bedienerführung entspricht eher der Nutzung im privaten Umfeld als einer Nutzung im schulischen Umfeld. So kann das Programm nach erfolgter Installation über die Eltern- und Kinder-Einstellungen konfiguriert werden. Der Software liegt die Grundidee einer Steuerung des Internetzugangs über Zeitkontingente für bestimmte Kinderprofile zugrunde. So kann mittels eigener Regeln definiert werden, wann und wie viele Stunden Kinder pro Tag und Woche das Internet nutzen dürfen.

[77] Der exakte Produktlink lautet: http://service.t-online.de/c/51/88/20/5188204.html

Die Einstellungen erlauben zudem, Zuordnungen zu bestimmten Altersgruppen zu treffen. Das Programm greift dabei auf eine integrierte Positivliste zurück, die nach Herstellerangaben von Pädagogen regelmäßig gepflegt und aktualisiert wird.

Eltern oder Lehrer haben die Möglichkeit, die Liste selbst zu pflegen und um gewünschte Einträge zu ergänzen. Wollen Kinder eine Seite besuchen, die nicht über die Positivliste freigegeben ist, so können sie den entsprechenden Link an die Eltern/Lehrer senden, die dann über eine Freigabe und Aufnahme in die Whitelist entscheiden können.

Über die Internetnutzung hinaus kann die Nutzung weiterer Internetdienste, beispielsweise Chat, Newsgroups oder E-Mail, gesondert geregelt werden.

Seit Mitte 2005 kann die T-Online Kinderschutz-Software für T-Online-Kunden kostenlos heruntergeladen werden. Eine technische Beratung zur Installation und Konfiguration steht telefonisch und über E-Mail zur Verfügung.

Weitere Informationen sowie eine ausführliche Leistungsbeschreibung und Angaben zu Systemvoraussetzungen und Installationshilfen finden Sie im Internet unter: www.t-online.de/kinderschutz-software

Weitergehende Fragen zu T@School werden beantwortet unter:
www.slmuenster.de

4.15 webwasher

Produktinformation

Produkt	webwasher
Hersteller/Anbieter	webwasher AG Vattmannstr. 3 D-33100 Paderborn
Internet	www.webwasher.com
Vertriebsform	Software, kommerziell
Demoversion:	ja, nach Registrierung
Bedieneroberfläche	deutsch
Einzelplatz / Netzwerk	ja / ja
Black- / Whitelist	ja / ja
Wortfilter ergänzbar	ja
Self Rating / Site Labelling	k. A.
Bildanalyse	ja
Protokollfunktion	ja
Update der Filterlisten	ja
Betriebssystem	Windows, Linux, MacOS, Solaris
Sonstiges	umfangreiche Protokollfunktionen optionale Zusatzpakete für Mail und mehr

Das Produkt webwasher ist ursprünglich als Contentfilter zur Beseitigung von störenden Werbebannern und -grafiken entwickelt worden. Die von der Paderborner Webwasher AG nunmehr unter ihrem Namen angebotene Programmsammlung besteht aus verschiedenen Einzelpaketen mit speziellen Funktionalitäten. So wird neben den Paketen Anti-Virus, Anti-Spam und Mailschutz auch ein URL-Filter angeboten.

Die Filtersoftware arbeitet auf einzelnen Clients, ist jedoch grundsätzlich für den zentralen, serverbasierten Einsatz ausgelegt. Das Produkt kann auf Windows- und Linux-Servern sowie unter MacOS und Solaris eingesetzt beziehungsweise in bestehende Nutzerverwaltungen eingebunden werden. Dabei

werden auch Techniken unterstützt, die sich an große und sehr große Netzwerkumgebungen richten. Der Filter wird im Schulumfeld somit auch in größeren, schul- oder gar schulträgerübergreifenden Installationen eingesetzt.

Der webwasher URL-Filter greift bei der Filterung jugendgefährdender Inhalte auf umfangreiche Filterlisten zurück, die auch einen deutschsprachigen Bezug berücksichtigen. Die Listen werden in knapp 60 Kategorien organisiert, die ihrerseits noch einmal in weitere Bereiche untergliedert sind. Bei der täglichen Aktualisierung werden von dem Hersteller auch öffentlich verfügbare Sperrlisten in diese Aktualisierung einbezogen. Die Inhalte der Listen werden im Bedarfsfall zusätzlich von einer Redaktion überprüft.

Das Programm erlaubt umfangreiche Konfigurationsmöglichkeiten in der Steuerung der verschiedenen Funktionen. Die Nutzung der vielfältigen Einstellmöglichkeiten setzt eine fundierte Einarbeitung voraus. Nachfolgend lassen sich Filterlisten pflegen und ergänzen, Zugriffsrechte detailliert regeln und individuelle Steuerungen im Schulbetrieb vornehmen. Zudem stehen umfassende Protokolle und Auswertungen der Internetnutzung zur Kontrolle der Einhaltung der Nutzungsregeln zur Verfügung.

Die Flexibilität und Skalierbarkeit der webwasher-Module sowie die breite Palette unterstützter System-Plattformen erlauben Einsatzmöglichkeiten auch in größeren Umgebungen. Der Anbieter wirbt in diesem Zusammenhang gerne mit dem Einsatz des Produkts bei der Lernstatt Paderborn.[78]

Informationen zum webwasher sowie die Möglichkeit zum Download einer Evaluations-Version nach Registrierung werden im Internet angeboten unter:
www.webwasher.com

[78] http://www.paderborn.de/microsite/lernstatt/konzeption/sp_auto_9746.php

5. Kommunen und Bundesländer

Sowohl auf kommunaler Ebene als auch in einzelnen Bundesländern gibt es Initiativen und Einrichtungen, die Schulen und Schulträger bei der Auswahl und Pflege von Filtersoftware unterstützen oder eigene Strukturen zur zentralen Nutzung anbieten. Exemplarisch werden nachfolgend einige zentrale Lösungsansätze skizziert.

5.1 Kommunale Initiativen

Bundesweit haben sich mehrere Schulträger für eine schulübergreifende Bereitstellung einer Filterlösung für ihre Schulen entschieden. Neben dem Angebot zur Nutzung zentraler Filterfunktionen stehen vor allem die Hilfestellung bei der konkreten Einbindung in ein entsprechendes System sowie der Support für einen störungsfreien Betrieb im Vordergrund der Angebote.

5.1.1 Bremen

Der Schul-Support-Service e.V. in Bremen (S3) stellt sicher, dass alle 160 Bremer Schulen an das Internet angeschlossen sind und somit flächendeckend eine Versorgung der Schulen erfolgt.[79] Die Schulen sind über einen kommunalen Kommunikationsdienstleister an das Internet angebunden. In dem Projekt agiert der Senator für Bildung und Wissenschaft quasi als Provider. Die Filterung bedenklicher Inhalte findet dabei an zentraler Stelle und somit nicht in jeder Schule einzeln statt.

5.1.2 Hamburg

In Hamburg bietet der Schul-Support Service (3S) seit Dezember 2000 allen allgemein bildenden Schulen Unterstützung bei der Behebung technischer Schwierigkeiten mit Computern und Netzwerken an.[80] Das Kooperationsprojekt zwischen dem HITeC e.V. und der Behörde für Bildung und Sport besteht aus einer telefonischen Hotline sowie einem Vor-Ort-Service, der pro Schule zwei feste Betreuer - meistens Studierende - vorsieht. Eine Arbeitsgruppe widmet sich explizit dem Thema Filtersoftware. Eine zentrale Lösung wird in Hamburg nicht angeboten. Vielmehr leistet der Schul-Support-Service Unterstützung bei der Installation und Administration von Filterprodukten.

[79] Informationen zu S3 finden Sie im Internet unter www.schul-support-service.de
[80] Informationen finden Sie im Internet unter: http://3s.hh.schule.de/wissen/handouts/Filtersoftware.pdf und http://3s.hh.schule.de

5.1.3 Frankfurt am Main

Ähnlich den beiden Support-Services in Bremen und Hamburg unterstützt das Projekt „fraline" Schulen in Frankfurt am Main.[81] Es handelt sich um ein Kooperationsprojekt zwischen dem Schulamt der Stadt Frankfurt und der Fachhochschule Frankfurt, University of Applied Sciences. Die Hotline sowie der Vor-Ort-Service für die Schulen der Stadt werden von Studierenden betreut. Diese arbeiten auch an Projekten zur weiteren Optimierung der Schul-Support-Konzepte mit. Im Rahmen des Leistungsspektrums bietet fraline auch die Beratung und Unterstützung bei der Auswahl und Implementierung von Sicherheitsmaßnahmen sowie Schutzkonzepten, wie beispielsweise Filtersoftware, an. Anfang 2005 hat fraline einen Projektbericht zum Thema „Contentfilter" erstellt.[82]

5.1.4 Paderborn

Seit Herbst 2001 hat die Stadt Paderborn mit der „Lernstatt Paderborn" eine flächendeckende und wartungsarme EDV-Infrastruktur in allen Schulen Paderborns aufgebaut. Im Rahmen dieses Projekts stellt ein kommunales Rechenzentrum sowohl die Vernetzung der Schulen untereinander als auch die Anbindung der Schulen an das Internet sicher. Eine zentrale Filtersoftware schützt dabei den Internetzugang aller angebundenen Schulen vor unerwünschten Internetangeboten. Umfassende Informationen zu dem Projekt sowie ein Bericht zu der von IT works durchgeführten Evaluation sind im Internet verfügbar.[83]

5.2 Landesweite Initiativen

Auch auf Ebene der Bundesländer ist ein übergreifendes Engagement zum Thema Jugendschutz in Schulen und Filtersoftware erkennbar. Einige zentrale Angebote leisten damit sogar schulträgerübergreifende Unterstützung zur Realisierung des Jugendmedienschutzes.

5.2.1 Baden-Württemberg

BelWü steht für „Baden-Württembergs extended LAN" und ist das Netz der wissenschaftlichen Einrichtungen in Baden-Württemberg.[84] Die Schulen des Landes können sich per Wähl- oder Festverbindung diesem Netz anschließen. Dabei arbeitet BelWü serverbasiert mit einer Proxy-Filtersoftware. Bei allen Verbin-

[81] Die Serviceleistungen von fraline werden auf der Website http://www.fraline.de aufgeführt.
[82] Der vollständige Abschlussbericht kann im Internet unter:
http://www.fraline.de/media/bps_docs/Abschlussbericht_ContentFilter_Jan_Kaiser_Sep2004.pdf heruntergeladen werden.
[83] Alle Informationen finden Sie unter http://itworks.schulen-ans-netz.de/aktuelles/lernstattpaderborn/index.php
[84] Ausführliche Informationen zu BelWü finden Sie im Internet unter http://www.belwue.de/services/wwwproxy.html

dungen, die über den BelWü-Proxy laufen, werden die entsprechenden Internetseiten auf jugendgefährdende Inhalte geprüft. Es besteht zudem die Möglichkeit, in der Schule ebenfalls einen Proxy-Server einzusetzen. Dieser greift dann in einem zweiten Schritt auf den BelWü-Filter zurück und nutzt so die zentrale Filterfunktion.

5.2.2 Bayern

Beratende Unterstützung erfahren Schulen in Bayern durch das Bayerische Staatsministerium für Unterricht und Kultus in München. Medienerziehung wird dort als Gemeinschaftsaufgabe verstanden, die das Kultusministerium und der Bayerische Schulserver durch vielfältige Aktivitäten unterstützen. Im Rahmen einer Aussprachetagung in der Akademie für Lehrerfortbildung wurde ein Ergebnisbericht zum Thema „Internetfilterung für Schulen" erstellt.[85] Weitere Informationen gibt es auf der Homepage des Bayerischen Staatsministeriums für Unterricht und Kultus.[86] Das Bayerische Kultusministerium hat außerdem Anfang 2005 das Pilotprojekt „Filtersurf" aktiv unterstützt.[87]

Das Staatsinstitut für Schulqualität und Bildungsforschung in München stellt zudem auf seiner Homepage eine ausführlich kommentierte Linkliste zum Thema Kinder- und Jugendmedienschutz zur Verfügung.[88]

5.2.3 Hessen

Im Bundesland Hessen wurden in den vergangenen Jahren verschiedene Aktivitäten rund um das Thema Jugendmedienschutz in Schulen initiiert und unterstützt. Auch die hessische Initiative Zukunft@Schule hat sich in diesem Bereich engagiert. Die verschiedenen Aktivitäten sind auf dem Bildungsserver Hessen ausführlich dokumentiert.[89]

5.2.4 Thüringen

Der Thüringer Arbeitskreis Schulsoftware bietet in Zusammenarbeit mit dem Thüringer Kultusministerium und der Friedrich-Schiller-Universität Jena einen Jugendschutzfilter für den Internetzugang der Thüringer Schulen an. Dies erfolgt als Ergänzung zum Thüringer Bildungsserver, wobei alle Schulen des

[85] Die Ergebnisse finden Sie im Internet unter http://www.schule.bayern.de/beratung/iuk/filter/filterloesungen.pdf
[86] Infos unter http://www.stmuk.bayern.de/km/aufgaben/medien/index.shtml sowie http://www.stmuk.bayern.de/km/aufgaben/medien/einrichtungen/index.shtml
[87] http://www.filtersurf.de/pilotprojekt.php
[88] http://www.isb.bayern.de/isb/download.asp?DownloadFileID=7a0b28802a438cffefad96d50b9c48a8
[89] http://medien.bildung.hessen.de/jugendschutz

Landes auf das Angebot zugreifen können. Das System arbeitet als zentraler Proxy-Server auf der Basis von regelmäßig gepflegten und aktualisierten Filterlisten. Einzelrechner beziehungsweise interne Schulserver können den zentralen Proxy zum Schutz der Schulnetzwerke vor jugendgefährdenden Inhalten nutzen.

Eine weitergehende Beschreibung des Thüringer Schulfilters steht im Internet zur Verfügung.[90]

[90] http://filter.th.schule.de/menue/hauptseite.php

6. Jugendmedienschutz im internationalen Kontext

Der Umgang mit dem Thema „Jugendschutz und Internet“ ist sowohl innerhalb Europas als auch im außereuropäischen Vergleich, beispielsweise mit den USA, recht unterschiedlich. Dabei stellt sich einerseits die Frage nach der Relation zwischen bewusstseinsbildenden Maßnahmen und Technikeinsatz, andererseits aber auch nach der politischen, gesellschaftlichen und rechtlichen Definition der landesspezifischen Moralvorstellungen und kulturellen Werte. Das Thema hat also nicht nur eine ethische und technische Dimension, sondern muss neben pädagogischen auch unter soziokulturellen Gesichtspunkten betrachtet werden. Dies gilt insbesondere für die Fragen, die sich innerhalb des schulischen Umfelds eines jeden Landes unter diesen Aspekten ergeben.

6.1 Gemeinsam für ein sicheres Internet - Jugendmedienschutz in Europa

Aktionsplan „Safer Internet“

Mit ihrem Aktionsplan „Safer Internet“[91] zur Förderung der sicheren Nutzung des Internets hat die Europäische Union im Jahr 1999 eine Initiative ins Leben gerufen, die unter anderem eine sichere Verwendung des Internets fördern sowie illegale und schädigende Inhalte im Netz bekämpfen soll.

Der Aktionsplan umfasst vier Arbeitsbereiche, für die jeweils konkrete Maßnahmen vorgeschlagen und entwickelt wurden. Einer dieser Bereiche widmet sich dem optimalen Schutz Minderjähriger vor Inhalten, die ihrer Entwicklung schaden könnten. Als Maßnahme hierzu wird angeregt, Anbieter der einschlägigen Branchen zur Bereitstellung von Filterwerkzeugen und Bewertungsverfahren zu ermutigen. Diese Hilfsmittel sollen es Eltern und Lehrkräften ermöglichen, die geeigneten Inhalte für die Kinder auszuwählen.

Der Aktionsplan konzentrierte sich zunächst auf den Zeitraum vom 1. Januar 1999 bis zum 31. Dezember 2002. Er wurde jedoch bis Ende 2004 und in einem zweiten Schritt bis Ende 2008 verlängert. Der Rat „Telekommunikation" der EU verabschiedete im Dezember 2004 das Programm „Mehr Sicherheit im Internet“, das Eltern und Lehrern Instrumente zur sicheren Nutzung des Internets an die Hand geben möchte. Das von der Europäischen Kommission vorgeschlagene Vierjahresprogramm (2005-2008) ist mit 45 Millionen Euro ausgestattet und soll

[91] http://europa.eu.int/scadplus/leg/de/lvb/l24190.htm

dem Kampf gegen illegale und schädliche Inhalte im Internet dienen. Das Programm richtet sich vor allem an die Endnutzer, also an Eltern, Lehrer und Kinder. Die Umsetzung des Aktionsplans erfolgt jeweils auf nationaler Ebene der beteiligten EU-Länder.

GMK Bielefeld

In Deutschland oblag die Umsetzung des Plans in der ersten Phase der Gesellschaft für Medienpädagogik und Kommunikationskultur (GMK) in Bielefeld. Inhaltlich ging es vor allem darum, eine größere Aufmerksamkeit für die Risiken des Internets zu schaffen und ein entsprechendes Hilfsinstrumentarium für Pädagogen zu entwickeln. Informationen zur ersten Phase stellt die GMK auf ihrer Webseite bereit.[92]

Auf der Homepage von s@ferinternet[93] stehen auch die Publikationen „Was Lehrende tun können: Sichere und verantwortungsvolle Internetnutzung in Schulen" sowie „Computer im Unterricht" als Download zur Verfügung.[94]

InS@fe

Der Übergang des Aktionsplans in die zweite Phase erfolgte mit InS@fe. Das Kooperationsnetzwerk zum Thema Internet-Sicherheit wird gemeinsam getragen von der Landeszentrale für private Rundfunkveranstalter Rheinland-Pfalz, der Landesanstalt für Medien Nordrhein-Westfalen sowie dem Europäischen Zentrum für Medienkompetenz (ecmc). Dabei steht vor allem die Netzwerkbildung im Vordergrund. Hierfür wurde mit dem unabhängigen Informationsportal klicksafe.de zum Thema „Sicherheit im Internet" eine neue bundesweite Plattform geschaffen.

klicksafe.de

Als nationaler Knotenpunkt im europäischen Netzwerk trägt klicksafe.de im Auftrag der Europäischen Kommission dazu bei, in Deutschland auf die Chancen und Risiken des Internets aufmerksam zu machen und die verschiedenen Akteure und Initiativen zusammenzubringen und zu einem Netzwerk zu verknüpfen. Dabei wurde eine Reihe von Angeboten für verschiedene Zielgruppen zusammen getragen, die Wissenswertes zu relevanten und brisanten Sicherheitsthemen für Kinder, Jugendliche, Eltern und Pädagogen bündeln. Umfassende Informationen stehen im Internet auf der Webseite des Projekts unter www.klicksafe.de zur Verfügung.

[92] Infos unter http://www.gmk-net.de/ und http://www.safernet.info/NationalPages.asp?country_id=3
[93] http://www.safer-internet.net
[94] www.safernet.info/NationalPages.asp?country_id=3&menu_item=Downloads

6.2 Die Situation in Europa und den USA

Es existieren international verschiedene Lösungsansätze, die die Sicherstellung des Jugendschutzes im Umgang mit dem Internet gewährleisten sollen. Dies belegt ein Blick auf die Situation in anderen europäischen Staaten und in den USA.

6.2.1 Europa

Stellvertretend für den europäischen Raum seien die Länder Norwegen und Großbritannien genannt, die sehr unterschiedlich an das Thema Jugendschutz herangehen. Entsprechend verschieden sind auch ihre Maßnahmen für ein sicheres Internet an Schulen.

Norwegen fördert die Sensibilisierung

Das norwegische Schulsystem setzt bei der Erziehung zur Medienkompetenz verstärkt auf Maßnahmen zur Steigerung des Bewusstseins denn auf den Einsatz von Filtertechnologien. In Norwegen konzentrieren sich daher mehr als zwei Drittel der Schulen auf Sensibilisierungsmaßnahmen, beispielsweise in Form von Projekten und Kursen, die fest in den Lehrplan integriert sind.

Großbritannien setzt auf Technik

Ganz anders die Situation in Großbritannien. Hier bildet der Einsatz von Filterlösungen einen Eckpfeiler der britischen Methode zur Gewährleistung eines sicheren Internets an Schulen. Dabei wird eine inhaltliche Modifikation angestrebt. Aus dem Thema Sicherheit wird das Thema Verantwortung, unterstützt durch einen gezielten Einsatz von Filtersoftware. Schulen und Behörden streben hier eine Balance zwischen Risikobewusstsein und einer positiven Grundeinstellung der Lehrkräfte und der Eltern gegenüber dem Internet an.

6.2.2 USA

US-amerikanische Schulen nutzen häufig Blacklists

Auch in den USA dienen Filtersysteme vorwiegend als Ergänzung der Richtlinien zur Internetnutzung. Diese sind allerdings nicht per Bundesgesetz geregelt und existieren auch nicht in allen Staaten der USA. Sehr verbreitet sind in den Vereinigten Staaten zentrale Proxy-Server, die über Blacklists bedenkliche Internetseiten blockieren. Viele Schulbezirke haben eigene Filtersysteme eingeführt oder nutzen die Filtersoftware von kommerziellen Anbietern.

Verstöße werden registriert

Als zusätzliches technisches Hilfsmittel zur Kontrolle der Internetnutzung an Schulen werden in einzelnen Schulbezirken - beispielsweise in Santa Ana, Kalifornien - Nutzungsprotokolle und Logins verwendet. Die Protokolle zeichnen alle versuchten Zugriffe von Schülern auf gesperrte Seiten auf und leiten die Einträge dann an die zuständige Schule weiter. Da die Schulen jedoch bislang nicht durchgängig solche Systeme installiert haben oder diese in bestimmten Bereichen - beispielsweise in der Bibliothek - komplett fehlen, können Verstöße nicht immer eindeutig zugeordnet werden.

Auch in Plano, Texas, setzt man auf Kontrolle. Hier hat jeder Schüler vom Kindergarten bis zur Highschool einen eigenen Nutzernamen und ein eigenes Passwort. Dies ermöglicht jeweils die eindeutige Zuordnung von Netzwerkaktivitäten zu den entsprechenden Nutzern.

Weitergehende Informationen

Im Rahmen einer Studie der Bertelsmann-Stiftung zum Thema „Internet-Verantwortung" ist der Länderbericht USA[95] erschienen. Darin kommt man zu dem Ergebnis, dass sich Filter - trotz einiger Mängel - als guter Ansatz erwiesen haben, um eine sichere Internetumgebung im Schulunterricht zu schaffen.

Auf Basis der Erfahrungen eines Deutsch-Amerikanischen Dialoges hat die Bertelsmann-Stiftung im Oktober 2000 zudem einen „Leitfaden zum Thema Internet-Verantwortung an Schulen"[96] entwickelt. Dieser enthält neben Betrachtungen zur Medienkompetenz und Schulentwicklung auch eine Reihe Tipps zu technischen Kontrollmaßnahmen und sinnvollen Verhaltensrichtlinien für eine altersgerechte Internetnutzung im schulischen Kontext. Der Leitfaden steht im Internet als Download zur Verfügung.[97]

Der Verein Schulen ans Netz hat ausführliche Informationen zum Thema „Jugendmedienschutz International" in einem Infoletter zusammengetragen. Der Infoletter kann ebenfalls im Internet heruntergeladen werden.[98]

[95] http://www.internet-verantwortung.de/usa.html
[96] http://www.internet-verantwortung.de/leitfaden.pdf
[97] http://www.internet-verantwortung.de/empfehl.html
[98] http://www.schulen-ans-netz.de/internationales/infoletter/dokus/Infoletter0304.pdf

6.3 Filtersoftware aus den USA

Als die „großen Drei" in Sachen Filtersoftware aus den USA sind CYBERsitter, Net Nanny und SurfControl anzusehen. Die Namen dieser drei konkurrierenden Produkte werden häufig als Inbegriff für Filtersoftware verwendet. Sowohl CYBERsitter als auch Net Nanny sind für den Einsatz auf Einzelplatz-Rechnern konzipiert. SurfControl hingegen bietet neben der Filtersoftware CyberPatrol für Einzelplatz-Rechner auch einen Filter zum Schutz von Netzwerken an. Im Folgenden werden einige spezifische Merkmale der drei Produkte betrachtet.

6.3.1 CYBERsitter

CYBERsitter ist eine kommerzielle Filtersoftware für Einzelplatz-Rechner unter dem Betriebssystem Windows. Sie arbeitet basierend auf Listen (Blacklists/ Whitelists) und unterstützt auch Wortfilter. Die auf englischsprachige Webseiten optimierten Filterlisten enthalten zirka 30 Filterkategorien und lassen sich manuell durch eigene Einträge erweitern. Das Programm hat keine Userverwaltung, demnach erfolgt die Steuerung des Filterschutzes allein über die Verwendung des Kennwortes für die Software. Unterschiedliche Berechtigungen für Lehrer und Schüler können daher nicht realisiert werden.

E-Mail-Filter, Chat-Filter, Zeitsteuerung sowie eine Protokollfunktion stehen als erweiterte Features zur Verfügung. Eine einzigartige Funktion ist zudem mit der „Suche auf dem eigenen Computer" implementiert, die auch eine Kontrolle der Festplatte nach bedenklichen Inhalten erlaubt.

Das Programm sowie eine kostenlose Demoversion für zehn Tage sind auf der Webseite von CYBERsitter bereitgestellt.[99]

6.3.2 Net Nanny

Bei dem Programm Net Nanny der Firma Looksmart handelt es sich um ein kommerzielles Produkt aus den USA. Auch Net Nanny arbeitet nach dem Listen- und Wortfilterverfahren. Manuelle Einstellungen ermöglichen eine Individualisierung der Software. Neben dem Zugriff auf Internetseiten durch den Internetbrowser können auch Programme auf dem PC sowie Mail- und Chat-Dienste überwacht werden.

[99] http://www.cybersitter.com/cybinfo.htm

Durch zahlreiche Einstellungen des Programms können vier Sicherheitsstufen an die eigenen Wünsche sehr differenziert angepasst werden, was jedoch eine intensive Einarbeitung in das Programm voraussetzt. Das Programm ist multiuserfähig und verfügt zudem über die Möglichkeit, die Funktion des ICRA-Filters[100] zuzuschalten. Eine Schutzfunktion, die die Weitergabe von persönlichen Daten wie Kreditkartennummer oder Adresse in Internetformularen unterbindet, steht ebenfalls zur Verfügung.

Weitere Informationen zu Net Nanny, das in deutscher Fassung auch in dem Produkt PC Babysitter[101] enthalten ist, sowie eine kostenlose Demo-Version sind im Internet abrufbar.[102]

6.3.3 SurfControl

Der Filterhersteller SurfControl bietet mit dem gleichnamigen Produkt einen auf verschiedene Serverplattformen spezialisierten Netzwerkfilter an. SurfControl lässt sich zudem in viele professionelle Firewall-Lösungen einbinden.

Neben der Netzwerklösung wird ein zweites Produkt namens CyberPatrol[103] angeboten. Dieses Produkt ist für den Schutz von Windows-Rechnern vorgesehen und kennt vielfältige Einstellungsoptionen. So werden Black- und Whitelists, Wortfilter, Programmsperren und Protokollfunktionen angeboten. Eine eigene Userverwaltung sowie ein integriertes Zeitmanagement erlauben eine exakte Planung der Zugriffsberechtigungen.

Die englischsprachigen Filterlisten von SurfControl werden von einem eigenen Content-Team redaktionell gepflegt. Die deutschsprachigen Listen betreut ebenfalls ein eigenes Team mit Sitz in Wien. In Deutschland wird der Support durch eine Niederlassung in Frankfurt am Main angeboten. Informationen hierzu stehen im Internet zur Verfügung.[104]

[100] Siehe Kapitel 4.3.
[101] http://www.pc-babysitter.de
[102] http://www.netnanny.com
[103] http://www.cyberpatrol.com
[104] http://www.surfcontrol.com

Zusammenfassung und Ausblick

Computer und Internet haben zweifellos Einzug in unsere Gesellschaft gehalten. Die Computernutzung in Schulen etabliert sich zum festen Bestandteil des modernen Unterrichts. Der Einsatz von Lehr- und Lernsoftware lässt sich exakt an den Schulbedürfnissen ausrichten. Anders sieht es aus, sobald man die sicheren Pfade der Lernsoftware verlässt und gegen das weltweite Angebot des Internets eintauscht. Neben den sehr informativen und lehrreichen Angeboten stößt man über kurz oder lang auf jugendgefährdende Inhalte. Insbesondere sind hier pornografische, rechtsextreme oder gewaltverherrlichende Webseiten zu nennen, die - je nach Alter der Kinder - aus rechtlicher Sicht als illegal, entwicklungsbeeinträchtigend, jugendgefährdend oder - unabhängig vom Alter - sogar als absolut verbotene Inhalte einzustufen sind.

Die gesetzlichen Bestimmungen des Jugendmedienschutzes definieren daher auch an Schulen den Handlungsspielraum, in dessen Rahmen Themen und Inhalte im Unterricht verbreitet oder zugänglich gemacht werden dürfen. Schulleitungen und Lehrkräfte stehen somit vor einer rechtlichen, aber auch technisch-organisatorischen sowie pädagogischen Herausforderung, denn ihnen obliegt die Aufsichtspflicht über die Kinder.

Grundsätzlich ist es wichtig, **alle** Beteiligten - also Schülerinnen und Schüler, Eltern und Lehrkräfte - für einen präventiven Jugendmedienschutz zu sensibilisieren. In diesem Kontext wird zunehmend von der Vermittlung von Medienkompetenz durch Schule und Elternhaus gesprochen. Diese Qualifikation kann durch Aus- und Weiterbildung erworben sowie durch Aufklärungsarbeit der Medien[105] unterstützt werden.

Schulen fixieren mit den Eltern oftmals eine Nutzungsordnung,[106] um eindeutige Spielregeln für den Umgang mit dem Computerraum, den Medienecken oder dem Internetcafé der Schule aufzustellen. Sofern solche Regeln existieren, finden Lehrkräfte erste Rahmenbedingungen für die Unterrichtsgestaltung mit Computer und Internet vor.

[105] Beispielsweise durch http://www.klicksafe.de/ oder http://www.jugendschutz.net
[106] http://www.lehrer-online.de/url/nutzungsordnung

Viele Lehrerinnen und Lehrer wünschen sich zudem Unterstützungsangebote, die über das Rechtliche hinausgehen. Die Bereitstellung von altersgerechten und fachspezifischen Unterrichtsinhalten, die mithilfe des Internets vermittelt werden, kann für Lehrkräfte eine wertvolle pädagogische Unterstützung darstellen. Hierbei erweist sich der Einsatz von Filterprogrammen, die gut ausgewählt und den schulspezifischen Bedürfnissen angepasst werden müssen, als effektive technische Hilfe.

Der Einsatz von Filterlösungen an Schulen muss den spezifischen pädagogischen, rechtlichen, technischen und organisatorischen Anforderungen der Schulumgebungen gerecht werden. Zentrale Aspekte bilden dabei die altersdifferenzierte Einhaltung des Jugendmedienschutzes sowie die Förderung von Medienkompetenz der Schülerinnen und Schüler unter pädagogischen Gesichtspunkten.

Die vorliegende Broschüre hat die Rahmenbedingungen und den Einsatz von Filterprodukten aus verschiedenen Blickwinkeln beleuchtet. Die Anforderungen an eine individuelle Lösung sind so vielfältig wie die unterschiedlichen Einsatzszenarien in der Praxis. Bei dem Einsatz von Filterprogrammen in Schulen stellt sich neben der Kostenfrage immer auch die Frage von Betreuung, Aktualisierung und Wartung der jeweiligen Produkte. In der Praxis sind hier Einzellösungen durch betreuende Lehrkräfte ebenso zu finden wie Soft- oder Hardwarelösungen, die gegen eine - meist jährliche - Lizenzgebühr per Fernwartung durch einen Dienstleister weitestgehend automatisch betreut werden.

Die große Anzahl und die verschiedenen technischen Grundlagen der Filterprogramme machen deutlich, dass es die perfekte Lösung bislang kaum geben kann. Der Entscheidung für ein bestimmtes Produkt sollte immer die sorgfältige Recherche der aktuellen Produktpalette und die eingehende Beratung durch die Filterhersteller vorangehen. Neue Entwicklungen versprechen dabei immer effektivere Filterqualitäten und zeigen neue Wege zur sicheren Internetnutzung auf.

Auf verschiedenen politischen Ebenen ist das Thema derzeit ebenfalls präsent. Mit der Verabschiedung des Jugendmedienschutz-Staatsvertrags (JMStV) im April 2003 hat die Gesetzgebung die Rahmenbedingungen für eine sichere

Nutzung des Internets geschaffen und Filterprogramme als ein „technisches Mittel" zur Sicherstellung des Jugendschutzes im Internet definiert. Die Kommission für Jugendmedienschutz (KJM) ist vom Gesetzgeber beauftragt, Filterprogramme zu prüfen, zu bewerten und, bei Vorliegen der Voraussetzungen, in der Wirksamkeit durch eine Anerkennung zu bestätigen. Mehrere Hersteller von Filterprogrammen bemühen sich derzeit um eine Anerkennung ihrer Produkte durch die KJM.

Im Koalitionsvertrag vom 11. November 2005 wurden zwischen CDU, CSU und SPD weitere Schritte konkretisiert. So sollen die Neuregelungen im Jugendschutz aus dem Jahr 2003 schnellstmöglich evaluiert werden, um notwendige Konsequenzen rechtzeitig ziehen zu können.[107]

Ein bedeutender Impuls kommt zudem aus Brüssel.[108] Der Rat „Telekommunikation" der EU verabschiedete im Dezember 2004 das Programm „Mehr Sicherheit im Internet". Das von der Europäischen Kommission vorgeschlagene Vierjahresprogramm (2005-2008) ist mit 45 Millionen Euro ausgestattet und soll dem Kampf gegen illegale und schädliche Inhalte im Internet dienen.

Die Rahmenbedingen für eine sichere Nutzung des Internets wurden in Deutschland durch den Gesetzgeber gesteckt. Hersteller bieten Produkte zur technischen Unterstützung an und entwickeln diese ständig weiter. Aufklärungskampagnen sensibilisieren für das Thema - zum Beispiel durch Fernsehspots - und erreichen dadurch breite Bevölkerungsschichten.

Mit dieser Broschüre möchte der Verein Schulen ans Netz einen Beitrag dazu leisten, das Thema Jugendmedienschutz im Schulumfeld zu festigen und damit die Entwicklung für eine sichere Nutzung des Internets im schulischen Umfeld voranzutreiben und zu unterstützen.

[107] Weitere Informationen unter http://www.lehrer-online.de/dyn/500463.htm
[108] Siehe Kapitel 6.1.

Anhang

Glossar

BIOS BIOS (Basic Input Output System) bezeichnet die Funktion, die ein Computer direkt nach dem Einschalten ausführt, um ange schlossene Geräte wie Festplatte, DVD-Laufwerk oder USB-Stick zu finden.

Blacklist / Negativliste Eine Blacklist oder Negativliste enthält alle Angebote oder Wörter, deren Aufruf das Filterprogramm nicht zulässt und die somit geblockt werden.

Chat Der Chat ist ein Internetdienst, in dem mehrere Nutzer mittels Tastatur miteinander „plaudern" können (= to chat). Zu den Grundregeln im Chat gehört die anonymisierte Kommunikation über Pseudonyme oder Spitznamen.

Domain Eine Domain ist ein zusammenhängender Bestandteil einer Internet-Adresse. Beispiel: schulen-ans-netz.de

Domaingrabbing Der englische Begriff Domaingrabbing bezeichnet das Sammeln oder missbräuchliche Reservieren von Internetdomänen.

Download Bei einem Download werden Daten zum Beispiel von einem Internet-Server auf einen Heimrechner heruntergeladen (= download). Der Download ist das Gegenstück zum Upload.

Filterprogramm/ Filtersoftware Ein Filterprogramm ist in der Lage, das aufgerufene Internet-Angebot nach vorgegebenen Kriterien zu klassifizieren und dadurch erwünschte Informationen von unerwünschten zu unter scheiden. Ist eine Filtersoft-ware installiert, erhält der Benutzer nur die Informationen, die der Filter nicht abgeblockt hat.

Filter-Box Eine Filter-Box ist ein in sich geschlossenes, aus feststehenden Hard- und Softwarekomponenten bestehendes System zur Regelung des Internetzugangs.

Forum Ein Forum dient dem Austausch von Informationen zwischen den Mitgliedern einer virtuellen Gemeinschaft.

Internetdienste Das Internet wird häufig mit dem world wide web (www) gleichgestellt. In Wahrheit ist das www nur einer der „Dienste" im Internet. Zu den Internetdiensten gehören u. a. auch die E-Mail oder der Chat.

IP-Adresse Eine IP-Adresse ist eine einmalig vergebene Nummernkombination, die Computer in Netzwerken zweifelsfrei identifiziert. Die IP-Adresse besteht aus einem Zahlencode von vier Zahlen von 0 bis 255 (zum Beispiel 192.168.0.55).

LDAP LDAP ist die Abkürzung für das Lightweight Directory Access Protocol. Dieses Protokoll unterstützt einen Verzeichnisdienst.

Logdatei Eine Logdatei ist das automatisch erstellte Protokoll aller Aktionen, die von einem Nutzer an einem Rechner ausgeführt werden, zum Beispiel das Verzeichnis aller aufgerufenen Webseiten.

Netzwerk Ein Netzwerk ist ein Verbund von Computern, die über verschiedene Leitungen (Kabel oder Funknetz) verbunden sind und gemeinsam auf Daten und Geräte, wie zum Beispiel Drucker, zugreifen.

Proxy-Server Ein Proxy-Server ist ein Computer, der als Zwischenspeicher für oft aufgerufene Webseiten dient. Internetnutzer können schneller auf die dort gespeicherten Seiten zugreifen, weil nicht erst das Internet durchsucht werden muss.

Robots Robots sind Programme, die sehr schnell und weitgehend selbstständig und ohne Benutzerinteraktion Aufgaben lösen (zum Beispiel Inhalte des Internets analysieren).

Router Ein Router ist ein Vermittlungsrechner, der in einem Netzwerk dafür sorgt, dass bei ihm eintreffende Daten zum vorgesehenen Ziel(netz) weitergeleitet werden.

Self Rating / Site Labelling Das System des Self Rating funktioniert so, dass Inhaltsanbieter ihre Webseiten anhand eines nach Themen geordneten Fragenkatalogs selbstständig bewerten (= Self Rating). Diese Bewertung fügt er in den Quellcode seiner Webseiten ein (= Site Labelling), die dann von der entsprechenden Filtersoftware maschinell ausgelesen werden kann.

Server Ein Server (= Diener) ist ein Computer, der in einem Netzwerk oder im Internet seine Dienste zur Verfügung stellt, die dann von anderen vernetzten Rechnern genutzt werden können. Im Internet gibt es zum Beispiel Web-Server und Mail-Server.

URL Die URL (Uniform Resource Locator) ist die eindeutige Adresse Internetangebots, zum Beispiel http:// itworks.schulen-ans-netz.de.

Überfiltern Überfiltern, auch Overblocking genannt, bezeichnet das Filtern beziehungsweise Abblocken von unbedenklichen Inhalten, die aber von der Filtersoftware als unzulässig interpretiert und damit abgeblockt werden.

Upload Bei einem Upload werden Daten von einem Rechner zur Gegenstelle (zum Beispiel Netzrechner, Mailbox, Internet-Server) übertragen. Der Upload ist also das Gegenstück zum Download.

Whitelist / Positivliste Eine Whitelist ist eine Sammlung von Webseiten, deren Aufruf das Filterprogramm gezielt zulässt.

world wide web Das world wide web (www) ist einer der Internetdienste, in dem multimediale Dokumente wie Text-, Bild- und Tondateien von den Webservern abgerufen werden können. Um diese Dateien ansehen zu können, benötigt man einen Browser (zum Beispiel Microsoft Internet Explorer, Mozilla Firefox, Opera), der das Blättern (= to browse) in den Inhalten ermöglicht.

Worterkennung Filterprogramme, die mit dem System der Worterkennung arbeiten, suchen die angefragte Webseite nach vorher festgelegten Schlüsselwörtern ab. Findet sich ein als bedenklich kategorisiertes Wort, wird die Seite vom Filterprogramm abgeblockt.

Checklisten und Vorlagen

Alle Links sind nur einen Mausklick entfernt. Eine komplette Linkliste zu dieser Broschüre finden Sie unter:
http://itworks.schulen-ans-netz.de/publikationen.php

Checkliste: Schutz für Lehrer/Pädagogen

- www.sicher-im-netz.de/content/sicherheit/hilfreiches/downloads/checkliste_lehrer.pdf

Diese Checkliste für Pädagoginnen und Pädagogen bietet Punkt für Punkt Tipps für einen relativ sicheren Umgang mit Rechner und Internet in der Schule.

Internetverantwortung an Schulen: Ein Leitfaden

Bertelsmann Stiftung (Hrsg.), Gütersloh 2000.

- www.internet-verantwortung.de/leitfaden.pdf

Ratgeber inklusive Checklisten zur Erstellung von Verhaltensrichtlinien zur Internetnutzung an Schulen.

Muster für eine Nutzungsordnung der Computereinrichtungen an Schulen

Bildungsportal.NRW

- www.bildungsportal.nrw.de/BP/Schule/Multimedia/Internetnutzung/NutzungsordnungComputer.doc

Muster-Nutzungsordnung, die an die individuellen Voraussetzungen von Schulen angepasst werden kann.

Mustertext einer Computer-Nutzungsordnung für Schülerinnen und Schüler nebst ausführlicher Erläuterungen

Schulen ans Netz e.V., Lehrer-Online

- http://www.lehrer-online.de/url/nutzungsordnung

Lehrer-Online hat in Kooperation mit der Ludwig-Maximilians-Unversität zu München den Mustertext einer Computer-Nutzungsordung für Schülerinnen und Schüler entwickelt. Ausführliche Erläuterungen zu den einzelnen Punkten der Nutzungsordnung erklären detailliert die Bedeutung einzelner Passagen des Textes und geben Hilfestellungen zur Anpassung an den jeweiligen Bedarf.
Der gesamte Text nebst Erläuterungen steht im Internet zum Download zur Verfügung. Die Nutzungsordnung (ohne Erläuterungen) ist auf den folgenden Seiten abgedruckt.

Mustertext
Computer-Nutzungsordnung für Schülerinnen und Schüler

Vorbemerkung
Der nachfolgende Mustertext einer Nutzungsordnung bezieht sich auf Schuleinrichtungen, die Schülerinnen und Schülern im Rahmen des Unterrichts und/oder außerhalb des Unterrichts die Möglichkeit der Internetnutzung und -kommunikation einräumen (zum Beispiel Computerraum, Medienecke, Schul-Internetcafé).

Der Mustertext berücksichtigt verschiedene Nutzungsszenarien, die - zumindest in Teilbereichen - nicht beziehungsweise nicht in vollem Umfang auf jede Schule zutreffen dürften. Der Text ist also **kein allgemein gültiges Muster, sondern muss stets an die konkreten Gegebenheiten an Ihrer Schule angepasst werden**. Dabei helfen Ihnen die jeweils den einzelnen Bestimmungen zugeordneten Fußnoten, die die Bedeutung einzelner Passagen des Mustertextes erläutern und erklären, wo Änderungen vorgenommen oder Passagen gestrichen werden können. Den Text der Nutzungsordnung **einschließlich** der hier aus Platzgründen nicht abgedruckten Fußnoten finden Sie als bearbeitbare RTF-Datei unter: www.lehrer-online.de/url/nutzungsordnung

Außerdem ist es sinnvoll, Raum- und Personenbezeichnungen zu konkretisieren (beispielsweise ist an vielen Stellen des Mustertextes von der „für die Computerbenutzung an der Schule verantwortliche Person“ die Rede - hier könnte auch „der Administrator“, die „Administratorin Frau X“ oder eine andere, auf Ihre Schule zutreffende Bezeichnung / ein konkreter Name stehen).

Nutzungsordnung der Schule [Schulname]
vom [Tag].[Monat].[Jahr]

Präambel

Die nachfolgende Nutzungsordnung stellt wichtige Grundregeln im Umgang mit Computern der Schule durch Schülerinnen und Schüler auf. Insbesondere müssen Schülerinnen und Schüler darauf achten, dass

- mit den Computern der Schule und dazugehörigen Geräten sorgfältig umgegangen wird,
- die persönlichen Zugangsdaten für die Computernutzung (Passwort) geheim gehalten und ausschließlich vom jeweiligen Nutzungsberechtigten verwendet werden,
- fremde Rechte und insbesondere das Urheberrecht beachtet werden, vor allem, dass Materialien, die von anderen Personen stammen, nicht unberechtigt veröffentlicht werden und dass kein unberechtigter Download von Musikdateien, Spielen etc. erfolgt,
- illegale Inhalte weder veröffentlicht noch im Internet aufgerufen werden,
- persönliche Daten (Name, Geburtsdatum, Personenfotos) von Lehrkräften, Schülerinnen und Schülern und sonstigen Personen nicht unberechtigt im Internet veröffentlich werden.

A. Benutzung der Computer und sonstiger Hardware in der Schule

§ 1 Anwendungsbereich
Die Regelungen des Abschnitts A gelten für die Nutzung der Computer, Computerdienstleistungen und Netzwerke, die von der Schule **[Schulname]** betrieben werden. Hierzu zählen insbesondere die Nutzung der von der Schule gestellten Computer in den Computerräumen und in den Bibliotheken sowie die Nutzung zentraler Server-Dienste der Schule.

Darüber hinaus gelten die Regelungen für Computer und sonstige mit digitaler Netzwerktechnik ausgestattete digitale Endgeräte, die von den Schulangehörigen in die Schule mitgebracht werden, soweit sie nach Sinn und Zweck auch auf diese Geräte anwendbar sind.

§ 2 Nutzungsberechtigte

(1) Die in § 1 Satz 1 genannten Computer und Dienste der Schule **[Schulname]** können grundsätzlich im Rahmen der verfügbaren Kapazitäten von allen angehörigen Schülerinnen und Schülern unter Beachtung der nachfolgenden Bestimmungen genutzt werden, soweit die Computer nicht im Einzelfall besonderen Zwecken vorbehalten sind. Die Schulleitung oder in Absprache mit dieser der verantwortliche Administrator kann weitere Personen zur Nutzung zulassen (z.B. Gastschüler). Die Benutzung kann eingeschränkt, (zeitweise) versagt oder (zeitweise) zurückgenommen werden, wenn nicht gewährleistet erscheint, dass die betreffende Schülerin oder der betreffende Schüler ihren bzw. seinen Pflichten als Nutzer nachkommen wird.

(2) Mit ihrer Zulassung wird den nach Absatz 1 nutzungsberechtigten Schülerinnen und Schülern ein Benutzerausweis ausgestellt. Sie haben der aufsichtsführenden Person den Benutzerausweis auf Verlangen vorzuzeigen.

§ 3 Zugangsdaten

(1) Alle gemäß § 2 berechtigten Schülerinnen und Schüler erhalten für den Zugang zu den Computersystemen der Schule und zum schulischen Netzwerk jeweils eine individuelle Nutzerkennung und wählen sich ein Passwort (Zugangsdaten). Mit diesen Zugangsdaten können sie sich an allen zugangsgesicherten Computersystemen der Schule anmelden. Das Computersystem, an dem sich ein Nutzer im Netz angemeldet hat, ist aus Sicherheitsgründen durch diesen niemals unbeaufsichtigt zu lassen. Nach Beendigung der Nutzung hat sich der Nutzer an seinem Computersystem ordnungsgemäß abzumelden.

(2) Die Nutzer haben ihre Passworte in einer die Sicherheit des Systems wahrenden Weise zu wählen. Passworte müssen daher aus einer Folge von 8 bis 10 Zeichen bestehen und sowohl Buchstaben als auch Ziffern oder Sonderzeichen enthalten.

§ 4 Datenschutz der Zugangsdaten

(1) Die im Rahmen der Zuteilung der Zugangsdaten erhobenen persönlichen Daten der Schülerinnen und Schüler (z.B. Name, Klassenzugehörigkeit) werden von Seiten der Schule nicht an Dritte weitergegeben, es sei denn, die Weitergabe erfolgt in Erfüllung einer gesetzlichen Verpflichtung (z.B. im Rahmen von strafrechtlichen Ermittlungen); in diesem Falle werden nur solche Informationen weitergegeben, zu deren Weitergabe die Schule gesetzlich verpflichtet ist.

(2) Mit der Anerkennung der Nutzungsordnung erklärt sich der Nutzer - bei minderjährigen Schülerinnen und Schülern in gesetzlicher Vertretung durch zusätzliche Einwilligung einer personensorgeberechtigten Person - zugleich einverstanden, dass die Schule berechtigt ist, seine persönlichen Daten im Rahmen der geltenden Datenschutzbestimmungen zu speichern.

§ 5 Passwortweitergabe

(1) Die Schülerinnen und Schüler sind verpflichtet, ihr Passwort geheim zu halten. Dieses darf insbesondere nicht an andere Personen weitergegeben werden und ist vor dem Zugriff durch andere Personen geschützt aufzubewahren. Die für die Computernutzung in der Schule verantwortliche Person ist unverzüglich zu informieren, sobald dem Nutzer bekannt wird, dass sein Passwort unberechtigt durch andere Personen genutzt wird. Die Schulleitung ist berechtigt, die Zugangsdaten eines Nutzers unverzüglich zu sperren, wenn der begründete Verdacht besteht, dass das Passwort durch unberechtigte Personen genutzt wird; der betroffene Nutzer wird hierüber informiert und erhält ein neues Passwort zugeteilt, soweit er nicht selbst bewusst zu dem Missbrauch beigetragen hat.

(2) Das Arbeiten unter einem fremden Passwort („Passwort-Sharing“) ist untersagt. Wer ein fremdes Passwort erfährt, ist verpflichtet, dies der Schulleitung oder der für die Computernutzung verantwortlichen Person mitzuteilen.

§ 6 Schulorientierte Nutzung

Die schulische IT-Infrastruktur (z.B. schulische Computersysteme, Internetzugang, Software, Peripheriegeräte wie Drucker oder Scanner) darf nur für schulische Zwecke genutzt werden. Als Nutzung zu schulischen Zwecken ist neben Arbeiten im Rahmen des Unterrichts sowie der Vor- und Nachbereitung des Unterrichts z.B. auch die Nutzung zum Zwecke der Ausbildungs- und Berufsorientierung und der politischen, zeitgeschichtlichen, technischen oder sprachlichen Weiterbildung sowie ein elektronischer Informationsaustausch anzusehen, der unter Berücksichtigung seines Inhalts und des Adressatenkreises mit der schulischen Arbeit im Zusammenhang steht.

§ 7 Gerätenutzung

(1) Die Bedienung der von der Schule gestellten oder erlaubterweise von Schülerinnen und/oder Schülern mitgebrachten privaten stationären oder portablen Computer einschließlich jedweder Hard- und Software hat entsprechend den Anweisungen der aufsichtsführenden Lehrkraft oder sonstigen Aufsichtsperson oder der für die Computernutzung verantwortlichen Person zu erfolgen.

(2) Gegenüber den nach § 2 nutzungsberechtigten Schülerinnen und Schülern, welche die Geräte entgegen den Instruktionen und Anweisungen der aufsichtsführenden Person nutzen, können geeignete Aufsichtsmaßnahmen ergriffen werden, damit die Betriebssicherheit aufrechterhalten bzw. wieder hergestellt werden kann. In Betracht kommt insbesondere die Untersagung der weiteren Nutzung der Geräte auf Dauer oder für einen bestimmten Zeitraum.

(3) Die Schülerinnen und Schüler sind zum sorgsamen Umgang mit den von der Schule gestellten Geräten verpflichtet. Insbesondere sind die Computertastaturen vor Beschmutzungen oder Kontaminierung mit Flüssigkeiten zu schützen. Das Essen und Trinken während der Nutzung der von der Schule gestellten Computer ist untersagt.

(4) Nach Beendigung der Nutzung muss der Raum ordnungsgemäß verlassen werden. Dabei ist jeder Nutzer für seinen Arbeitsplatz verantwortlich (PC ordnungsgemäß herunterfahren, Gerät/Monitor ausschalten, Arbeitsplatz aufräumen, Stuhl ordentlich an den Tisch stellen).

§ 8 Beschädigung der Geräte

Störungen oder Schäden an den von der Schule gestellten Computern sind der aufsichtsführenden Person oder der für die Computernutzung verantwortlichen Person unverzüglich zu melden. Die vorsätzliche Beschädigung von Sachen ist strafbar und kann zur Anzeige gebracht werden. Wer schuldhaft Schäden verursacht, hat diese zu ersetzen. Darüber hinaus kann der handelnden Person die weitere Nutzung dieser Geräte auf Dauer oder für einen bestimmten Zeitraum untersagt werden.

§ 9 Sonstige Einwirkung auf Geräte oder gespeicherte Daten

(1) Veränderungen der Installation und Konfiguration der von der Schule gestellten Computersysteme und des Netzwerkes (z.B. durch das Einschleusen von Viren, Würmern oder Trojanischen Pferden) sowie Manipulationen an der schulischen Hardwareausstattung sind untersagt. Fremdgeräte (insbesondere private Notebooks oder sonstige mit drahtgebundenen oder drahtlosen Netzwerktechniken ausgestattete digitale Endgeräte) dürfen nicht ohne Zustimmung der aufsichtsführenden Lehrkraft oder der für die Computernutzung verantwortlichen Person an Computersysteme der Schule oder an das schulische Netzwerk angeschlossen werden. Das Ein- und Ausschalten der von der Schule gestellten Computersysteme erfolgt ausschließlich durch die aufsichtsführende Lehrkraft bzw. die für die Computernutzung verantwortliche Person oder mit deren ausdrücklicher Zustimmung.

(2) Das Verändern, Löschen, Entziehen oder sonstige Unbrauchbarmachen von Daten, die auf den von der Schule gestellten Computern von anderen Personen als dem jeweiligen Nutzer gespeichert wurden, ist grundsätzlich untersagt. Automatisch geladene Programme (wie Virenscanner) dürfen nicht deaktiviert oder beendet werden. Ausnahmsweise darf eine Veränderung oder Löschung solcher Daten auf Anweisung oder mit Zustimmung der aufsichtsführenden Lehrkraft oder der für die Computernutzung verantwortlichen Person erfolgen, wenn hierdurch keine Rechte dritter Personen (z.B. Urheberrechte, Datenschutz) verletzt werden. Dies ist insbesondere dann der Fall, wenn die Datenlöschung oder -veränderung im Einvernehmen mit dem Berechtigten erfolgt.

(3) Die Installation von Software - egal in welcher Form - auf den von der Schule gestellten Computern ist nur nach Genehmigung durch die für die Computernutzung verantwortliche Person zulässig.

§ 10 Kosten

Die Nutzung der Computerarbeitsplätze und die Bereitstellung des Zugangs zum Internet stehen den nutzungsberechtigten Schülerinnen und Schülern kostenfrei zur Verfügung. Für das Drucken werden folgende Kosten berechnet: pro DIN A4-Seite - **[.....]** €; pro DIN A3 Seite - **[.....]** € . Die Druckkosten werden über das Schuljahr summiert und am Ende des Schuljahres dem Nutzer individuell in Rechnung gestellt.

B. Abruf von Internet-Inhalten

§ 11 Verbotene Nutzungen

Die gesetzlichen Bestimmungen, insbesondere des Strafrechts, Urheberrechts und des Jugendschutzrechts, sind zu beachten. Es ist vor allem verboten, pornografische, gewaltverherrlichende, rassistische oder sonst jugendgefährdende Inhalte (z.B. nach dem Jugendschutzgesetz indizierte oder die Menschenwürde verletzende Inhalte) aufzurufen oder zu speichern. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu

schließen und der aufsichtsführenden Lehrkraft oder der für die Computernutzung verantwortlichen Person unverzüglich Mitteilung zu machen.

§ 12 Download von Internet-Inhalten

(1) Der Download, d.h. das Kopieren von Dateien (vor allem von Musikstücken und Filmen), die in so genannten File-Sharing-Netzwerken angeboten werden, ist untersagt. Auch die Umgehung von Kopierschutzmechanismen ist generell nicht erlaubt. Im Übrigen sind für Kopien die gesetzlichen Schrankenbestimmungen der §§ 44a ff. UrhG zu beachten.

(2) Die Installation von heruntergeladenen Anwendungen auf von der Schule zur Verfügung gestellten Computern ist entsprechend § 9 Absatz 3 nur nach Genehmigung durch die für die Computernutzung verantwortliche Person zulässig. Unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien (z.B. Grafiken ab einem Datenvolumen von 100 KB) aus dem Internet ist zu vermeiden. Sollte ein Nutzer außerhalb schulischer Zwecke oder sonst unberechtigt Daten in seinem Arbeitsbereich ablegen, ist die Schulleitung bzw. die für die Computernutzung zuständige Person berechtigt, diese Daten zu löschen.

§ 13 Online-Abschluss von Verträgen; kostenpflichtige Angebote

Schülerinnen und Schüler dürfen im Rahmen der Nutzung von Internetinhalten weder im Namen der Schule noch im Namen anderer Personen oder selbstverpflichtend Vertragsverhältnisse aufgrund von Angeboten in Informations- und Kommunikationsdiensten eingehen. Ohne Erlaubnis der Schulleitung dürfen des Weiteren keine für die Schule kostenpflichtigen Dienste im Internet in Anspruch genommen werden.

C. Veröffentlichung von Inhalten im Internet

§ 14 Illegale Inhalte

(1) Es ist untersagt, pornografische, gewaltverherrlichende, rassistische, jugendgefährdende, beleidigende oder sonst strafrechtlich verbotene Inhalte im Internet zu veröffentlichen, zu versenden oder sonst zugänglich zu

machen. Ferner dürfen Inhalte, die dem Ansehen oder dem Erscheinungsbild der Schule schaden, nicht verbreitet werden.

(2) Kommerzielle und parteipolitische Werbung sind untersagt, soweit die Schulleitung oder eine von ihr autorisierte Person sie nicht im Einzelfall in Übereinstimmung mit den einschlägigen Regelungen zulässt.

§ 15 Veröffentlichung fremder urheberrechtlich geschützter Inhalte
Texte, (gescannte) Bilder oder sonstige urheberrechtlich geschützte fremde Inhalte (z.B. Audio- und Videodateien) dürfen nur mit Zustimmung des Urhebers oder der sonstigen Rechteinhaber im Internet zum Abruf bereitgestellt, also veröffentlicht werden. Gemeinfreie Werke (insbesondere amtliche Fassungen von Gesetzen, Verordnungen, Erlassen und Bekanntmachungen sowie Werke, bei denen die Schutzfrist abgelaufen ist) dürfen jedoch ohne Erlaubnis im Internet veröffentlicht werden. Ist in einem Einzelfall zweifelhaft, ob Urheberrechte durch eine Veröffentlichung verletzt werden, ist entweder die zuständige Lehrkraft [z.B. Klassenlehrer(in)] oder - soweit vorhanden - die Internetbeauftragte bzw. der Internetbeauftragte vor der Veröffentlichung zu kontaktieren.

§ 16 Beachtung von Bildrechten
Das Recht am eigenen Bild ist zu beachten. Die Veröffentlichung von Fotos im Internet ist nur gestattet mit der Genehmigung der abgebildeten Personen, im Falle der Minderjährigkeit auch von deren Erziehungsberechtigten.

§ 17 Schulhomepage
Nach § 2 nutzungsberechtigte Schülerinnen und Schüler dürfen Inhalte auf der Schulhomepage nur mit Zustimmung der Schulleitung oder der für die Computernutzung zuständigen Person veröffentlichen. Die Veröffentlichung von Internetseiten im Namen oder unter dem Namen der Schule bedarf stets der Genehmigung durch die Schulleitung oder einer durch sie autorisierten Person. Dies gilt auch im Falle von Veröffentlichungen

außerhalb der Schulhomepage - etwa im Rahmen von Schul- oder Unterrichtsprojekten.

§ 18 Verantwortlichkeit

Die nach § 2 nutzungsberechtigten Schülerinnen und Schüler sind für die von ihnen im Internet veröffentlichten Inhalte und Äußerungen innerhalb der gesetzlichen Grenzen (z.B. Vorliegen der Strafmündigkeit ab 14 Jahren; zivilrechtliche Deliktsfähigkeit) verantwortlich, soweit sie nicht glaubhaft machen können, dass ein Missbrauch ihrer Nutzerkennung durch andere Personen - etwa nach vorher vergessener Abmeldung des nach § 2 Nutzungsberechtigten - stattgefunden hat. Gegenüber der verantwortlichen Schülerin oder dem verantwortlichen Schüler können Maßnahmen nach § 2 Satz 3 und § 5 Absatz 1 Satz 3 und 4 ergriffen werden.

§ 19 Bekanntgabe persönlicher Daten im Internet

Schülerinnen und Schülern ist es untersagt, ihre persönlichen Daten (z.B. Telefonnummer, Adresse, E-Mail-Adresse oder Ähnliches) oder Personenfotos ohne Einwilligung der aufsichtsführenden Lehrkraft oder der für die Computernutzung verantwortlichen Person im Internet, etwa in Chats oder Foren, bekannt zu geben.

D. Datenschutz, Fernmeldegeheimnis

§ 20 Aufsichtsmaßnahmen, Administration

(1) Die Schule ist zur Erfüllung ihrer Aufsichtspflicht berechtigt, den Datenverkehr zu speichern und zu kontrollieren. Darüber hinaus können bei der Inanspruchnahme von schulischen Computersystemen oder Netzwerken die zur Sicherung des Betriebs, zur Ressourcenplanung, zur Verfolgung von Fehlerfällen und zur Vermeidung von Missbrauch erforderlichen personenbezogenen Daten elektronisch protokolliert werden. Die für die Administration zuständige Person ist berechtigt, zum Zwecke der Aufrechterhaltung eines ordnungsgemäßen Netzwerkbetriebes (z.B. technische Verwaltung des Netzwerkes, Erstellung zentraler Sicherungskopien, Behebung von Funktionsstörungen) oder zur Vermeidung

von Missbräuchen (z.B. strafbare Informationsverarbeitung oder Speicherung) Zugriff auf die Daten der Nutzer zu nehmen, sofern dies im jeweiligen Einzelfall erforderlich ist. Gespeicherte Daten werden in der Regel nach einem Monat, spätestens jedoch zu Beginn eines jeden neuen Schuljahres gelöscht. Dies gilt nicht, wenn Tatsachen den Verdacht eines schwer wiegenden Missbrauches der schulischen Computer begründen. Die Schule wird von ihren Einsichtsrechten nur in Fällen des Verdachts von Missbrauch und bei verdachtsunabhängigen Stichproben Gebrauch machen.

(2) Die Wahrung des Fernmeldegeheimnisses im Sinne des § 88 TKG wird gewährleistet.

(3) Die für die Computerinfrastruktur Verantwortlichen haben die ihnen im Zusammenhang mit ihrer Tätigkeit für die vorgenannten Systeme bekannt gewordenen Daten geheim zu halten. Zulässig sind Mitteilungen, die zum Betrieb der Rechner und Dienste, zur Erstellung von Abrechnungen, zur Anzeige strafbarer Handlungen und zur Durchführung von Ordnungsmaßnahmen erforderlich sind.

E. Ergänzende Regeln für die Nutzung außerhalb des Unterrichtes

§ 21 Nutzungsberechtigung

(1) Schülerinnen und Schüler dürfen außerhalb des Unterrichts in den Räumen **[…]** und in der Medienecke des Foyers **[…]** die dort aufgestellten Computer in der Zeit von **[…]** bis **[…]** nutzen, wenn sie einen Benutzerausweis (§ 2 Abs. 2) bei sich führen.

Eigenes Arbeiten am Computer außerhalb des Unterrichts ist für Schülerinnen und Schüler nur unter Aufsicht und nur mit Benutzerausweis möglich. Schülerinnen und Schülern unter 14 Jahren ist eine Nutzung außerhalb des Unterrichts nur bei Anwesenheit einer Lehrperson oder einer sonstigen für die Computernutzung verantwortlichen Person gestattet.

(2) Ausnahmsweise kann darüber hinaus außerhalb des Unterrichts im Rahmen der medienpädagogischen Arbeit Schülerinnen und Schülern ein weitergehendes Recht zur Nutzung der Schulcomputer und der Netzwerkinfrastruktur im Einzelfall gewährt werden. Die Entscheidung darüber und auch in Bezug darauf, welche Dienste genutzt werden können, trifft die Schulleitung unter Beteiligung der schulischen Gremien.

(3) § 6 (schulorientierte Nutzung) bleibt unberührt.

§ 22 Aufsichtspersonen

Als weisungsberechtigte Aufsicht können neben Lehrkräften und sonstigen Bediensteten der Schule auch Eltern und für diese Aufgabe geeignete, insbesondere volljährige Schülerinnen und Schüler eingesetzt werden. Sie werden von **[Name des Verantwortlichen]** in den Aufsichtsplan eingetragen, der **[Ort]** aushängt.

G. Schlussvorschriften

§ 23 Inkrafttreten, Nutzerbelehrung

(1) Diese Nutzungsordnung ist Bestandteil der jeweils gültigen Hausordnung und tritt am Tage nach ihrer Bekanntgabe durch Aushang in der Schule in Kraft. Alle nach § 2 Nutzungsberechtigten werden über diese Nutzungsordnung unterrichtet. Einmal zu jedem Schuljahresbeginn findet eine Aufklärungs- und Fragestunde hinsichtlich der Inhalte der Nutzungsordnung statt, die im Klassenbuch protokolliert wird.

(2) Die nach § 2 nutzungsberechtigten Schülerinnen und Schüler, im Falle der Minderjährigkeit außerdem ihre Erziehungsberechtigten, versichern durch ihre Unterschrift (siehe Anhang), dass sie diese Nutzungsordnung anerkennen. Dies ist Voraussetzung für die Nutzung.

§ 24 Verstöße gegen die Nutzungsordnung

Schülerinnen und Schüler, die unbefugt Software von den Arbeitsstatio-

nen oder aus dem Netz kopieren oder verbotene Inhalte nutzen, können gegebenenfalls zivil- oder strafrechtlich verfolgt werden. Zuwiderhandlungen gegen diese Nutzungsordnung können neben dem Entzug der Nutzungsberechtigung für das Netz und die Arbeitsstation schulordnungsrechtliche Maßnahmen zur Folge haben.

§ 25 Haftung der Schule

(1) Es wird keine Garantie dafür übernommen, dass die Systemfunktionen den speziellen Anforderungen des Nutzers entsprechen oder dass das System fehlerfrei oder ohne Unterbrechung läuft.

(2) Aufgrund der begrenzten Ressourcen können insbesondere die jederzeitige Verfügbarkeit der Dienstleistungen sowie die Integrität und die Vertraulichkeit der gespeicherten Daten ungeachtet der sich aus § 20 ergebenden Pflichten nicht garantiert werden. Die Nutzer haben von ihren Daten deswegen Sicherheitskopien auf externen Datenträgern anzufertigen.

(3) Die Schule haftet vertraglich im Rahmen ihrer Aufgaben als Systembetreiber nur, soweit ihr, den gesetzlichen Vertretern, Erfüllungsgehilfen oder Dienstverpflichteten ein vorsätzliches oder grob fahrlässiges Verhalten zur Last fällt. Im Falle leichter Fahrlässigkeit ist eine Haftung der Schule sowie ihrer jeweiligen gesetzlichen Vertreter, Erfüllungsgehilfen oder Dienstverpflichteten bei Vermögensschäden hinsichtlich mittelbarer Schäden, insbesondere Mangelfolgeschäden, unvorhersehbarer Schäden oder untypischer Schäden sowie entgangenen Gewinns ausgeschlossen. Bei Vermögensschäden im Falle leichter Fahrlässigkeit ist die Haftung jedenfalls auf einen Höchstbetrag von EUR 2.000 begrenzt.

§ 26 Änderung der Nutzungsordnung, Wirksamkeit

(1) Die Schulleitung behält sich das Recht vor, diese Nutzungsordnung jederzeit ganz oder teilweise zu ändern. Über Änderungen werden alle Nutzer durch Aushang informiert. Die Änderungen gelten grundsätzlich als genehmigt, wenn der jeweilige Nutzer die von der Schule gestellten

Computer und die Netzinfrastruktur nach Inkrafttreten der Änderungen weiter nutzt. Werden durch die Änderungen Datenschutzrechte oder sonstige erhebliche persönliche Rechte der Nutzer betroffen, wird erneut die schriftliche Anerkennung der geänderten Nutzungsbedingungen bei den Nutzern eingeholt. Bei Änderungen der Nutzungsordnung, welche die Rechte minderjähriger Nutzer beeinträchtigen, wird in jedem Fall die Einwilligung der personensorgeberechtigten Personen eingeholt.

(2) Sollten einzelne Bestimmungen dieser Nutzungsordnung ganz oder teilweise unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

Anhang

Anerkennung der Nutzungsordnung und Einwilligung in die Verwendung personenbezogener Daten

für:

_____ _____

[Vorname des Schülers/der Schülerin] **[Nachname des Schülers/der Schülerin]**

1. Hiermit erkläre(n) ich/wir, die Nutzungsordnung der Schule **[Name der Schule]** vom **[Datum]** vollständig gelesen zu haben und einschließlich der darin enthaltenen Bestimmungen über den Datenschutz und das Fernmeldegeheimnis durch Unterschrift anzuerkennen.

2. Darüber hinaus willige(n) ich/wir in die in § 4 der Nutzungsverordnung genannte Verwendung von personenbezogenen Daten ohne weitere Genehmigung ein.

_____

[Ort, Datum]

_____ _____

[Unterschrift des Schülers/der Schülerin] **[Unterschriften der Erziehungsberechtigten]**

Hinweis

Die rechtliche Situation im Bereich des Internet-Rechts unterliegt in weiten Bereichen einem raschen Wandel und ist darüber hinaus noch in vielen Bereichen unklar. Der vorliegende Mustertext stellt deswegen lediglich eine erste Hilfestellung dar, und darf nur unter Berücksichtigung möglicher Besonderheiten des jeweiligen Einzelfalles angewendet werden. Vor der Verwendung des Mustertextes sollten daher in jedem Falle die im Rechtsportal von Lehrer-Online abrufbaren Hintergrundinformationen beachtet werden. In Zweifelsfällen sollte stets ein entsprechend spezialisiertes Anwaltsbüro hinzugezogen werden.

Die vorstehenden Angaben erfolgen ohne Gewähr. Der Mustertext gibt die Auffassung der Redaktion Recht bei Lehrer-Online wieder. In dem sich rasch entwickelnden Gebiet des Internetrechts sind abweichende oder dem Mustertext widersprechende Entscheidungen der Rechtsprechung durchaus möglich. Die Autoren und der Verein Schulen ans Netz übernehmen deswegen keine Haftung für die Richtigkeit des Mustertextes und der darin enthaltenen rechtlichen Hinweise.

Literatur

Chatten ohne Risiko?
Zwischen fettem Grinsen und Cybersex
Jugendschutz.net - Jugendschutz in Telemedien (Hrsg.), 2. Auflage 2005
- www.jugendschutz.net/pdf/chatten_ohne_Risiko.pdf

Der praxisorientierte Ratgeber richtet sich an Eltern und Pädagoginnen und Pädagogen und gibt Tipps, worauf Kinder und Jugendliche beim Chatten achten sollten.

Chatten Surfen Mailen - Computer- und Internetnutzung von Kindern und Jugendlichen
Evangelische Familienbildungsstätte Hannover, Landesstelle Jugendschutz Niedersachsen (Hrsg.), Hannover 2005
Das niedersächsische Modellprojekt „aktion familien online" wird von der Landesstelle Jugendschutz und der Evangelischen Familienbildungsstätte Hannover durchgeführt und möchte Eltern und Multiplikatoren Unterstützung beim Umgang mit neuen Medien geben. Neben Hintergrundinformationen zu den Themen Kinder und Internet sowie Kinder und Computerspiele sind zahlreiche Tipps für die praktische Arbeit enthalten.

Ein Netz für Kinder - Surfen ohne Risiko?
Bundesministerium für Familie, Senioren, Frauen und Jugend (Hrsg.),
Ersterscheinung 2000
- www.bmfsfj.de/Kategorien/Publikationen/Publikationen,did=4712.html

Die vom Bundesministerium für Familie, Senioren, Frauen und Jugend herausgegebene Broschüre kann hier als PDF-Datei heruntergeladen werden.
Seit 2000 ist die Broschüre mehrfach überarbeitet worden; eine komplette Neuauflage wird voraussichtlich Mitte 2006 erscheinen.

Experimentelle Bewertung von Blocking- und Filtersystemen im Internet
Ein Vergleich der Systeme von Net Nanny, Cyber Patrol, CYBERsitter und Surf Watch

Tröndle, M., Diplomarbeit im Fach Informationswissenschaft an der Universität Konstanz, Konstanz August 1999

- http://www.ub.uni-konstanz.de/v13/volltexte/2000/561//pdf/troendle.pdf

Tröndle beschäftigt sich in seiner Arbeit mit der experimentellen Bewertung der Blocking- und Filtersysteme Net Nanny, Cyber Patrol, CYBERsitter und Surf Watch im Internet.

Funktionsweise des Internets und sein Gefährdungspotenzial für Kinder und Jugendliche
Ein Handbuch zur Medienkompetenzvermittlung

Volpers, Helmut (Hrsg.), NLM-Band 17, vistas Medienverlag, Berlin 2004

Das Handbuch vermittelt die Funktionsweise und Vielfalt des Internets, informiert über die Gefahrenstellen und nennt Optionen zum Jugendmedienschutz, indem es sowohl Filtersoftware als auch Materialien zur Medienkompetenzvermittlung beschreibt.

Gespenst oder Schutzengel
Filter-, Abblock- und Rating-Verfahren im Internet
UNESCO darf nicht bloß zuschauen

Kuhlen, Rainer, erschienen in UNESCO heute, 1/2000

- www.inf-wiss.uni-konstanz.de/People/RK/Publikationen1995-2000/unesco_heute00.pdf

Rainer Kuhlen ist Vorsitzender des Fachausschusses Kommunikation und Information der deutschen UNESCO-Kommission sowie Inhaber des UNESCO-ORBICOM-Chairs in Communications für Deutschland. Seine Schwerpunkte im Rahmen der UNESCO sind Informationsethik, kulturelle und sprachliche Vielfalt, Informationskompetenz und Urheberrecht.

internet abc - Wissen, wie's geht

Internet-ABC e.V. (Hrsg.), Düsseldorf 2006

Die CD-ROM ist für Lehrer und Eltern gedacht, die Kindern im Grundschulalter kompetent und anschaulich den Weg ins world wide web weisen möchten. Zu Themen wie Sicherheit und Risiken beim Surfen im Netz, E-Mail, Chatten, Umgang mit Suchmaschinen oder Viren bietet sie zahlreiche Unterrichtsmaterialien, Informationen und Tipps. Kostenlose Bestellmöglichkeit unter www.internet-abc.de

Internet für Kinder
Hilfen für Eltern, Erzieher und Lehrer
Deutsches Jugendinstitut - DJI / Feil, Christine (Hrsg.), Opladen 2001
Die Autorin fasst die Ergebnisse des 1999-2000 vom Deutschen Jugendinstitut durchgeführten Projekts „Internet - außerschulische Lernangebote für Kinder und Jugendliche bis zum 14. Lebensjahr" zusammen. Die dokumentierten Ergebnisse richten sich an Eltern, Erzieher und Pädagogen, die sich unter medienpädagogischen Aspekten über die Bedeutung des Internets im Alltag der Kinder und das entsprechende Webangebot informieren wollen.

JIM-Studie 2004, Jugend, Information, (Multi-) Media, Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger
mpfs medienpädagogischer forschungsverbund südwest
- www.mpfs.de/studien/jim/Brosch%FCre%20JIM%2004.pdf

Seit 1998 wird mit der JIM-Studie jährlich eine Basisstudie zum Umgang von 12- bis 19-Jährigen mit Medien und Information durchgeführt. Neben einer aktuellen Standortbestimmung sollen die Daten zur Erarbeitung von Strategien und Ansatzpunkten für neue Konzepte in den Bereichen Bildung, Kultur und Arbeit dienen.

Jugendmedienschutz
Sicherer Umgang mit den neuen Medien in der Schule
Schulen ans Netz e.V. (Hrsg.), Bonn 2004
- www.schulen-ans-netz.de/service/publikationen/jugendmedienschutz.php

Die Broschüre gibt einen Überblick über pädagogische, rechtliche und technische Aspekte. Außerdem informiert sie über Erfahrungen und Lösungsansätze aus der Praxis und enthält Unterrichtsvorlagen und Linktipps. Bestellmöglichkeit gegen Schutzgebühr unter www.schulen-ans-netz.de/service/publikationen/jugendmedienschutz.php

Jugendschutz und Filtertechnologien im Internet

Eine Untersuchung der Secorvo Consulting GmbH im Auftrag des Projektträgers Multimedia des Bundesministeriums für Wirtschaft und Technologie (BMWi), 1999

- www.secorvo.de/publikationen/secorvo-studie-jugendschutz.zip

Die Studie zeigt eine Übersicht über verfügbare technische Lösungen zur Umsetzung von Jugendschutz-Maßnahmen beim Zugriff auf das Internet unter Berücksichtigung des rechtlichen Rahmens und der psychologisch-sozialen Durchsetzbarkeit. Die Studie enthält zudem sehr ausführliche Hintergrundinformationen.

Kinder- und Jugendmedienschutz
Eine kommentierte Linksammlung

Staatsinstitut für Schulqualität und Bildungsforschung (ISB) (Hrsg.), 2005

- www.isb.bayern.de/isb/index.asp?MNav=2&QNav=5&TNav=1&INav=0&Pub=680

Die Linksammlung bietet einen Überblick über relevante Gremien und Institutionen des Jugendmedienschutzes, verweist auf die dem Jugendmedienschutz zugrunde liegenden gesetzlichen Grundlagen und stellt Möglichkeiten der Prävention durch Filtersoftware vor.

Multimedia-Empfehlungen Baden-Württemberg

Gemeindetag, Landkreistag, Städtetag und Ministerium für Kultus, Jugend und Sport Baden Württemberg (Hrsg.), Stuttgart 2002

- www.support-netz.de/mme.html

Empfehlungen für die Ausstattung der weiterführenden allgemein bildenden und beruflichen Schulen mit Multimedia, die Vernetzung der Schulen und die Sicherstellung des laufenden Betriebs der Schulnetze.

Technischer Schutz vor Internetschmutz:
Filterprogramme, die effektive Lösung für den Jugendschutz im Internet?

Gleis, Andreas**,** Mitteilungen des Landesjugendamts Nr. 151, Münster 2002

- www.lwl.org/lja-download/pdf/Technischer_Schutz_vor_Internetschmutz.pdf

In seinem Beitrag informiert der Autor über Funktionsweisen von Filtersoftware, ihre Vor- und Nachteile sowie pädagogische Strategien für eine sichere Internetnutzung.

Verantwortung im Internet - Selbstregulierung und Jugendschutz
Waltermann, Jens / Machill, Marcel, Verlag Bertelsmann Stiftung (2000)
In diesem Band werden die Ergebnisse einer repräsentativen Internet-Nutzer-Befragung in Deutschland, Australien und den USA zum Thema Selbstregulierung und Jugendschutz im Internet vorgestellt. Im Service-Teil enthalten ist eine ausführliche Bibliografie maßgeblicher englisch-, deutsch- und französischsprachiger Publikationen zu den behandelten Themen.

Links

Alle in dieser Broschüre enthaltenen Links sind nur einen Mausklick entfernt.
Eine komplette Linkliste zu dieser Broschüre finden Sie unter:
http://itworks.schulen-ans-netz.de/publikationen.php

Nationale Institutionen / Organisationen / Projekte

Aktion Jugendschutz Landesarbeitsstelle Bayern e.V.

- www.bayern.jugendschutz.de

Die Seite bietet umfangreiche Informationen zum Thema Medienpädagogik und Jugendmedienschutz sowie Internet-Tipps für Eltern und Kinder.

Bildungsportal NRW

- www.bildungsportal.nrw.de/BP/Jugend/KuJNRW/Jugendschutz/index.html

Im Bereich „Service Kinder und Jugend" bietet das Portal Infos zum Thema Jugendschutz und Medienkompetenz sowie zahlreiche weiterführende Links.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- www.bsi-fuer-buerger.de

Sehr umfassende Informationen rund um das Thema IT-Sicherheit.

Bundesarbeitsgemeinschaft Kinder- und Jugendschutz (BAJ)

- www.bag-jugendschutz.de/index-baj.html

Unter der Adresse www.handbuch-jugendschutz.de bietet die BAJ ein „Online-Handbuch" an, das wichtige Begriffe des Kinder- und Jugendschutzes erläutert. Neben den zurzeit 120 Begriffserläuterungen gibt es Hinweise auf Literatur und weitere Quellen, die laufend aktualisiert und ergänzt werden. Es wurde im Fachbereich Bildungswissenschaften erarbeitet und wird in Kooperation mit der Bundesarbeitsgemeinschaft Kinder- und Jugendschutz in Berlin zu einem zentralen Informationsinstrument ausgebaut.

Bundesprüfstelle für jugendgefährdende Medien

- www.bundespruefstelle.de

Informationen über Aufgaben und Organisation der BpjM, den Ablauf von Indizierungsverfahren, rechtliche Gundlagen und mehr.

Bundeszentrale für politische Bildung (BpB)

- www.bpb.de

Die BpB hält besondere Angebote für Lehrerinnen, Lehrer und Personen in der Bildungs- und Jugendarbeit bereit und bietet zahlreiche Informationen zum Thema Medienpädagogik.

Freiwillige Selbstkontrolle Multimedia-Diensteanbieter

- www.fsm.de

Die FSM betreibt eine Beschwerdestelle, an die sich jedermann kostenlos mit Beschwerden über Inhalte von Webseiten innerhalb des world wide web wenden kann. Darüber hinaus findet man dort Infos zu Funktionsweisen diverser Filtersoftware.

Gesellschaft für Medienpädagogik und Kommunikationskultur (GMK)

- www.gmk-net.de

Die GMK ist deutscher Netzknotenpunkt der Kampagne S@ferinternet. Auf ihrer Webseite finden Sie weitere Informationen und Materialien zum Download und Bestellen.

Internauten

- www.internauten.de

Die Internauten sind ein Internetangebot der Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., dem Deutschen Kinderhilfswerk e.V. und MSN Deutschland GmbH. Die Webseite richtet sich speziell an Kinder und Jugendliche und möchte dazu beitragen, deren Medienkompetenz zu fördern.

jugendschutz.net

- www.jugendschutz.net

Die von den Jugendministerinnen und Jugendministern der Länder eingerichtete staatliche Stelle jugendschutz.net überprüft das Internet auf Verstöße gegen den Jugendschutz.

Kinder- und Jugendschutz

- www.jugendschutz.de

Liste der Adressen der Fach- und Landesstellen zum Kinder- und Jugendschutz sowie der Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V.

klicksafe

- www.klicksafe.de

klicksafe.de initiiert eine nationale Sensibilisierungskampagne zur Förderung der Medienkompetenz im Internet, informiert umfassend über Sicherheitsthemen im Internet und vernetzt als Plattform bundesweit Initiativen und Akteure.

Medienpädagogischer Forschungsverbund Südwest mpfs

- www.mpfs.de/index.html

Der Medienpädagogische Forschungsverbund Südwest ist ein Kooperationsprojekt zwischen der Landesanstalt für Kommunikation Baden-Württemberg und der Landeszentrale für Medien und Kommunikation Rheinland-Pfalz. Die Homepage bietet Studien, Materialien, Termine sowie einen umfangreichen Service-Bereich zum Thema Medienpädagogik.

Mekonet - Medienkompetenz-Netzwerk NRW

- www.mekonet.de

Mekonet vernetzt Einrichtungen, die Orientierung im Bereich der Medienkompetenz anbieten. Mekonet unterstützt seine Partner durch verschiedene Serviceleistungen und Angebote.

naiin - no abuse in internet e.V. - der Verein gegen Missbrauch im Internet

- www.naiin.org/de

Naiin wurde im August 2000 von der Internet-Industrie zusammen mit Verbänden, Initiativen und Privatpersonen gegründet, um Maßnahmen gegen den Missbrauch im Internet zu entwickeln. Naiin betreibt Aufklärung im Internet und erarbeitet relevante rechtliche sowie technische Maßnahmen.

NetProtect

- www.net-protect.org/en/scope.htm

NetProtect fand als Projekt im Rahmen der Handlungslinie zur Entwicklung von Internet-Filtersystemen statt. Das Projektziel bestand im Erarbeiten eines Filter-Prototyps für Eltern und Lehrer unter Beachtung der Sprach- und Kulturenvielfalt in Europa.

secure-IT

- www.secure-it.nrw.de/schulen/materialien.php

Die Initiative für mehr Sicherheit bei Internetprozessen secure-IT stellt auf ihrer Webseite Unterrichtsmaterialien für Lehrkräfte aller Schulformen zur Verfügung. Sie eignen sich für den Unterricht ab Klasse 8 in den Fächern Ethik, Informatik, Medienbildung, ökonomische Bildung, Politik und Sozialwissenschaften.

Stiftung Digitale Chancen

- www.digitale-chancen.de/content/stories/index.cfm/aus.2/secid.11/secid2.70

Die Stiftung Digitale Chancen arbeitet zusammen mit einem Netzwerk von Expertinnen und Experten verschiedener Fachrichtungen sowie mit Vertreterinnen und Vertretern der gesellschaftlichen Gruppen. Im Bereich Jugendschutz bietet die Homepage zahlreiche aktuelle Beiträge rund um das Thema.

Unterhaltungssoftware Selbstkontrolle (USK)

- www.usk.de

Die Webseite bietet eine Datenbank mit den seit 1994 durch die USK ausgesprochenen (und seit 2003 rechtsverbindlichen) Altersempfehlungen für Computerspiele sowie Infos zur Arbeit der USK.

Internationale Institutionen / Organisationen / Projekte

Commission on Online Child Protection (COPA)

- www.copacommission.org

Die COPA-Initiative der US-Regierung beschäftigt sich seit 1998 mit den technischen Möglichkeiten, das Netz für Kinder sicherer zu machen.

Europe's Information Society

- www.europa.eu.int/information_society/programmes/iap/index_en.htm

Das Safer Internet plus Programm der EU setzt sich für eine sichere Internetnutzung mit Hilfe von neuen Technologien ein, die vor allem Kinder vor illegalen und gefährdenden Inhalten schützen soll.

Observatory for the Safer Use of the Internet (OFSI)

- www.ofsi.org

Das OFSI stellt Eltern, Pädagoginnen und Pädagogen, Behörden und allen Interessierten hilfreiche und interessante Informationen zur sicheren und erzieherisch wertvollen Internetnutzung zur Verfügung.

S@ferInternet

- www.safer-internet.net/deutschland

SaferInternet ist eine Kampagne im Rahmen des europäischen Projekts SafeBorders, die in Deutschland auch durch das Bundesministerium für Familie, Senioren, Frauen und Jugend unterstützt wird. Die Kampagne hat zum Ziel, für das Thema Internetsicherheit zu sensibilisieren und eine sichere Internetnutzung zu fördern.

Safer Internet for Knowing and Living (SIFKaL)

- www.sifkal.org/Deutsch/about_objectives_de1.htm

Zentrales Ziel des SIFKaL-Projekts ist es, Informationen und Empfehlungen zu pädagogisch und gesellschaftlich relevanten Nutzungsmöglichkeiten des Internets zu entwickeln und diese mehrsprachig und in verschiedenen Formaten zu verbreiten.

Recht

Jugendmedienschutz-Staatsvertrag (JMStV)

- www.artikel5.de/gesetze/jmstv.html

Staatsvertrag der Länder über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk (Fernsehen) und Telemedien (Internet).

Jugendschutzrichtlinien (JuSchRiL)

- www.kjm-online.de/public/kjm/index.php?show_1=122,57

Die Jugendschutzrichtlinien der KJM konkretisieren die gesetzlichen Anforderungen des Jugendmedienschutz-Staatsvertrags.

Kommission für Jugendmedienschutz der Landesmedienanstalten

- www.kjm-online.de

Die KJM dient der jeweils zuständigen Landesmedienanstalt als Organ bei der Erfüllung ihrer Aufgaben und sorgt für die Umsetzung des Jugendmedienschutz-Staatsvertrags. Die KJM prüft, ob Verstöße vorliegen und entscheidet über die Maßnahmen.

Kriterien für die Aufsicht im Rundfunk und in den Telemedien

- www.kjm-online.de/public/kjm/downloads/Kriterien%20der%20KJM.pdf

Die „Kriterien für die Aufsicht im Rundfunk und in den Telemedien" der KJM widmen sich insbesondere den Wirkungsrisiken, die eine „Entwicklungsbeeinträchtigung" von Kindern und Jugendlichen beziehungsweise eine Entwicklungsgefährdung zur Folge haben.

Portal zum Jugendmedien- und Datenschutz sowie Urheberrecht

- www.lmz.bildung-rp.de/medienschutz.0.html

Infos rund um den Jugendmedienschutz, zum Datenschutz, zu pädagogischen Empfehlungen im Umgang mit Multimedia und Internet sowie zum Urheberrecht.

Feedback zur Broschüre

Sie haben Anregungen, Kritik oder Lob zu dieser Broschüre. Sie setzen selbst eine Filterlösung an Ihrer Schule ein? Welche Erfahrungen haben Sie mit Filterprogrammen gemacht?

Über Ihre Rückmeldung freuen wir uns sehr!

Senden Sie einfach eine E-Mail an **itworks@schulen-ans-netz.de**

Weitere Veröffentlichungen aus der IT works Themenreihe finden Sie unter:
http://itworks.schulen-ans-netz.de/publikationen.php

Gefördert von

www.schulen-ans-netz.de/itworks

Die Nutzung des Internets an Schulen wird ein immer wichtigerer Bestandteil einer zeitgemäßen Unterrichtskultur. Schulträger, Schulleitungen und Lehrkräfte stehen vor der gemeinsamen Herausforderung, die gesetzlich verankerte Aufsichtspflicht auch bei der Nutzung des Internets im Unterricht sicherzustellen. Die Publikation greift den Themenkomplex „Jugendmedienschutz - Filterlösungen im schulischen Umfeld" unter pädagogischen, rechtlichen, technischen sowie praxisbezogenen Aspekten auf. Sie möchte für das Thema sensibilisieren und bei der Planung und Umsetzung von Schutzmaßnahmen zur Sicherstellung des Jugendmedienschutzes unterstützen.

Schulen ans Netz e.V.
IT works
Thomas-Mann-Straße 4
53111 Bonn

Telefon +49 (0)228 91048-261
Telefax +49 (0)228 91048-1261
E-Mail: itworks@schulen-ans-netz.de
Web: http://www.schulen-ans-netz.de/itworks