2. HAMBURGER INTERNET-FILTERKONFERENZ

Innere Sicherheit und Jugendschutz: Gefährdungspotenziale aus dem Internet

Hamburg, 11. März 2004

Konferenzbericht

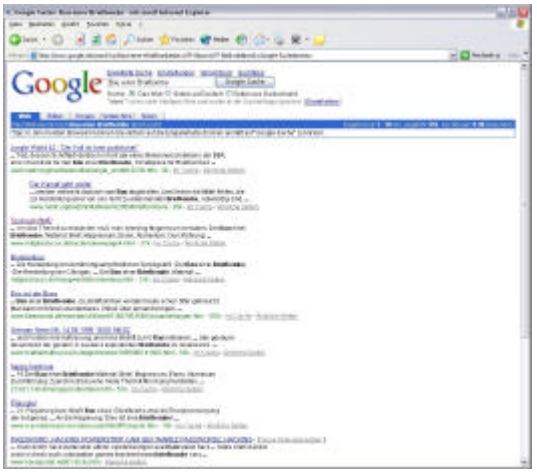
Inhalt

Einleitung

Die Fernsehbilder des verheerenden Bombenanschlages von Istanbul am 20. November 2003 und die schnelle Gewissheit, dass es sich um einen selbst hergestellten Sprengsatz handelte, sowie die Serie von Briefbomben-Attentaten in ganz Europa am Ende des vergangenen Jahres, veranlassten die Internet-Filterexperten der PAN AP AG, sich eine eine Reihe von Fragen zu stellen:

- Sind solche Bombenbauanleitungen ohne weiteres im www zu finden?
- Wenn ja, wie einfach ist die Suche?
- Wieviele derartige Angebote lassen sich in kurzer Zeit finden?
- Sind diese Angebote auf deutschen Servern vorhanden?
- Welches Bedrohungspotenzial bergen diese Anleitungen?
- Sind die zuständigen Behörden informiert, und wenn ja, welche Maßnahmen werden ergriffen?
- Wie reagieren insbesondere die für den Jugendschutz zuständigen Behörden und Institutionen auf all dies?

Der Einsatz der unternehmenseigenen Suchtechnologie unter dem Stichwort „Bau einer Briefbombe“ brachte binnen kürzester Zeit ein verheerendes Ergebnis:



Google Sucheraebnis. 2004

Innerhalb weniger Minuten konnten die Robots der PAN AMP AG hunderte von Fundstellen nachweisen, die sich auf den Seiten der gängigsten Suchmaschinen dokumentieren lassen. Viele dieser Angebote waren auf deutschen Servern vorhanden, und für jedermann, und damit auch für Jugendliche problemlos zu erreichen.

Die gefundenen Anleitungen waren zum überwiegenden Teil sehr detailliert und im wesentlichen auch von technisch unerfahrenen Menschen problemlos umzusetzen, und stellen somit eine Gefahr dar, die weit über die Aspekte des Jugendschutzes hinausgeht.

> ***"Unter den Anleitungen sind einige darunter, wo man mit relativ geringen Aufwand eine maximale Schädigung hervorrufen kann. Es ist einfach nachzubauen und nach zuexperimentieren. Von daher kann man mit einigen der Anleitungen eine sehr große Gefahr produzieren".***
>
> Zitat: Dr. Dietrich Eckhardt, Leiter der Sprengstoffabteilung der Bundesanstalt für Materialforschung in der Sendung stern-TV am 21.01.2004.

Die Behörden reagieren hilflos: Während das Bundesministerium des Inneren bereits im Dezember 2003 gegenüber stern TV erklärte, dass zu diesem Thema aus zeitlichen Gründen keine Stellungnahme abgegeben werden kann, standen die Stellungnahmen zur strafrechtlichen Relevanz solcher Angebote des Bundesministerium der Justiz im Widerspruch zum BKA.

Die von den Jugendministerinnen und Jugendministern der Länder gemeinsam eingerichtete staatliche Stelle für die Beachtung des notwendigen Jugendschutzes in den neuen Informations- und Kommunikationsdiensten (Multimedia, Internet), "Jugendschutz.net" (www.jugendschutz.net) setzt noch immer auf die freiwillige Selbstkontrolle: "Wir streben eine freiwillige Herausnahme oder Veränderung durch diejenigen an, die Inhalte zugänglich machen. Wir bemühen uns darum, zu informieren, inwiefern bestimmte Medienprodukte schädigende Wirkungen auf Kinder und Jugendliche haben können" (Zitat www.jugendschutz.net).

Bereits mit der Tatsache, dass trotz Verbot, aus nahezu jedem an das Internet angeschlossenen Schul-PC und somit über das Klassenzimmer indizierte Computerspiele herunter geladen werden können, zeigte der Vorstand der PAN AMP AG, Bert Weingarten mit seiner Presseerklärung bereits im März 2003 auf, dass der Zweck des Jugendmedienschutz-Staatsvertrages (JMSTV) nicht von den hierfür verantwortlichen Stellen umgesetzt wird.

Das Aufgreifen der Thematik durch die Sendung SternTV am 21.01.2004 steigerte das Interesse für diese Problematik weiter, ohne dass sich jedoch die zuständigen Stellen aus Politik und Justiz zu weiteren Auskünften oder gar einer konstruktiven Diskussion veranlasst sahen. Vor diesem Hintergrund initiierte die PAN AMP AG die 2. Hamburger Internet-Filterkonferenz, um allen Beteiligten und Interessierten ein Forum zu bieten und die Diskussion über die Fachkreise hinaus zu tragen.

Zum Unternehmen

Die PAN AMP AG mit Sitz in Hamburg konzentriert sich seit Ihrer Gründung im Jahre 1998 auf den Vertrieb und die Entwicklung von Lösungen für den sicheren Einsatz von Internet und E-Commerce in Unternehmensanwendungen. Das umfassende Produktportfolio der beiden Geschäftsfelder Secure E-Commerce und Network Management bietet sowohl Industriekunden als auch Interessenten aus dem öffentlichen Bereich die Möglichkeit, integrierte state-of-the-art-Lösungen, aus einer Hand zu beziehen

Agenda

10.00 h Begrüssung und Einführung
durch den Vorstandsvorsitzenden der PAN AMP AG, Bert Weingarten

Teil 1: Internetfilterung: Der Status Quo

10.30 h Auswirkungen für die Praxis: Anforderungen und Grenzen der Provider
Referent: Dr. Reiner Demski, 7eins Internetprovider

11.00 h Gefährdungspotential aus dem Internet?
Referent: Peter Wirnsperger, Senior Manager Security Services Group, Deloitte & Touche

11.30 h Internetfilterung = Zensur?
Referent: Rechtsanwalt Tobias H. Strömer

12.00 h Internetnutzung und Innere Sicherheit/Jugendschutz
Referent: Carsten Lüdemann, Innenexperte der CDU Hamburg

12.30 h Mittagspause

Teil 2: Internetfilterung: Ansätze und Lösungen

13.10 h Jugendschutz - ein Thema in der kirchlichen Internet-Seelsorge?
Referent: Tom O. Brok, Pastor, Leiter der Internetarbeit der Evangelischen Kirche in Deutschland (EKD)

13.40 h Rechtliche Grundlagen und Bewertung
Referent: Rechtsanwalt Tobias H. Strömer

14.10 h Das "reine" Positiv-Portal für Kinder zwischen 4 - 14 Jahren
Referent: Peter Kolb, VICTORY Media Gruppe

14.40 h Die wichtigsten Erfahrungen über Landes- und Schul-Internetfilterung
Referent: Bert Weingarten, PAN AMP AG

15.10 h Podiumsdiskussion: Recht und Realität in Einklang bringen

Referenten

Tom O. Brok

Leiter der Internet-Arbeit der Evangelischen Kirche in Deutschland. 1997 Spezialvikariat in der Arbeitsstelle Internet. 1998-2000 Projektkoordinator des ökumenischen EXPO-Untervorhabens "Kirche am Meer" in Wilhelmshaven, pastorale Aufgaben und Webworking bei einer Agentur für Publizistik und Kommunikation; Jugendschutzbeauftragter der christlichen Suchmaschine crossbot.

Dr. Rainer Demski

Sozial-Wissenschaftler, war Redaktionsleiter beim Schleswig-Holsteinischen Zeitungsverlag; bevor er sich als Projektleiter in den Neuen Medien auf Content & Providing spezialisierte. Seit 2002 ist Dr. Demski Geschäftsführer des DeNIC Mitglieds und Internet Providers 7eins GmbH und der Multimedia-Agentur 7eins media marketing GmbH, die jugendgerechte Angebote bietet.

Peter Kolb

Betriebswirt (VWA) mit 18-jähriger Erfahrung im Bereich Corporate Finance und Treasury in verschiedenen Funktionen, zuletzt als Prokurist und Direktor in diversen Banken. Seit 2001 Leiter Finanzen und Controlling der VICTORY Media Gruppe und Geschäftsführer der stream tec GmbH (frühere Junior Web GmbH). Hierbei konnte Herr Kolb wichtige Erfahrungen sammeln, welche für die Ergonomie eines "reinen" Kinderinternetportal von entscheidender Bedeutung sind. Dabei geht es hauptsächlich um die Gestaltung von Inhalten, die der Kommunikation, dem lernen und der Unterhaltung dienen.

Carsten-Ludwig Lüdemann

Rechtsanwalt und innenpolitischer Fachsprecher der CDU-Bürgerschafts-Fraktion Hamburg. 1993 bis 1997 Bezirksabgeordneter in der Bezirksversammlung Hamburg-Harburg. Mitglied der Bürgerschaft seit Oktober 1997. Schwerpunkte der politischen Arbeit: Innenpolitischer Fachsprecher der Fraktion und Mitglied im Rechts- und Kulturausschuss.

Tobias H. Strömer

Rechtsanwalt mit den Tätigkeitsschwerpunkten: Internetrecht, Markenrecht, Wettbewerbsrecht. Zahlreiche Veröffentlichungen in diversen Fachzeitschriften und Büchern; Bücher: "Online-Recht", 1997/1999/2002, "Das ICANN-Schiedsverfahren", 2002, und "L'Allemand Juridique", 1997, sowie Interviews für Rundfunk und Fernsehen. Letzter Medienauftritt: 29. Dezember 2003, WDR/Studiogast.

Bert Weingarten

Internet-Experte mit zahlreichen IT-Projekten, Vorträgen und Podiumsdiskussionen seit 1995 weltweit präsent. Seit 1995 verantwortlich für die Markteinführung von IT-Sicherheits-Lösungen in Deutschland, Österreich und der Schweiz wie CyberPatrol, GTA-Firewall-Systeme und verschiedene PKI und VPN-Verfahren. Verantwortlich für Landes- und Unternehmenslösungen zur Internetfilterung. Gründer und Vorstand der PAN AMP AG, Entwickler und Patentinhaber des Verfahrens zur Internetfilterung und von Kopierschutzsystemen. Mitbegründer der deutschen Domain-Registrierungsstelle Denic, zahlreiche Veröffentlichungen in diversen Fachzeitschriften; Letzter Medienauftritt: stern TV /Studiogast, 21. Januar 2004.

Peter J. Wirnsperger

Projektmanager für namhafte Software- und Security-Beratungsunternehmen, wie z.B. @stake. Leiter für die Überprüfung von IT-Systemen auf technische und organisatorische Sicherheit, Einhaltung von betrieblichen und gesetzlichen Richtlinien. Seit 2003 bei Deloitte & Touche verantwortlich für die Security Services Group in Deutschland; Mitglied des Internetausschuss der Handelskammer Hamburg, Vorsitzender des Arbeitskreis Security von Hamburg@Work.

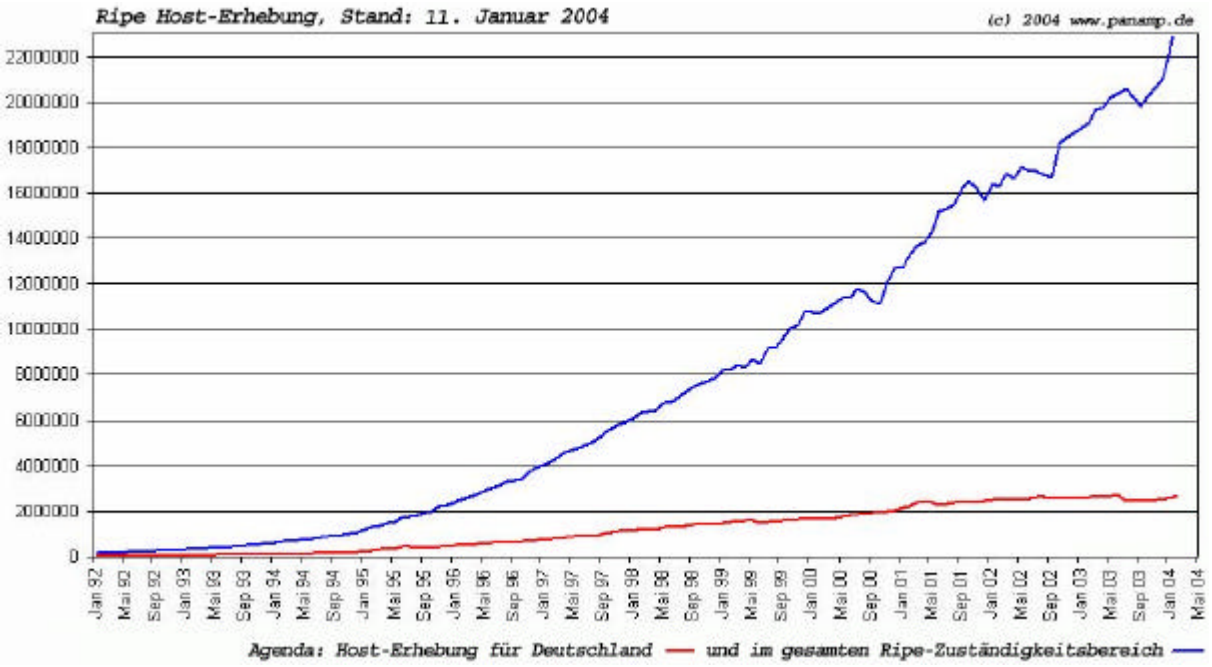
Begrüssung und Einführung

Bert Weingarten, Vorstandsvorsitzender der PAN AMP AG

Das Internet hat sich zu dem globalen Kommunikationsmedium entwickelt, da es leicht zu handhaben ist und die unterschiedlichsten Interessen in globalen Foren und über unterschiedliche Dienste zu bündeln und leicht zu kanalisieren sind. Seit 1992 steigert sich nicht nur die Anzahl der permanent an das Internet angeschlossenen Computer, sondern leider auch die Verbreitung von Extreminhalten. Hierzu gehören unter anderem extremistische Propaganda, Bombenbauanleitungen, Kinderpornografie, Gewaltdarstellungen, Suizidforen und indizierte Computerspiele.

Seither steigert sich nicht nur der globale Datenverkehr, sondern auch die Anzahl von Inhalten, die unsere Demokratie, die Innere Sicherheit und den Jugendschutz gefährden.

Anhand der folgenden Statistik, die die Anzahl der permanent ans Internet angeschlossenen Hosts (Computer) in Teilen von Europa, des Nahen und Mittleren Ostens, Teilen Asiens (die frühere UdSSR) und der nördliche Hälfte von Afrika aufzeigt, ist ersichtlich, dass alleine in dieser Region, heute mehr als 22.315.000 Computer an einem Datenaustausch beteiligt sind. Hinzu kommt eine weit größere Anzahl von sporadisch an das Internet angeschlossenen Computern.



Die Datenübertragung zwischen diesen Internet-Hosts wird über eine Vielzahl von Protokollen und Internet-Diensten ermöglicht. Der missbräuchliche Einsatz der unterschiedlichen Datendienste birgt ausgehende Gefahren, welche nicht zuletzt durch die internationalen Strukturen des Netzes und die Möglichkeiten, hierin anonym zu agieren, deutlich erhöht werden. Zu den am weitest verbreiteten Diensten gehören:

- World Wide Web (WWW), dem Standard zur Übermittlung von Multimedia-Dokumenten im HTML-Format.
- File Transfer Protocol (FTP) , dem Standard zur Übertragung von Dateien von einem Computer auf einen anderen.

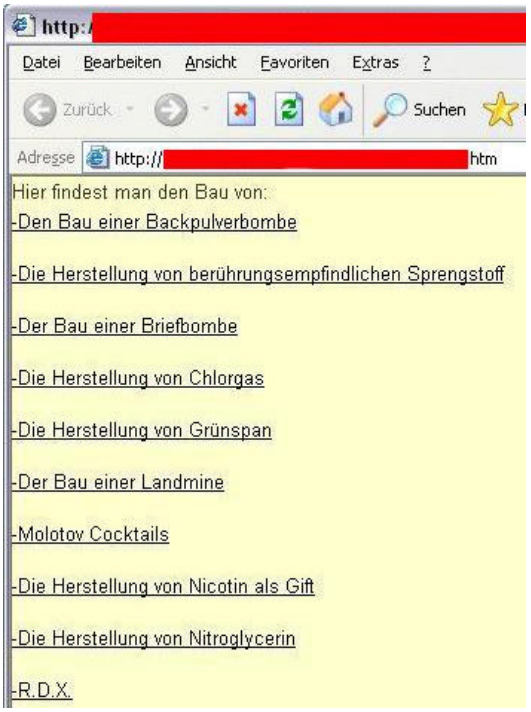
- E-Mail (SMTP), dem Standard für den Versand von E-Mails über das Internet und POP3 zur Übertragung eingegangener E-Mails von einem Mail-Server auf den eigenen Rechner.
- Newsgroups (auch Usenet), zur Übertragung von Netzwerk-Nachrichten.
- Internet Relay Chat (IRC), dem Internetdienst zum zeitgleichen Diskutieren mit Internet-Teilnehmern.
- Peer-to-Peer, jeder Host wird gleichzeitig durch eine Softwareerweiterung Client und Server. Die Verbindung zu anderen Peer-to-Peer Hosts kann entweder über einen Server erfolgen oder völlig dezentral aufgebaut werden.
- WAIS (Wide Area Information Server Protokoll), einem Datenbanksystem zum Auffinden von Internet-Ressourcen.
- ARCHIE, einem System zur Suche in Internet-Archiven. Gefundene Dateien werden dann per Anonymous FTP auf den eigenen Rechner übertragen.
- GOPHER, ein menügesteuerter Dienst, um Internet-Ressourcen zu durchsuchen.
- TELNET ist ein Terminal-Emulator mit dem es möglich ist, sich auf bestimmte Rechner einzuloggen und dort zu arbeiten, als säße man an einem lokalen Arbeitsplatz. Dieser älteste Internet-Dienst hat durch WWW-Techniken deutlich an Bedeutung verloren. Hingegen erlebte Telnet in der Verbreitung von Extrem-Angeboten eine Renaissance, da Telnet als relativ zugriffssicher eingeschätzt wird.

Der dezentrale Aufbau des Internets wird auch zukünftig immer wieder zur Gefährdung der inneren Sicherheit und des Jugendschutzes durch extreme Inhalte und Darstellungen führen. Hierzu gehören extremistische Propaganda, Pornografie und, nach wie vor, Anleitungen zur Herstellung von Waffen und indizierte Computerspiele, die als primäres Ziel das Töten von Menschen verfolgen. Für alle aufgeführten jugendgefährdenden Inhalte gilt: Sie sind leicht über das Internet erhältlich und heute über jede Schule und öffentliche Einrichtung mit Internetanschluss in Deutschland zu beziehen.

Index einer Webseite, 2004

Die verheerenden Bombenanschläge in Istanbul am 20.11.2003 brachten uns dazu, das deutsche Internet (Hosts mit Routing in der Bundesrepublik Deutschland/ Host mit einem Impressum, aus welchem eine Gerichtsbarkeit in Deutschland hervorgeht) nach Anleitungen zum Bombenbau, dem Bau von Sprengvorrichtungen und Giften zu prüfen. Das Ergebnis war erschreckend:

Neben konkreten Anleitungen zur Herstellung von R.D.X., einem der effektivsten militärischen Sprengstoffe, wurden zahlreiche und vollständige Anleitungen zur Herstellung von Briefbomben, Landminen bis hin zur Kalzium-Karbid Bombe entdeckt, die frei zugänglich waren.



Index einer Webseite, 2004

Ein Auszug der Bombenbaupläne aus dem Internet:

- Der Bau einer Briefbombe,
- Der Bau einer Landmine,
- Der Bau einer Rohrbombe
- Der Bau einer Trockeneisbombe
- Der Bau einer Backpulverbombe
- Der Bau einer Kalzium-Karbitbombe
- Der Bau eines Molotov-Cocktails
- Der Bau einer Splitterbombe

Ein Auszug der Anleitungen zur Herstellung von Sprengstoffen aus dem Internet:

- Die Herstellung von berührungsempfindlichem Sprengstoff
- Die Herstellung des Sprengstoffes R.D.X.
- Die Herstellung von TNT
- Die Herstellung von Nitroglycerin
- Die Herstellung von Napalm

Ein Auszug der Anleitungen zur Herstellung von Giften und Gasen aus dem Internet:

- Die Herstellung von Zyankali
- Die Herstellung von Nikotin-Gift
- Die Herstellung von Grünspan
- Die Herstellung von Thermit
- Die Herstellung von Chlorgas
- Die Herstellung von Schwefelsäure

Weiter wurden in Softwareentwicklungsforen Gruppen entdeckt, die detailliert über eine "ideale Fernzündung" debattieren.

Ein Auszug der Anleitungen zur Herstellung von Sprengstoffen aus dem Internet:

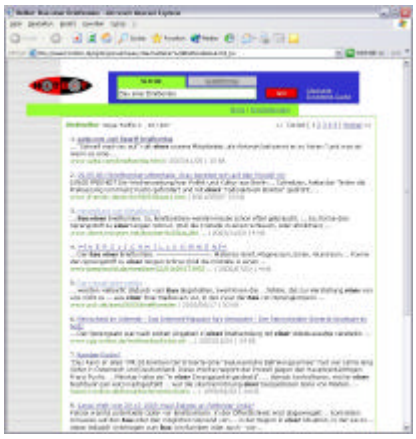
- Fernzündung per Modellflugzeug Servo
- Fernzündung per Piezo-Zündung
- Fernzündung per Mobil-Telefon
- Fernzündung per Telefonanlage

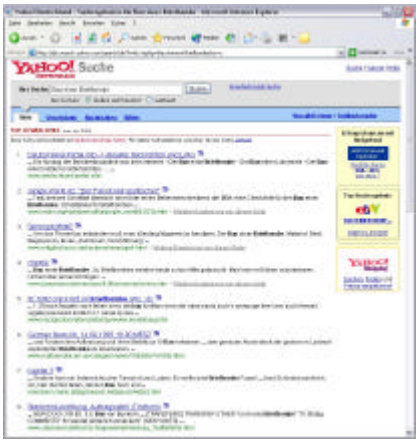
Die aufgeführten Anleitungen werden teilweise seit Monaten über Deutsche Web-Server angeboten und es wurde belegt, dass die Herstellung solch gefährlicher Stoffe wie Nitroglycerin oder Sprengstoff, Landminen oder Briefbomben für Internet-Benutzer überhaupt kein Problem mehr ist. Denn im Internet finden sich detaillierte Anleitungen zum Bombenbau, völlig unverschlüsselt, praktisch zum Selbermachen. Weiterhin wurden neue Suizidchats und eine Vielzahl von in Deutschland indizierten, aber per Internet frei zugänglichen Computerspielen, aufgefunden.

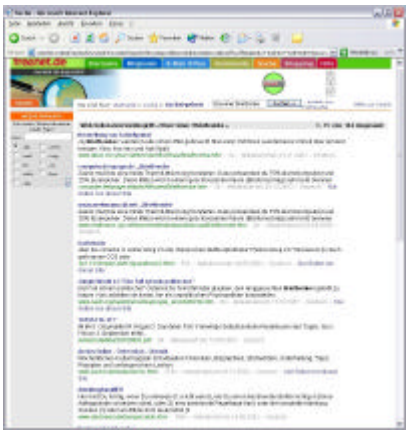
Es wunderte uns sehr, dass weder von staatlichen Stellen der inneren Sicherheit noch den für Jungendschutz und Internet Verantwortlichen, diesem Treiben Einhalt geboten wurde.

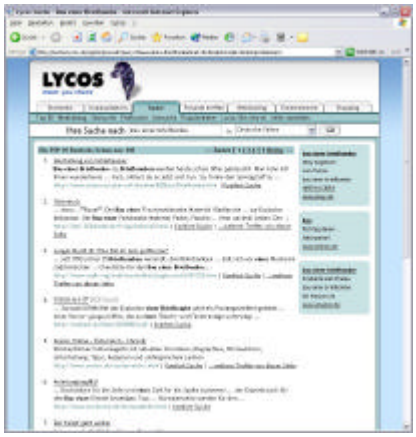
Die nüchterne Bestandsaufnahme zeigt auf, dass eine Gefährdungslage in Deutschland durch den Bezug von Sprengstoffanleitungen, Bombenbauanleitungen und Anleitungen zur Fernzündung akut ist, da die Anleitungen über das Internet frei erhältlich sind und mit ihnen Bomben mit verheerender Wirkung hergestellt werden können. Der Zugang zu indizierten Computerspielen, welche nicht einmal mehr über Erwachsenen-Videotheken ausgeliehen werden dürfen, ist kinderleicht und Suizidchats vermitteln alle Möglichkeiten für den Freitod von Minderjährigen und es ist kinderleicht, diese Extreminhalte aufzurufen. Als Beleg erstellte unser KI-Robot (intelligentes Suchsystem für öffentlich frei zugängliche Internetinhalte) Wort-Muster für den Bezug von Bombenbauanleitungen her.

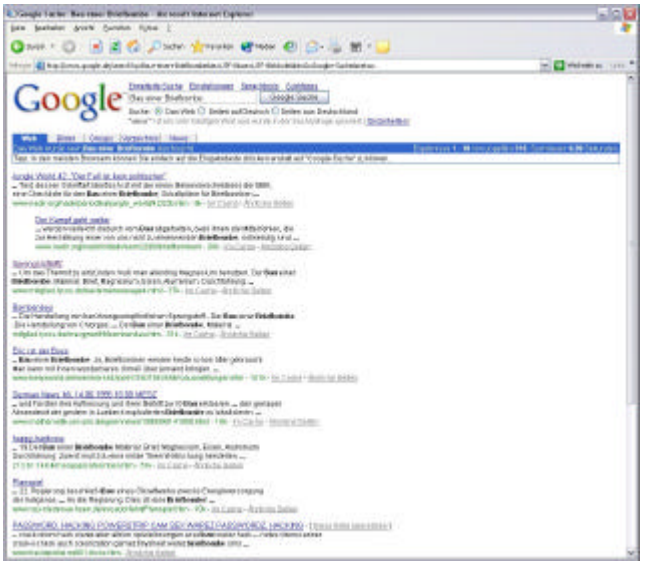
Die Eingabe des Wort-Musters „Bau einer Briefbombe“ führte zu mindestens 5 Treffern auf der jeweils ersten Ergebnisseite bei allen besucherstarken Suchmaschinen in Deutschland:











Die führenden Suchmaschinen und die hohe Trefferquote für Bombenbauanleitungen, 2004.

Als Sofortmassnahme wurde hierüber das Bundesinnenministerium informiert. Konkret wurden detaillierte Auszüge dem Anschreiben an Herrn Bundesinnenminister Otto Schily beigelegt, um eine Verfolgung einzuleiten.

Zeitgleich stellte die PAN AMP AG allen autorisierten staatlichen Stellen und Jugendschutzeinrichtungen in Deutschland die aufgefundenen Internet-Adressen kostenlos zur Verfügung, um schnellst möglichst die bestehenden Gefahrenquellen mit Internetfilterung abzuschalten.

Die Kunden der FAS –Filter-Administrations-Systeme der PAN AM AG erhielten alle notwendigen Sperrinformationen bereits automatisch bei den laufenden Filterupdates übertragen. Durch die Aktivierung der Kategorie „Millitant/Extremist“ sind alle aufgefundenen Bombenbauanleitungen nicht mehr erreichbar.

Unmittelbar nach der Freigabe der Pressemitteilung „Bombenbauanleitungen aus dem Internet“ wurde das erste Radiointerview mit dem Radiosender RSH – Radio-Schleswig-Holstein- geführt. Zahlreiche Tageszeitungen wie die Lübecker Nachrichten, Tagesspiegel und die Welt brachten das Thema in die Presse. Auch stern-TV ging der Spur der anonymen Bombenbauer nach und dokumentierte, wie gefährlich die Stoffe sind, die man sich nach den Anleitungen aus dem Netz herstellen kann. Am 21.Januar 2004 wurde in der Live-Sendung von Günter Jauch aufgezeigt, wie akut die Gefahr für die innere Sicherheit und den Jugendschutz durch Bombenbauanleitungen im Internet tatsächlich ist.

Zitate aus der Live-Sendung:

Dr. Dietrich Eckhardt, Sprengstoffexperte der Bundesanstalt für Materialforschung:

„Unter den Anleitungen sind einige darunter, wo man mit relativ geringem Aufwand eine maximale Schädigung hervorrufen kann. Es ist einfach nachzubauen und nachzuexperimentieren. … Von daher kann man mit einigen der Anleitungen eine sehr große Gefahr produzieren“.

Günter Jauch, Moderator von stern TV:

„Im Internet wird jedem, der es wissen will, haar genau erklärt, welche Bombe mit welcher Wirkung und vor allem mit welchem Aufwand, wie genau zu bauen ist“.

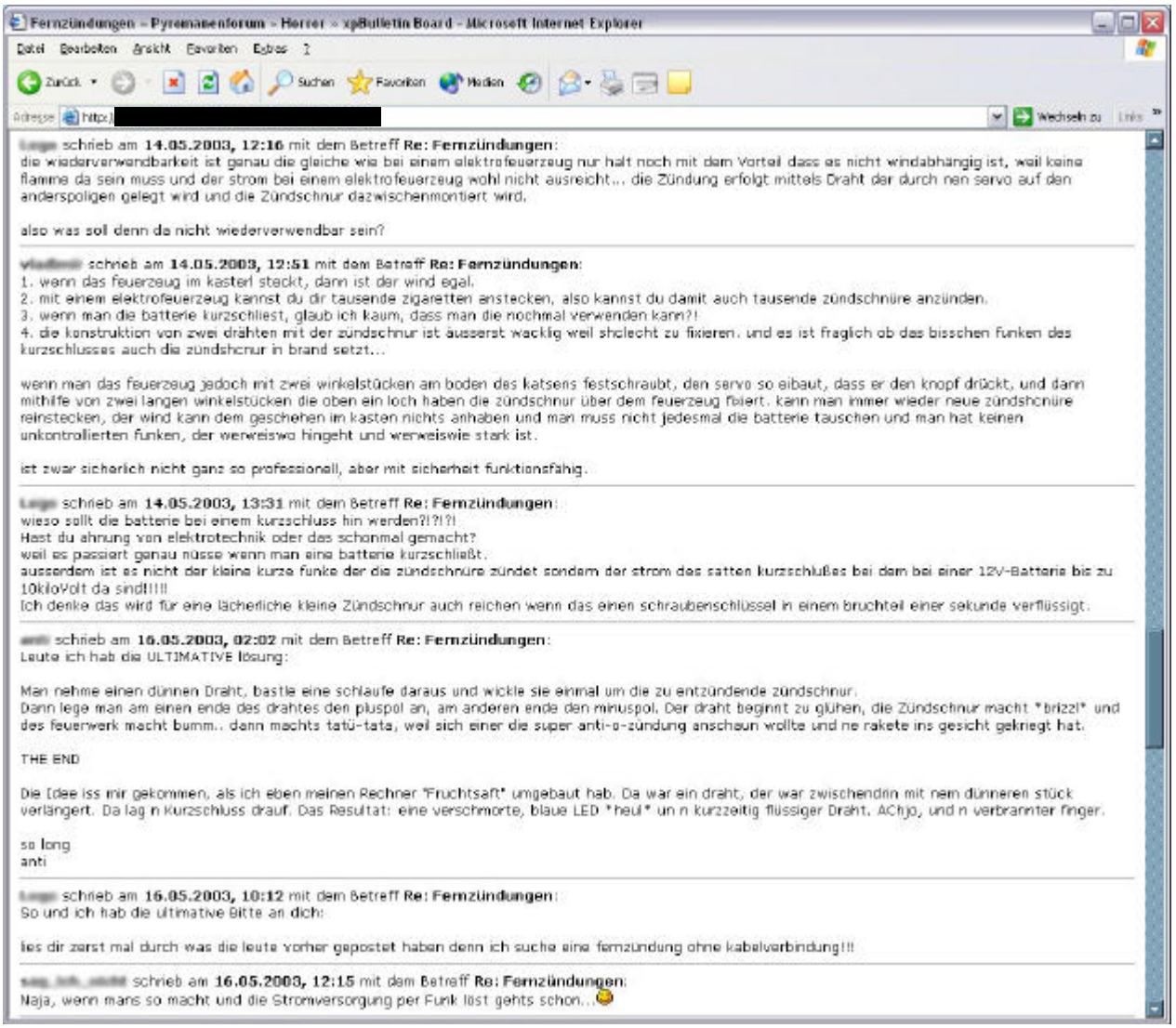
Yvonne Kuschminder, Praktikantin im EU-Parlament:

Die Praktikantin öffnete am ersten Arbeitstag im Büro des Europa-Abgeordneten Hans-Gert Pöttering einen Brief, der eine Bombe enthielt. Sie antwortete auf die Frage von Günter Jauch bei Stern TV, ob Sie gewusst habe, daß der Bau von Briefbomben so einfach ist: *„Nein, das wusste ich nicht und ich finde es erschreckend, daß man das überall nachlesen kann, dass man praktisch nur das Internet anklicken braucht, und dann kann man sich ganz detailliert darüber informieren, wie man dann so eine Bombe baut“.*

Bert Weingarten, Vorstand der PAN AMP AG

„Auf der einen Seite war ich absolut erschrocken davon, wie detailgetreu diese Anleitungen sind und wie spielerisch darin geschrieben wird, „wenn sich etwas leicht verfärbt, renn um dein Leben“.

Oder: „Du hast ca.10 bis 15 Sekunden Zeit“. Ich sehe auch dort eine Gefahr,“ ….. selbst wenn die Anleitungen nicht detailgetreu sind. Sollte jemand sie nachbauen, besteht sicherlich die Gefahr einen körperlichen Schaden zu erleiden und aus diesem Grund bin ich der Meinung, dass diese Angebote im Internet nichts zu suchen haben“.


Fernzündungen - Pyromanenforum - Horror - xpBulletin Board - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien

Adresse http:[redacted] Wechseln zu Links

[redacted] schrieb am **14.05.2003, 12:16** mit dem Betreff **Re: Fernzündungen**:
die wiederverwendbarkeit ist genau die gleiche wie bei einem elektrofeuerzeug nur halt noch mit dem vorteil dass es nicht windabhängig ist, weil keine flamme da sein muss und der strom bei einem elektrofeuerzeug wohl nicht ausreicht... die Zündung erfolgt mittels Draht der durch nen servo auf den anderspoligen gelegt wird und die Zündschnur dazwischenmontiert wird.

also was soll denn da nicht wiederverwendbar sein?

[redacted] schrieb am **14.05.2003, 12:51** mit dem Betreff **Re: Fernzündungen**:
1. wenn das feuerzeug im kasterl steckt, dann ist der wind egal.
2. mit einem elektrofeuerzeug kannst du dir tausende zigaretten anstecken, also kannst du damit auch tausende zündschnüre anzünden.
3. wenn man die batterie kurzschliest, glaub ich kaum, dass man die nochmal verwenden kann?!
4. die konstruktion von zwei drähten mit der zündschnur ist äusserst wacklig weil shclecht zu fixieren. und es ist fraglich ob das bisschen funken des kurzschlusses auch die zündshcnur in brand setzt...

wenn man das feuerzeug jedoch mit zwei winkelstücken am boden des katsens festschraubt, den servo so eibaut, dass er den knopf drückt, und dann mithilfe von zwei langen winkelstücken die oben ein loch haben die zündschnur über dem feuerzeug fixiert. kann man immer wieder neue zündshcnüre reinstecken, der wind kann dem geschehen im kasten nichts anhaben und man muss nicht jedesmal die batterie tauschen und man hat keinen unkontrollierten funken, der werweiswo hingeht und werweiswie stark ist.

ist zwar sicherlich nicht ganz so professionell, aber mit sicherheit funktionsfähig.

[redacted] schrieb am **14.05.2003, 13:31** mit dem Betreff **Re: Fernzündungen**:
wieso sollt die batterie bei einem kurzschluss hin werden?!?!?!
Hast du ahnung von elektrotechnik oder das schonmal gemacht?
weil es passiert genau nüsse wenn man eine batterie kurzschließt.
ausserdem ist es nicht der kleine kurze funke der die zündschnüre zündet sondern der strom des satten kurzschlußes bei dem bei einer 12V-Batterie bis zu 10kiloVolt da sind!!!!
Ich denke das wird für eine lächerliche kleine Zündschnur auch reichen wenn das einen schraubenschlüssel in einem bruchteil einer sekunde verflüssigt.

[redacted] schrieb am **16.05.2003, 02:02** mit dem Betreff **Re: Fernzündungen**:
Leute ich hab die ULTIMATIVE lösung:

Man nehme einen dünnen Draht, bastle eine schlaufe daraus und wickle sie einmal um die zu entzündende zündschnur.
Dann lege man am einen ende des drahtes den pluspol an, am anderen ende den minuspol. Der draht beginnt zu glühen, die Zündschnur macht *brizz!* und des feuerwerk macht bumm.. dann machts tatü-tata, weil sich einer die super anti-a-zündung anschaun wollte und ne rakete ins gesicht gekriegt hat.

THE END

Die Idee iss mir gekommen, als ich eben meinen Rechner "Fruchtsaft" umgebaut hab. Da war ein draht, der war zwischendrin mit nem dünneren stück verlängert. Da lag n Kurzschluss drauf. Das Resultat: eine verschmorte, blaue LED *heul* un n kurzzeitig flüssiger Draht. AChjo, und n verbrannter finger.

so long
anti

[redacted] schrieb am **16.05.2003, 10:12** mit dem Betreff **Re: Fernzündungen**:
So und ich hab die ultimative Bitte an dich:

lies dir zerst mal durch was die leute vorher gepostet haben denn ich suche eine fernzündung ohne kabelverbindung!!!

[redacted] schrieb am **16.05.2003, 12:15** mit dem Betreff **Re: Fernzündungen**:
Naja, wenn mans so macht und die Stromversorgung per Funk löst gehts schon..

Forum zur Herstellung von Fernzündungen für Bomben,2004

Während das Bundesministerium des Inneren bereits im Dezember 2003 gegenüber stern TV zu keiner Stellungnahme bereit war, erklärte das Bundesministerium der Justiz am 21. Januar 2004 durch die Stellvertretende Pressesprecherin Frau Christiane Wirtz: „Es ist nach unserem Recht strafbar, detaillierte Anleitungen zum Bau einer Bombe etwa im Internet zu veröffentlichen“.

Hiervon wusste zumindest im Dezember 2003 das BKA noch nichts, da BKA-Vize-Sprecher Dirk Büchner im Interview mit den Lübecker-Nachrichten erklärte: „Das Veröffentlichen von Anleitungen zur Herstellung von Sprengstoff und Bomben ist nicht generell strafbar, solange nicht zu ihrem Gebrauch aufgefordert wird.“ Weiter erklärte der BKA-Vize-Sprecher, „dass das BKA bisher keine Anzeige gegen „bombige“ Internet-Seiten erstattet, oder Internet-Provider aufgefordert hat, entsprechende Seiten zu sperren und das die Internet-Fahnder beim Bundeskriminalamt 80 bis 85 % ihrer Zeit mit der Jagd auf Kinder-Porno-Ringe verbringen.

Die von den Jugendministerinnen und Jugendministern der Länder gemeinsam eingerichtete staatliche Stelle für die Beachtung des notwendigen Jugendschutzes in den neuen Informations- und Kommunikationsdiensten (Multimedia, Internet). Jugendschutz.net (www.jugendschutz.net) setzte hingegen noch immer auf die freiwillige Selbstkontrolle: "Wir streben eine freiwillige Herausnahme oder Veränderung durch diejenigen an, die Inhalte zugänglich machen. Wir bemühen uns darum, zu informieren, inwiefern bestimmte Medienprodukte schädigende Wirkungen auf Kinder und Jugendliche haben können“ (Zitat der Webseite www.jugendschutz.net im März 2004).

Es ist eine Tatsache, dass trotz Verbot aus nahezu jedem an das Internet angeschlossenen Schul-Computer und somit über das Klassenzimmer, indizierte Computerspiele herunter geladen werden können. Der Vorstand der PAN AMP AG, Bert Weingarten, zeigte in der Presseerklärung am 2. März 2003 auf, das der am 01. März 2003 in Kraft getretene neue Jugendmedienschutzsstaatsvertrag (JMStV), von Bildungseinrichtungen - jeglicher Couleur – gar nicht eingehalten werden kann, da von Seiten der politisch Verantwortlichen weder ein Filtersystem zur Verfügung gestellt wird, noch eine Empfehlung vorliegt, wie die Schulträger den Jugendmedienschutzsstaatsvertrag (JMStV) überhaupt einhalten können, ohne ihre Internetzugänge abzuschalten.

Unserer Bitte an den Innenminister, Herrn Otto Schily, für die eng zusammenhängende Thematik der Inneren Sicherheit und des Jugendschutzes einen runden Tisch einzuberufen, wurde leider nicht entsprochen. Um sich der bestehenden Herausforderung anzunehmen, wurde zur 2. Hamburger Internet-Filter Konferenz eingeladen und Einladungen an alle uns bekannten Staatlichen Stellen und Vereinigungen, die für die innere Sicherheit und den Jugendschutz Verantwortung tragen, versendet. Ziel war es, ausgewiesene Experten mit ihren Erfahrungen und Vorschlägen zu Wort kommen zu lassen, um gemeinsam in der anschließenden Podiumsdiskussion Lösungen zu erarbeiten, um somit zeitnah die praktische Umsetzung herzustellen und diese zu veröffentlichen.

Zur Klärung der rechtlichen Lage der Provider und der Anbieter von Extremangeboten beauftragte die PAN AMP AG den ausgewiesen Online-Rechtsexperten Herrn Rechtsanwalt Tobias H. Stömer mit einer kritischen Ausarbeitung zur Frage, ob Internetfilterung Zensur ist. Herr Strömer stellt sein Ergebnis im Rahmen dieser Konferenz vor.

Auswirkungen für die Praxis: Anforderungen und Grenzen der Provider

Referent: Dr. Reiner Demski, 7eins Internetprovider

1. Einleitung

Wenn es um unerwünschte Internetinhalte geht, werden als quasi mitverantwortliche Quelle des Problems in der Regel auch diejenigen Technikdienstleister genannt, die die für die Veröffentlichung von Content erforderlichen Systeme bereitstellen: die Webhosting-Provider. Man argumentiert, ohne viel über technische und rechtliche Machbarkeit zu diskutieren, das Übel müsse bei der Wurzel gepackt, unerwünschter Content einfach gesperrt oder gelöscht werden; hierfür seien eben die Hosting-Provider zuständig.

Der vorliegende Beitrag soll erklären,

– warum das zu einfach gedacht und schlicht nicht umsetzbar ist,
– warum es sogar gefährlich ist, etwas derartiges zu fordern, und
– was statt dessen getan werden könnte, um das Problem nachhaltig zu beseitigen

2. Webhosting, Domains, TCP/IP und Überwachung

Die Zahl veröffentlichter Internetcontents wächst nach wie vor exponentiell. Allein die von der Suchmaschine Google gelisteten einzelnen Sites im Netz beträgt mittlerweile die schwindelerregende Größenordnung von über 4,2 Milliarden Webseiten. In Deutschland sind weit über 7 Millionen .de-Domains registriert. Rund 200 Provider sind hierzulande als direkte Mitglieder der Registrierungsstelle DeNIC Registrare für die Top-Level-Domain .de. Hinter ihnen verbergen sich mehrere Tausend Wiederverkäufer, die zum großen Teil eigene Systeme für Webhosting anbieten. Hinzu kommen unzählige eigenständige Hosts, sogenannte dedizierte Server, die unabhängig von den Webhosting-Systemen der Hosting-Provider von Privatkunden, öffentlichen Einrichtungen und Unternehmen betrieben werden. Da diese Systeme als Root-Server nur dem Zugriff des jeweiligen Betreibers unterliegen, sind sie weitestgehend autark. Solche Systeme können heute sogar im häuslichen Umfeld - etwa mit einem DynDNS-Account auf Basis eines herkömmlichen DSL-Zugangs - betrieben werden. Im Internet kommunizieren die Systeme über verschiedene Protokollwege. Wichtigstes Element für die Erkennung untereinander und damit für das Auffinden der Inhalte im weltweiten Datennetz sind die IP-Adressen der Systeme. Diese werden durch Domain- Name-Server (DNS) in Domainnamen (z.B. web.de) “übersetzt” - so können lokal installierte Systeme wie Internetbrowser oder E-Mail-Clients Inhalte finden, auflösen und darstellen bzw. übertragen.

Das einzelne Webhosting-System stellt die Inhalte über einen Webserver (z.B. Apache) bereit und teilt dem anfragenden System mit, in welchem Verzeichnis auf dem Webserver der Inhalt für die jeweilige Anfrage zu suchen ist. Ein durchschnittlich leistungsfähiger moderner Webserver kann mehrere Tausend Domains mit eigenen Inhalten gleichzeitig verwalten. Zusätzlicher Content kann auf anderen Protokollebenen – z.B. FTP-Servern, News-Servern oder im Rahmen von Peer-to-Peer-Netzen – verwaltet und bereitgestellt werden.

Nun könnte man versuchen, unerwünschte Inhalte wie Pornographie, Gewalt oder radikalpolitische Themen auf den Systemen ausfindig zu machen. Manche Provider versuchen, schon bei der Anmeldung von Domains und Hostingpaketen durch ein Verbot zum Beispiel Erotik auszusondern. Dennoch: Bei der Fülle an Domains und Inhalten könnten diese nur maschinell gescannt und gesucht werden. Und genau da liegt das Problem:

Maschinen handeln nach bestimmten Regeln. Sie werden niemals in der Lage sein, alle Inhalte anstelle menschlicher Überprüfung fehlerfrei ausfindig zu machen. Viele Ergebnisse werden auch harmlos sein - ohnehin wäre daher eine redaktionelle Prüfung erforderlich.
Hinzu kommt, dass jemand, der unerwünschten Content bereitstellen möchte, in der Regel versuchen wird, diesen zu verbergen und zu tarnen; entweder unter einem harmlosen Namen oder aber zum Beispiel in geschützten Verzeichnissen, auf die nur bestimmte User Zugriff haben – oder aber abseits der http-basierten Dienste.
Rechnet man also, dass ein durchschnittlicher Internetprovider für die Aufklärung und manuelle Prüfung nur einer betroffenen Seite im Durchnitt 3 Minuten Arbeitszeit aufwenden müßte – bei z.B. 20.000 Domains mit vielleicht 60.000 Seiten wäre das ein Zeitaufwand allein für die Bestandsdomains von 375 Arbeitstagen. Nicht gerechnet sind hier die Domains seiner Reseller und Partner, sowie alle Contents, die auf dedizierten Servern seiner Kunden laufen – ganz zu schweigen von den Inhalten, die über andere Internetprotokolle wie News, FTP oder Mail ausgetauscht werden. Schon hier ist erkennbar, dass eine Kontrolle in diesem Rahmen unmöglich professionell zu leisten wäre.

Auch nicht geklärt ist die rechtliche Fragestellung: Darf ein Webhosting-Anbieter die Seiten seiner Kunden einfach scannen und klassifizieren? Ohne einen staatlichen Auftrag, zum Beispiel im Rahmen eines polizeilichen Ermittlungsverfahrens wäre ein solcher Eingriff eine Verletzung der Privatsphäre und der Integrität des Kunden – die nicht zuletzt auch seinem Geschäft kaum förderlich sein dürfte, wenn dies erst einmal bekannt würde. Und schließlich würden Anbieter unerwünschter Inhalte innerhalb kurzer Zeit in der Lage sein, mit ihren Inhalten der Kontrolle zu entfliehen – zum Beispiel auf Systeme im Ausland oder im Untergrund, jeglicher Kontrolle entzogen. Der Umzug entsprechender Inhalte ist mit heutigen Methoden problemlos binnen Minuten durchführbar.

Eine Kontrolle des Internet über die Hosting-Provider ist weder zielführend noch durchführbar. In gleicher Konsequenz müßte man dann auch etwa Suchmaschinen auffordern, bestimmte Links nicht aufzunehmen, oder etwa die Registrare von Top-Level- Domains, bestimmte Domains erst gar nicht zur Registrierung freizugeben. An diesen Beispielen wird offenbar: Forderungen dieser Art sind schlicht nutzlos und allenfalls sprechendes Zeugnis der Hilflosigkeit von Behörden und Organisationen, die sich jetzt mit Recht der Kritik der Öffentlichkeit gegenüber sehen, weil ihnen die Kontrolle über das Medium entglitten ist.

3. Sinnvolle Zugangsüberwachung durch Filterung und Medienerziehung

Das Internet ist ein Kommunikationsmedium wie andere Medien auch. Niemand würde auf den Gedanken kommen, etwa eine Telefongesellschaft dafür verantwortlich machen zu wollen, wenn über ihre Netze ein Verbrechen geplant wird – oder die Post, wenn der Briefträger eine Briefbombe ausliefert. Daher ist der Ansatzpunkt für jeden Schutz dort zu suchen, wo das Medium lokal angebunden ist.

Jeder Internetnutzer, jeder Administrator entscheidet selbst, welche Internetinhalte er für seine Systeme zugänglich machen will. Sinnvoll wäre es nun, auch technisch weniger versierten Usern die Möglichkeit zu geben, unerwünschte Inhalte ohne großen Aufwand zu filtern. Dies gilt sowohl für die Netzwerkfilterung, etwa in öffentlichen Netzen oder Unternehmen, als auch für die lokale Internetfilterung im privaten Haushalt.
Seit Jahren werden diverse Filterprogramme wie CyberPatrol oder NetNanny angeboten, eine integrierte Technologie aber, etwa als Bestandteil der Zugangssoftware oder der Verwaltungskonsole für den Internetrouter oder die Firewall, ist in den meisten Standardtools noch nicht vefügbar.

Mit intelligenten Systemen, die neben sogenannten Black- und Whitelists für die Filterung auch über eine frei konfigurierbare Künstliche Intelligenz (KI) verfügen, wäre die Umsetzung einer solchen netzweiten Kontrollfunktion deutlich effektiver machbar. Damit verschwindet zwar nicht jeder unerwünschte Inhalt aus dem Netz, aber er wird zumindest seiner Erfolgsmöglichkeiten beraubt. Inhalte, die niemand findet, können sich auch nicht wirkungsvoll verbreiten.

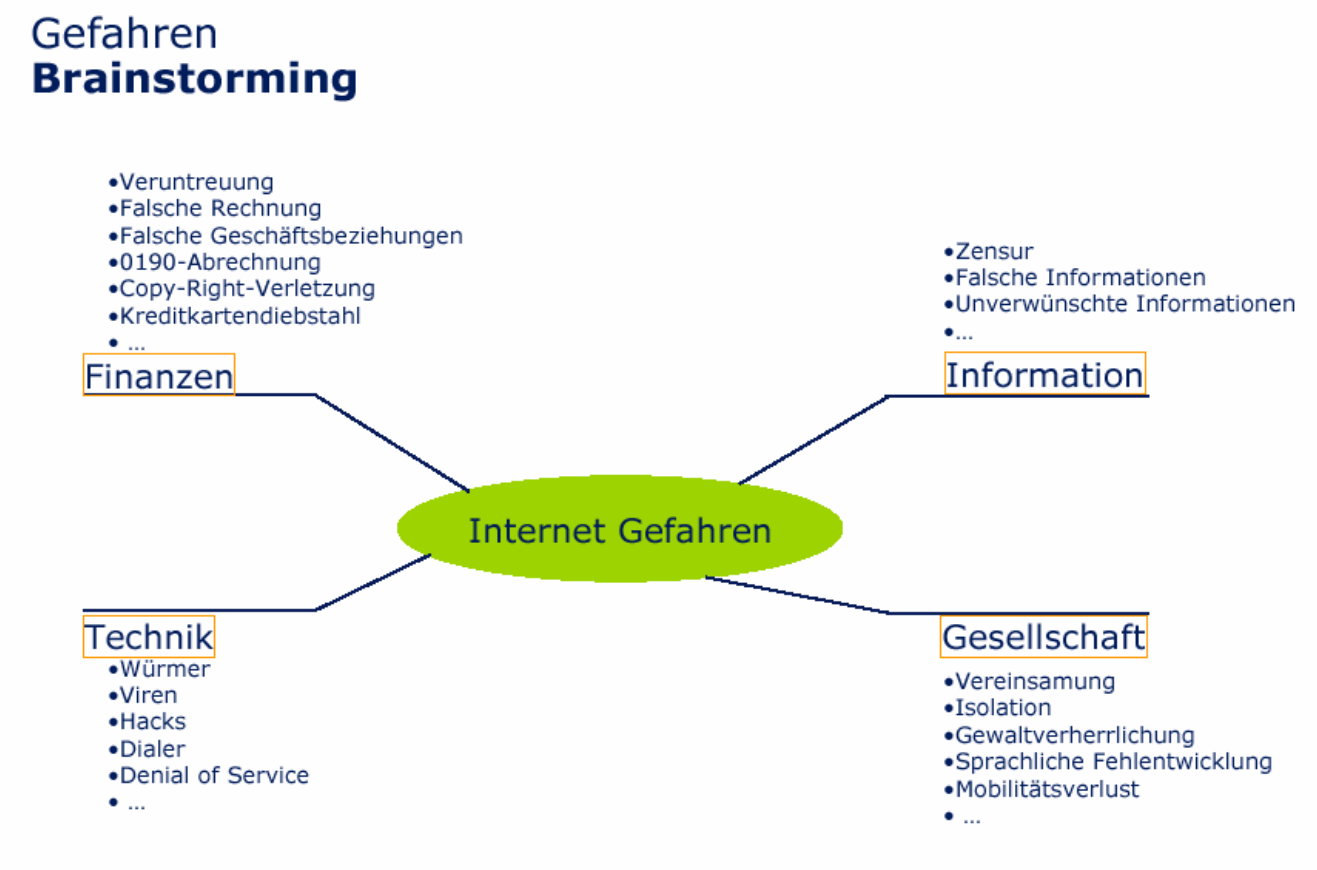
Darüber hinaus fehlt bislang – vor allem auch behördlicherseits – die notwendige Aufklärung und Erziehung im Umgang mit öffentlichen Medien des digitalen Zeitalters. Staat und Politik haben die Probleme und Gefahren, die ein Medium wie das Internet birgt, bislang weder erkannt noch im Ansatz aufbereitet. Die rasante Entwicklung des Mediums, das heute nur noch wenige Jahre vom Einbruch auch in die mobilen Netze steht, überfordert Ministerien, Schutzorganisationen und öffentliche Erziehung in einer bisher nicht gekannten Weise. Dabei wäre gerade hier ein wirkungsvoller Ansatzpunkt für Prävention zu suchen:

Effektive Medienerziehung schon im Schulalter ist eine der dringlichsten Anforderungen an die staatliche Erziehungskultur der kommenden Jahre. Der mündige, aufgeklärte Bürger, der die Gefahren und Konsequenzen im Umgang mit modernen, freien Medien kennt, wird im Zweifel richtiger und sinnvoller entscheiden als derjenige, der ohne jede Vorbereitung mit unerwünschten Inhalten und Infiltration via Internet konfrontiert wird.

4. Fazit

Als das Internet entfesselt wurde, ahnte noch niemand, welche Dynamik es einmal entfalten würde. Heute ist es das Werkzeug, in dem jeder ohne nennenswerte Kosten Inhalte jeder Art verbreiten und empfangen kann – gleich welche Ziele er verfolgt.
Zensur findet so gut wie gar nicht statt. Das Internet ist heute vergleichbar mit der Brisanz etwa der Erfindung der Buchdruckerkunst – Unmengen neuer Inhalte werden in viel kürzerer Zeit einem viel größeren Publikum verfügbar gemacht als noch vor wenigen Jahren. Diese Entwicklung birgt ebenso viele Chancen wie Gefahren. Es ist die Verantwortung der Gesellschaft und der staatlichen Stellen, dass dieser Prozess nutzbringend und im Sinne der verfassungsmäßigen Ordnung stattfindet. Die Forderung nach Sperrung der Inhalte auf den Hosting-Systemen geht ins Leere. Was wir statt dessen brauchen, sind effektive Medienerziehung zu einem verantwortungsbewussten Nutzerverhalten und konsequente Filtermöglichkeiten überall dort, wo Internettechnologien verfügbar sind.

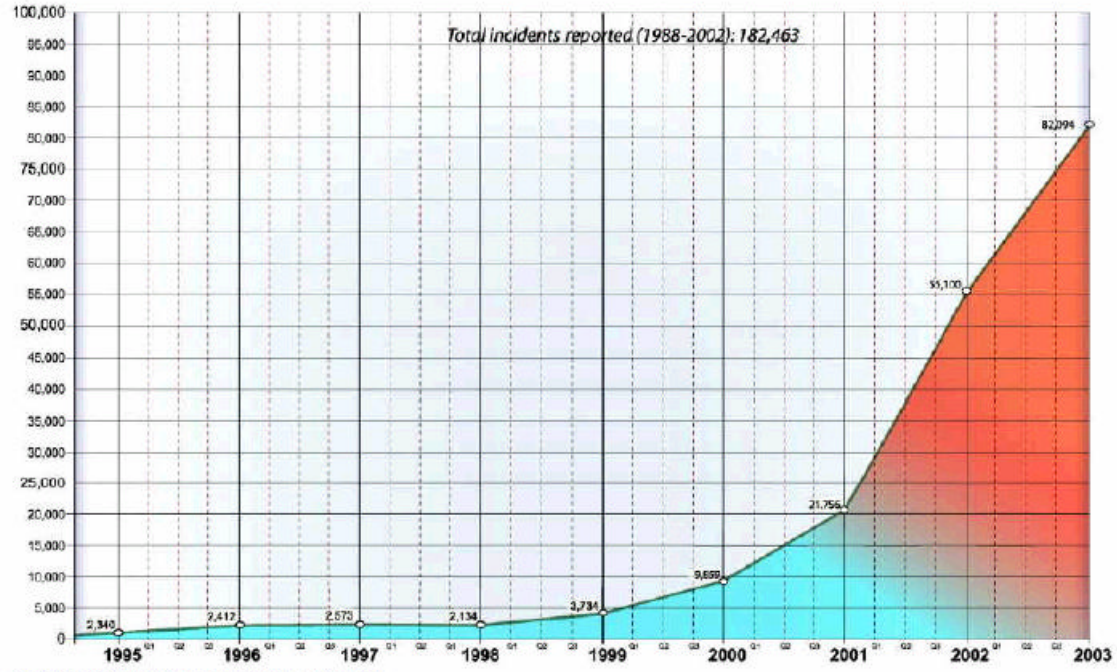
Gefährdungspotential aus dem Internet?
Referent: Peter Wirnsperger, Senior Manager Security Services Group, Deloitte & Touche



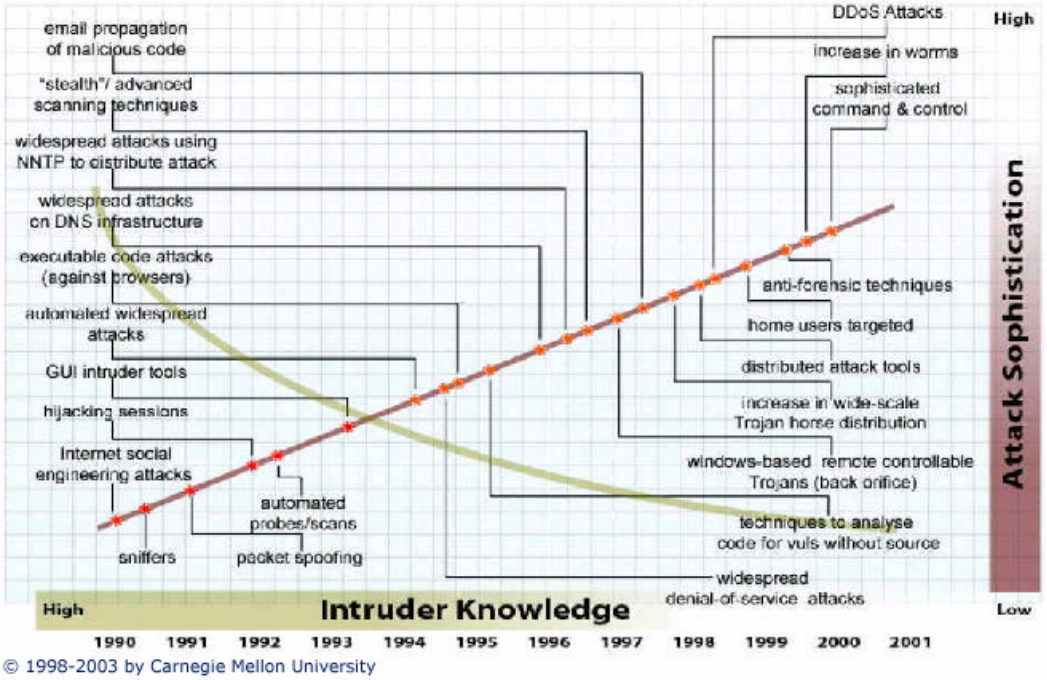
Risiko – Die Realität

- Studien belegen, dass der erste Zugriff auf eine neue Seite im Internet durchschnittlich bereits **28 Sekunden** nach ihrer Freischaltung erfolgt.
- Nach durchschnittlich **5 Stunden** wird sie das erste Mal angegriffen.
- **60%** aller Unternehmensnetzwerke verzeichnen mehr als **30** erkannte Hackerangriffe pro Jahr.

Entwicklung der gemeldeten Vorfälle
CERT Statistik von 1995 - 2003



Entwicklung
Attacken vs. Angreifer Know-how



Was sind typische Angriffsziele?

Überblick

- Alles und jeder, der sich nicht schützt
- Private Anwender:
  Über Viren, Backdoors als Sprungbrett für große Attacken.
- Kleine Firmen:
  Einfach nur zum Spaß
- Große Konzerne:
  Weil man was beweisen will
  Politische Motive

Wer sind die Angreifer?
Was ist die Motivation?

Gruppe	Motivation
• Hacker, Cracker, Phischer	⏩ Ruhm, und Ehre und Idealismus
• Script Kiddies und Möchtegerns	⏩ Fun! Fun! Fun!
• Geheimdienste	⏩ Nationale Sicherheit ;-)
• Betriebsspione	⏩ ¥ € $
• Mitarbeiter!	⏩ Um 10.000 € reicher...

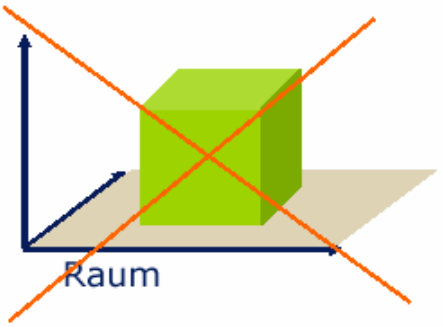
Attacken

Aktuelle Trends

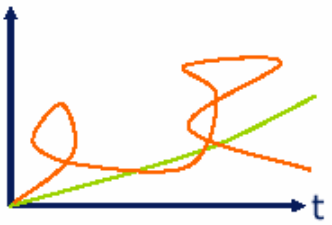
- Automatisierung und Geschwindigkeit der Attacktools
  ⏩ Scanning etc
- Steigende „Qualität“ und Professionalität der Tool
  ⏩ „Anti-Forensics“, dynamische Anpassung, modularer Aufbau
- Schnelle Entdeckung von Verwundbarkeiten
  ⏩ „täglich“ NEU
- Steigendende Durchlässigkeit von Firewalls
  ⏩ Tools und Software-Anforderungen machen aus jeder Firewall einen Schweizer Käse
- Steigende Asymmetrie der Bedrohungen
  ⏩ Ein Angreifer gegen komplexe verteilte Systeme
- Wachsende Bedrohung von Infrastrukturattacken
  ⏩ Bedrohung gegen die originäre Infrastruktur des Internet, der Zugänge etc.

Das Internet
Unendliche Weiten

Gefahren werden bisher über
Zeit und Raum
über den Globus verteilt
-> Raum – Zeit – Kontinuum



Der Raum spielt im Internet
kaum eine Rolle
-> die Verteilung von
möglichen Gefährdungen
entfällt!



Abwehr
Was kann man tun?

- Große Unternehmen ⏩ Sicherheitsmanagement und Beratung
- KMU ⏩ Berater hinzuziehen und ernst nehmen
- Private Anwender ⏩ Kritisch sein,
  argwöhnisch werden,
  nicht immer „JA“ klicken,
  Systeme pflegen

⏩ **Bewusster Umgang mit dem Medium Internet**!

Internetfilterung = Zensur?

Rechtsanwalt Tobias H. Strömer, Düsseldorf

Der Präsident des Zentralrates der Juden in Deutschland, Dr. Paul Spiegel, hat sich vor einigen Monaten für ein entschiedenes Vorgehen gegen rechtsextreme Webseiten im Internet ausgesprochen. Beim einem internationalen Kongress in Düsseldorf sagte er, er habe sich vor 15 Jahren nicht vorstellen können, dass es heute wieder möglich sein würde, öffentlich zum Hass aufzurufen. Nachdem es gelungen sei, Kinderpornografie weitgehend aus dem Netz zu verbannen, verstehe er mit Blick auf Webseiten, die Gewalt verherrlichen und NS-Propaganda verbreiten, nicht, dass solche Gewaltaufrufe noch möglich seien. Gleichzeitig forderte er wirksame Maßnahmen gegen Gewaltaufrufe im Internet. Über den Weg könne man zwar streiten, aber nicht über das Ziel.

Das Internet, wir es uns heute begegnet, bietet einen in dieser Form zuvor nie gekannten Marktplatz der Ideen und Meinungen. Das Netz erlaubt einen einfachen und unkomplizierten Austausch von Ansichten, erleichtert den Kontakt zu Gleichgesinnten und den Aufbau und die Organisation von Interessengruppen. Jeder einzelne Nutzer gewinnt Zugang zu einem wesentlich breiteren Meinungsspektrum. Das Internet wird dadurch zu einem Medium, das die Meinungs- und Informationsfreiheit und damit nicht zuletzt die Demokratie fördert. Dieses Potenzial wird vor allem durch die weltumspannende Dimension des Internets erreicht. Die Menschen erhalten Zugang zu vorher unerreichbaren Informationen, lernen bislang unbekannte Kulturen kennen und können Kontakte über weite Entfernungen aufbauen und unterhalten

Rechtsanwalt Tobias H. Strömer (Mitte)

Die Ausgangssituation

Neue Möglichkeiten bergen jedoch immer auch Gefahren, insbesondere für Kinder und Jugendliche. Einzelne Personen und Organisationen missbrauchen die neuen Freiheiten, indem sie illegale Inhalte über das Netz verfügbar machen, eben auch zu Gewalt gegen Andersdenkende aufrufen oder aus Profitgier Kinderpornographie verbreiten. Nicht alle jugendgefährdenden Inhalte sind hinreichend vor dem Zugriff durch Kinder und Jugendliche geschützt.

Auch Wertunterschiede in verschiedenen Kulturen und Rechtssystemen, die bei der Einschätzung bestimmter Inhalte zu unterschiedlichen Ergebnissen kommen, zeichnen sich ab. Deutsche Nutzer können auf Inhalte zugreifen, die im Widerspruch zu deutschen Jugendschutzregeln oder zu allgemeinen Verbotsgesetzen stehen, möglicherweise in ihrem Ursprungsland jedoch völlig legal sind. Umgekehrt gilt das natürlich auch: Nicht alles, was in Deutschland erlaubt ist, darf auch in anderen Ländern, etwa in Saudi-Arabien oder in China ohne weiteres abgerufen werden. Arbeitgeber, die ihren Mitarbeitern Internet-Zugänge am Arbeitsplatz zur Verfügung stellen, möchten verhindern, dass wertvolle Arbeitszeit mit privaten Chats oder der

Suche nach neuen eBay-Angeboten vergeudet wird. Und Eltern möchten ihre Sprösslinge davor schützen, dass diese ungefiltert an Suizid-Chats teilnehmen, Erotik-Seiten anschauen oder nach Internet-Anleitung Bomben basteln.

Allen Szenarien gemeinsam ist das prinzipiell hohe Gefährdungspotential, das jedoch in den einzelnen Szenarien als unterschiedlich bedrohlich zu bewerten ist.

Bei Themen aus dem sexuellen Bereich besteht die Besonderheit darin, dass je nach Alter eine ganz normale und durchaus entwicklungsförderliche, starke Neugiermotivation besteht. Diese lässt Jugendliche explizit nach auf Sexualität bezogenen Inhalten suchen. Die Problematik liegt dann darin, dass die Darstellung von „unnormalen“, erniedrigenden oder pathologischen Sachverhalten und Handlungen in Wort, besonders aber in Bild und Video die Rezipienten überrascht. Kinder und Jugendliche verfügen nicht über die passenden Abwehrmechanismen, um solche Inhalte verarbeiten zu können. Deshalb werden sexuellerotische Inhalte, ganz besonders jedoch anstößige Darstellungen durch das Jugendschutzgesetz Kindern und Jugendlichen vorenthalten. Diese Schutzfunktion fehlt beim unkontrollierten Internetzugang und kann deshalb zu schweren „Verletzungen“ führen.

Beim Stichwort „Sex“ etwa wirft Google 273.000.000 Seiten aus, von denen immerhin 5,56 Millionen auf deutschen Rechnern gespeichert sind. Im Jahr 1999 waren es weltweit „nur“ 15 Millionen Seiten. Es ist anzunehmen, dass ein großer Teil dieser Seiten wegen der vielen möglichen Bedeutungen des englischen Wortes "sex“ keinerlei jugendgefährdendes Potential haben. Nimmt man aber nur an, dass zehn Prozent der so gefundenen Seiten für Kinder ungeeignet sind – eine Betrachtung der ersten hundert Treffer deutet auf einen deutlich höheren Anteil hin – so lässt sich immer noch eine so große Menge von potentiell jugendgefährdenden Seiten konstatieren, dass die Gefährdung keinesfalls als unerheblich eingestuft werden kann.

Bei Gewaltdarstellungen ist die Sachlage ähnlich. Einen Unterschied kann man allerdings in der Neugiermotivation vermuten. Die Neugiermotivation nach sexuellen Inhalten ist entwicklungspsychologisch anders gelagert als die Neugiermotivation, anderen Leiden zuzufügen und/oder andere leiden zu sehen. Prinzipiell ist jedoch auch diese Neugiermotivation schon im Kinder- und Jugendlichenalter vorhanden, wenngleich die Ausprägung als schwächer einzuschätzen ist.

Wer verhindern will, dass im Internet jeder jederzeit jeden Inhalt zu Gesicht bekommt, der irgendwo auf der Welt auf einer Website zum Abruf angeboten wird, kann auf die Anbieter der Inhalte selbst einwirken, er kann die Provider anhalten, Seiten mit verbotenen Inhalten zu sperren oder er kann beim Endverbraucher ansetzen und dort unerwünschte Inhalte ausfiltern.

Verbote

Bei Maßnahmen zur Bekämpfung illegaler oder unzureichend geschützter jugendgefährdender oder sonst erbotener Inhalte im Internet ist es wichtig, zwischen den verschiedenen Beteiligten im weltweiten Internet zu unterscheiden und deren gestufte Verantwortlichkeit anzuerkennen, wie sie sowohl im deutschen (§ 8 ff. Teledienstegesetz, § 6 ff. Mediendienste-Staatsvertrag) als auch im europäischen Recht (Artikel 12 ff. E-Commerce-Richtlinie) festgelegt ist. Vorrangiges Ziel muss stets sein, den jeweiligen Anbieter des inkriminierten Inhaltes selbst in Anspruch zu nehmen, also den Content-Provider. Gegen ihn kann die ganze Bandbreite straf- oder ordnungsrechtlicher Maßnahmen ergriffen werden. Gegen den Anbieter solcher Inhalte können im Übrigen auch Wettbewerber, Verbraucherschutzverbände und Wettbewerbszentralen mit Erfolg vorgehen. Vor allem die Behörden sind aufgerufen, diese Instrumente, gerade bei den illegalen, oft menschenverachtenden Inhalten auch in vollem Umfang einzusetzen.

Zuzugeben ist allerdings, dass in der Praxis die Inanspruchnahme der Anbieter selbst sehr rasch an Grenzen stößt. Die meisten unzulässigen Inhalte werden nämlich – auch von offenkundig deutschen Website-Betreibern – aus dem fernen Ausland aus angeboten. Eine Verfolgung solcher

Angebote verbietet sich nicht zuletzt aus wirtschaftlichen Gründen, weil das Abschalten einer einzigen Website mit unzulässigen Angeboten Tausende von Euro verschlingen kann. In anderen

Fällen ist ein erfolgreiches Vorgehen gegen den Anbieter schon deshalb nicht möglich, weil der Staat, in dem der Internet-Server mit dem inkriminierten Angebot steht, die Verbreitung des Angebots als Ausfluss der Meinungsfreiheit ausdrücklich erlaubt. In vielen Ländern ist man geradezu stolz darauf, auch rassistische Äußerungen oder (einfache) Pornographie ertragen zu müssen, weil nur so dem Grundrecht auf Meinungs- und Informationsfreiheit wirkungsvoll Rechnung getragen werden könne.

Sperren

Diejenigen, die ein unzulässiges Angebot nicht selbst betreiben, sondern nur Speicherplatz für fremde Inhalte vorhalten (Host-Provider), haften nur insoweit, als ihnen diese Inhalte bekannt sind. Eine Pflicht zur Prüfung von oder gar Suche nach bestimmten Inhalten trifft sie dabei nicht. Die reinen Zugangsvermittler zum Internet, deren Dienstleistung sich auf die Durchleitung fremder Inhalte beschränkt (Access-Provider), sind für die von ihnen vermittelten Inhalte sogar in keinem Fall verantwortlich. Sie verschaffen nur den Zugang zum Internet in technischer Hinsicht. Sie können daher im Prinzip nicht Adressat von Maßnahmen wegen illegaler und jugendgefährdender Inhalte sein, zu denen Nutzer über ihre Vermittlungsdienste Zugang erhalten. Auch der Jugendmedienschutz-Staatsvertrag sieht ausdrücklich vor, dass die entsprechenden Regeln aus TDG und MDStV von den neuen Vorschriften nicht berührt werden (§ 2 Abs. 3 JMStV).

Allerdings eröffnen einige gesetzliche Regelungen in dem Fall, dass Maßnahmen gegen die Verantwortlichen keinen Erfolg versprechen, die Option zur Inpflichtnahme der Zugangsvermittler (§ 22 Abs. 3 MDStV, hierauf verweisend § 20 Abs. 4 JMStV). Diese Regelungen stellen allerdings keine Ausnahmen vom Prinzip der Nichtverantwortlichkeit dar, sondern sind nur besondere Ausprägungen der allgemeinen ordnungsrechtlichen Möglichkeit, zur Gefahrenabwehr auch den selbst nicht verantwortlichen, so genannten Nichtstörer in Anspruch zu nehmen.

Auf diese Rechtsgrundlage hat in der Vergangenheit die Bezirksregierung Düsseldorf Verfügungen gestützt, mit denen eine große Zahl von in Nordrhein-Westfalen ansässigen Access-Providern verpflichtet werden sollte, den Zugang zu zunächst zwei in den Vereinigten Staaten gehosteten und aus deutscher Sicht illegalen Webangeboten zu sperren. Augenblicklich sind zu diesen Sperrungsverfügungen zahlreiche gerichtliche Verfahren im vorläufigen Rechtsschutz und in der Hauptsache anhängig.

Die Inanspruchnahme nicht verantwortlicher Personen kann allerdings immer nur subsidiär gegenüber den polizeirechtlich Verantwortlichen erfolgen. Erst wenn alle denkbaren Maßnahmen nicht zu einer erfolgreichen Gefahrenabwehr führen können, ist die Heranziehung des „Nichtstörers“ zu rechtfertigen. Diesen zentralen ordnungsrechtlichen Grundsatz gilt es bei allem Verwaltungshandeln in diesem Bereich zu beachten. Dabei kann es nicht genügen, dass Maßnahmen gegen den eigentlich verantwortlichen Inhalteanbieter aufwändiger oder vielleicht auch in ihrem Erfolg weniger gewiss sind. Der Zugriff auf die Access-Provider darf, wie jede Maßnahme gegen nicht verantwortliche Personen, nie erstes, sondern stets nur letztes Mittel sein.

Darüber hinaus ist bei jedem Verwaltungshandeln das Prinzip der Verhältnismäßigkeit zu beachten, was insbesondere die Geeignetheit der jeweiligen Maßnahme erfordert. An dieser fehlt es, wenn die Maßnahme keinen oder jedenfalls nur geringen Erfolg verspricht. Bei den aktuell diskutierten technischen Wegen zur Implementation anbieterseitiger Zugangssperren, etwa der Manipulation der Domain-Name-Server (DNS), bestehen jedoch erhebliche Zweifel an den Erfolgsaussichten. Die Sperren können mit wenigen Schritten durch Wahl eines anderen Domain Name Servers oder die Nutzung eines ausländischen Providers umgangen werden. Anleitungen hierzu sind schon heute im Netz verfügbar. Der Sperrwirkung entfaltet sich damit gerade nicht gegenüber den potentiellen Interessierten an schädlichen Inhalten, sondern nur gegenüber Zufallsbesuchern, die sich auch auf andere Art, etwa durch nutzerseitige Filtersysteme schützen

können. Andere technische Ansätze, wie die Sperrung ganzer IP-Adressen oder der Einsatz von Proxy-Servern, sind nicht in der Lage, hinreichend zielgenau einzelne Inhalte zu sperren, sodass auch nicht problematische Inhalte betroffen wären, oder sie behindern maßgeblich die technischen Funktionen des Internets, indem sie die Leistungsfähigkeit und Ausfallsicherheit der Infrastruktur gefährden.

Zu beachten ist in diesem Zusammenhang auch, dass die Einrichtung und Pflege der Sperren – unabhängig vom hierzu gewählten technischen Ansatz – erheblichen Aufwand und damit Kosten bei den betroffenen Internetunternehmen verursachen, deren betrieblichen Ablauf maßgeblich beeinträchtigen und diese damit im internationalen Wettbewerb erheblich benachteiligen. Auch dieser Aspekt ist bei der im Verhältnismäßigkeitsprinzip niedergelegten Abwägung von Zielerreichung und damit verbundenen Belastungen zu berücksichtigen, selbst wenn die Unternehmen nach allgemeinen ordnungsrechtlichen Grundsätzen einen Anspruch auf eine aufwandsgerechte Entschädigung für ihre Inpflichtnahme haben.

Vor diesem Hintergrund ist es jedenfalls nicht angemessen, wenn – wie zum Teil gefordert – auf alle illegalen oder unzureichend geschützten jugendgefährdenden Inhalte im weltweiten Internet mit entsprechenden Sperrungsverfügungen gegen Access-Provider in Deutschland reagiert würde.

Zweifel an der Verhältnismäßigkeit bestehen insbesondere beim Einsatz von Sperrungsverfügungen gegen Access-Provider zur Erreichung von Jugendschutzzielen. Da eine differenzierte Wirkung der Sperren nach dem Alter der betroffenen Nutzer nicht möglich ist, führen solche Maßnahmen in diesen Fällen zusätzlich zu Freiheitseingriffen erwachsener Internetnutzer, für die völlig legale Inhalte nur noch erschwert zugänglich wären. Diese Drittbetroffenheit sollte dazu führen, von Sperrungsmaßnahmen zu Jugendschutzzwecken ganz abzusehen. Jugendschutz sollte grundsätzlich durch Filtersysteme auf den Endgeräten der Nutzer – gegebenenfalls im Zusammenwirken mit einer beschreibenden Kennzeichnung der Inhalteanbieter wie beim internationalen Filtersystem der Internet Content Rating Association (ICRA) –, nicht jedoch durch pauschale Sperrungen auf Seiten der Zugang vermittelnden Access-Provider sichergestellt werden.

Filter

Wer Filterprogramme einsetzt, schützt den Nutzer des Rechners weitgehend vor der Konfrontation mit unzulässigen Inhalten. Er greift aber zugleich in dessen Möglichkeit ein, sich frei und ungehindert aus allen zugänglichen Quellen zu informieren. Solange eine Filterung dazu dient, auf dem lokalen Rechner Seiten zu sperren, die Gewaltverherrlichung, Kinderpornographie und Rassenhass verherrlichen, mag ein breiter Konsens zur Vertretbarkeit bestehen.

Anders sieht es möglicherweise dann aus, wenn solche Programme auch solche Inhalte herausfiltern sollen, die nur aus der Sicht des Verwenders oder bestimmter Interessengruppen unerwünscht sind. Filter können dazu verwendet werden, unliebsame Meinungen zu unterdrücken, jeden Kontakt mit nackter Haut im Internet zu vermeiden oder dem Nutzer eines Internetrechners bestimmte Themen insgesamt vorzuenthalten. Wer rechtsradikale Seiten wegfiltert, verhindert damit die Verbreitung verbotener Inhalte. Wer eine Diskussion um Suizid bei Kindern, vielleicht auch Anleitungen hierzu unterdrückt, kann unter Umständen zwar mit der moralischen Unterstützung einer breiten Bevölkerung rechnen, er erfüllt aber keinen gesetzlichen Auftrag. Ähnliches gilt für das Filtern von Bombenbastel-Anleitungen, die – darauf werde ich später noch zu sprechen kommen – regelmäßig rechtlich zulässig sind. Und erst recht handelt der Arbeitgeber, der jede Teilnahme an Chats, Diskussionsforen, Online-Versteigerungen oder Gewinnspielen während der Arbeitszeit verhindern möchte, nicht aus altruistischen, sondern ausschließlich eigennützigen Beweggründen. Aus rechtlicher Sicht ist aber gegen den Einsatz von Filterprogrammen auch zu solchen Zwecken nichts einzuwenden. Der Einsatz solcher Filterprogramme ist insbesondere nicht gleichzusetzen mit unerwünschten oder gar unzulässigen Zensurmaßnahmen.

Zum einen kann Zensur schon von der Bedeutung des Begriffs her nur im Über-Unter-Ordnungs-Verhältnis stattfinden. Der Bürger ist vor Zensurmaßnahmen geschützt, die staatliche Behörden verfügen. Wer im Gleichordnungsverhältnis, also etwa als Arbeitgeber oder Betreiber eines Internet-Cafés, freiwillig anderen einen Internet-Zugang bereitstellt, kann frei darüber entscheiden, welche Inhalte er verfügbar machen möchte. Ob und in welchem Umfang er eine solche Entscheidung sogar treffen muss, darauf werde ich in meinem zweiten Vortrag heute noch zurückkommen. Umgekehrt obliegt es natürlich der freien Entscheidung des Kunden, ob er seinen Informationsbedarf gerade in einem Internet-Café stillt, das Inhalte restriktiv filtert. Auch der Jugendliche am Ausbildungsplatz oder in der Schule oder der Arbeitnehmer, dem vom Arbeitgeber nur ein eingeschränkter Internetzugang zur Verfügung gestellt wird, kann ja an einem eigenen oder einem anderen Rechner die Informationen abrufen, die ihm durch Filtermaßnahmen vorenthalten werden.

Zum anderen gehören nach unserem Verfassungsverständnis zur grundrechtlich geschützten Meinungs- und Informationsfreiheit aber nicht die Verbreitung rechtsextremistischen Gedankenguts. Nach Art. 5 GG finden die Meinungs- und Informationsfreiheit ihre Schranken in den Vorschriften der allgemeinen Gesetze und in den gesetzlichen Bestimmungen zum Schutz der Jugend (also etwa im Strafgesetzbuch oder Jugendschutzgesetz), die ihrerseits im Licht des Grundrechts auszulegen sind. Wann danach im Einzelfall die Verbreitung rechtsextremistischen Gedankenguts gesetzlich verboten und außerhalb der Schutzes der Meinungsfreiheit liegt, ist naturgemäß am konkreten Fall zu entscheiden.

Förderung von Medienkompetenz

Der Jugendschutz wird durch das Internet und seine Möglichkeiten vor neue Herausforderungen gestellt. Auf dem Weg in die Informationsgesellschaft unterliegen gesellschaftliche Werte und Normen einem Wandlungsprozess. Auf Kinder und Jugendliche gerichtete Orientierungshilfen müssen diesem Prozess Rechnung tragen.

Kinder und Jugendliche sehen sich heute nicht nur im Internet, sondern auch an anderen Orten viel stärker als noch vor einigen Jahren Einflüssen ausgesetzt, die teils unerwünscht, teils sogar verboten sind. Die Grenzen zwischen unerwünschten und verbotenen Inhalten sind dabei fließend. Kinderpornographie und Aufruf zum Rassenhass sind aus Gründen verboten, über die wir hier und heute nicht diskutieren müssen. Beides ist unterliegt einem strengen und – in unserer heutigen Gesellschaft – eben nicht ernsthaft diskutablen Verbot, weil eine Zulassung der damit verbundenen Handlungen mit unserer Gesellschaftsordnung nicht in Übereinklang zu bringen sind, ja sogar schier unerträglich wirken. Über andere Verbote wird man lebhaft streiten können. Tatsächlich geschieht das auch. Wenn in den Niederlanden Haschischkonsum und die Verbreitung einfacher Pornographie straffrei ist oder in den USA nach dem First Amendment auch Auschwitzlügen verbreitet werden dürfen, wird man sich ernsthaft fragen dürfen, ob die Erfüllung solcher Tatbestände vom deutschen Gesetzgeber zwingend unter Strafandrohung verboten werden müssen.

Tatsächlich geht es aber gar nicht darum, ob ein bestimmter Sachverhalt mit Strafe bedroht ist oder nicht. Allein die Strafdrohung in Deutschland hält Täter nämlich nicht davon ab, ihre Meinungen und Inhalte in Deutschland kundzutun. Daran wird sich auch in Zukunft nichts ändern. Es ist vielmehr abzusehen, dass Kinder und Jugendliche sogar verstärkt Einflüssen ausgesetzt sind, die allein mit Strafdrohungen oder staatlichen Eingriffen nicht zu verhindern sind. Offensichtlich ist auch, das Heranwachsende nicht durch Überwachung und Verbote allein davon abgehalten werden können, unzulässige Inhalte zu rezipieren. Zwingend erforderlich ist daher die Förderung von Medienkompetenz, also die Erziehung zum verantwortungsvollen und selbstbewussten Umgang gerade auch mit unangenehmen Inhalten, unabhängig davon, ob dem

Betroffenen solche Inhalte an der Tankstelle, im Bezahlt-Fernsehen oder im Internet begegnen.

Die Förderung von Medienkompetenz bei Heranwachsenden hat absoluten Vorrang vor dem Einsatz von Verboten, Sperren und Filtern, die zwangsläufig unvollkommen sind. Medienkompetenz meint dabei sowohl die technische Beherrschung der Medien als auch einen qualifizierten, eigenverantwortlichen Umgang mit den Inhalten. Die Vermittlung von Medienkompetenz liegt dabei im Spannungsfeld zwischen Jugendschutz und Informationsfreiheit. Als Handlungsoptionen bieten sich neben dem Aufbau von Medienkompetenz die Nutzung von sozialen Kontrollmechanismen (Aufsicht, Kontrolle von aufgesuchten Web-Seiten, soziale Ächtung von Verstößen etc.) und die Weiterentwicklung der technischen Unterstützung sowie – vor allem – Kombinationen dieser Maßnahmen an.

Daneben ist es erforderlich, dass die Gesellschaft den Urhebern und den potentiell empfänglichen Adressaten rassistischer oder fremdenfeindlicher, gewaltverherrlichender und (kinder)pornographischer Inhalte mit intensiver Aufklärungs- und Überzeugungsarbeit begegnet.

Parallel muss über die in rassistischen, fremdenfeindlichen und gewaltverherrlichenden Botschaften liegenden Gefahren und Irrtümer informiert und vor ihnen gewarnt werden. Ziel sollte letztlich nicht das Blockieren von Meinungsäußerungen, sondern das Bemühen sein, die dahinter stehenden Ideologien und Irrtümer durch Aufklärung zu bekämpfen. Hierzu kann am besten eine offene, freie und von gelebter Toleranz geprägte Gesellschaft beitragen. Alle Kräfte in dieser Gesellschaft sollten dabei den bewussten und verantwortlichen Umgang mit Freiheit – gerade auch mit der Meinungsfreiheit und damit auch mit den Möglichkeiten der neuen Medien – fördern und fordern.

Wo immer ein Wertekonsens erreicht werden kann, sind die Staaten zu einer Stärkung der internationalen Zusammenarbeit aufgerufen, um so den Zugriff auf die Urheber illegaler Meinungsäußerungen auch über nationale Grenzen hinweg zu ermöglichen. Oft wird ein solcher Konsens aber nicht zu erreichen sein.

Das Teledienstegesetz und der Mediendienstestaatsvertrag weisen den Diensteanbietern eine differenzierte Verantwortung für Inhalte zu. Jugendmedienschutz-Staatsvertrag und Jugendschutzgesetz heben neben staatlichen Maßnahmen entscheidend auf eine freiwillige Selbstkontrolle, den technischen Selbstschutz und auf die maßgebliche Rolle der Erziehungsberechtigten ab. Dabei darf aber nicht aus den Augen verloren werden, dass technische Lösungen zur Filterung der Inhalte weder adäquaten noch absoluten Schutz bieten. Verfügbare Filterprogramme zeigen wenig Treffsicherheit und sind leicht zu manipulieren; ihre Bedienung ist mühsam. Die deutsche Sprachfunktionalität ist unzureichend. Kategoriensysteme zur Kennzeichnung von Inhalten sind bisher nicht weit genug verbreitet, um als Basis für eine flächendeckende qualifizierte Filterung zu dienen. Ein auf den deutschen oder europäischen Kulturraum zugeschnittenes Werte- und Kategoriensystem existiert nicht. Die Filterprogramme eines Anbieters können daher nur relativ besser sein als die eines Mitbewerbers. Jedes System zur Inhaltsfilterung kann außerdem bei falscher Konfiguration und fehlender Kontrolle zur Beschränkung der Informationsfreiheit missbraucht werden. Daher ist es notwendig, dies bei der Konzeption zu beachten und organisatorische Maßnahmen zur Missbrauchsverhinderung vorzusehen.

Jugendschutz - ein Thema in der kirchlichen Internet-Seelsorge?

Tom O. Brok, Leiter der Internetarbeit der Evangelischen Kirche in Deutschland (EKD)

Sehr geehrte Damen und Herren,

herzlich danke ich für die Gelegenheit, die Aktivitäten der Internetarbeit der Evangelischen Kirche in Deutschland im Bereich des Jugendmedienschutzes auf dieser Konferenz vorstellen zu können. Die EKD gehörte mit dem eigenen Internetangebot ekd.de mit zu den ersten kirchlichen Websites, die Anfang 1996 überhaupt im Internet zu finden waren. Als Betreiber öffentlicher Internetforen im Rahmen unserer Öffentlichkeitsarbeit wurde schnell klar, dass wir es nicht nur mit harmlosen Informationssuchern und theologischen Diskutanten zu tun haben. Unsere Foren bieten uns nicht nur die Möglichkeit, den Kontakt zu unseren Mitgliedern zu gestalten und mit Kritikern und religiös Interessierten den Diskurs aufzunehmen. Unsere Foren sind, zwar in unregelmäßigen Abständen und zum Glück recht selten, aber auch ein Ort, an dem Forennutzer versuchen, illegale Inhalte zu publizieren und auf entsprechende Internetangebote zu verlinken. Warum sollte die Kirche von diesem Versuch verschont bleiben. Entscheidend ist, dass er nicht gelingt.

Unsere Systeme arbeiten mit Wortfiltern, die verdächtige Forenbeiträge zunächst sperren. Unsere Online-Redaktion sichtet mehrfach täglich alle Beiträge und kann ggf. schnell eingreifen. Uns ist es wichtig, dass die kirchlichen Internetangebote eine verlässliche Adresse für die Recherche religiöser Themen sind, die von allen Altersgruppen bedenkenlos genutzt werden können.

Aber mit dem Einsatz von Wortfiltern und einer Redaktion, die auch eingreift, waren wir mitten drin in der Diskussion zwischen Meinungsfreiheit und Zensur. Mitten drin in der Frage, wie viel Meinungsfreiheit eigentlich die eigene Öffentlichkeitsarbeit verträgt, bevor sie Image-schädigend wirkt. Ich denke, es ist kein Zufall, dass sich nur noch recht wenige kommerzielle Internetangebote ein eigenes Gästebuch leisten - sofern Community-Funktionen nicht zum Geschäftsmodell gehören.

Der tägliche Aufwand für den Betrieb von Internetforen ist sehr hoch. Mit dem Betrieb unserer Foren waren wir aber auch mitten drin in den Problemen eines Wortfilters und seiner Funktionalität. Ein wenig pathetisch könnte man sagen, Sehnsucht nach semantischen Systemen stellt sich ein, die erkennen, ob sensible Wörter in Kontexten einer kritischen Auseinandersetzung stehen oder in eher zweifelhaften Kontexten vorkommen.
Nichts ist schlimmer für eine lebendige Diskussion, als wenn harmlose Beiträge im Filter stecken bleiben. Nichts ist schlimmer als wenn ein Beitrag nicht automatisch erkannt wurde, der auf problematische Seiten verlinkt. Insgesamt stellt sich die Situation so dar, dass wir zum Glück recht selten eingreifen müssen. Unsere Foren werden redaktionell betreut, damit wir dauerhaft eine Diskussionsplattform bieten können, die sowohl der Meinungsfreiheit Rechnung trägt, wie auch die Grenzen publizierbarer Inhalte klar aufzeigt.

Drei relevante Projekte aus dem Bereich des Jugendmedienschutzes möchte ich Ihnen heute vorstellen. Beginnen werde ich mit der Internetseelsorge. In einem zweiten Punkt möchte ich Ihnen den Verhaltenscodex unserer eigenen Suchmaschine crossbot vorstellen. Und als dritten Punkt werde ich auf den Erfurter Netcode eingehen.

1. Internetseelsorge

Zu den grundlegende Aufgaben und Kompetenzen unserer Kirche gehört die Seelsorge. So wie der Pfarrer oder die Pfarrerin in der Gemeinde vor Ort auf Probleme ansprechbar ist, so können sich Ratsuchende auch über das Internet mit ihren Anliegen an uns wenden.

Die klassische Telefonseelsorge, die seit über 50 Jahren tätig ist, bietet zugleich Internetseelsorge an - unter der Adresse www.telefonseelsorge.org. Über eine Web-Mail-Plattform besteht die Möglichkeit, einen Gesprächspartner zu finden. Auf das Versenden von Emails wird dabei bei diesem Beratungsangebot aus Sicherheitsgründen komplett verzichtet. Noch nicht einmal seine E-Mail-Adresse muss der Ratsuchende preisgeben.

Die Qualitätsstandards einer langjährigen Seelsorge-Ausbildung und einer ständigen Supervision der Beratenden gehören selbstverständlich zum Konzept hinzu. Die Niedrigschwelligkeit des Internet ermöglicht es Menschen, sich an die Seelsorge zu wenden, die sich nicht in der Lage fühlen, über ihre Probleme zu sprechen und ihre Stimme am Telefon preiszugeben, die aber in der Schriftform nach Worten suchen.

Zu den Grundsätzen der Internetseelsorge gehört die Anonymität ebenso wie die Vertraulichkeit. Ein anonymer Internetkontakt öffnet für viele Menschen die Möglichkeit, neue Wege zu gehen und zum Beispiel einen Erstkontakt zu einer helfenden Einrichtung zu wagen. Hilflosen und verzweifelten Menschen durch die Telefon- und InternetSeelsorge vertrauliche und unentgeltliche Hilfe anzubieten, gehört zum diakonischen Auftrag unserer Kirche.

Die Vertrauenswürdigkeit, dass Kirche ein offenes Ohr für die Fragen der Menschen hat, wird uns auch im Internet entgegengebracht. Die Anzahl der Beratungsanfragen betrug im Jahr 1999 noch 2.500, im Jahre 2001 dagegen schon über 11.000.

Im Herbst letzten Jahres startete die Hannoversche Landeskirche das neue Projekt chatseelsorge.de. An drei Abenden pro Woche stehen Seelsorger und Seelsorgerinnen entweder in einem Einzelchat oder einem Gruppenchat zum Gespräch zur Verfügung. Pro Abend treffen sich etwa 25 Menschen auf dieser Chat-Plattform.

Insgesamt merken wir, dass die Nachfragen über das Internet stetig steigen. Unser Dienst ist von den Menschen gefragt. Kirchlicherseits ist die Seelsorge ein Dienst, den wir nach unserem diakonischen Selbstverständnis natürlich gerne anbieten. Eine Nachfrage bei den Verantwortlichen der einzelnen Seelsorge-Angebote erbrachte das Ergebnis, dass solch' brisante Themen wie Bombenbauanleitungen oder Gewaltverherrlichende Internetseiten keine nennenswerte Rolle spielen. Entweder gibt es wenige Menschen, die mit solchen Seiten in Berührung kamen und sich dann an uns wandten. Oder wenige Menschen stoßen überhaupt auf solche Angebote im Netz. Was die Erreichbarkeit dieser Angebote natürlich nicht weniger problematisch macht.

Jugendschutzrelevante Themen kommen in den Anfragen an die Seelsorger eher selten vor. Aber natürlich stehen Internet-, E-Mail- und Chatseelsorge als Anlaufstellen mit ihrem Beratungspotential allen Hilfesuchenden zur Verfügung - als offenes Ohr für die Nöte und Ängste der Menschen. Das Zuhören (auch am Bildschirm) hat alleine schon eine entlastende Funktion. Der gemeinsame Versuch zwischen dem Ratsuchenden und dem Seelsorger, die Not wenigstens mit Worten zu formulieren und so zu konkretisieren, kann Handlungsspielräume eröffnen und helfen die Situation zu klären. Die Möglichkeit, auf andere Beratungsangebote und Beschwerdestellen hinweisen zu können, bietet sogar konkrete Handlungsoptionen mit Erfolgsaussicht.

2. Verhaltenscodex der EKD-Suchmaschine Crossbot

Es ist kein Geheimnis. Die meisten Menschen erschließen sich das Internet über die großen Suchmaschinen oder die Einstiegsportale der großen Online- Dienste. Diese bekommen damit eine nicht zu unterschätzende Bedeutung für den Weg, den Internetnutzer und -nutzerinnen durch die virtuelle Welt nehmen. Als Gatekeeper lenken sie die Aufmerksamkeit der Nutzer.

Sie stehen am Beginn der Internet-Recherche vieler Menschen und haben somit publizistische und ökonomische Macht. Sie prägen die Wahrnehmung von Lebenswelten und stehen damit in einer besonderen Verantwortung für die Art und Weise, in der Suchmaschinen genutzt werden können, was mit ihnen gefunden wird und in welcher Reihenfolge sie die einzelnen Angebote listen.

Im Rahmen des Projektes „Transparenz im Netz“ hatte die Bertelsmann Stiftung die Initiative ergriffen, einen Verhaltenskodex, einen Code of Conduct, zu entwickeln, dem sich die Betreiber von Suchdiensten freiwillig unterwerfen sollen. In einer Studie der Stiftung aus dem Jahre 2002 zeigte sich, dass nur wenige Nutzer wissen, wie die Rankings innerhalb der Suchergebnisse zustande kommen oder wie sich Suchmaschinen finanzieren.

Diese Initiative hat zwei Ziele: Zum einen sollte gegenüber den Suchmaschinennutzern Transparenz hergestellt werden. Es geht dabei z.B. um die Frage: Nach welchen Kriterien die Listung der Ergebnisse im Ranking erfolgt? Oder: Welche Einträge ihre Position gekaufter Werbung verdanken?

Zum anderen ging es aber auch um die Frage, welche jugendschutzrelevanten Informationen über die Suchmaschinen gefunden werden. Die Studie der Bertelsmann Stiftung kam zu dem Ergebnis, dass nur wenige der 146 untersuchten Suchmaschinen Auskunft über ihre Maßnahmen für den Jugendschutz geben. Die Untersuchung beschreibt weiter, dass illegale Inhalte von den meisten Anbietern ausgeschlossen werden, dass aber nur ein Fünftel z.B. einen Family-Filter anbieten und dass fast niemand mit PICSLabeln etikettierte Seiten bevorzugt. Im Jahre 2002 hatte nur ein Viertel aller Betreiber einen Jugendschutzbeauftragten benannt; dies mag heute anders sein.

Eine weitere Untersuchung im Mai 2003 erbrachte das Ergebnis, dass Suchmaschinenbenutzer auch gegen ihren Willen auf jugendgefährdende Inhalte geleitet werden, indem sich Adult-Anbieter falscher Schreibweisen von Namen wie Britney Spears oder Kylie Minogue zu Nutze machen.

Die Bertelsmann Stiftung schlug daher einen freiwilligen Verhaltenscodex für Suchmaschinen vor, der die beiden Aspekte Transparenz für die Nutzer und Jugendmedienschutz betrifft. Im Verhaltenskodex festgeschrieben ist das Ziel, Kinder und Jugendliche vor jugendgefährdenden Inhalten zu schützen. Die Suchmaschinenbetreiber sollten daher Familienfilter zur Verfügung stellen. Dabei sollten sie nicht auf den Hinweis verzichten, dass Filter keine absolute Sicherheit gewährleisten können und Kinder nicht ohne Aufsicht der Eltern das Internet nutzen sollten.

Die Suchmaschine Crossbot hat als erste und bisher einzige Suchmaschine den Verhaltskodex akzeptiert und zum Bestandteil der Nutzungsbedingungen gemacht. Crossbot garantiert das Bemühen, jugendschutzrelevante Inhalte aus dem Suchdienst fernzuhalten. Crossbot ist ein Dienst der evangelischen Kirche, der im Sommer 2003 gestartet wurde. Er ist die Kombination eines klassischen Web-Katalogs kombiniert mit einer Suchmaschine. Wir nennen crossbot die Christliche Qualitätssuchmaschine. Wir gehen davon aus, dass crossbot eine Suche mit anderen Suchdiensten sicherlich nicht überflüssig macht. Doch wer im kirchlichen Bereich, oder weiter gefasst im christlichen Bereich nach Informationen recherchiert, dürfte mit crossbot schneller zu validen Ergebnissen kommen.

Crossbot soll einen Teilbereich des Internet erschließen helfen und dabei gerade auch kleineren kirchlichen Angeboten die Chance eröffnen, nicht unterhalb der Wahrnehmungsgrenze, erst auf Seite 35 der Ergebnisse gelistet zu werden. Eine Redaktion prüft die Internetadressen, bevor sie in den Katalog aufgenommen werden. Derzeit sind eine halbe Million Seiten auffindbar. Obwohl ein solcher gut gepflegter Katalog eine hohe Garantie gibt, keine jugendgefährdenden Inhalte zu listen, so wird dennoch auf die bleibende Notwendigkeit hingewiesen, dass Eltern mit ihren Kindern nicht aus der medienpädagogischen Verantwortung entlassen sind.

Unsere Nutzungsbedingungen erinnern an diese Verantwortung. Zwei Jugendschutzbeauftragte dienen in diesen Fragen als Ansprechpartner.

Wir hoffen sehr, dass sich weitere Suchmaschinenbetreiber diesen Verhaltscodex zu eigen machen und in Form einer Selbstkontrolle zeigen, dass sie sich ihrer Verantwortung bewusst sind. Wenngleich ich gerne zugebe, dass unsere recht überschaubare Suchmaschine natürlich in einer besseren Ausgangslage ist.

Ein Nebeneffekt dieses Suchdienstes könnte sein, dass wir daraus recht schnell eine Positivliste von Angeboten kreieren könnten, die verschiedenen Filtersystemen zulieferbar wäre. Wenngleich sich daran natürlich sofort weitere Fragen anknüpfen wie: Was würde passieren, wenn solche Systeme z.B. nicht-demokratischen Staaten in die Hände fielen. Wer hätte Einsicht in diese Listen? Können diese Listen ausgelesen werden? Können Positivlisten in Negativlisten verwandelt werden? Aber auch die Frage, ob Positivlisten verschiedener gesellschaftlich relevanter Gruppen einen wirklichen Sinn machen. Das derzeit wenig bekannte und somit wenig effektive ICRA-System hatte solches einmal angedacht. Diese und andere Fragen müssen im Vorfeld bedacht werden.

Herr Tom O. Brok

2. Erfurter Netcode

Unter maßgeblicher Beteiligung der Rundfunkbeauftragten der beiden großen Kirchen und der Landeshauptstadt Erfurt wurde im Jahre 2002 in Kooperation mit dem Kinderkanal der Erfurter Netcode e.V. gegründet. Der Netcode möchte im ethischen Diskurs zwischen Anbietern und Nutzern Kriterien für kindgerechte Internetseiten entwickeln und die Anbieter von Inhalten ermuntern, entsprechend den formulierten Qualitätsstandards Angebote für Kinder zu publizieren.

Fünf Aspekte sind dabei von besonderer Bedeutung:

1. Soll eine Selbstdarstellung des Anbieters für Transparenz und Vertrauen sorgen.
2. Sind die Jugendschutzbestimmungen einzuhalten.
3. Soll das Angebot Kinder an eine eigenverantwortliche Internetnutzung heranführen, inkl. Der Möglichkeiten zur Kommunikation.
4. Ist der Verkauf von Waren klar zu trennen von redaktionellen Inhalten.
5. Ist höchste Transparenz und Sicherheit geboten bei der Verwendung persönlicher Daten.

Durch begleitende wissenschaftliche Studien zur "Kinderkultur im Internet" wird unter ethischen und pädagogischen Fragestellungen die Rezeption von Kinderseiten untersucht und nach einer kinder- und jugendspezifischen Netzkultur gefragt. Zusammen mit den kommerziellen Anbietern sollen die vorgestellten Kriterien zu einem Gütesiegel für kindgerechte Internetangebote weiterentwickelt werden. Der Schwerpunkt des Erfurter Netcode liegt auf den medienpädagogischen Aspekten. Kinder sollen zu einem selbstständigen und verantwortlichen

Umgang mit dem Internet befähigt werden. Auf einer geschützten, spielerischen Plattform sollen sie an das Medium herangeführt werden, damit sie sich später im Bewusstsein der Gefahren im Internet orientieren können und in Konfliktsituationen Strategien zu deren Bewältigung eingeübt haben. Ein sicheres und möglichst gehaltvolles Internetangebot auf geschützten und Medienkompetenz vermittelnden Kinderseiten ist das erklärte Ziel des Netcode.

Kinder sollen die Fertigkeiten erwerben, sich in der Vielzahl der Informationen orientieren zu können. Sie sollen diese Informationen mit anderen Werturteilen vergleichen und sie auf die eigene Lebenssituation beziehen können. "Leitend für diese Zugangsweise ist ein Konzept des Empowerments, verstanden als der Versuch, Heranwachsende zu moralischer Selbstbestimmung im Blick auf die Lebensführung zu befähigen. Diese (...) gestützte Selbstbestimmung zielt auf die Ausbildung einer Persönlichkeit, die sich selbständig in der pluralen Medien- und Wissenslandschaft orientieren kann." (Grundsätze, Erfurter Netcode).

Zum Schluss

Das christliche Menschenbild weiß einerseits um die Verführbarkeit des Menschen. Gesetzte Grenzen zu überschreiten und damit den Bereich des Lebensdienlichen zu verlassen, ist im Menschen angelegt. Sein Drang nach Erkenntnis des Guten und des Bösen führt den Menschen zum Fortschritt, aber gleichzeitig auch zur Schuld. Ist die Freiheit des Menschen die eine Seite der Medaille, so ist die Verantwortung des Menschen für sein Handeln die andere.

Zu des Menschen Verantwortungsbereich gehört dabei eben auch die Sorge um alle Menschen, die unter seinem Schutz leben. Freiheitlicher, kritischer Diskurs und verantwortliche Fürsorge sind zwei Dimensionen des Menschen, der sein Leben einer ganz anderen Dimension verdankt.

Unser gemeinsames Engagement für Jugendschutz und Kinderkultur kann daher nicht eindimensional gesehen werden. Diensteanbieter (wie Suchmaschinen) sollten im Rahmen einer freien Selbstkontrolle auf der Grundlage der gesetzlichen Regelungen die Verantwortung z.B. durch die Akzeptanz eines Verhaltenskodex wahrnehmen.

Technische Lösungen durch Filtersysteme andererseits scheinen gerade im Bereich der Lebenswelt von Kindern im Internet sinnvoll, sofern am Markt funktionierende Systeme zur Verfügung stehen. Alle technischen Maßnahmen werden nie eine 100%-ige Sicherheit bieten können. Nicht nur aus diesem Grund gehört die Medienpädagogik zum Bildungsauftrag unserer Gesellschaft. "Der mündige Umgang mit dem Internet kann dann einen im Ethos des Individuums verankerten Filter bilden, der das wesentliche Element der Selbststeuerung ausmacht." (Markus Wolf in: Thomas Hausmanninger (Hg.): Handeln im Netz, 2003, S. 204)

Erlauben Sie mir am Ende den Hinweis, dass die kirchlichen Seelsorge-Angebote im Internet überkonfessionell, kostenlos, anonym und vertraulich allen Menschen offen stehen. Es kann nur als gemeinsame Anstrengung aller Beteiligten gelingen, dass das Internet zu einem alltäglichen Lebensraum wird, in dem sich Kinder und Erwachsene gleichermaßen aufgehoben und vielleicht sogar beheimatet fühlen.

Wichtige Internetadressen zum Thema
www.ekd.de
www.erfurter-netcode.de
www.crossbot.de
www.telefonseelsorge.org
www.chatseelsorge.de

Rechtliche Grundlagen und Bewertung

Rechtsanwalt Tobias H. Strömer, Düsseldorf

Das Internet hat die Juristen in den vergangenen Jahren immer wieder vor neue Herausforderungen gestellt. Das nicht so sehr deshalb, weil das Netz neue Unrechtstatbestände geschaffen hat. Nahezu alle Delikte, die im Internet begangen werden können, gab es auch schon vor der Erfindung des World Wide Web. Herausgefordert wurden Gesetzgeber und Rechtsanwender vor allem deshalb, weil sie technische Zusammenhänge verstehen lernen mussten und auf die enormen Möglichkeiten, die das Internet praktisch jedem Einzelnen weltweit bietet, reagieren mussten und müssen. Nie war es so leicht, innerhalb von Minuten seine eigenen Ansichten einer Weltöffentlichkeit zu präsentieren. Nie war es so leicht, auf so einfache und rasche Weise gegen Strafrecht, Markenrecht, Urheberrecht und Wettbewerbsrecht zu verstoßen – um nur einige der Fallstricke aufzuzählen, die auf den Internetnutzer im Netz warten.

Anwälte und Gerichte werden bei internetrechtlichen Angelegenheiten in aller Regel mit zivilrechtlichen Fragestellungen befasst. Meist geht es um Domainstreitigkeiten, Wettbewerbs- und Urheberrechtsverletzungen. Ich möchte Ihnen aber heute in der Kürze, die die zur Verfügung stehende Zeit gebietet, aufzeigen, in welcher Weise im Internet gegen solche Normen verstoßen wird, die den Jugendschutz zum Gegenstand haben. Außerdem will ich Ihnen etwas sagen zur Verantwortlichkeit derjenigen, die verbotene Inhalte Jugendlichen zugänglich machen. Dabei sollten Sie aber bitte nicht aus dem Auge verlieren, dass wir uns der Materie aus einem rein deutschen Betrachtungswinkel nähern. Selbstverständlich haben saudiarabische Sittenwächter völlig andere Vorstellungen etwa von Alkoholwerbung oder Erotikangeboten, als die deutschen Behörden.

Verbotsnormen

Im Internet kommen bei der Beurteilung straf- oder ordnungswidrigkeitstatbestandlichen Verhaltens vorrangig solche Bestimmungen in Betracht, die das Verbreiten und Zugänglichmachen jugendgefährdender oder sonst unzulässiger Medien pönalisieren. Solche Normen finden sich insbesondere im Strafgesetzbuch (StGB), in dem am 1. April 2003 in Kraft getretenen Jugendschutzgesetz (JuSchG) sowie im Jugendmedienschutz-Staatsvertrag (JMStV).

Von den Bestimmungen des Strafgesetzbuchs sind im Hinblick auf den Jugendschutz insbesondere die Verbreitungsdelikte relevant. Zu beachten sind namentlich die Straftatbestände nach §86 StGB (Verbreiten von Propagandamitteln verfassungswidriger Organisationen), §86a StGB (Verwenden von Kennzeichen verfassungswidriger Organisationen), § 111 StGB (Öffentliche Aufforderung zu Straftaten), §§ 129, 129a StGB (Unterstützen einer kriminellen oder terroristischen Vereinigung), § 130 (Volksverhetzung und Holocaust-Leugnung), § 130a StGB (Anleitung zu Straftaten), § 131 StGB (Gewaltdarstellung), § 140 StGB (Belohnung und Billigung von Straftaten), § 166 StGB (Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen), § 184 StGB (Pornografie), § 185 ff. StGB (Beleidigung, üble Nachrede, Verleumdung, Verunglimpfung des Andenkens Verstorbener) und §§ 284 ff. StGB (unerlaubtes Glücksspiel). Die Straftatbestände setzen dabei – von wenigen Ausnahmen abgesehen – vorsätzliches Verhalten voraus. Die vorgenannten Verbotsnormen des Strafgesetzbuchs sind aber weitgehend in den Unzulässigkeitskatalog des §4 Abs. 1 JMStV eingebunden worden. Hier ist bereits das fahrlässige Verbreiten mit einem Bußgeld von bis 500.000 € bedroht.

Der bloße Abruf unzulässiger Inhalte im Internet stellt dagegen keine Straftat dar. Jeder darf sich – solange ihm das technisch möglich ist – frei informieren und jede Seite abrufen, die er gerne sehen möchte. Er darf die abgerufene Seite anschließend auch auf seinem Rechner speichern, ausdrucken oder archivieren. Hiervon gibt es nur eine Ausnahme: Internetseiten, auf denen sich Inhalte befinden, die als Kinderpornographie zu werten sind, darf ein Internetnutzer nicht dauerhaft speichern. Hier ist der bloße Besitz bereits strafbar, erst recht natürlich die Archivierung. Wer auf

solche Seiten mehr oder minder zufällig stößt, sollte daher auch der Versuchung widerstehen, die Inhalte auf Datenträger zu speichern, um sie später Ermittlungsbehörden zugänglich zu machen.

Verbreitungs- und Äußerungsdelikte

Wer auf Seiten mit strafbarem Inhalt verweist oder auch nur den Zugriff ermöglicht, muss sich unter Umständen den Vorwurf gefallen lassen, im strafrechtlichen Sinne als Täter, als Mittäter oder als Gehilfe verurteilt zu werden. Maßgeblich ist, wie intensiv die Zusammenarbeit mit dem für die zugänglich gemachte Website Verantwortlichen ist.

Darüber hinaus ist zu entscheiden, ob sich der dem Täter gemachte Vorwurf auf ein Verbreitungs- oder ein Äußerungsdelikt bezieht. Manche Straftatbestände sind so ausgestaltet, dass schon die bloße Verbreitung eines unzulässigen Inhalts strafbar ist. Hierzu gehört etwa die Verbreitung von pornografischen Schriften. Es kommt deshalb überhaupt nicht darauf an, ob derjenige, der einen Link auf eine Seite mit verbotenen pornografischen Inhalten setzt, mit dem Inhalt der Site einverstanden ist; es reicht aus, dass er den Inhalt kennt. Anders verhält es sich bei den Äußerungsdelikten, etwa bei der Anleitung zu Straftaten oder bei Beleidigungstatbeständen. Hier kommt es darauf an, ob der Verweisende sich den verbotenen Inhalt zu Eigen machen, also wie eine eigene Äußerung behandelt wissen wollte. Ob das im Einzelfall so war, entscheidet der Richter auf der Grundlage der ihm bekannten Informationen. Indiz für eine solche Absicht kann etwa die Vorgeschichte sein: Wer sich persönlich über einen anderen ärgert, dem ist häufig nicht an einer objektiven Berichterstattung gelegen. Wer umgekehrt auch in der Vergangenheit immer wieder gezeigt hat, dass er sich bemüht, über Sachverhalte objektiv zu berichten, dem wird man nur im Ausnahmefall eine Beleidigungsabsicht unterstellen können. Letztendlich kommt es darauf an, welche Überzeugung der Richter im Rahmen des Prozesses, insbesondere in der mündlichen Verhandlung, gewinnt.

Falls der Richter die Überzeugung gewinnt, dass der Linkende im Einzelfall selbst beleidigen wollte, kommt es im Übrigen auf die technische Ausgestaltung nicht an. Strafbar macht sich deshalb auch derjenige, der statt eines Links andere Möglichkeiten aufzeigt, mit denen die von ihm gutgeheißene Website im Internet gefunden werden kann. Verboten ist es deshalb auch, explizit Suchworte einzugeben, mit denen in Suchmaschinen nach den verbotenen Inhalten gesucht werden soll. Auch der Hinweis „Hier auf keinen Fall nachschauen“ oder „Ich distanziere mich ausdrücklich von diesem interessanten Inhalt“ reichte selbstverständlich dann nicht aus, wenn tatsächlich die Absicht verfolgt wird, den Angesprochenen „in die Pfanne zu hauen“.

Eine Strafbarkeit scheidet – jedenfalls bei den Äußerungsdelikten – dann aus, wenn dem Linkenden der Inhalt der Seite, auf die verwiesen wird, nicht bekannt war. Das gilt etwa dann, wenn die Seite seit dem erstmaligen Setzen des Links zwischenzeitlich ohne Wissen des Verweisenden geändert wurde. Das Amtsgericht Berlin-Tiergarten hat im Fall der ehemaligen PDS-Bundesvorsitzenden Angela Marquardt, die auf verbotene Inhalte der Online-Ausgabe der Zeitschrift „radikal“ verwiesen hatte, klargestellt, dass es keine Verpflichtung gibt, den Inhalt einer einmal in eine Link-Liste aufgenommenen Website laufend zu kontrollieren. Falls der Linkende später von einer Änderung der Site erfährt, hat er sich allerdings selbstverständlich zu vergewissern und den Link gegebenenfalls zu entfernen.

Anders verhält es sich bei bloßen Verbreitungsdelikten, wie etwa der verbotenen Verbreitung von Pornografie. Hier reicht es aus, wenn durch einen Link vorsätzlich die Verbreitung pornografischer Schriften gefördert wird. Unerheblich ist dabei, ob dem Täter an einer Verbreitung gelegen war.

Fallbeispiele

Schon im September 1996 wurden neue Verfahren gegen Internet-Provider eingeleitet, weil sie sich angeblich Zugang zu einem niederländischen Server verschafft hatten. Dort fand sich die

Online-Ausgabe Nr. 154 der linksradikalen Zeitschrift „radikal“, in der unter anderem ein „Kleiner Leitfaden zur Behinderung von Bahntransporten aller Art“ wiedergegeben wurde.[1] Die in der Interessengemeinschaft „ECO“ zusammengeschlossenen deutschen Provider reagierten darauf, indem sie die Adresse der Internetseite „sperrten“. Viel geholfen hat diese Maßnahme – wen wundert’s – nicht, weil die Radikal-Seiten sofort auf einer Vielzahl von Servern gespiegelt wurden. Im Sommer 1997 musste sich die PDS-Politikerin Angela Marquardt vor dem Amtsgericht Berlin-Tiergarten verantworten. Es ging um einen Link auf ihrer Homepage im Internet, der auf die Online-Ausgabe der Autonomenzeitschrift verwies. Nach Auffassung der Staatsanwaltschaft hatte die Politikerin damit ihre Homepage zur Verbreitung von Auszügen aus „radikal“ zur Verfügung gestellt, in denen zu Straftaten angeleitet wird beziehungsweise Straftaten gebilligt werden. Rechtlich sei das als Beihilfe zur Störung öffentlicher Betriebe im Sinne des § 316 b StGB zu bewerten. Die Höchststrafe: Zehn Jahre Gefängnis. Das Amtsgericht Berlin-Tiergarten mochte die Rechtsfrage offensichtlich nicht entscheiden: Das Gericht konnte der Angeklagten nicht nachweisen, dass sie von den verbotenen Inhalten wusste, als sie den Link einrichtete, und sprach Frau Marquardt frei.

Auch das Oberste Bayerische Landesgericht entschied im November 1997 zugunsten des Angeklagten, dem vorgeworfen wurde, gegen § 53 Abs. 1 S. 1 Nr. 5 WaffG (Anleitung zur Herstellung bestimmter Waffen) verstoßen zu haben.[2] Der Betroffene hatte in eine Mailbox ein im Internet gefundenes digitales Handbuch zur Herstellung von Molotow-Cocktails eingestellt. Das Gericht konnte dem Täter nicht nachweisen, dass er sich den Inhalt der Anleitung zu Eigen gemacht hat, also selbst zur Herstellung anleiten wollte. Da es sich hier aber um ein Äußerungs-, nicht um ein Verbreitungsdelikt handle, sei das bloße Weitergeben einer Datei nicht strafbar.

Ähnlich dürfte es sich bei einem Verweis auf solche Internetseiten verhalten, die beleidigende Äußerungen enthalten: Hier kommt es entscheidend darauf an, ob der Verweisende mit dem Link selbst eine Missachtung zum Ausdruck bringt oder jedenfalls die beleidigende Äußerung billigt. Das kann etwa dadurch geschehen, dass er den Link mit: „Hier geht’s zum Dorftrottel des Monats“ bezeichnet.

Das Landgericht Hamburg hat deshalb im Frühjahr 1998 in einer viel beachteten Entscheidung einen Website-Betreiber zum Schadensersatz verurteilt, weil er auf eine fremde Seite mit beleidigenden und ehrverletzenden Inhalten gelinkt hatte. [3] Dort wurde unter der Überschrift „Der D-Orfdepp des Monats“ von einem Anwalt berichtet, der für seine Mandantin in einer Vielzahl von Fällen angeblich bestehende Rechte an Internetdomains eingeklagt hatte, die mit „D-“ begannen. Der Linkende hatte zwar darauf hingewiesen, dass der fremde Inhalt von ihm nicht verantwortet werde. Das aber reichte nach Ansicht des Gerichts – im entschiedenen Fall wohl zu Recht – nicht aus. Erforderlich sei eine deutliche Distanzierung und vor allem eine redliche Absicht, etwa das Bemühen, „ein Kaleidoskop von Behauptungen in einer die Öffentlichkeit berührenden Angelegenheit möglichst umfassend in alle möglichen Richtungen vertiefend wiederzugeben, um der Wahrheitsfindung nachzuhelfen.“

Verantwortlichkeit Dritter

Für Rechtsverstöße im Internet haften in erster Linie natürlich diejenigen, die für die Inhalte unmittelbar verantwortlich sind. Das sind vor allem die Betreiber einer Website mit unzulässigen Inhalten, unter Umständen auch die Inhaber der Internet-Domains, mit denen das Angebot adressiert wird.

Vor allem im Zivilrecht, bei dem es häufig um Unterlassungs- und Schadensersatzansprüche aus dem Marken-, Wettbewerbs- und Urheberrecht geht, ist aber gerade in den letzten Wochen

1 AG Berlin-Tiergarten, Beschl. v. 30.06.97, 260 DS 857/96 – *radikal*.

2 BayOLG, Beschluss vom 11. November 1997, 4 St RR 232/97, CR 1998, 564 – *Terrorist's Handbook*.

3 LG Hamburg, Urt. v. 12.05.98, 312 O 85/98 – *Best's Linking Case*.

und Monaten eine deutliche Tendenz zu beobachten, den Kreis der Verantwortlichen möglichst weit zu ziehen. Die Gerichte neigen zunehmend dazu, jeden mit in die Haftung zu nehmen, der in irgendeiner Weise adäquat-kausal Einfluss auf ein Internet-Angebot nehmen kann. Wer etwa 0190er-Rufnummern vermietet, soll für den Missbrauch, den ein Kunde mit einer solchen Service-Nummer betreibt, den Kopf hinhalten müssen. Im Strafrecht sind die Grenzen schon wegen des hier geltenden Bestimmtheitsgrundsatzes zwar enger gezogen. Ob ein Internet-Mediär erfolgreich in die Haftung genommen werden kann, richtet sich aber auch hier vorrangig danach, welchen Beitrag er zur Verbreitung der unzulässigen Inhalte liefert. Grundsätzlich gilt auch im Strafrecht: Webhosting-Provider, die fremde Inhalte lediglich speichern und zum Abruf bereithalten, sind für solche Inhalte erst dann verantwortlich, wenn sie nach einer Aufklärung über ihre rechtliche Unzulässigkeit nicht unverzüglich handeln, §§ 11 TDG, 9 MDStV. Access-Provider, die lediglich den Zugang zum Internet vermitteln, sollen grundsätzlich nicht haften, §§ 9 Abs. 1 TDG, 7 Abs. 1 MDStV.

Wer anderen lediglich Rechner zur Verfügung stellt, um Internet-Angebote abzurufen, dürfte am ehesten mit Access-Providern vergleichbar sein. Nach den Regeln des Teledienstegesetzes müssen deshalb Betreiber von Internet-Cafés, Arbeitgeber und Schulleiter im Prinzip nicht befürchten, für die von ihnen zugänglich gemachten Inhalte haften zu müssen. Tatsächlich wurden daher strafrechtliche Ermittlungsverfahren etwa gegen die Betreiber von Internet-Cafés – soweit ersichtlich – bislang immer eingestellt.[4]

Gleichwohl wird ein bloßer Blick auf die Privilegierungstatbestände des Teledienstegesetzes den rechtlichen Anforderungen nicht gerecht. Das Teledienstegesetz soll nämlich Internet-Mediäre nur insoweit privilegieren, als sich ihr Haftungsrisiko gerade aus der Nichtbeherrschbarkeit internettypischer Sachverhalte ergibt. Wer anderen, insbesondere auch Jugendlichen, Internet-Rechner zugänglich macht, kann durchaus durch geeignete Maßnahmen sicherstellen, dass das Risiko der Verbreitung strafbarer Inhalte minimiert wird. In der Rechtsliteratur wird daher zu Recht die Ansicht vertreten, dass allzu sorglose Anbieter durchaus verantwortlich gemacht werden können.[5] Gefordert wird zum einen, dass der Anbieter in zumutbaren Umfang überwacht, ob Jugendliche unzulässige Angebote abrufen. Das soll etwa geschehen durch unüberhör- und unübersehbare Hinweise und Stichprobenkontrollen. Selbstverständlich ist dabei auch gegenüber Jugendlichen das Fernmeldegeheimnis zu wahren. Zum anderen sollen die Anbieter aber auch und vor allem geeignete Filterprogramme einsetzen, die einen Zugriff auf unzulässige Seiten nach Möglichkeit vor vorne herein verhindern. Wer solche Filter nicht generell einsetzen möchte, sollte wenigstens an den Rechnern installieren, die Jugendlichen zur Verfügung gestellt werden.

Das Grundgesetz schützt neben der Meinungs- und Pressefreiheit auch die Informationsfreiheit, also die Gewährleistung, sich grundsätzlich aus allen zur Verfügung stehenden Informationsquellen zu informieren. Wie viele andere Grundrechte auch besteht allerdings die Informationsfreiheit unter dem Vorbehalt gesetzlicher Schranken. Solche Schranken stellen insbesondere die Strafvorschriften dar, die Jugendliche, unter Umständen aber auch Erwachsene vor einer Konfrontation mit unzulässigen Inhalten schützen sollen. Dabei unterscheidet der Strafrechtrechtler zwischen Äußerungs- und Verbreitungsdelikten. Während bei den einen schon die bloße Veröffentlichung den Straftatbestand ohne weiteres erfüllt, muss bei den anderen für eine Strafbarkeit hinzukommen, dass sich der Anbieter mit den Inhalten identifiziert, indem er sie sich zu Eigen macht. Detaillierte Anleitungen zur Herstellung von Molotow-Cocktails etwa sind nicht per se verboten. Sie werden es erst, wenn mit der Anleitung erkennbar verbotene Ziele verfolgt werden. Auch die Werbung für Schusswaffen oder Anleitungen zu ihrem Gebrauch sind nicht unzulässig; unzulässig ist lediglich die Anstiftung zu Straftaten, bei denen solche Waffen eingesetzt werden sollen. Wer andere im Internet beleidigt oder ungeschützt Pornographie

4 vgl. StA München, Bescheid v. 16.01.97, 4678 Js 319998/96; StA Heidelberg, Vfg. v. 27.07.01.

5 vgl. Liesching, MMR 2003, 562, 567.

verbreitet, verstößt dagegen auch dann gegen geltendes Recht, wenn er über die Verbreitung der Inhalte hinaus keine weiteren Ziele verfolgt.

Sollten sich Maßnahmen gegen die Anbieter unzulässiger Informationen selbst als unzureichend erweisen, etwa deshalb, weil sich diese im nicht erreichbaren Ausland aufhalten und ihre Server von dort aus betreiben, steht den Verwaltungsbehörden als ultima ratio die Möglichkeit zur Verfügung, Sperrungsverfügungen zu erlassen. In solchen Verfügungen wird den in Deutschland ansässigen Providern der potentiellen Empfänger der Inhalte unter Androhung eines empfindlichen Ordnungsgelds aufgegeben, die inszenierten Inhalte zu sperren, den eigenen Kunden also einen Zugriff auf solche Seiten zu verwehren. Die Legitimität solcher Verfügungen und die Voraussetzungen, unter denen sie zulässig sind, sind allerdings heftig umstritten. Neben einer Reihe von bislang weitgehend ungeklärten Rechtsfragen führen Kritiker zu Recht die Frage nach Wirksamkeit solcher Maßnahmen ins Feld. Wer halbwegs zuverlässig dafür Sorge tragen möchte, dass Inhalte auf ausländischen Servern für Deutsche Internetnutzer nicht mehr erreichbar sind, muss geradezu stündlich neue Verfügungen erlassen. Dem entspricht es, dass Internet-Provider mit erheblichen Aufwand immer wieder neue Seiten sperren müssen. In der Praxis dürfte das letztendlich vollkommen unzumutbar sein. Das gilt vor allem dann, wenn man dem Nutzen solcher Verfügungen die damit verbundenen Nachteile gegenüber stellt.

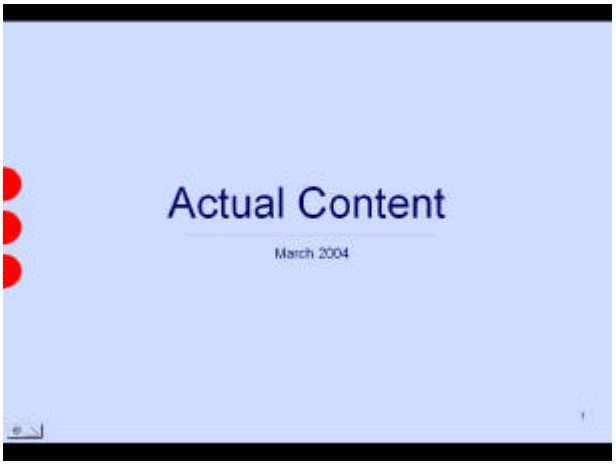
Hinzukommt, dass gerade Jugendliche zu denjenigen Internetnutzern gehören, die Zugangsbeschränkungen am ehesten durch eigene Kenntnisse umgehen könne. Vor dem Einsatz rabiater, gleichzeitig aber in der Wirksamkeit höchst umstrittener Sperrungsverfügungen sollte die Politik daher auf die Erziehung zu eigenverantwortlichen Umfang mit neuen Medien hinwirken. In einer omnipräsenten Informationsgesellschaft werden Kinder und Jugendliche zunehmend weniger durch Zwangsmittel davon abgehalten werden können, unzulässige Inhalte wahrzunehmen und sich mit ihnen auseinandersetzen zu müssen.

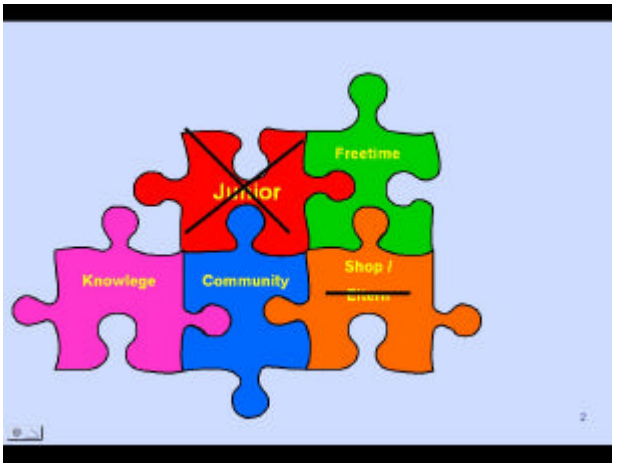
Dieses Postulat ändert aber nichts daran, dass Lehrer, Ausbilder und Arbeitgeber, die für die Eltern zeitweise Erziehungsaufgaben übernehmen, selbst zumutbare Mittel ergreifen müssen, ohne Inhalte von Kindern und Jugendlichen fernzuhalten. Das gebietet nicht nur das Vertrauen, dass die Eltern und der Staat in Ausbilder setzen, sondern vor allem die Rechtsordnung. Wer durch das zur Verfügung stellen von Internet-Zugängen Gefahrenquellen schafft, begibt sich selbst in eine Garantenstellung.

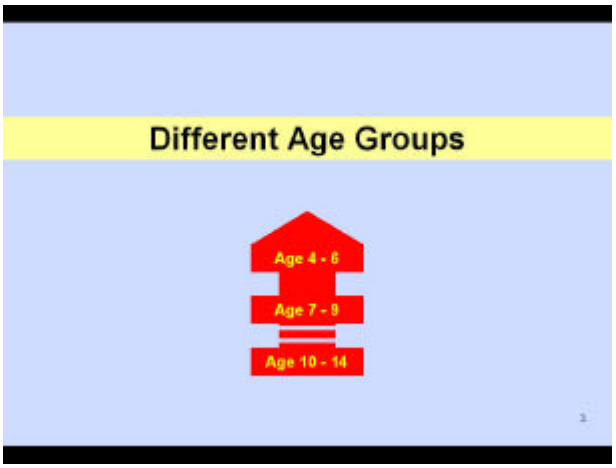
Das "reine" Positiv-Portal für Kinder zwischen 4 - 14 Jahren

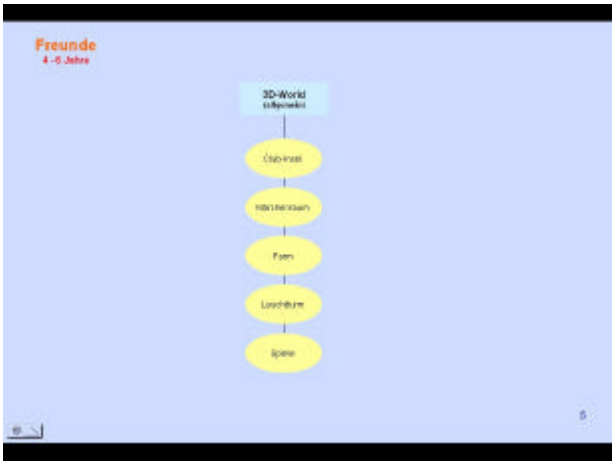
Referent: Peter Kolb, VICTORY Media Gruppe

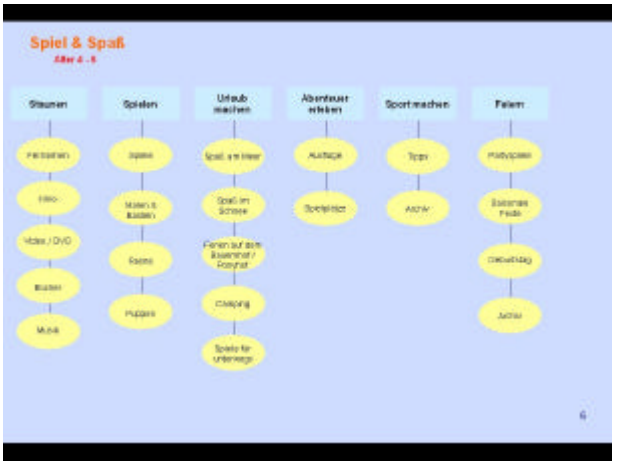
Herr Kolb informierte über den Stand der Entwicklung, die Struktur und Inhalte sowie die geplante Umsetzung des von der Victory Media Gruppe vorangetriebenen Portals KIDS-WEB:

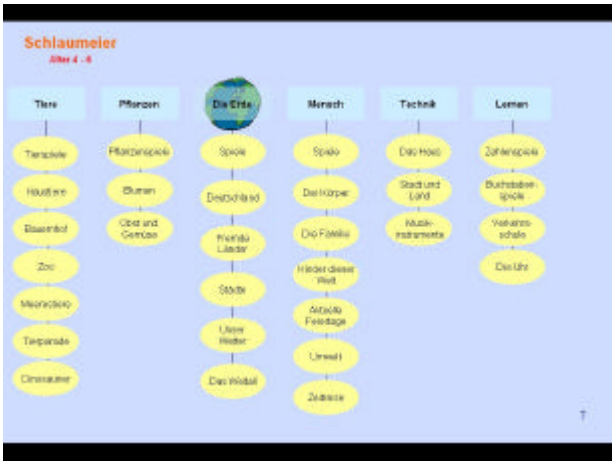


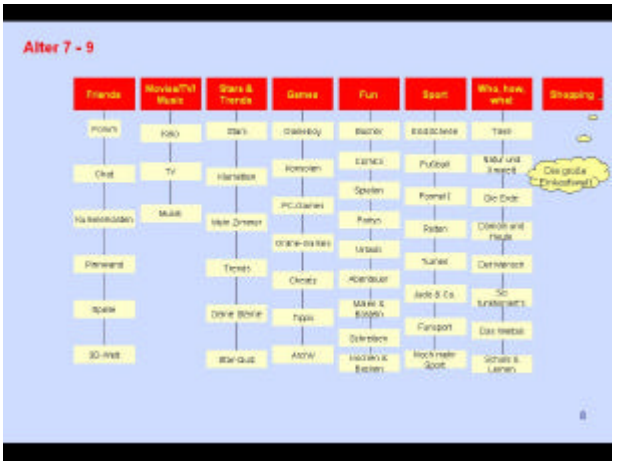




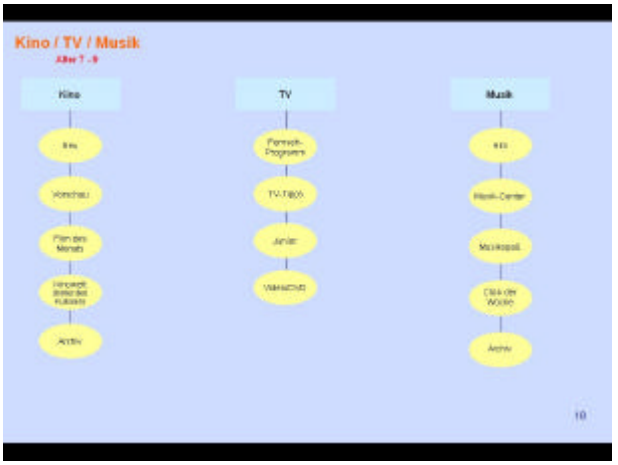


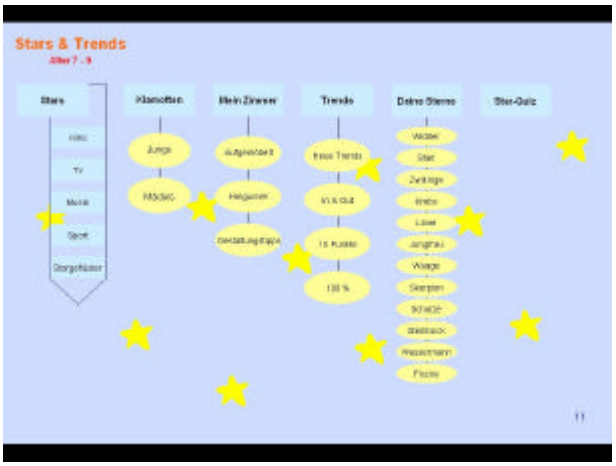



Schlaumeier
Tiere
Pflanzen
Die Erde
Mensch
Technik
Lernen

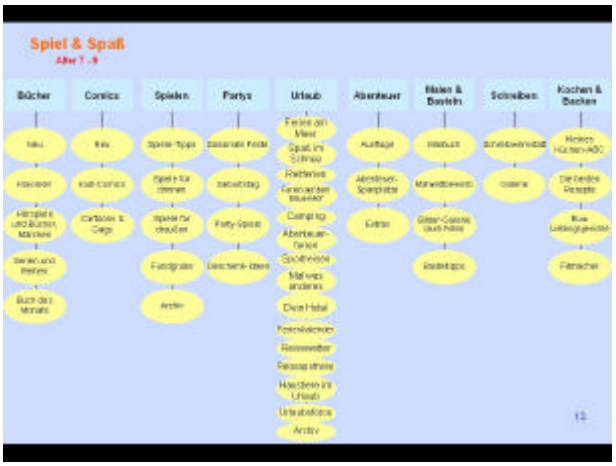

Alter 7 - 9
Freunde
Games
Fun
Sport
Shopping

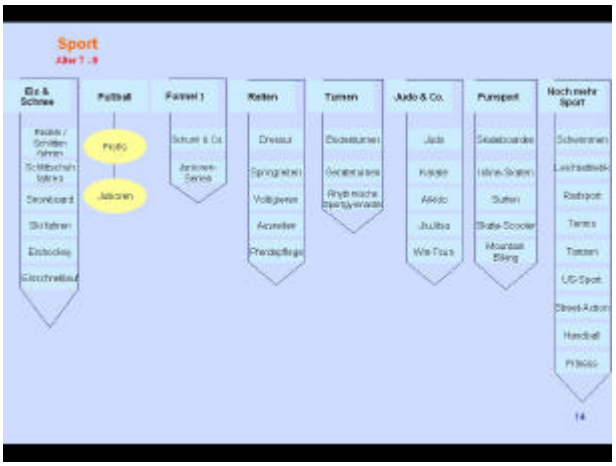

Freunde
7 - 9 Jahre
Foren
Chat
Kummer-kasten
Pinnwand
3D-Welt


Kino / TV / Musik
Alter 7 - 9
Kino
TV
Musik

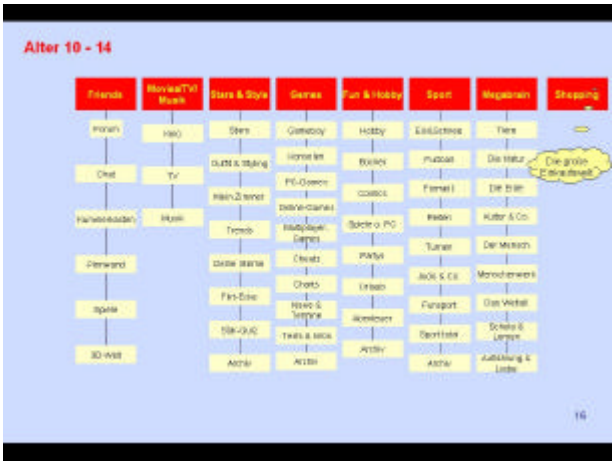

Stars & Trends
Alter 7 - 9
Stars
Klamotten
Mein Zimmer
Trends
Deine Sterne
Star-Quiz


Games
Alter 7 - 9
Gameboy
Konsolen
PC-Games
Online-Games
Cheats
Tipps
Archiv

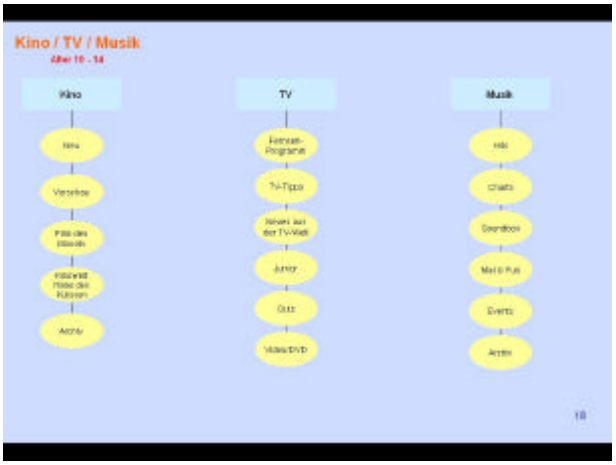

Spiel & Spaß
Bücher
Comics
Spielen
Partys
Urlaub
Abenteuer
Basteln & Bauteln
Schreiben
Kochen & Backen

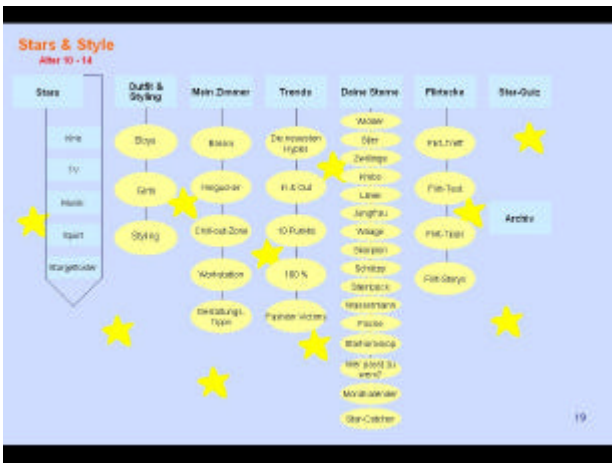

Sport
Eis & Schnee
Fußball
Formel 1
Reiten
Turnen
Judo & Co.
Pumpen!
Noch mehr Sport

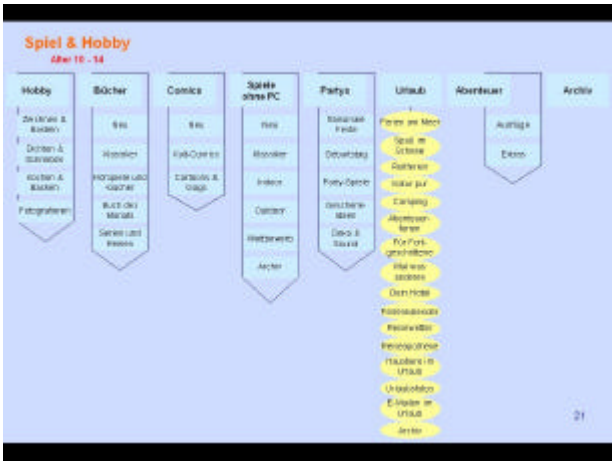

Wer, Wie, Was
Tiere
Natur und Umwelt
Damals & Heute
Der Mensch
So funktioniert's
Das Weltall
Schule & Lernen

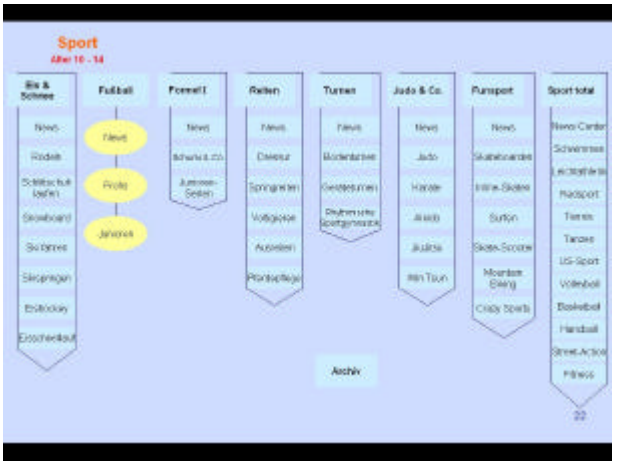

Alter 10 - 14
Friends
Movies/TV/ Musik
Stars & Style
Games
Fun & Hobby
Sport
Wissen
Shopping


Freunde
Forum
Chat
Kummer-kasten
Pinnwand
Spiele
3D-Welt


Kino / TV / Musik
Kino
TV
Musik







Herr Peter Kolb

Die wichtigsten Erfahrungen über Landes- und Schul-Internetfilterung

Bert Weingarten, PAN AMP AG

Die zunehmende Zahl von Internet-Zugängen und die damit verbundenen Gefahren führten seit 1995 zu einer stetig ansteigenden Nachfrage nach wirkungsvollen Sicherheitsinstrumenten. Seither liegt unser Aufgabenschwerpunkt in der Entwicklung und der Markteinführung von IT-Sicherheitsprodukten. Neben der Markteinführung von CyberPatrol, der GNAT-Box-Technologie, Produkten wie Network Address Translation (NAT) und VPN (Virtual Private Network), entwickelte unser Unternehmen ein Hochleistungsfiltersystem für AIX, UNIX und Linux-Systeme, welches bereits in Fortune-500-Unternehmen Anwendung findet. Das FAS (Filter Administration System), das eine modulare Lösung zur zentralen Administration von Internet-Filtersystemen und somit einen Einsatz bei heterogenen und örtlich getrennten Netzwerken ermöglicht. So ist FAS in der Lage, mit einer unbegrenzten Anzahl von Filter-Generationen gleichzeitig zu arbeiten, diese zu administrieren und eigene Filter einzupflegen. Die Kategorisierung und die Erprobung fand in einer Kooperation mit Sozialwissenschaftlern und Internetprovidern statt.

So entstanden verschiedenste Filter, wie der Sperrfilter NotList, der den Aufruf von indizierten Internetangeboten verhindert, Freigabefilter wie Business-List, welcher nur gezielt themenrelevante Angebotsbereiche des Internets zur Nutzung frei gibt und Semantic Keyword-Filter, die einen Aufruf von Internet-Angeboten unterbinden, wenn diese bestimmte Schlüsselwörter in eindeutig definierten Mustern enthalten. So werden auch unerwünschte Domains erfasst, die z. B. rassistische oder pornografische Inhalte unter Tarnnamen anbieten. Der Administrator erhält so schnelle Eingriffsmöglichkeiten in ein Filtersystem, das aufgrund der zur Verfügung stehenden Einzelfilter eine hohe Qualität der Filterergebnisse gewährleistet.

Herr Bert Weingarten (Links)

So wurden Filtersysteme zur Förderung der Produktivität bei Panasonic Europa und zum Schutz der Auszubildenden bei den Berliner Wasserbetrieben eingeführt. Landesweite Pilotversuche wie mit dem Freistaat Bayern wurden umgesetzt. Verschiedene Referenzen stehen hierzu in unserem Internetangebot zur Verfügung. Im Fall des landesweiten Pilotversuches vom 02. Juli bis zum 10. Oktober 2001 an den bayerischen Schulen steht der vollständige Bericht bereit: http://www.panamp.de/de/docs/unternehmen/public_relations/presse_service/abschlussbericht_bayern.html

Als Experte auf dem Gebiet Internet-Filterung und IT-Sicherheit kann PAN AMP auf vielfältige Erfahrungen in Wirtschaft und Bildung zurückgreifen. Die Praxis hat gezeigt, dass im Internet eine Vielzahl von Angeboten existiert, deren Sperrung - unabhängig von der politischen Anschauung –

befürwortet wird. Zum allgemeinen Konsens in der Ablehnung bestimmter Inhalte gehören Bombenbauanleitungen, Kinderpornographie, politischer Extremismus jeder Couleur, Suizid-Chats und indizierte Computerspiele.

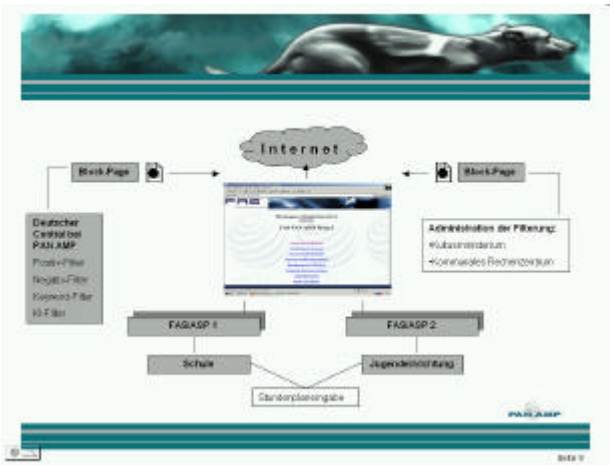
Das Internet hat sich in Unternehmen, Behörden und Schulträgern zum zentralen Medium der Kommunikationsstrukturen entwickelt. Datenbestände werden ausgetauscht, Angebote abgerufen, es wird gechattet, gesurft und ferngewartet. Aber die grenzenlose Online-Freiheit hat ihre Kehrseite: Wer während der Arbeitszeit surft, beschäftigt sich fast die Hälfte der Zeit mit Dingen, die nichts mit dem Job zu tun haben (Quelle: Meta Group Consulting). Das Resultat: die Produktivität im Unternehmen sinkt und die Kosten steigen. Denn beschäftigt sich ein Mitarbeiter nur eine Stunde pro Tag mit für sein Unternehmen nicht produktiven Internetseiten, summieren sich diese Zeitverluste auf rund 240 Arbeitsstunden im Jahr. Somit ist verständlich, dass Internet-Filterung in Unternehmen erstrangig zur Produktivitätssteigerung eingesetzt wird. Schulträger und öffentliche Netze stehen hingegen vor anderen Herausforderungen. Indizierte Texte, Audio- und Video-Aufzeichnungen, sowie verbotene Computerspiele können über nahezu jedes öffentliche Terminal, WLan oder den Schulcomputer eingesehen, aufgerufen oder kopiert werden. Während in Erwachsenen-Videotheken verschiedene Videos und Computerspiele durch ein Verbot nicht einmal mehr von Erwachsenen ausgeliehen werden dürfen, bestehen im Internet für verbotene Inhalte unbegrenzte Verbreitungsmöglichkeiten, welche direkt von Kindern und Jugendlichen in nahezu jeder Schule, im Kindergarten und von Zuhause aus abgerufen werden können.

Während die Integration von Internet-Filter-Systemen in Unternehmen zum Tagesgeschäft gehört, erschwerten bisher besondere technische Herausforderungen den Einsatz einer Filtertechnologie an Schulen, Kindergärten und Jugendeinrichtungen. Hierzu gehören unterschiedliche Betriebssysteme auf Servern und Benutzersystemen, unterschiedliche Provider mit verschiedensten Netzwerkstrukturen, Bandbreiten und unterschiedlichsten Sicherheitsmerkmalen.

Der Bedarf der Schulträger wurde klar identifiziert: Eine stabile und einfach zu handhabende Internet-Filter-Technologie wird benötigt, die einen provider-unabhängigen Einsatz unterstützt. Die Integration und die laufenden Kosten müssen dabei für Schulen bzw. für deren Schulträger tragbar sein. Eine Administration der Filterung muss nach einer landesspezifischen Vorgabe möglich sein. Kurz, kein bestehendes Internet-Filter-Produkt war bisher in der Lage, diese Anforderungsmerkmale zu erfüllen.

Diese Herausforderung wurde von uns 1999 angenommen. Ab dem 01. April 2004 ist die FAS/ASP Technologie für Schul- und Bildungsträger verfügbar. FAS/ASP ist eine völlig neuartige Lösung für Schul- und Bildungsträger, sämtliche Möglichkeiten der Internet-Filterung zu einer modularen Gesamtlösung zu verknüpfen. Basierend auf einer entsprechenden Hardware-Empfehlung ergänzen sich Negativ-, Positiv-, Keyword- und Individual-Filter in der zeitlichen und kooperativen Filterung nach den Lehrplanvorgaben der jeweiligen Bildungseinrichtung.

Ein intelligentes, administrierbares System koordiniert den Einsatz der Filter nach Stundenplankriterien. Zusätzlich wird ermöglicht, dass die Administration des Filtersystems global per Mausklick gesteuert werden kann. Dazu gehören Gruppen- und Nutzerverwaltungen sowie die Möglichkeit der Editierung der Individual-Filter. Optional stehen über die FAS/ASP Systeme ab dem 3. Quartal 2004 ein gesicherter Zugang in ein jugendoptimiertes Portal für Kinder und Jugendliche, sowie Anleitungen zum Umgang mit dem Internet in Form von integrierten E-Learning-Angeboten zur Verfügung.



Aufbau des FAS/ASP-Systems

Die Sicherheit des FAS/ASP-Systems wird durch integrierte Firewall-Systeme unterstützt. Hierdurch wird z.B. der Zugriff in die virtuelle Welt des PAN AMP-Kinderportales für Jugendliche abgesichert, so dass kein Zugriff aus anderen Netzen möglich ist. So ist es nicht möglich, dass zum Beispiel Pädophile über das Internet Zugang zu Chatforen und die Begegnungswelt erhalten. Der erste Einsatz für FAS/ASP findet gemeinsam mit dem Kultusministerium Schleswig-Holstein statt.

Die bisherige Planung sieht einen Piloteinsatz an 10 Schulen vor. Die Installation der Systeme ist für 06/2004 vereinbart. Unser Antrag auf Zulassung der FAS/ASP-Technologie als Jugendschutzprogramm im Rahmen eines nach § 11 JMStV vorgesehenen Modellversuchs wurde gestellt.

Fazit

Staat und Politik haben die Probleme und Gefahren, die das Medium Internet birgt, bislang nicht ausreichend erkannt und ungenügend aufbereitet:

- Das Internet und seine Möglichkeiten stellen eine Herausforderung für die innere Sicherheit und für den Jugendschutz dar. Deswegen muß eine effektive Medienerziehung und die Prävention schon in öffentlichen Netzen erfolgen.

- Der Gesetzgeber sollte eindeutig und für alle Bürgerinnen und Bürger verständlich bekannt geben, welche Art von Inhalten im Internet verboten sind und durch welche Handlungen man sich strafbar macht. Im gleichen Online-Angebot sollte ersichtlich sein, an wen man sich wenden kann, um auf mögliche Straftaten aufmerksam zu machen. Hierbei sollten Ansprechpartner und Telefonnummern veröffentlicht werden, die nicht auf einen Anrufbeantworter verweisen. Dieses vorausgesetzt muss die Anzahl der Internetermittler in Bundesorganen deutlich aufgestockt und mit aktueller Technologie bestückt werden. Internetangebote mit Bombenbauanleitungen gehören verboten.

- Dienstanbieter, wie Suchmaschinen, sollten dringend im Rahmen einer freien Selbstkontrolle auf der Grundlage der gesetzlichen Regelungen die Verantwortung z.B. durch die Akzeptanz eines Verhaltenskodex wahrnehmen.

- Wer durch das zur Verfügungstellen von Internet-Zugängen Gefahrenquellen schafft, begibt sich selbst in eine Garantenstellung. Damit Lehrer, Ausbilder und Arbeitgeber, die für die Eltern zeitweise Erziehungsaufgaben übernehmen, dieser Verantwortung überhaupt gerecht werden können, bedarf es der dringenden Empfehlung für anzuwendende Produkte und Lösungen durch die hierfür verantwortlichen Medienanstalten.

- Wo immer ein Europäischer Wertekonsens für die vorstehenden Forderungen erreicht werden kann, sind die Staaten zu einer Stärkung der internationalen Zusammenarbeit aufgerufen, um so den Zugriff auf die Urheber illegaler Inhalte auch über nationale Grenzen hinweg zu ermöglichen.

Hamburg, den 11.03.2004

Bert Weingarten
Vorstand

Impressum:
Die 2. Hamburger Internetfilter-Konferenz wurde auf Initiative des Vorstandes der PAN AMP AG, Herrn Bert Weingarten, am 11.03.2004 abgehalten. Die Veranstaltung wurde ermöglicht durch die Kostenübernahme der PAN AMP AG.

PAN AMP AG
Borsteler Chaussee 111
D-22453 Hamburg
Tel.: +49 (40) 55 30 02 - 0
Fax : +49 (40) 55 30 02 - 100
E-Mail: info@panamp.de
Internet: www.panamp.de

Danksagung

Wie bedanken uns bei den folgenden Medien für die Berichterstattung und kritische Begleitung:

Ein besonderer Dank gebührt Herrn Viehhauser im Hafen-Klub Hamburg,

www.viehhauser.de/hafen-klub/