Die 14. JMStV–Novelle: Eine technische Betrachtung

(Version 1.0)

2. November 2010

Zusammenfassung

Dieses Dokument betrachtet die geplante Umsetzung des Jugendmedienschutz–Staatsvertrags (JMStV) und seine Auswirkungen auf das Internet allein aus technischer Sicht. Auf diverse Verfahren zur Umgehung und Schwachstellen in der möglichen Umsetzung gehen wir ebenfalls ein. Pädagogische und politische Aspekte werden - wenn überhaupt - bewusst nur gestreift, sind für eine Gesamtbetrachtung jedoch ebenfalls unerlässlich.

Wir, die Autoren, arbeiten seit vielen Jahren – teils freiberuflich – in verschiedenen Bereichen der IT (siehe Anhang), sind oder waren für Banken, Versicherungen und andere Großunternehmen tätig. Gerade in solchen Unternehmen ist eine restriktive Nutzung des Internets – wenn auch aus anderen Gründen – an der Tagesordnung. Wir weisen ebenfalls langjährige Erfahrung in der Nutzung und Gestaltung von Internetinhalten auf.

In diesem Papier werden wir zunächst die Position der Anbieter von Inhalten untersuchen. Anschließend betrachten wir die beiden Alternativen *Jugendschutzsoftware* und *zeitliche Einschränkungen*. Im letzten Abschnitt gehen wir auf die Umsetzung des JMStV aus Sicht der Erziehungsberechtigten ein.

Da einige Paragraphen in der JMStV-Novelle nicht sehr präzise formuliert sind und viel Spielraum zu Interpretationen lassen, sind wir in der Beurteilung der technischen Umsetzung an einigen Stellen auf Schwierigkeiten gestoßen. Diese Stellen sind entsprechend gekennzeichnet. Wir haben versucht, die Beschreibung von technischen Aspekten möglichst einfach, also auch für einen Laien verständlich zu gestalten. Das ist aufgrund der Thematik jedoch nicht immer möglich.

Kai Schmalenbach und Achim Müller

Inhaltsverzeichnis

1 Einführung

Das Internet hat sich seit seinen Anfängen in den frühen Siebzigern des vergangenen Jahrhunderts unglaublich entwickelt. Mit Erfindung des ersten grafikfähigen Browsers und der damit verbundenen rasanten Verbreitung des *World Wide Web* vollzog sich vor etwa zwanzig Jahren der erste Quantensprung[1]. Einen weiteren Schub erfuhr das Internet vor etwa zehn Jahren, als Breitbandzugänge auch für Privatanwender bezahlbar wurden. Das neue Medium wurde auf einmal massentauglich.

Heute jedoch von dem *einen* Medium Internet zu sprechen, ist nach unserer Ansicht sachlich falsch. Als noch schlimmer empfinden wir die Vorstellung, Radio, Fernsehen und Internetangebote in einen Topf zu werfen, bzw. Regularien des einen Mediums ungeprüft auf ein anderes zu übertragen. Leider wird mit der Novellierung des Jugendmedienschutz-Staatsvertrag genau dieser Versuch unternommen.

Die aus unserer (technischen) Betrachtung wichtigen Paragraphen der JMStV-Novelle sind:

- §3(2) Definition des Anbieter
- §5(1) Alterstufen
- §5(2) Kennzeichnung/FSK/KJM
- §5(3) Anbieter/Nutzer!
- §5(5) technische Mittel, zeitliche Einschränkung
- §11(1) Jugendschutzprogramm/Zugangssystem

2 Beurteilung aus Sicht der Content-Anbieter

Bezogen auf Anbieter, Präsentation, vermittelte Inhalte sowie Zugriffs- und Kommunikationsmöglichkeiten lässt sich ‚das Internet'– allerdings sehr vereinfachend – in folgende Kategorien gliedern (in Klammern bekannte Beispiele):

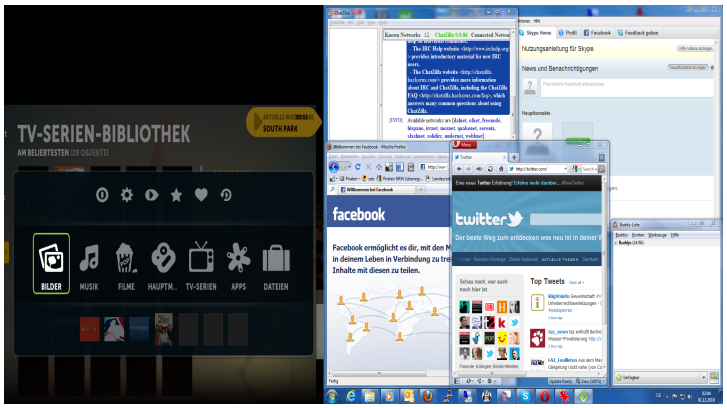

Abbildung 1: Das Internet ist komplex geworden

- Das klassische WWW (Web 1.0, die *erste* Generation)

[1] Ja, wir wissen, dass diese Metapher eigentlich falsch ist ;-).

- Mitmachportale oder ‚User Generated Content' (Wikimedia mit dem wichtigsten Projekt Wikipedia)
- Multimedia-Archive (Youtube, Clipfish, Flickr, Google-Bilder und -Videos)
- Suchmaschinen (Google, Yahoo, Bing)
- Web- und Dokumentenarchive (Google-Cache, Internet Archive)
- Bloghoster (Wordpress, Blogger.de)
- Communitys (Facebook, SchülerVZ, StayFriends)
- Chats (IRC, ICQ, Skype, Jabber)
- Diskussionsforen, autark oder großen Portalen angegliedert (Google-Groups)
- Newsaggregatoren (Google-News, Yahoo! Nachrichten, RSS- und Atomfeeds)
- Microblogging (Twitter, Tumblr, Identi.ca)
- Online Gaming (E-Sports, Schach, verschiedene Gesellschaftsspiele, Casinos)

Leider lassen sich viele Angebote nicht so einfach in eine bestimmte Schublade packen, andere wiederum fallen gleich unter mehrere Kategorien. Auch ist diese Liste mit Sicherheit nicht vollständig und wahrscheinlich in spätestens drei Jahren aufgrund des technischen Fortschritts überholt. Sie vermittelt aber hoffentlich einen Eindruck darüber, welchen Grad an Komplexität das Internet in den vergangenen zehn Jahren erreicht hat.

Laut §5(2) fordert die Neufassung des Jugendmedienschutz-Staatsvertrags eine Kennzeichnung von Internetinhalten nach definierten Altersklassen. Alternativ werden Anbieter die Möglichkeit haben, ihre Inhalte zu bestimmten Sendezeiten zur Verfügung zu stellen. Aus Zeit- und Platzgründen werden wir nicht jedes der oben aufgelisteten Szenarien betrachten. Anhand von ausgesuchten Beispielen soll aber der Versuch unternommen werden, die Praktikabilität der im Staatsvertrag beschlossenen Reglementierungen darzustellen.

2.1 Die Alterskennzeichnung

Abbildung 2: Alterskennzeichnung nach FSK

Die Kennzeichnung von sogenannten *statischen* Webseiten, also Inhalten, die ein Mal erstellt und danach nicht mehr verändert werden, ist technisch relativ einfach zu realisieren, wenn auch aufgrund der großen Anzahl von Seiten sehr zeitaufwendig. Gleiches gilt für Angebote mit einem eng gefassten und exakten Fokus, Als Beispiel sei der Internetauftritt der Fachzeitschrift *Kicker* [2] genannt.

[2] http://www.kicker.de

Bei dynamischen, also sich ständig verändernden Inhalten, sowie Webseiten, die überwiegend nicht vom Betreiber, sondern von Usern gefüllt werden, ändert sich die Situation. Eine Kennzeichnung nach Alterskategorien mag vielleicht in der Theorie denkbar sein, stößt in der Praxis jedoch auf unüberwindbare Hürden. Einige ausgewählte Beispiele sollen dies verdeutlichen:

Beispiel: Wikipedia

Die Online-Enzyklopädie Wikipedia[3] ist ein typischer Fall von *User Generated Content*. Weltweit haben sich im Laufe der vergangenen Jahre unzählige Benutzer zusammengefunden und in einem richtungweisenden Projekt ein frei verfügbares Lexikon erschaffen.

Allein für den deutschsprachigen Teil weist die aktuelle Statistik von Wikipedia insgesamt über drei Millionen Seiten, eine Millionen Artikel und etwa zweihunderttausend gespeicherte (Multimedia-)Dateien aus.

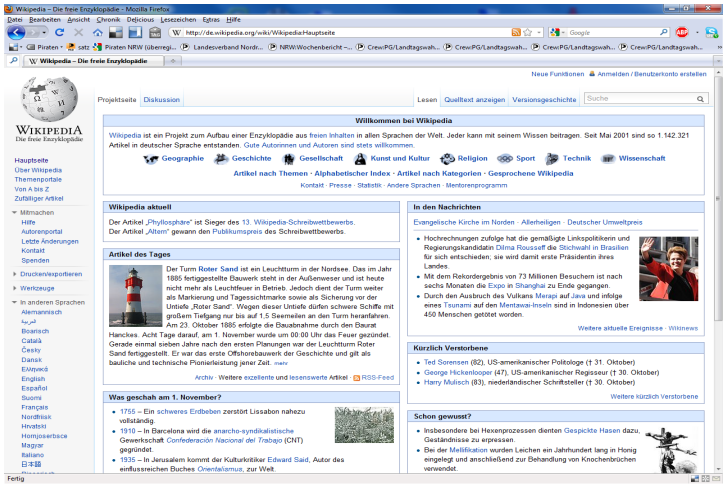

Abbildung 3: Die freie Online-Enzyklopädie Wikipedia

Damit jedoch nicht genug. Wikipedia wird ständig erweitert, bestehende Artikel werden täglich diskutiert, korrigiert und verbessert. Ausufernde, heftige Löschdiskussionen verdeutlichen ebenfalls die manchmal sehr konträren Positionen der freiwilligen Helfer.

Aufgrund der riesigen Anzahl der vorhandenen Seiten und der zu erwartenden Diskussionen über die Alterskennzeichnungen kann es für die Betreiber von Wikipedia eigentlich nur eine Lösung geben: die durchgängige Wahl *‚Ab 18‘*, um im Zweifel rechtlich auf der sicheren Seite zu stehen. Aktuell dokumentiert der *AK Zensur* dieses Szenario sehr eindringlich[4].

Sollte eine solche Kennzeichnung praktiziert werden, fiele mit einem Schlag ein riesiges Wissensportal für minderjährige Schüler weg.

Beispiel: Youtube und Bloghoster

Ein ähnliches Problem existiert für Youtube[5], Cliphfish[6], Flickr[7], andere Communitys, di-

[3] www.wikipedia.de
[4] http://ak-zensur.de/jmstv/
[5] http://www.youtube.com
[6] http://www.clipfish.de
[7] http://www.flickr.com

verse Bloghoster sowie alle übrigen ‚Mitmach'-Portale. Die Betreiber haben auch hier eigentlich nur zwei Möglichkeiten:

Entweder prüfen sie jeden einzelnen Eingang von User Content und versehen ihn mit einer - aus ihrer Sicht geeigneten - Alterskennzeichnung. Oder sie wählen den einfachen Weg und setzen ihr ganzes Projekt auf die Altersstufe *‚Ab 18'*.

Kai Schmalenbach, Mitadministrator des freien und kostenlosen Bloghosters *antville.org*[8], sieht schon bei dem relativ kleinen Kreis von ca. 2.000 Blogs keine Möglichkeit, alle Beiträge der Blogger auf ihre Alterskennzeichnung zu kontrollieren. Der Aufwand ist aufgrund des Arbeitspensums und bezüglich der dann anfallenden Kosten nicht vertretbar.

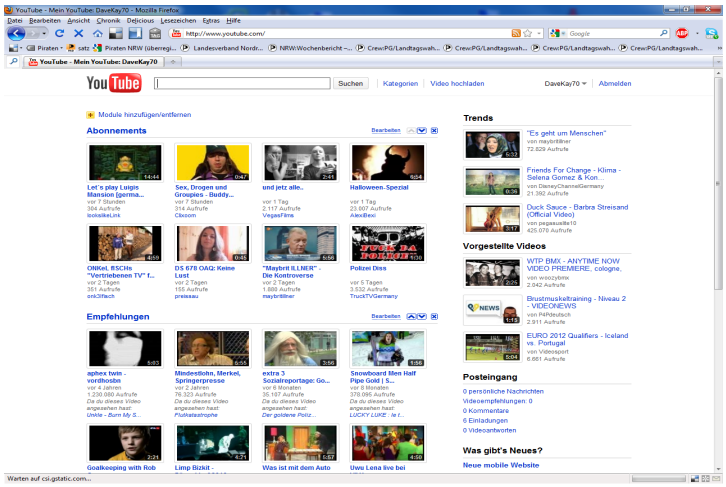

Abbildung 4: Youtube

Anbieter und Autoren von Webblogs aktivieren außerdem in den meisten Fällen die Kommentarfunktion zu ihren Beiträgen. Selbst bei einem relativ kleinen Hoster wie *Antville* sind etwa 70.000 angemeldete Benutzer verzeichnet, die regelmäßig Kommentare in den verschiedenen Blogs hinterlassen. All diese Kommentare gilt es in Zukunft möglichst zeitnah zu kontrollieren und gegebenenfalls zu kennzeichnen.

Ein Spezialfall sind Diskussionsforen. Stark frequentierte Foren erzeugen mehrere Hundert Einträge in der Stunde. Schon die Debatte um die sogenannte *Störerhaftung* sowie einige Grundsatzurteile[9] dazu hat gezeigt, dass es für einen Anbieter nicht zumutbar ist, Beiträge im Vorfeld auf rechtliche Aspekte zu überprüfen.

§5(3) des JMStV soll Anbietern zwar die Möglichkeit erschliessen, mit einem Beitritt zu einer FSK die oben beschriebenen Probleme zu umgehen (*‚Der Nachweis, dass ausreichende Schutzmaßnahmen ergriffen wurden, gilt als erbracht, wenn sich der Anbieter dem Verhaltenskodex einer anerkannten Einrichtung der Freiwilligen Selbstkontrolle unterwirft'*). Dies ist jedoch mit Kosten verbunden und stellt keine Alternative für private oder nichtkommerzielle Internetangebote dar.

Abmahnungen bei fehlerhafte Kennzeichnung

In einigen Diskussionsbeiträgen zur geplanten Novellierung des JMStV wurde auch auf die Gefahr von Abmahnungen bei falscher Kennzeichnung hingewiesen. Weiter oben haben

[8] http://antville.org

[9] http://juris.bundesgerichtshof.de/cgi–bin/rechtsprechung/document.py?Gericht=-bgh&Art=en&sid=6001c95def897c850d5a171abbf1b3a8&nr=30359&pos=0&anz=1

wir bereits den Praxistest des AK Zensur erwähnt, der unserer Meinung nach sehr deutlich die Problematik der Einteilung in eine falsche Alterskategorie aufzeigt.

Möglicherweise entsteht nach der Einführung zur Pflicht einer Kennzeichnung eine neue *Blockwart* -Mentalität im deutschsprachigen Teil des Internets, auch wenn wir dieses Szenario für wenig wahrscheinlich halten.

Im Falle von kommerziellen Angeboten ist aber durchaus denkbar, dass Wettbewerber versuchen werden, einen unliebsamen Konkurrenten mit Hilfe von Abmahnungen oder Anzeigen bei der Kommission (§24) zu torpedieren. Die Historie des Abmahnwesens in Deutschland - gerade in Bezug auf das Internet - lässt hier viel Spielraum für Phantasien.

2.2 Praktikabilität der zeitlichen Einschränkungen

Auf einem physikalischen Host befinden sich üblicherweise hunderte oder tausende von Domains. Dabei beschränken sich diese selten auf eine bestimmte Länderkennzeichnung (.de, .com, .it, etc.). Der administrative Aufwand, serverseitig dediziert Content zu bestimmten Zeiten anzubieten, steht für Provider in keinem Verhältnis zum Ertrag.

Eine Umsetzung erscheint uns - wenn überhaupt - nur in den Fällen möglich, wo große Unternehmen ihre eigenen Serverparks pflegen und professionelle Webadministratoren mit dieser Aufgabe betreuen.

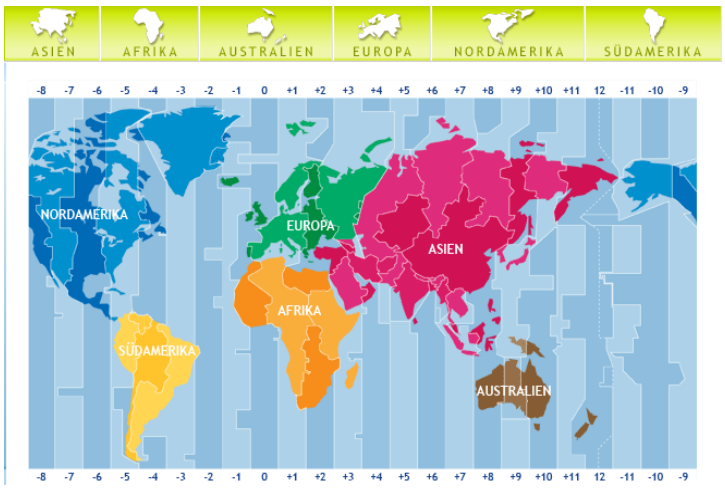

Abbildung 5: Die Zeitzonen der Erde

Die im JMStV genannten Sendezeiten beziehen sich auf unsere Zeitzone. Dadurch werden Inhalte, die wir hier erst ab 22 Uhr ‚*senden*', morgens um 6 Uhr in Australien und um 16 Uhr an der Westküste von Amerika ‚*ausgestrahlt*'.

Ebenso logisch ist der umgekehrte Fall, wenn jugendgefährdender Inhalt um 22 Uhr einer anderen Zeitzone zur Verfügung gestellt wird. Diese Problematik ist spätestens seit der Einführung des Satelliten-TV bekannt.

Download bei Nacht

Eine wirklich simple Methode, den Schutz durch vorgeschriebene Sendezeiten auszuhebeln, besteht in einem automatisierten und zeitgesteuerten Download von jugendgefähr-

denden Inhalten. Jedes gängige, auf einem PC oder Notebook installierte Betriebssystem liefert die Werkzeuge dafür frei Haus. In ihrer Handhabung optimierte Applikationen sind ebenfalls kostenlos überall im Internet zu finden.

Die kleinen Helfer laden komplette Webseiten zu voreingestellten Uhrzeiten - in diesem Fall nachts - auf den heimischen Rechner. Einzige Voraussetzung: PC oder Notebook müssen eingeschaltet und ein Zugang ins Internet vorhanden sein. Downloadhelfer arbeiten heute so präzise, dass ausschließlich gesuchtes Material auf die lokale Festplatte kopiert wird.

2.3 Definition des Anbieters

Erhebliche Bedenken haben wir bei der Definition des Begriffs ‚*Anbieter*', wenn es um Mitmachportale, Blogs, Foren oder die schon erwähnte Kommentarfunktion in veröffentlichten Beitrgen geht. Ab welcher Menge Inhalt ist der technische Betreiber der Seite nicht mehr Anbieter im Sinne des JMStV? Unterliegen Kommentare der Verantwortung des Verfassers oder ist es die Pflicht des ursprünglichen Autors, einen Artikelkommentar entsprechend zu kennzeichnen?

Auch wenn man als Anbieter einer kleinen Webseite oder eines eigenen Blogs selbst in der Pflicht stehen wird, eine geeignete Alterskennzeichnung anzubringen: Woher weiß der Anbieter, was nach geltendem Recht ‚*geeignet für die Altersgruppe XY*' ist?

Wie ein Test des AK Zensur zeigt[10], ist es dem Laien kaum möglich, selbst eine Kennzeichnung vorzunehmen. Auch hier wäre die logische Folge, aus Angst vor Konsequenzen auf Nummer sicher zu gehen und die Alterskategorie ‚*Ab 18*' zu wählen. Eine professionelle Klassifizierung kostet Geld, welches gerade kleine Projekte oder private Anbieter nicht aufbringen können oder wollen.

2.4 Echtzeitkommunikation

Völlig unbeachtet bleibt in der ganzen Diskussion um die Praktikabilität des JMStV die Kennzeichnung von Echtzeitkommunikation und Microblogging. *Chatten* und *twittern* ist für die heutige Jugend so normal wie das Versenden von Kurznachrichten (SMS) per Mobilfunktelefon für die Generation davor.

Chatclients bieten außerdem schon lange sowohl die Möglichkeit der einfachen Übertragung von Dateien, als auch eine Verschlüsselung der Kommunikation[11]. Sogenannte *URL-Shortener* wie *bit.ly* [12], verschleiern den ursprünglichen Namen eines publizierten Links. So wird aus *http://www.playboy.com* z.B. *http://bit.ly/GhdTf*.

Wer ist in diesem Fall überhaupt für eine Klassifizierung verantwortlich? Der Betreiber eines Chatservers? Der Hersteller der Chatsoftware? Die Administratoren der einzelnen Chatkänale? §3 (‚*Im Sinne dieses Staatsvertrages sind ... Anbieter Rundfunkveranstalter oder Anbieter von Telemedien.*') liefert keine befriedigende Antwort.

[10] http://ak-zensur.de/jmstv/

[11] http://de.wikipedia.org/wiki/Off–the–Record_Messaging

[12] http://bit.ly/

2.5 Einfache Formen der Umgehung

Es ist eine altbekannte Weisheit: Das Internet kennt keine Staatsgrenzen. Ordnungsmaßnahmen und Bestrafungen setzen üblicherweise voraus, dass eine Tat im Inland begangen wurde. Solange der Anbieter von Internetinhalten seine Domains physikalisch in Deutschland betreibt, scheint der Fall klar. Wie aber wird z.B. mit deutschsprachigem Inhalt umgegangen, der auf einem Server im Ausland gehostet wird? Möglicherweise gelten dort andere Jugendschutzbestimmungen. Welches Recht greift dann?

Contentanbieter können im Zweifel ihre gehosteten Domains ins Ausland umziehen und dort Inhalte mit einer bestimmten Jugendfreigabe kennzeichnen. Das Jugendschutzprogramm würde diesen Content durchlassen. Eine rechtliche Verfolgung gestaltet sich möglicherweise als sehr schwierig. Uns ist auch nicht ganz klar, welches Recht an dieser Stelle greifen würde.

Die Motivation hinter diesen Umzügen ist klar und bereits jetzt Bestandteil des Internetalltags. Anbieter mit zweifelhaften Inhalten gehen schon länger den Weg, ihre Server in Staaten zu mieten, deren Gesetzgebung ‚toleranter' ist. Als Klassiker dieser Praxis sind Musikportale, Online-Casinos oder Wettanbieter zu nennen. Auch im Falle des JMStV besteht die Gefahr, dass gerade kommerzielle Anbieter ihre Sever im Zweifel ins Ausland umziehen und die Altersfreigabe deutlich heruntersetzen werden.

Das *Taggen* mit einer niedrigen Alterskennzeichnung für deutsche Konsumenten könnte sich bei Webentwicklern in aller Welt außerdem als routinemäßige Optimierung zur Steigerung der Besucherzahlen etablieren. Die Anbieter verschaffen sich so ohne größeren Aufwand einen Vorsprung vor den Wettbewerbern. Die Kommission oder andere Kontrollinstanzen stehen hier vor einen wohl eher nicht realisierbaren Aufwand, diese Seiten zu ermitteln.

3 Das Jugendschutzprogramm

3.1 Hardware und Betriebssysteme

Die Zeiten, in denen Privatanwendern zur Nutzung des Internets ausschließlich Personal Computer mit einem Microsoft-Betriebssystem zur Verfügung standen, sind lange vorbei. Die Liste der internetfähigen Geräte ist mittlerweile sehr groß geworden:

- klassische Personal Computer und Notebooks
- Tablet-PCs
- EBook-Reader
- Spielekonsolen
- Mobilfunktelefone
- Smartphones
- TV-Geräte
- Kabel- und Satellitenreceiver

- Router

Mindestens ebenso lang fällt eine Aufzählung der heute verwendeten Betriebssysteme aus:

- Microsoft Betriebssysteme (Windows XP, Windows Vista, Windows 7, Windows Mobile)
- Linux (SuSE, (K)Ubuntu, RedHat, Debian,...)
- Apple (MacOS Tiger, Leopard, Snow Leopard, iOS)
- Android
- Symbian
- Blackberry

Eine verlässliche Statistik zu unter Privatanwendern meist benutzten Betriebssystemen existiert leider nicht. Sicherlich haben die Betriebssysteme von Microsoft (noch) den größten Anteil. Diverse Linuxderivate, MacOS von Apple und die Betriebssysteme verschiedener Mobiltelefonanbieter steigen jedoch kontinuierlich in der Gunst der Benutzer.

3.2 Anforderungen an die Software

Eine geeignete Jugendschutzsoftware muss für alle bekannten Betriebssysteme entwickelt werden. Sie muss auf jeder verwendeten Hardware für die Erziehungsberechtigten einfach zu installieren sein. Dabei sollten die Softwareentwickler - unter anderem aus rechtlichen Gründen - stets folgende Kriterien im Auge behalten:

- Die Software darf die grundsätzliche Funktionalität und Leistung des Geräts nicht beeinträchtigen.
- Da es keine bundesweit einheitliche Software geben wird (siehe §11(1-3)), müssen sich alle beteiligten Provider auf standardisierte Schnittstellen für die Kennzeichnung und geplante Filterung von Inhalten einigen.
- Der relativ kurze Lebenszyklus vieler Betriebssystemversionen erfordert ein pausenloses Entwickeln und Bereitstellen von Updates der Jugendschutzsoftware. Diese Updates müssen in einfach zu installierenden Paketen zur Verfügung gestellt werden.
- Parallel müssen regelmäßige Sicherheitsupdates - ebenfalls mittels einfach zu installierender Pakete - zu allen in Verwendung befindlichen Betriebssystemen bereitgestellt werden.
- Die ständige Entwicklung neuer Kommunikationsprotokolle erfordert eine zeitnahe Anpassung der Jugendschutzsoftware.

Orientiert man sich hierbei an den von größeren Softwareunternehmen kalkulierten Supportzeiten (in der Regel 5 Jahre) und den Lebenszyklen in den drei großen Betriebssystemgruppen Microsoft Windows, Linux, MacOS/Apple, erkennt man sehr schnell, dass der zu leistende Aufwand für Entwicklung und Pflege einer Jugendschutzsoftware immens sein wird.

Voraussetzung: hierarchische Accounts

Ein wesentliches Kriterium bezüglich der noch zu entwickelnden Jugendschutzsoftware berücksichtigt das Gesetz überhaupt nicht:

Die Verwendung einer solchen Software funktioniert ausschließlich auf Hardware mit Betriebssystemen, welche eine sogenannte *hierarchische Benutzerstruktur* mit privilegierten und nicht privilegierten Accounts zur Verfügung stellen.

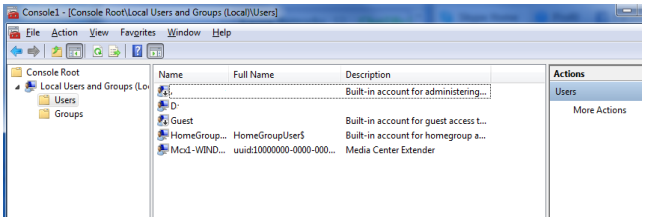

Abbildung 6: Benutzerverwaltung bei MS Windows

Um überhaupt einen Schutz vor jugendgefährdenden Inhalten zu ermöglichen, muss die Software mit den Rechten eines privilegierten Benutzeraccounts (Administrators) installiert werden.

Der zu schützende Jugendliche darf zu keinem Zeitpunkt Zugriff auf diesen privilegierten Account haben, weil er die installierte Jugendschutzsoftware sonst entweder deaktivieren, deinstallieren oder auf anderem Wege umgehen könnte.

3.3 Einfache Formen der Umgehung

Die Praxis (Tests, Umfragen) zeigt, dass eine Trennung zwischen privilegierten und nichtprivilegierten Benutzern auf vielen PCs nicht stattfindet. In den wenigsten Haushalten besitzen Eltern das technische KnowHow für diese Konfiguration. Und der Schluss liegt nahe, dass gerade Erziehungsberechtigte, welche dieses Wissen besitzen, auch über die vieldiskutierte, sogenannte *Medienkompetenz* verfügen, eine Jugendschutzsoftware also eher nicht benötigen werden.

Geräte wie Spielekonsolen, Mobilfunktelefone, Smartphones, EBook-Reader und diverse Tablet-PCs, allesamt internetfähig, besitzen in der Regel keine Konfigurationsoptionen für eine Unterscheidung zwischen privilegierten und nichtprivilegierten Accounts. Ein Benutzer ist so immer Administrator mit allen Rechten auf dem System. Eine hier installierte Jugendschutzsoftware ist so gut wie wirkungslos, da jeder Benutzer diese Software wiederum sofort deaktivieren, deinstallieren oder umgehen kann. Eine Filterung wäre hier nur seitens des Providers möglich.

Virtuelle Maschinen

Virtuelle Betriebssysteme sind eine weitere Herausforderung für die zu entwickelnde Jugenschutzsoftware. Virtuelle Maschinen (für Laien: *die Emulation eines physikalischen PC im PC*) findet man schon lange nicht nur in professionellen Entwicklerumgebungen. Die frei verfügbare Virtualisierungssoftware *Virtualbox* [13] wird von dem Unternehmen Sun Microsystems unterstützt. Auch die Firma *Vmware*[14] bietet freie Varianten ihrer Software.

[13] http://www.virtualbox.org/
[14] www.vmware.com

Bereits vorkonfigurierte Images von Gastbetriebssystem finden sich überall im Internet. Jeder halbwegs versierte Anwender ist heute in der Lage, in 30 Minuten eine virtuelle Instanz mit einem Windows- oder Linux-Betriebssystem aufzusetzen. Eine installierte Jugendschutzsoftware auf dem Hostsystem wird dann praktisch arbeitslos.

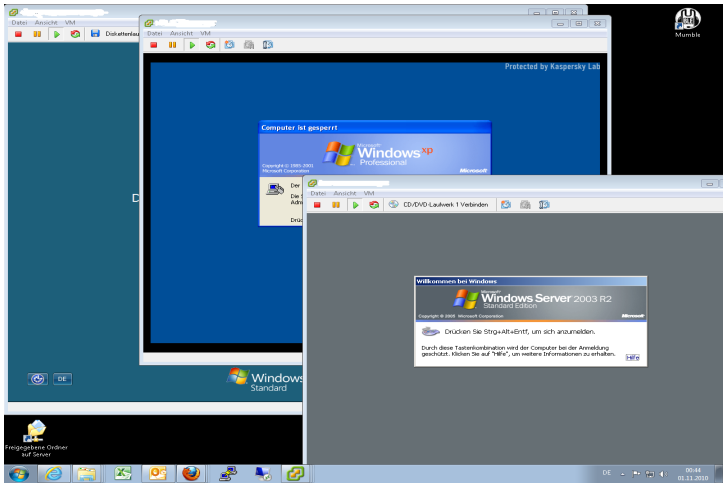

Abbildung 7: Die Virtualisierungssoftware Vmware

Live-CDs und -DVDs

Die bei weitem simpelste Methode, eine auf einem Notebook oder klassischen PC installierte Jugendschutzsoftware unabhängig vom Betriebssystem zu umgehen, wird heute als Beigabe jedes zweiten PC-Magazin geliefert: Die *Live-CD* oder *-DVD*. Es handelt sich hierbei um eine bootfähige CD oder DVD, auf der ein komplettes Betriebssystem (meist Linux) benutzerfertig installiert ist. Der Anwender legt die CD ein und startet seinen PC oder das Notebook von diesem Medium. Die wohl bekannteste Edition *Knoppix* [15] erkennt nahezu jede gängige Hardware, läuft problemlos auf den allermeisten Rechnern und erlaubt sogar das Speichern von Dateien auf dem ursprünglichen Datenträger.

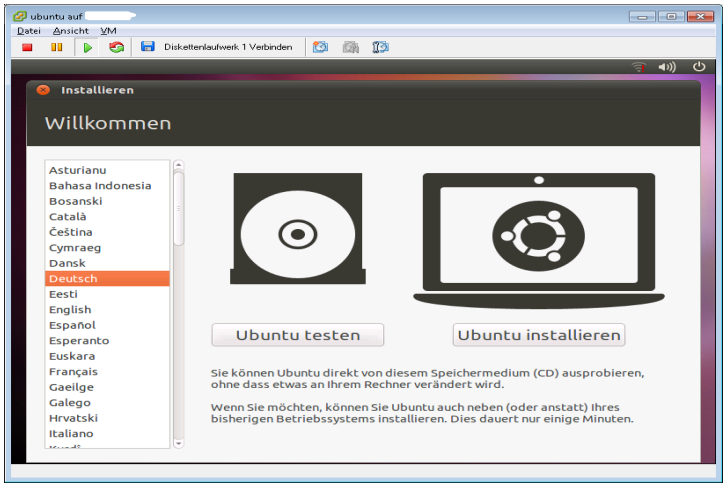

Abbildung 8: Ubuntu als Live–CD

Die Verwendung von Live-CDs erfreut sich aus diversen Gründen immer größerer Beliebt-

[15] http://www.knopper.net/knoppix/

heit. Anwender können so ohne großen technischen oder zeitlichen Aufwand ein neues Betriebssystem testen.

Live-CDs werden auch für einen gefahrlosen Umgang mit dem Internet empfohlen, hier sei als Beispiel nur das Online-Banking genannt. Sogar das Bundesamt für Sicherheit in der Informationstechnik[16] bietet eine selbst entwickelte Live-CD an.

Ähnlich wie bei der Konfiguration von Benutzeraccounts bedarf es eines größeren technischen Wissens, die Verwendung von Live-Medien auf einem PC oder Notebook zu erschweren. Ein hundertprozentiger Schutz existiert außerdem nie, sobald Jugendliche physikalischen Zugriff haben. Und den haben sie praktisch bei jeder Nutzung.

Schulhofmethode

Wie bei allen Dingen, die Jugendlichen ausdrücklich verwehrt sind, wird nach Einführung einer Alterskennzeichnung von Internetangeboten ein zusätzlicher Reiz des Verbotenen entstehen. Das war vor zwanzig bis dreißig Jahren so und hat sich seither nicht geändert. Jugendgefährdende Inhalte - völlig gleichgültig, ob es sich dabei um ein Pornoheft in den Siebzigern, das Videoband oder die Musik-CD in den Achtzigern, um einen verbotenen Ego-Shooter oder Multimediadaten aus den Schmuddelecken des Internet handelt - waren, sind und werden immer ein beliebtes Tauschgut unter Jugendlichen sein.

Ein Schüler, der auf dem heimischen Rechner keinen Filter installiert oder diesen ausgetrickst hat, könnte große Mengen von nicht jugendfreien Inhalten, als Tauschmasse anbieten. Ob in P2P-Netzwerken oder per Bluetooth auf dem Schulhof, ob mit mobilen Datenträgern, als Download auf einem eigenen FTP-Server, über den Chat-Client oder per Mail, ob bei Dropbox oder anderen Anbietern, die es heute zulassen, große Dateien für andere zu hinterlegen, die technischen Entwicklungen der letzten Jahre erlauben reichlich Phantasie beim Verteilen des beliebten, weil verbotenen Guts.

3.4 Anwendungen und Content-Erkennung

Zu guter Letzt muss die geplante Jugendschutzsoftware in der Lage sein, den Datenstrom von Applikationen zu filtern. Die aufgerufene Verbindungen sollen sowohl auf Alterskennzeichnungen überprüft, als auch - so kein *Tagging* existiert - auf mögliche Jugendgefährdung untersucht werden (*§11(2) „. . . eine hohe Zuverlässigkeit bei der Erkennung aller Angebote bieten*‘). Aus rechtlichen Gründen ist eine besondere Sorgfalt bei der Verhinderung von *False Positives/Negatives* erforderlich.

Zu den eingangs aufgelisteten Gruppen von Webinhalten gibt es für jedes Betriebssystem eine Reihe von Anwendungen, mit deren Hilfe ein Benutzer auf angebotene Inhalte zugreifen kann. Die zu prüfenden Inhalte können anhand der verwendeten Programmiertechniken und Kommunikationsprotokolle grob wie folgt gegliedert werden:

- statische Webseiten
- dynamische Webseiten
- Grafiken, Flash, Filme, Streams
- Verbindungen zu Spieleservern
- Internet-TV

[16] https://www.bsi.bund.de

- Echtzeitkommunikation (IRC, ICQ, Skye, etc)
- P2P-Netzwerke (Tauschbörsen)

Beachtet werden müssen weiter:

- Angebote mit Mischcontent
- Fremdsprachiger Content

Ebenfalls unterschieden werden sollte zwischen:

- unverschlüsselten Verbindungen (http, ftp, . . .)
- verschlüsselten Datenverbindungen (ssl, ssh, VPN, etc.)

Aufgrund der Vielzahl der Verbindungstypen (*Protokolle*) in Kombination mit verschiedenen Betriebssystemen und Anwendungen ist eine Überprüfung und Filterung eigentlich nur direkt auf der *Anwendungsebene* des sogenannten *TCP/IP-Stacks* möglich. Die geplante Jugendschutzsoftware muss also als Applikation ähnlich einer professionellen Firewall- oder Proxyfiltersoftware konzipiert werden.

Vergleich zu Antivirensoftware

Der Vergleich mit einer klassischen und (preiswerten?) Antivirensoftware ist hier fehl am Platz, weil diese üblicherweise nur bereits lokal gespeicherte Dateien oder noch zu speichernde Dateianhänge z.B. von E-Mails, aber keine bestehenden Internetverbindungen auf Schadcode überprüft. Ein Echtzeitscan ist sehr ressourcenintensiv.

Ebenso lassen sich die zahlreichen, für Privatanwender angebotenen und empfohlenen Firewalllösungen nicht verwenden, weil diese fast ausschließlich auf *IP-Ebene* arbeiten, also nicht die Inhalte filtern, sondern nur aufgrund von Verbindungstypen unterscheiden.

Die in sensiblen Umgebungen (Banken, Versicherungen, etc.) verwendeten Lösungen sind meist Kombinationen aus diversen Applikationen. In Anschaffung und Unterhalt sind sie sehr kostenintensiv und außerdem mit einem großen administrativen Aufwand verbunden.

Obwohl in diesen - aufgrund der Sicherheitsanforderungen - sehr restriktiv gestalteten Netzwerken viele Verbindungen schon auf IP-Ebene gefiltert werden können, ist immer noch ein großes Maß an weiteren Anpassungen notwendig. Contentfilter müssen wegen der hohen Anzahl an False Positives/Negatives nahezu täglich manuell korrigiert werden.

Nicht gekennzeichnete Inhalte

Lässt sich das Erkennen einer bestehenden Alterskennzeichnung in den oben aufgeführten Kategorien in einer Jugendschutzsoftware noch relativ einfach vorstellen, so stößt diese Software spätestens bei der Überprüfung von nicht gekennzeichneten Inhalten auf Schwierigkeiten. Sogenannte Pornofilter in heute verwendeter Proxysoftware müssen praktisch täglich aktualisiert und gepflegt werden, funktionieren außerdem nur bei statischen Webseiten einigermaßen problemlos.

Jedoch wird auch hier nur *binär* gearbeitet, soll heißen, die verwendeten Filter entscheiden ausschließlich darüber, ob ein überprüfter Inhalt durchgelassen wird oder nicht. Eine weitere Unterscheidung in verschiedene Altersklassen erschwert die Konfiguration oder macht eine technische Umsetzung aufgrund der Komplexität vielleicht sogar unmöglich.

Die Überprüfung von Grafiken, Flashanimationen, Filmen oder Livestreams ist nach dem Stand der heutigen Technik ebenfalls nicht umsetzbar. Und die nächste Herausforderung stellt sich bei der Filterung von fremdsprachigem Inhalt.

Wie eine geplante Jugendschutzsoftware Echtzeitkommunikation inhaltlich überprüfen soll, ist völlig ungeklärt. Chatprogramme bieten - wie schon erwähnt - fast immer den problemlosen direkten Austausch von Dateien zwischen den Kommunikationspartnern an. Darüber hinaus sind diese Verbindungen oft verschlüsselt und erschweren somit grundsätzlich eine Contentüberprüfung.

4 Anforderungen an die Erziehungsberechtigten

Im Abschnitt *Beurteilung der Jugendschutzsoftware – Hardware und Betriebssysteme* haben wir bereits an mehreren Stellen auf das notwendige KnowHow in Bezug auf die Installation der geplanten und noch zu entwickelnden Software hingewiesen.

Um einen effektiven Schutz vor jugendgefährdenden Inhalten im Internet für ihre Kinder zu gewährleisten, müssen Eltern grundsätzlich einen Wissensvorsprung haben bzw. sich diesen erarbeiten. Unabhängig einer geplanten Erweiterung des Jugendmedienschutz-Staatsvertrags sollten Erziehungsberechtigte - neben eines Mindestmaßes an administrativem Wissen - auch in der Lage sein, gewisse Grundlagen der IT-Sicherheit und den Umgang mit dem Internet zu beherrschen. Dazu gehören sowohl ein verantwortungsvoller Umgang mit Anwendungssoftware und Spielen sowie deren Auswahl, als auch das Wissen bzw. Bewusstsein um:

- sichere und unsichere Passwörter
- Viren, Trojaner, andere Malware und mögliche Schutzmaßnahmen
- die Abwehr von Spam
- *sicheres* Surfen im WWW
- weitere gängige Formen der Kommunikation im Internet
- Stärken und Schwächen verschiedener Betriebssysteme
- die Notwendigkeit regelmäßiger Security-Updates für Betriebssysteme und Anwendungssoftware.

Sehr häufig jedoch kennen sich Jugendlichen wesentlich besser in diesem Metier aus, nutzen dies auch oft zu ihrem eigenen Vorteil.

Naiver Umgang

Nach unserer Meinung ist das erforderliche technische Wissen nur dort vorhanden, wo mindestens ein Elternteil im Bereich der IT-Administration beruflich tätig ist oder selbst den Umgang mit Computern von klein auf gelernt hat. Wir sprechen hier aus eigener, oft leidvoller Erfahrung. Regelmäßig werden wir im Bekanntenkreis zu Hilfe gerufen, wenn Probleme mit dem PC oder Notebook existieren. Sehr häufig stellen wir dort einen nahezu naiv zu nennenden Umgang mit Software unbekannter Herkunft oder dem ‚Ansurfen' suspekter Webseiten fest. Hinweise auf mögliche Ursachen der Probleme werden meist mit dem Argument ‚*aber ich habe doch das Schutzprogramm XYZ installiert*' abgetan.

Technisch eher unbedarfte Eltern werden nach Installation der Jugendschutzsoftware dem Gesetzgeber vertrauen und sich ebenfalls in Sicherheit wähnen. Sie werden ebenso weniger Motivation verspüren, sich mit der Förderung der oft zitierten *Medienkompetenz* ihrer Kinder - oder ihrer eigenen - auseinanderzusetzen. Die geplante Software kann also eine sehr kontraproduktive Wirkung entfalten. Wir sind der Ansicht, dass die Philosophie einer Verbotspolitk Medienkompetenz nicht fördern wird, im Gegenteil, es wird ihre Entwicklung behindern.

Öffentlich zugängliche Netzwerke

Einige weitere, für Eltern eventuell relevante Fragen, kann die Neufassung des JMStV ebenfalls nicht lösen: Was ist mit den zahlreichen öffentlichen Netzwerken (Starbucks, Freifunk, Fon, etc. [17])? Was mache ich, wenn mein Kind ungesicherte Internetzugänge im Freundeskreis benutzt?

Es versteht sich von selbst, dass alle hier genannten Aspekte auch aus pädagogischer Sicht betrachtet werden müssen. Aber - wie eingangs erwähnt - behandelt dieses Papier ausschließlich die fachlichen und technischen Voraussetzungen der geplanten Erweiterung des Jugendschutzes auf das Internet.

5 Fazit

Das *Internet* ist kein eindimensionales Angebot im Sinne eines Fernsehsenders, Kinos oder einer Verkaufstheke für Spiele- und Film-DVDs mit einer klar definierten Struktur von Sender und Empfänger. Anbieter und Konsument lassen sich hier nicht mehr voneinander trennen. Jeder Empfänger eines Angebots ist oftmals auch Sender.

Es gibt keine Sende-, sondern allenfalls *Empfangszeiten*, weil in den meisten Fällen der Empfänger bestimmt, wann er oder sie eine Information oder ein Angebot abrufen möchte.

Die Entwicklung einer effizienten Softwarelösung ist aufgrund der technischen Komplexität des Internets nahezu unmöglich und aus betriebswirtschaftlicher Sicht fragwürdig. Ein effektiver Schutz der Kinder durch eine einfacher konzipierte Software ist nicht gewährleistet, wie wir anhand der zahlreichen Umgehungsmöglichkeiten aufgezeigt haben. Die technische Umsetzung funktioniert vielleicht in einem von Unternehmen aufgeteilten und bewirtschafteten Web, nicht aber in einem öffentlichen, für alle zugänglichen Mitmachnetzwerk.

Der Ansatz des JMStV entspricht eher einer Zeit des *Web 0.1*, nicht des *Web 2.0* und wird den Ansprüchen dieses dynamischen Mediums nicht gerecht. Die Neufassung ist nicht mehr als ein Placebo und birgt vielmehr die Gefahr der Vorspiegelung einer falschen Sicherheit. Mit der heutigen Informationstechnologie nicht vertraute Eltern werden sich nach Umsetzung der geplanten Novelle ‚auf den Staat verlassen' und möglicherweise keine weiteren Maßnahmen zum Schutz ihrer Kinder ergreifen.

Kurz gesagt: Aus unserer Sicht und den gesammelten praktischen Erfahrungen existiert keine Methode, Jugendschutz im Internet mit Hilfe einer Alterskennzeichnung in Kombination mit einer Jugendschutzsoftware sinnvoll umzusetzen.

[17] http://wiki.piratenpartei.de/wiki/images/5/5e/Fon-duesseldorf.gif

Die Autoren

Achim Müller, 46 Jahre alt, in den letzten fünfzehn Jahren als freiberuflicher IT-Dozent, -Autor und -Berater tätig, Schwerpunkte: Linux, Security, heterogene Netzwerke, seit 2009 in der Piratenpartei, Mitglied des Presseteams im Landesverband NRW.

Kontakt: acepoint@piratenpartei-nrw.de

Kai Schmalenbach, 40 Jahre alt, ist seit 2001 Systemadministrator in einem mittelständischen Unternehmen und Mädchen für alles. In dieser Funktion hat er das Intranet des Unternehmens aufgebaut und ist heute unter anderem für die Absicherung des Firmennetzwerkes verantwortlich. Seit 2009 Mitglied in der Piratenpartei.

Kontakt: kai.schmalenbach@piratenpartei-nrw.de