NETZPOLITIK.ORG

Technische Möglichkeiten im Jugendmedienschutz

Jörg-Olaf Schäfers, olaf@netzpolitik.org

Übersicht

- JMStV & JMStV-E aus netzpolitischer Sicht
- Worum geht es?
- Die eine Seite: Der Anbieter und sein Serviceprovider
- Die andere Seite: Zugangsprovider und eigener Rechner
- Beispiele & Zahlen: Surfsitter & die 1&1-Dystopie
- Worüber wir vielleicht auch noch reden sollten ...

Ursprünglich sollte ich über die technischen Möglichkeiten im Jugendmedienschutz referieren.

Alles halb so wild?

- Ultima ratio: Sperrverfügungen / Zensurinfrastruktur
- Zwangskennzeichnung & Blacklisting als Default

  „Die KJM prüft mittels eines Testszenarios, [...] ob das Programm Eltern die Möglichkeit bietet, nicht mit dem Labeling-Standard gekennzeichnete Angebote generell zu blockieren.“ (KJM, 11.05.2011)

- Fokussierung auf statisches Web1.0 & Familien-PC
- Standardisierung/modulare Konzepte etablieren Brückenköpfe

  „Das geplante Label-System in Verbindung mit standardisierter und somit zentral lenkbarer Filtersoftware ist zweifellos ein solides Fundament für eine spätere Zensurinfrastruktur“ (RA Udo Vetter, Wikipedia)

Dabei gab es 4 netzpolitische Kernprobleme, die ich unbedingt ansprechen wollte:

* Bereits der JMStV von 2003 sah Sperrverfügungen/Internetsperren vor. Die entsprechende Passage findet sich auch im Entwurf von 2010. Man kann es sehen und nennen, wie man will: Jede Sperrverfügung ist ein Schritt Richtung Zensurinfrastruktur. Die technische Grundlage ist ohnehin identisch.

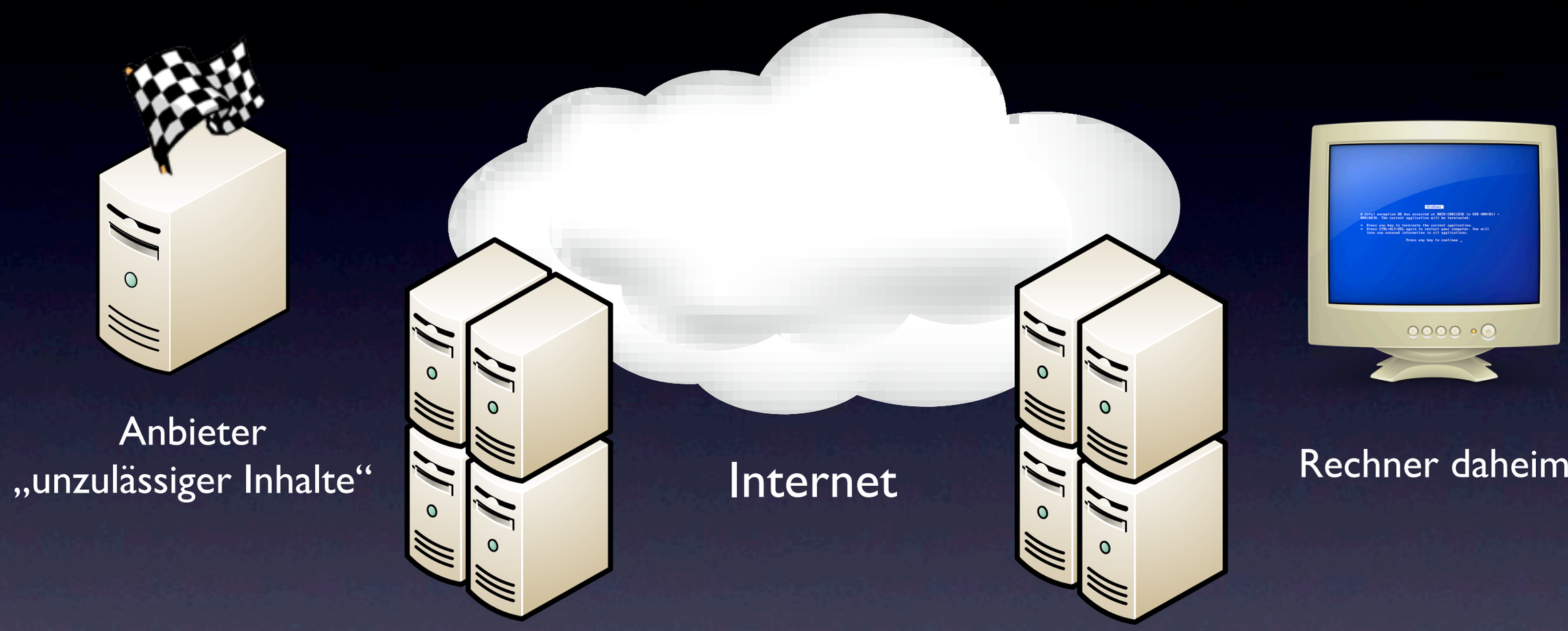
* Ob Jugendschutzsoftware in der Grundeinstellung nicht gekennzeichnete Inhalte blockieren soll, wurde noch im Dezember 2010 kontrovers diskutiert. In einer Stellungnahme von Mai 2011 empfiehlt die KJM Anbietern von Jugendschutzprogrammen „in den Altersgruppen „12 bis unter 16 Jahre“ und „16 Jahre und älter“ Blacklist-Konzepte einzusetzen und nicht gekennzeichnete Inhalte standardmäßig frei zu schalten“. Parallel prüft die KJM, ob das Jugendschutzprogramm Eltern die Sperrung ungekennzeichneter Inhalte erlaubt.

* Die Regulierungsansätze des JMStV-E orientieren sich an der Rundfunkwelt und werden dynamischen Webinhalten nicht gerecht.* Das Konzept „Jugendschutzsoftware“ mag bei einem zentralen Familien-PC greifen, wird der Hardwarerealität Jugendlicher (Smartphone, eigene Rechner und Internetzugänge, Spielekonsolen (vgl. JIM-Studie)) aber nicht gerecht.

* Die Kombination aus einheitlicher Kennzeichnung, modular einbindbaren Filterlisten und einer Filterung auf Routerebene führt - technische konsequent fortgeführt/weitergedacht - zum Modell „Jugendschutz als Service“ auf Provider-/Netzwerkebene. Bereits bei einer Filterung auf Routerebene wäre zu diskutieren, ob und unter welchen Umständen die Einbindung einer nicht mehr nutzerautonomen „BKA-Liste“ mit „absolut unzulässigen Inhalten“ geboten wäre. Siehe Folie 15ff.

*Nebenbei bemerkt: Auch das Konzept Selbst- bzw. Co-Regulierung funktioniert vor allem, wenn man es mit einer Branche oder Industrie zu tun hat. Gegenüber dem einzelner Nutzer, der im Internet immer auch Sender sein kann, greift es nicht oder bestenfalls mittelbar.

Worum geht es?



Spielen wir einmal die Möglichkeiten durch. Und zwar ausgehend vom Ansatz des JMStV. Wer im Internet Inhalte regulieren will, hat – im einfachsten Fall – 4 Punkte, wo er ansetzen kann.

a) Beim Anbieter der Inhalte (das „Ziel“)
b) Beim oder bei den Serviceprovider(n) des Anbieters (Hoster, Registrar, usw)
c) Beim Zugangsanbieter des Nutzers
d) Beim Nutzer selber

Worum geht es?

Anbieter
„unzulässiger Inhalte“

- jugendgefährdende Inhalte
  z.B. „Pro-Ana“, Pornographie, Killerspiele
- Nach deutschen Recht unzulässige Angebote, z.B. Glücksspiel
- Absolut unzulässige Angebote, z.B. Kinderpornographie

Nicht jeder Inhalt ist gleich unzulässig. Man sollte grundsätzlich zwischen ...

a) jugendgefährdenden Inhalten
b) nach deutschem Recht unzulässigen Inhalten
c) absolut unzulässige Inhalten

... unterscheiden.

Möglichkeiten beim Anbieter

Bitte um ...

- Alterskennzeichnung (ggf. Geolokalisierung)
- Sendezeitregelung (ggf. Geolokalisierung)
- Altersverifikationssystem (ggf. Geolokalisierung)
- Sperren des Angebots (ggf. Geolokalisierung)
- Löschen des Angebots

Aber:

- Kosten der Maßnahme
- Interessen des Anbieters
- Wirkung im Ausland fraglich

Erster Ansprechpartner bei problematischen Inhalten sollte der Anbieter sein (Es sei denn, man möchte ihn aus ermittlungstaktischen oder sonstigen Gründen nicht vorwarnen. Gilt auch für seine(n) Serviceprovider.)

Möglichkeiten beim Serviceprovider

Serviceprovider des Anbieters

Bitte um ...

- Prüfung des Angebotes, ggf. Sanktion
  (Ansatz: Löschen statt Sperren!)

Ohne Bitte:

- behördliches Eingreifen (via Amtshilfe)
- Entzug der Connectivität
- Rückgriff auf Registrare („Domain HiJacking“)

Aber:

- Wirkung im Ausland fraglich
- Kooperation im Interesse des Anbieters?

Erscheint eine Kontaktaufnahme mit dem Anbieter nicht erfolgversprechend oder war erfolglos, kann man sich an seine(n) Serviceprovider wenden. Grundlage: AGB und/oder die Rechtslage am jeweiligen (Geschäfts-)Standort.

Zum „Domain HiJacking“ siehe aktuell:
http://www.zeit.de/digital/internet/2011-06/domain-beschlagnahme
http://www.internet-law.de/2011/06/darf-die-staatsanwaltschaft-domains-beschlagnahmen.html

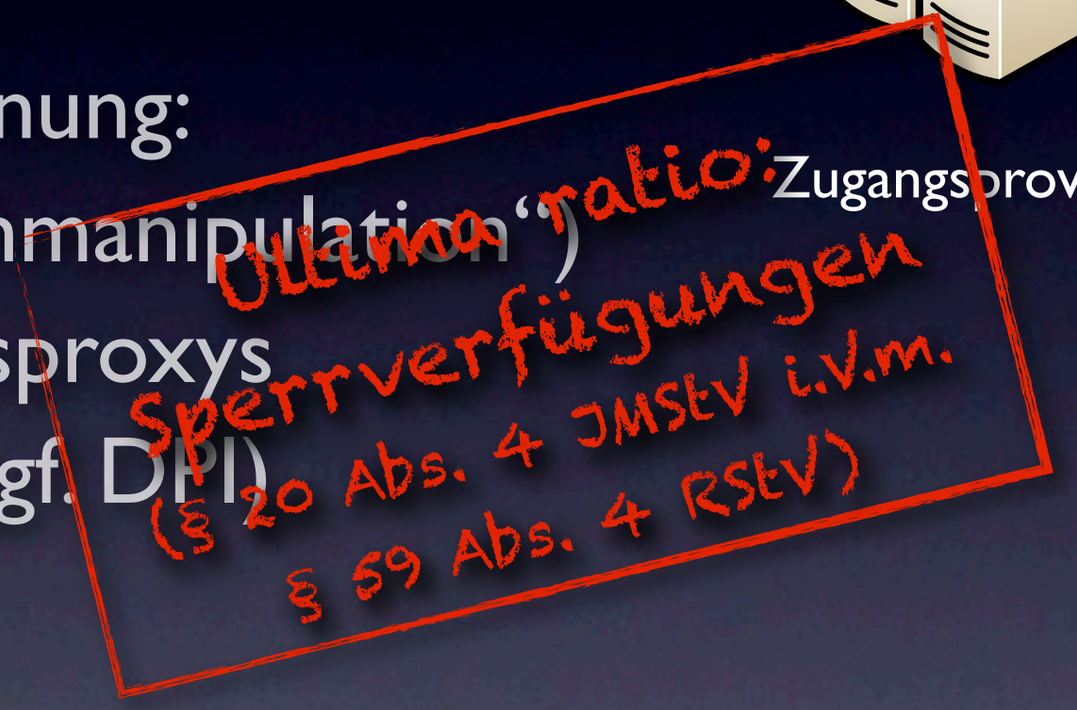
Möglichkeiten beim Zugangsprovider

Internetsperren auf Wunsch:

- „kindgerechter“ Zugang als Service

Internetsperren nach Anordnung:

- DNS-Sperre („Telefonbuchmanipulation“)
- Verwendung eines Zwangsproxys
- Eingriff ins Routing (BGP, ggf. DPI)



Aber:

- je höher der tatsächliche Wirkungsgrad, desto höher der technische Aufwand, der Schaden für Internet/Gesellschaft und die rechtsstaatlichen Hürden

Auch auf Seiten des Zugangsproviders gibt es zwei grundsätzliche Möglichkeiten.

a) Kindgerechte Zugänge als Geschäftsidee. Eine Differenzierung (z.B.: Eltern dürfen alles, Kind nur Whitelist) könnte auf Routerbasis an Hand von Mac-Adressen erfolgen (vgl. Cybits AG/1&1, Folie 13ff.).

b) Internetsperren auf Zugangsebene, wie sie der JMStV bereits seit 2003 vorsieht.

Aber: Eigentlich will man weder Internetsperren noch eine technische Eskalation (Cryptodebatte, DPI ...)

NETZPOLITIK.ORG

Möglichkeiten für Eltern/am Rechner daheim

Rechner daheim

Ansätze:

- Hostbasierte Jugendschutzsoftware
- Routerbasierte Jugendschutzsoftware

Stichworte:

- Blacklist (Negativliste) vs. Whitelist (Positivliste, „Surfraum“)
- Modulare Konzepte, Differenzierung nach Alter
- Nutzerautonomie vs. Kontrollverlust
- Blacklisting für ungelabelte Angebote?
- Blacklisting für unzulässige Angebote („Fürsorgepflicht“ des Staates?)

Eine hostbasierte Jugendschutzsoftware greift nur auf dem Rechner, auf dem sie installiert ist. Zudem ist sie potentiell leicht angreif-/bzw. umgehbar. Vor allem aber wird sie der Hardwarerealität Jugendlicher (Smartphone, eigene Rechner und Internetzugänge, Spielekonsolen, vgl. JIM-Studie 2010) nicht gerecht.

Eine Option, zumindest im Bereich der eigenen vier Wände (Nachbars WLAN und Surfsessions bei Dritten aussen vor ...) wäre eine routerbasierte Jugendschutzsoftware. Gängige Konzepte sind nutzerautonome aktivierbare Negativ- und Positivlisten und eine Differenzierung nach Alter (etwa: Positivliste bis 12 Jahre, ab 12 Jahre Negativliste ...)

Offene Fragen: Sollen ungekennzeichnete Angebote blockiert werden? Müssen unzulässige Angebote - nicht mehr nutzerautonom - blockiert werden, sobald eine (Jugend-)Schutzsoftware in der Fläche etabliert ist?

Beispiel: Surf-Sitter, Cybits AG

Anmerkung: Marktanteil laut Gartner 3,8% in Q1/2011

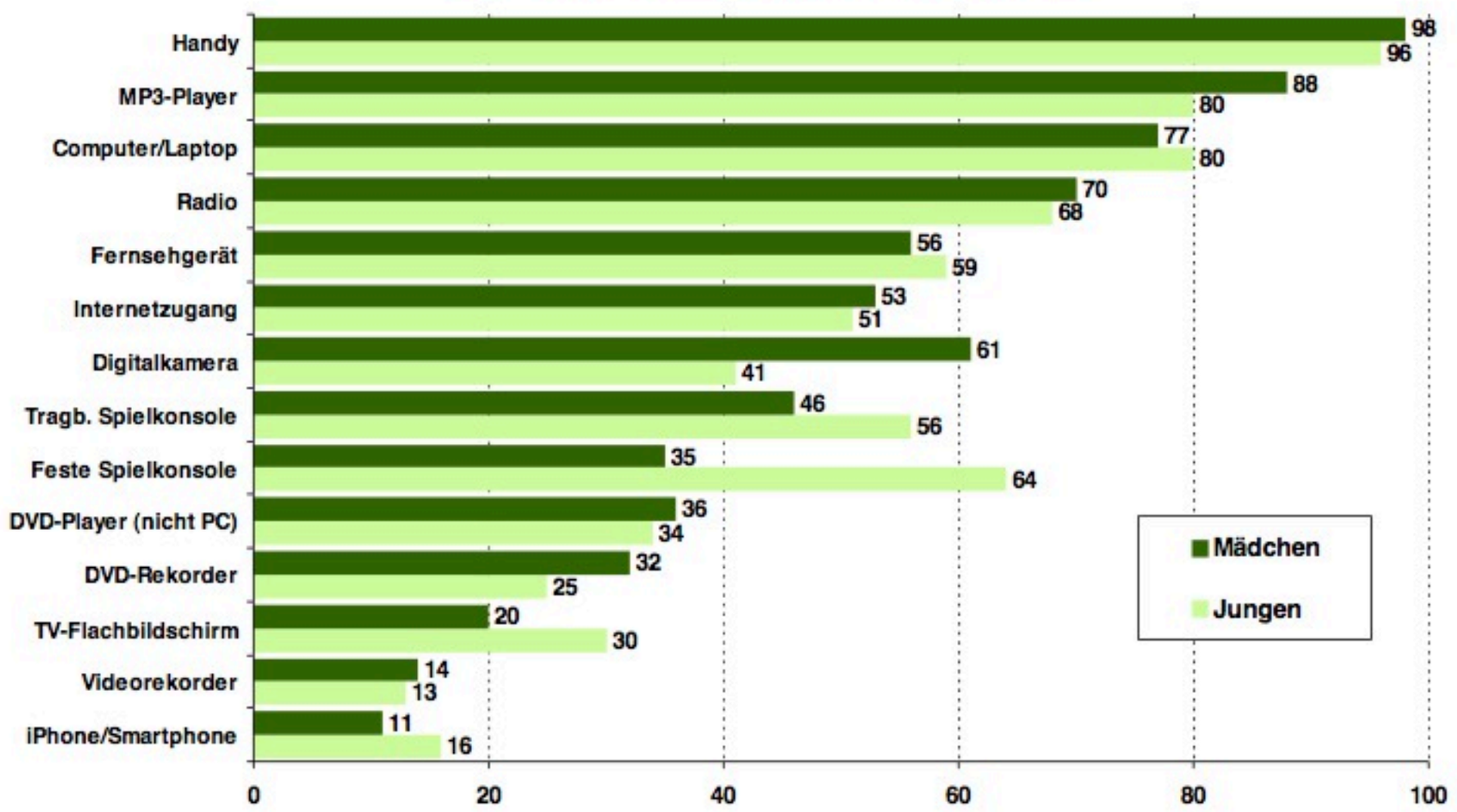
Ein schönes (nicht zwingend gutes oder schlechtes, darum geht es mir nicht) Beispiel für ein modulares Konzept bietet die Firma Cybits AG mit ihrem Surf-Sitter-Programm.

Nicht nur, dass für fast jeden Einsatzzweck (Rechner, Router, Handy*) etwas geboten wird, ...

... auch bei den Filterliste haben Eltern freie Wahl. Optionale Filter, die den Nutzer vor „Abzockseiten und Werbefallen“ schützen, sind ein zusätzliches Kaufargument.

*Ok, Windows Mobile hat nur noch einen Marktanteil von 3,8%, aber bei dieser Folien ist es noch der Gedanke, der zählt.

Zahlen: JIM-Studie 2010



Statistik zur Hardwarerealität Jugendlicher. Wir sehen warum es nicht reicht, nur den „Familien-PC“ zu schützen.

Zahlen: JIM-Studie 2010

„Bereits die jüngsten Teilnehmer der Studie, die 12- bis 13-Jährigen, sind sehr gut mit Mediengeräten ausgestattet.Fast jeder Zweite von ihnen hat einen eigenen Fernseher (48 %) im Zimmer, **zwei Drittel haben einen eigenen Computer (65 %) und drei Viertel eine tragbare Spielkonsole (feste Spielkonsole: 53 %)**. Bei einer Besitzrate von 95 Prozent kann man auch schon bei den 12- bis 13-Jährigen von einer **Vollausstattung bei Mobiltelefonen** sprechen. [...]“

-- Quelle: JIM 2010, Seite 8

Statistik zur Hardwarerealität Jugendlicher. Wir sehen, warum es nicht reicht, nur den „Familien-PC“ zu schützen. Der Anteil bei Smartphones lag 2010 bei 16% (JIM, 12- bis 19-Jährige) bzw. 20% (Nielsen [1]). Tendenz: explodierend.

[1] Quelle: http://www.areamobile.de/news/17489-studie-wie-die-jugend-smartphones-nutzt (Befragt wurden Jugendliche und junge Erwachsene im Alter von 15 bis 24 Jahren)

„Routerlösung“, modularer Aufbau.

Vgl. „Hanten-Runde“ / BKM, 2009

Der Trend im Heimbereich geht daher wohl zur „Routerlösung“. Werbeversprechen: „Schützt alle Geräte, die über ihr Netzwerk Zugriff auf das Internet haben. Egal ob PC‘s, Spielekonsolen, Handys oder mitgebrachte Geräte!“

Anmerkung: Auch diese Lösung lässt sich umgehen. Mir ging es zunächst aber um die Berücksichtigung der Hardwarerealität in deutschen Haushalten. Insbesondere, wenn ein Smartphone nicht über WLAN- sondern um die ihm eigene Mobilfunkverbindung ins Netz geht, ist der jeweilige Mobilfunkprovider gefragt.

Beispiel: Surf-Sitter, Cybits AG

Cybits AG August 2010

Ab 16 Jahre

Dieser Surfraum der Jugendlichen wird ebenfalls durch die Blacklists begrenzt. Im Gegensatz zur Altersstufe "ab 12 Jahre" ist der Surfraum jedoch erweitert. Dass heißt, dass der Surfraum weniger eingeschränkt ist als der ab 12 Jahre.

Ab 18 Jahre – BPjM-eingeschränkt

Der Gesetzgeber verlangt, dass bestimmte Inhalte grundsätzlich nicht zugänglich gemacht dürfen. Diese sogenannten indizierten Inhalte werden durch die Listen der Bundesprüfstelle für jugendgefährdende Medien geblockt.

Ab 18 Jahre - ohne Einschränkung

In dieser Einstellung gibt es keine Einschränkungen durch oben erwähnte Listen. Diese Altersstufe wird allein durch die von Ihnen angelegten Black- und Whitelisteinträgen reguliert.

Die fünf Surfräume im SURF-SITTER

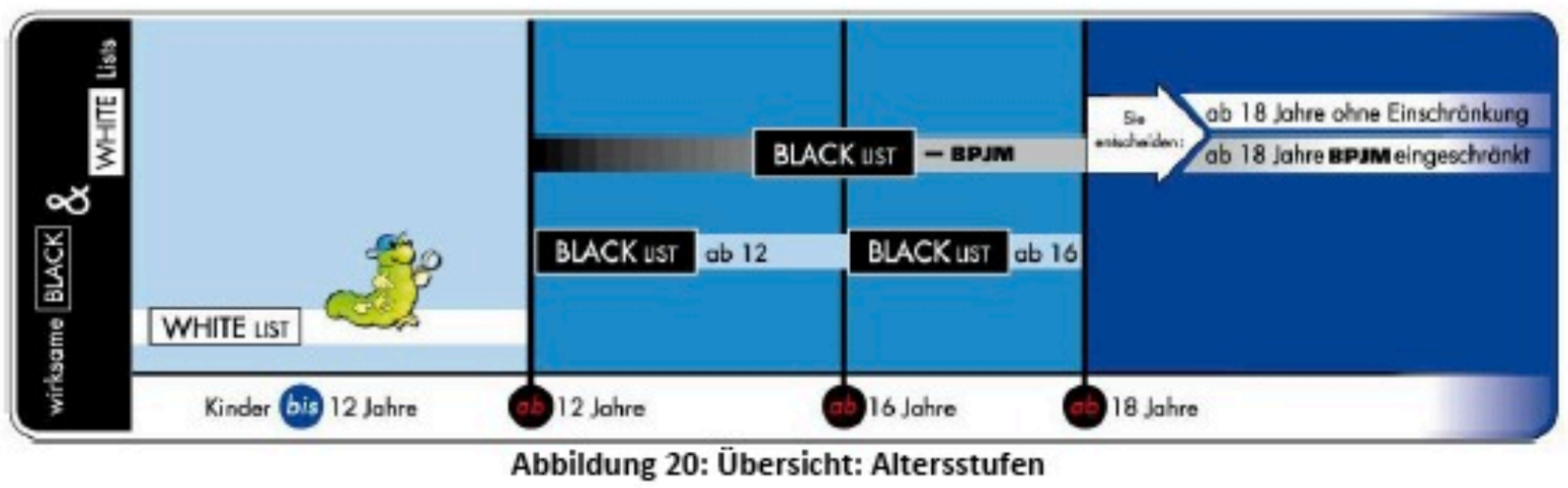


Abbildung 20: Übersicht: Altersstufen

Hier eine schematische Darstellung des Filtermodells von Surf-Sitter:

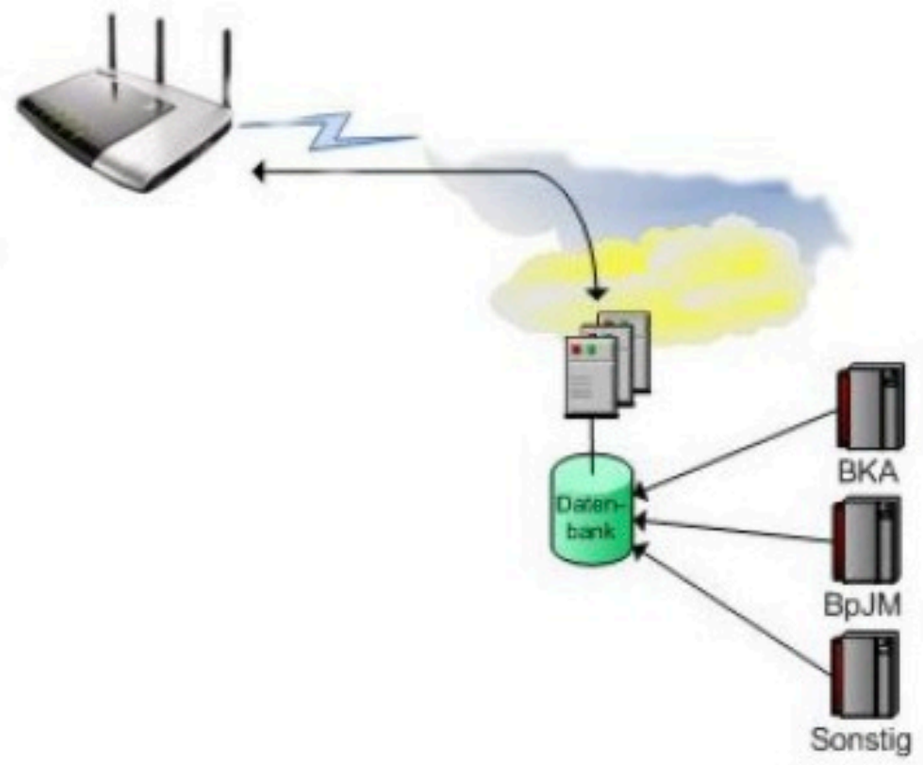
* Whitelist (Positivliste) bzw. Surfraum „FragFinn.de“ bis 12 Jahre
* Blacklisten (Negativlisten) ab 12/16 Jahren
* Einbindung des BPJM-Moduls, um indizierte Inhalte zu blockieren (Möglichkeit wird von der KJM empfohlen)

Die markierte Aussage, „dass bestimmte Inhalte grundsätzlich nicht zugänglich gemacht dürfen“ ist in dieser grundsätzlichen Form allerdings falsch.

Beispiel: Sperralternative (Mai 2009), 1&1

DSL-Router-Lösung

- **Abfrage der Datenbank durch den DSL-Router des Nutzers**



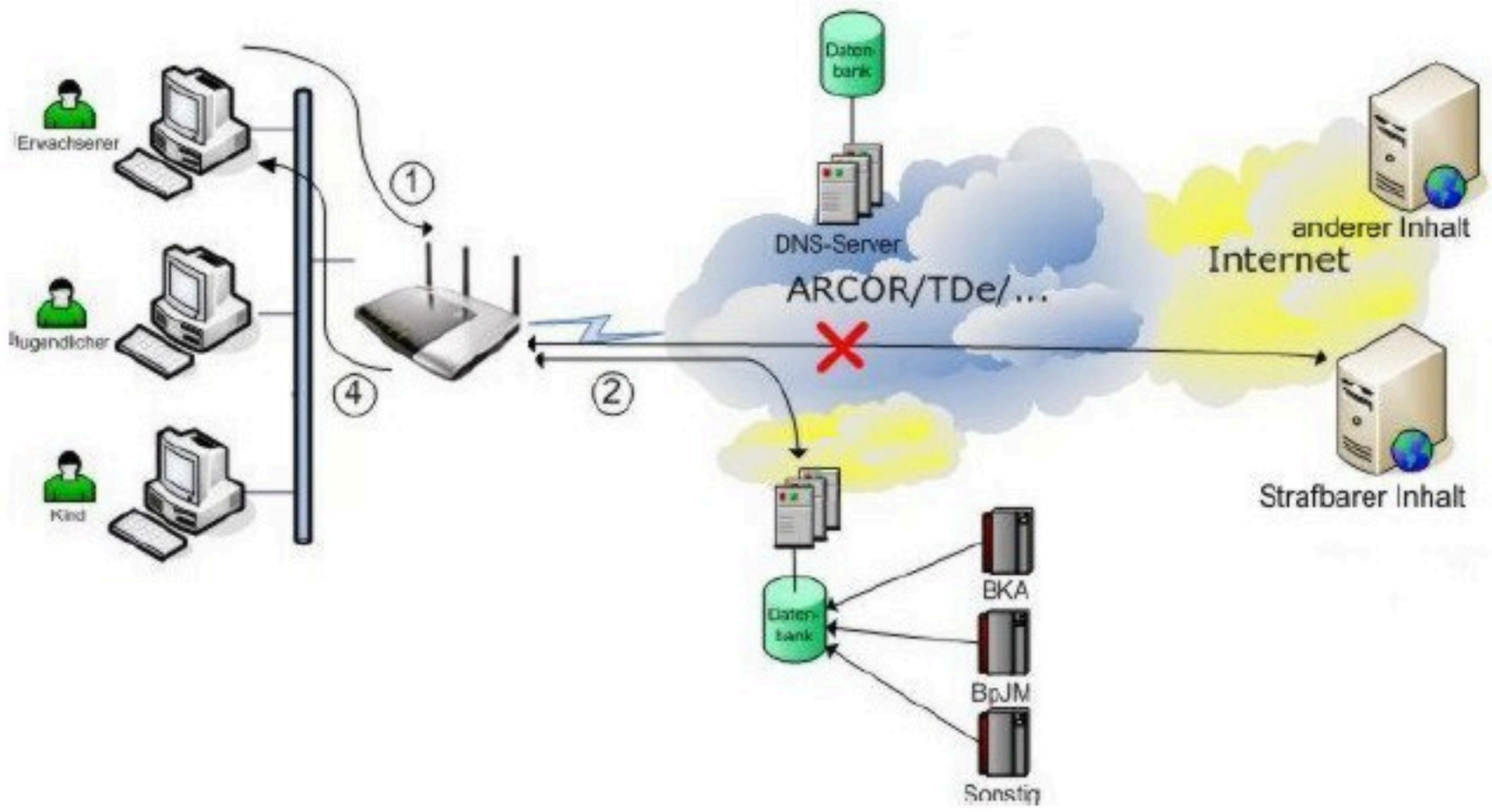
- **Bei Treffern generiert System des Benutzers eine Fehlermeldung**

Auch der Internetanbieter 1&1 hat 2009 schon einmal über eine „Routerlösung“ nachgedacht. Auslöser war die Debatte den Zugriff auf Kinderpornographie auf Zugangsebene zu sperren. Details siehe: http://www.netzpolitik.org/2009/netzpolitik-interview-eine-weitere-alternative-zu-netz-sperrungen/

Beispiel: Sperralternative, 1&1

DSL-Router-Lösung: Erweiterte Funktion

Standard-Einstellung blockt Kinderpornographie



Die von 1&1 vorgeschlagene „Routerlösung“ war als Alternative zu DNS-Sperren („Schäuble-/Leyen-Modell“ in der nächsten Folie) gedacht.

Pro und Kontra DSL-Router Lösung

+ Höhere Nutzer-Akzeptanz der Maßnahme
+ Keine zentrale Infrastruktur/kein Zensurvorwurf
+ Keine Echtzeit-Überwachung möglich
+ Keine Verbindungsdaten, d.h. kein Anlass für Massenstrafverfahren gegen so genannte Zufalls-Surfer
+ Zusätzliche Implementation Jugendschutz möglich
+ Umgehung mittels Eintrag alternativen DNS-Servers erheblich erschwert, d.h. erhöhter Schutz von Kindern und Jugendlichen vor Kinderpornographie
– Nutzer mit Administrator-Rechten kann wie im Schäuble/Leyen-Modell die „Sperre“ weiterhin umgehen
– Schutz nur möglich mit geeigneter Hardware, jedoch Firmware-Update bei vielen im Markt befindlichen Modellen möglich

Nach Vorstellung von 1&1 hätte man diese Lösung sogar „nutzerautonom“ realisieren können. Dieser Hinweis scheint mir, bei allem Respekt, allerdings naiv. Aus staatlicher Sicht dürfte es wohl indiskutabel sein, einen „Kinderporno-Filter“ als Nutzer einfach wieder abstellen zu können.

Die Idee hingegen bleibt interessant: Wäre es nicht sogar geboten, bei einer entsprechenden Verbreitung* der „Routerlösung“ die Sperrung „unzulässiger Inhalte“ durch nicht nutzerautonome Sperrlisten („BKA-Liste“, „Glückspiel-Liste“, usw. ...) zu realisieren?

In Verbindung mit dem ePass und einem entsprechenden Lesegerät ließe sich zudem der Zugang zu „geschlossenen Benutzergruppen“ regulieren. Eine Dystopie? Niemand hat die Absicht eine Netzmauer zu errichten: http://www.netzpolitik.org/2010/jugendmedienschutz-auf-dem-weg-in-die-zukunft/

*Die 5 größten Anbieter versorgen in Q1/11 ca. 84% des Breitbandmarktes in Deutschland, Quelle: http://www.dslweb.de/dsl-marktuebersicht.php. Die Nutzung eines geeigneten Router ließe sich ggf. mit sanftem Druck forcieren (Filter als Service, siehe Cybits AG).

Vielen Dank fürs Zuhören!

Kontakt: olaf@netzpolitik.org

NETZPOLITIK.ORG

Naja, fast...

Tagwolke

Umgehungsmöglichkeiten, Sendezeiten (Downloadtools, Proxies), Smartphones, Tablet-PCs, Spielekonsolen, Messenger, Microblogging, p2p, Mail, Nutzerautonomie, (Echtzeit-)Kommunikation, Web 2.0 Altersklassen, Selbstregulierung?, praktische Auswirkung, Technik kann Erziehung nicht ersetzen, Einstiegshürden bei Nutzung

---

Sperrverfügungen, Zwangskennzeichnung/Blacklisting (Transparenz), Surfräume (wer darf rein, wie realisieren?), Brückenkopf, Filterung auf Router-/Providerebene, Dystopie: Internet nur mit Token, nicht nutzerautonome Sperrlisten ...

Tagwolke als