Prof. Dr. Hannes Federrath
Universität Regensburg
http://www-sec.uni-regensburg.de

Öffentliches Expertengespräch
des Unterausschusses Neue Medien
des Ausschusses für Kultur und Medien des Deutschen Bundestages
zu den rechtlichen und technischen Möglichkeiten und Grenzen
von Sperrungsverfügungen kinderpornographischer Inhalte im Internet
am Donnerstag, 12. Februar 2009, 15:30 – ca. 16:30 Uhr,
Paul-Löbe-Haus, Raum 4.400, Berlin

Fragenkatalog

Technik:

1. Welche Formen der Sperrung von strafrechtlich relevanten Inhalten gibt es und wie bewerten Sie diese hinsichtlich ihrer Wirksamkeit und Effizienz, dem damit jeweils verbunden Aufwand sowie den jeweiligen Kosten?

Formen der Sperrung:

Im Wesentlichen kann man hinsichtlich des Ortes, an dem gesperrt (blockiert) wird, folgende Fälle unterscheiden:

a. Sperrung beim Host-Provider (wo die Inhalte abgelegt sind),

b. Sperrung auf dem Durchleitungsweg (z.B. bei einem Internet Service Provider oder an einem Übergabepunkt zwischen (Teil)-Netzen),

c. Sperrung beim Client (wo die Inhalte angesehen werden),

Hinsichtlich der Sperrmethode lassen sich zweierlei Prinzipien unterscheiden:

- **Erkennung des Bitmusters eines zu blockierenden Inhalts** und Verhindern der Weiterleitung: Dieses Sperrprinzip lässt sich in den Fällen a, b und c anwenden. Bei dieser Methode spielt es keine Rolle, von welcher Adresse der Inhalt abgerufen wird. Ein Filter verhindert nach Erkennung die Weiterleitung zum Client. Das Filterprinzip beruht auf der Idee, in einer Datenbank sog. Hashwerte der Inhalte zu speichern. Für jeden Inhalt wird der Hashwert berechnet und in der Datenbank nachgesehen, ob er enthalten ist. Dann wird der Inhalt blockiert.

  Der Inhalt der Datenbank unterliegt keinen besonderen Anforderungen an die Geheimhaltung: Aus dem Hashwert können weder Bildinformationen noch Adressen extrahiert werden. Für kinderpornographische Inhalte existiert die Datenbank *Perkeo*, in der die Hashwerte eindeutig kinder- und tierpornographischer Darstellungen gespeichert werden.

  Diese Form der Sperrung kann im **Fall a** (Sperrung beim Host-Provider) durch den Host-Provider selbst angewendet werden, um rechtswidrige Inhalte auf dem Server zu detektieren, ähnlich einem Virenscanner. Beispielsweise können Universitäten und

Firmen die Nutzerverzeichnisse regelmäßig überprüfen. Eine Anwendung im **Fall c** (Sperre beim Client) ist ebenfalls vergleichbar mit dem Einsatz eines Virenscanners. Die Anwendung im **Fall b** (Sperrung beim ISP) hat den Nachteil, dass für alle Inhalte zunächst der Hashwert berechnet werden muss, bevor er ausgeliefert wird, was bei hohem Verkehrsaufkommen zu Performanceverlusten führen kann.

- **Adressbezogene Sperrung**: Der Filter basiert auf einer Datenbank, in der die Adressen hinterlegt sind, unter denen die Inhalte abgerufen werden können. Dieses Sperrprinzip ist praktisch nur für den **Fall b** (Sperrung beim ISP) relevant. Im **Fall a** (Sperrung beim Host-Provider) muss nicht mehr gefiltert werden, weil die Sperre entweder direkt durchgesetzt werden kann, indem der Server mit der besagten Adresse geschlossen wird (bzw. der Inhalt entfernt wird), oder die Schließung/ Löschung ist nicht durchsetzbar (z.B. weil der Server im Ausland betrieben wird). **Fall c** (Sperre beim Client) scheidet aus, weil der Client dann den Inhalt der Sperrliste (Adressen der rechtswidrigen Inhalte) erfährt.

  Bei der adressbezogenen Sperrung können zwei Varianten unterschieden werden: Entweder wird die **Durchleitung von IP-Paketen** von oder zu der gesperrten Adresse **verhindert** (Datenbank enthält IP-Adressen der Form 132.199.128.33) oder es wird die **Namensauflösung im Domain Name System (DNS) zur Sperrung** genutzt. Bei dieser Variante wird die bei der Kontaktaufnahme eines Client zum Server notwendige Übersetzung eines Rechnernamens (z.B. http://www-sec.uni-regensburg.de) in die IP-Adresse (hier die o.g. IP-Adresse) überhaupt nicht oder mit einer IP-Adresse beantwortet, die auf einen Server führt, der anstelle des eigentlichen Ziels einen Warnhinweis im Browser anzeigt.

Wirksamkeit und Effizienz:

Sperren die auf der Speicherung von Hashwerten (Erkennung des Bitmusters eines zu blockierenden Inhalts) beruhen, sind wirksamer als adressbezogene Sperren. Adressbezogene Sperren von IP-Adressen sind wirksamer als Sperren auf Basis des DNS.

Hashwert-bezogenes Filtern versagt bereits, wenn 1 Bit des Inhaltes (Bildes, Videos, Textes) verändert wurde (verursacht zur Umgehung für jeden Inhalt neuen Aufwand beim Bereitsteller des Inhalts). IP-Adressen-bezogenes Filtern lässt sich mit Hilfe eines Proxy oder eines Anonymisierers umgehen (verursacht zur Umgehung für jede Internet-Verbindung Aufwand beim Client). DNS-bezogenes Filtern lässt sich umgehen, indem in der Internet-Konfiguration des PCs oder DSL-Routers die IP-Adresse des DNS-Servers verändert wird (verursacht zur Umgehung 1x Aufwand für das Eintragen der neuen Adresse beim Client).

Ein Hashwert-bezogener Filter prüft jeden einzelnen Inhalt und gewährleistet, dass nur die tatsächlich bekannten und relevanten Inhalte blockiert werden. Adressbezogenes Filtern blockiert *alle* auf dem Server befindlichen Inhalte. Befindet sich z.B. auf dem Server flick.com genau ein kinderpornographischer Inhalt, der zum Sperren der Adresse flickr.com führt, dann sind alle Inhalte nicht mehr abrufbar. Eine feingranulare Sperrung einzelner Pfade ist mit einem IP-Adressen-bezogenen Filter mühsam (mit Hilfe spezieller Firewalls) realisierbar, mit einem DNS-bezogenen Filter überhaupt nicht.

2. Lässt sich verhindern, dass diese technischen Möglichkeiten nicht nur zur Sperrung von kinderpornographischen Inhalten, sondern zur Sperrung von rechtmäßigen Inhalten missbraucht werden können?

Nein.

3. Wie kann verhindert werden, dass die Listen der zu sperrenden Inhalte bekannt werden? Was sind die Folgen, wenn – wie in einigen skandinavischen Ländern – die Listen der zu sperrenden Inhalte bekannt werden?

Bei der **Speicherung von Hashwerten** (Erkennung des Bitmusters eines zu blockierenden Inhalts) in einer Sperrliste können weder Bildinformationen noch Adressen extrahiert werden. Die Weitergabe der Datenbank führt somit zu keinem Informationsgewinn über Zugänge oder die Inhalte selbst.

Bei der **Speicherung von Adressen** (adressbezogene Sperrung) in einer Sperrliste kann die Weitergabe technisch nicht verhindert werden. Eine Folge des Bekanntwerdens der Sperrliste ist deren Überprüfbarkeit der darauf befindlichen Adressen. So könnte leicht festgestellt werden, dass tatsächlich keinerlei zweckfremde Sperren vorhanden sind. Wegen der primitiven Umgehungsmöglichkeiten von adressbezogenen Sperren dürften denjenigen, die an kinderpornographischen Inhalten interessiert sind, keinerlei Vorteile durch das Bekanntwerden der Listen entstehen. Schlimmstenfalls könnten Neugierige die Adressen „ausprobieren“.

4. Mit welchen Kosten sind die unterschiedlichen Formen der Sperrung verbunden? In den Medien wurde berichtet, dass das BMFSFJ mit Investitionskosten von ca. 40.000 Euro rechnet. Wie bewerten Sie diese Kostenabschätzung?

Die **Kosten** zur Realisierung von Hashwert-bezogenen Filtern sind deutlich höher als die Kosten adressbezogener Filterung. Für genauere Bewertungen fehlen mir die Grundlagen.

5. Wie bewerten Sie die Erfahrungen bezüglich der Wirksamkeit derartiger Sperren in anderen vergleichbaren Staaten?

Momentan wird insb. der Child Sexual Abuse Anti Distribution Filter eingesetzt, der einen DNS-bezogenen Filter verwendet. Neben der positiven Signalwirkung gegen Kinderpornographie sind positive Effekte nach meiner Kenntnis bisher nicht nachgewiesen.

Negativ zu bewerten sind die simplen Umgehungsmöglichkeiten, das Logging der DNS-Requests, die umgeleitet wurden und die fehlende Kontrolle der Sperrlisten auf eine strenge Zweckbindung (nur Blocken von Kinderpornographie, keine Ausweitung auf andere rechtswidrige Inhalte).

Recht:

Als Informatiker beschränke ich mich auf eine Stellungnahme zu den technischen Fragen.

10. Februar 2009

Prof. Dr. Hannes Federrath