Bundesministerium
des Innern

Freiheit
Einheit
Demokratie

Kabinett- und Parlamentsreferat

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

An den
Sekretär des 4. Ausschusses
des Deutschen Bundestages (Innenausschuss)
Herrn Ministerialrat Dr. Heynckes
Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-1069
FAX +49 (0)30 18 681-1019
E-MAIL KabParl@bmi.bund.de
INTERNET www.bmi.bund.de

DATUM Berlin, 27. Februar 2009

BETREFF **Sperrung von kinderpornographischen Inhalten im Internet**

BEZUG Unterrichtungsbitte der Mitglieder des Innenausschusses

ANLAGE - 1 -

Sehr geehrter Herr Dr. Heynckes,

in seiner Sitzung am 21. Januar 2009 hatte der Innenausschuss das Bundesministerium des Innern um Unterrichtung zu der Frage gebeten, ob es bei der Bekämpfung von Kinderpornographie im Internet reale technische Möglichkeiten gibt, solche inkriminierten Internetseiten dauerhaft aus dem Internet zu entfernen. Dieser Bitte entsprechend übersende ich anliegend eine Darstellung der derzeitigen technischen Möglichkeiten zur Sperrung von kinderpornographischen Inhalten im Internet.

Mit freundlichen Grüßen
Im Auftrag

Knaack

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
VERKEHRSANBINDUNG S-Bahnhof Bellevue; U-Bahnhof Turmstraße
Bushaltestelle Kleiner Tiergarten

Bundesministerium
des Innern

Bericht für den Innenausschuss des Deutschen Bundestages

Technische Möglichkeiten der Entfernung bzw. Sperrung kinderpornographischer Inhalte im Internet

Bundesministerium
des Innern

Technische Möglichkeiten der Entfernung bzw. Sperrung kinderpornographischer Inhalte im Internet

Die dauerhafte und vollständige Entfernung kinderpornographischer Inhalte aus dem Internet **ist technisch nicht möglich**. Sobald die entsprechenden Inhalte von einem Host – d.h. einem Computer im Internet, der anderen Internetnutzern Inhalte oder Dienste zur Verfügung stellt – entfernt werden, kann der Anbieter seine Inhalte über andere Hosts wieder zugänglich machen.
Die temporäre Entfernung ist dagegen technisch grundsätzlich möglich, entweder indem der Host die entsprechenden Inhalte von dem von ihm betriebenen Host entfernt oder indem die Inhalte durch technische Maßnahmen ohne den Willen des Host-Betreibers („Hacking") von dem Host gelöscht werden. Die erstgenannte Konstellation setzt die Mitwirkung des Host-Betreibers voraus. Werden kinderpornographische Inhalte auf Hosts in Deutschland festgestellt, werden die Inhalte von den jeweiligen Host-Providern in der Regel bei deren Kenntnisnahme von derartigen Inhalten, spätestens auf Aufforderung durch Dritte entfernt. Schwieriger gestaltet sich die Lage jedoch, wenn sich der Host im Ausland befindet. In diesen Fällen besteht für deutsche Strafverfolgungsbehörden keine Möglichkeit, direkt gegen die Host-Provider vorzugehen und die Entfernung der entsprechenden Inhalte zu veranlassen. Die zweite Variante, das „Hacking" entsprechender Seiten, ist rechtlich und politisch höchst problematisch.
Vor diesem Hintergrund ist die Verhinderung des Zugriffs auf entsprechende Inhalte durch technische Mittel und damit deren weitere Verbreitung der erfolgversprechenste Weg, um die Verbreitung von Kinderpornographie im Internet einzudämmen. Eine solche Sperrung des Zugriffs auf entsprechende Inhalte kann grundsätzlich auf drei verschiedenen technischen Ebenen erfolgen. Diese sind

a) der Computer des Nutzers,

b) der Computer des Anbieters (Host) und

c) das für den Abruf solcher Inhalte genutzte Verbindungsnetz (Internet).

zu a) Auf dem Computer des Nutzers würde eine Sperrung z. B. durch Filterung in der Anwendungssoftware (z. B. dem Web-Browser) oder im Betriebssystem erfolgen. Solche Mechanismen sind bereits heute (kommerziell) verfügbar, um etwa die Nutzung des Internets durch Kinder zu beschränken. Für die Sperrung auf dem Computer des Nutzers müssen regelmäßig aktuelle Listen dem Computer des Nutzers zur Verfügung gestellt werden, damit dieser den Zugriff auf die relevanten Seiten sperren kann. Dazu müssten möglichst alle Computer über standardisierte Mechanismen zur Sperrung und Verarbeitung der Sperrlisten

verfügen, wofür die Anpassung der Anwendungssoftware oder des Betriebssystems erforderlich ist.
Eine Sperrung auf dem Computer des Nutzers wird seitens des Verbandes der deutschen Internetindustrie (eco) und BITKOM favorisiert, ist aber wegen der Möglichkeit ihrer Umgehung, der Schwierigkeit einer kurzfristigen Umsetzung und wegen des zu betreibenden Aufwands als Lösung eher ungeeignet.

zu b) Die Löschung von Internet-Inhalten auf Seiten des Anbieters erscheint als technisch beste Methode zur Unterbindung des Angebotes. Da viele der entsprechenden Inhalte jedoch aus dem außereuropäischen Ausland angeboten werden und Deutschland darauf nur eingeschränkt Einfluss nehmen kann (Rechtshilfe), scheidet diese Möglichkeit zumindest als kurz- bis mittelfristige Lösung aus.

zu c) Eine Sperrung des Zugangs im Rahmen der technischen Möglichkeiten des Internets erscheint derzeit am schnellsten und effizientesten realisierbar. Allerdings bestehen auch hier Umgehungsmöglichkeiten, die Zugangsanbieter können mit zusätzlichen Kosten belastet werden und möglicherweise kann die Effizienz und Integrität der Datenübertragung im Internet eingeschränkt werden. Dabei gibt es drei geläufige Ansätze:

- **Sperrung der Internet-Adresse (IP-Adresse)**

  Die IP-Adresse im Internet hat eine ähnliche Funktion wie eine Telefonnummer. Die IP-Adresse bezeichnet zum einem einen Computer im Internet, zum anderen beschreibt sie aber auch den Weg, wie Daten von einem Quell- zu einem Zielcomputer vermittelt werden. Der Fachbegriff für die Vermittlung im Internet ist *Routing*. Die Sperrung auf Ebene der IP-Adresse würde typischerweise an den *Routern* ansetzen und diese z. B. veranlassen, den Datentransport zu einer gesperrten IP-Adresse abzulehnen.
  Eine IP-Adresse kann einzelne Computer, aber auch ganze Computernetzwerke bezeichnen, deren Computer über eine einzige IP-Adresse erreicht werden können, ähnlich wie einer Telefonanlage eine einzige Telefonnummer zugeordnet sein kann. Sperrt man im letzteren Fall ein ganzes Computernetzwerk, so werden neben den zu sperrenden Inhalten möglicherweise auch zahlreiche legale Inhalte und Dienste innerhalb dieses Netzwerks gesperrt. Bei großen Web-Hostern käme ein solches Vorgehen einer Stilllegung des Betriebs gleich, die in Regel als unverhältnismäßig anzusehen wäre.

- **Sperrung über das Domain Name System (DNS)**

  Das Domain Name System ist funktional vergleichbar mit einem Telefonbuch. Über DNS werden leicht zu merkende Adressbezeichnungen (www.bmi.bund.de), so genannte

Domainnamen, in schwer zu merkende dafür aber technisch verarbeitbare IP-Adressen (77.87.229.1) aufgelöst.
Ebenso wie die Löschung eines Teilnehmers aus einem Telefonbuch nicht zur Sperrung seines Telefonanschlusses führt, kann auf Inhalte (z. B. einer Web-Seite) auch nach einer Löschung oder Veränderung des DNS-Eintrags nach wie vor zugegriffen werden, wenn die IP-Adresse des Computers mit den inkriminierten Inhalten bekannt ist.
Der Zugang zu einem DNS-Server wird von den Internetzugangsanbietern zumeist gemeinsam mit dem Internetzugang angeboten. In den Ländern, die das Access Blocking auf Ebene des DNS durchführen, werden die Tabellen der DNS-Server der großen Zugangsanbieter modifiziert, so dass bei Aufruf einer gesperrten Seite dem Nutzer ein Hinweis gegeben wird, das der vom Nutzer angeforderte Inhalt kinderpornographisches Material enthält. Im DNS wird also zu dem Domain-Namen statt der ursprünglichen IP-Adresse die IP-Adresse einer entsprechenden Hinweisseite hinterlegt. Eine der Umgehungsmöglichkeiten der DNS-basierten Sperrung besteht daher in der Nutzung „freier DNS-Server" im Ausland, auf denen die auf deutschen DNS-Servern durch Umleitung gesperrten Seiten nicht entsprechend gesperrt sind.
Im Gegensatz zur vorangehend genannten Sperre von IP-Adressen lässt die DNS-basierte Sperre eine gezieltere Auswahl der zu sperrenden Inhalte zu. So verwenden z. B. große Web-Hoster so genannte Subdomains, um ihren Nutzern möglichst individuelle Domainnamen zu ermöglichen (z.B. im Bereich des Bundes: bmi.bund.de; bmj.bund.de; bmf.bund.de – „bmi", „bmj" und „bmf" sind Subdomains von „bund.de"). Eine Vielzahl von Subdomains verweist dabei auf eine kleine Menge von IP-Adressen eines Web-Hosters (so könnten z. B. die Internettauftritte des BMI und des BMJ unter einer einzigen IP-Adresse vorgehalten werden). Würden diese IP-Adressen gesperrt, wäre, wie vorangehend ausgeführt, kein Nutzer des Web-Hosters mehr erreichbar. Der Vorteil der Sperrung auf DNS-Ebene ist also im Gegensatz zur Sperrung der IP-Adresse, dass nur die Inhalte des Nutzers eines Web-Hosters der auch illegale Inhalte anbietet, gesperrt werden.

- **Sperrung über den Uniform Resource Identifier (URI)**

  Einzelne Ressourcen im Internet werden über einen URI gekennzeichnet. Bei diesen Ressourcen handelt es sich beispielsweise um Web-Seiten, Bilder usw. So steht etwa der URL[1] http://www.bundestag.de/layout/bilder/logo.gif für das Logo des Deutschen Bundestages auf seiner Homepage. Auch Dienste wie Email, Filetransfer, Newsfeed usw. werden über den URI benannt. Der URI ist somit eine der genauesten Möglichkeiten, um illegale Internet-Inhalte zu bezeichnen und nachfolgend zu sperren.

[1] Ein Uniform Resource Locator ist eine Unterkategorie der URI

Aufgrund des technischen Aufbaus des Internets ist eine Filterung auf Ebene von URIs sehr aufwendig und würde, falls flächendeckend eingeführt, zum Zusammenbruch des Internets führen. Daher hat man sich z. B. in GBR entschlossen, ein Hybridverfahren einzusetzen, das wie ein mehrstufiges Sieb arbeitet. Im ersten Schritt werden IP-Adressen mit potentiell zu sperrenden Inhalten mit Hilfe einer Liste identifiziert. Die an diese IP-Adressen gesendeten Daten werden in einem zweiten Schritt näher analysiert und falls sie an eine zu sperrende URI bzw. URL gerichtet sind, wird die Verbindung oder der Datentransport abgebrochen. Eine Umleitung auf eine Hinweisseite wäre ebenfalls möglich.
Die Methode ist sehr zielsicher und beschränkt den Zugang zu nicht zu sperrenden Inhalten minimal im Vergleich zu den vorangehend genannten Sperrverfahren. Allerdings ist die hybride Technik bei bestimmten verschlüsselten Internetverbindungen wirkungslos.

Fazit:
Die unter c) genannten Sperrverfahren erfordern Eingriffe in die Weiterleitungs- und Vermittlungsstrukturen des Internets. Diese Eingriffe verlangen Investitionen auf Seiten der deutschen Netzbetreiber. Ob die Eingriffe zu Sicherheitslücken oder Betriebsstörungen im deutschen Teil des Internet führen können, bedarf der weiteren Prüfung. Keines der vorgestellten Verfahren bietet hohe Umgehungssicherheit, so dass voraussichtlich nur der „normale Nutzer" am Zugang zu illegalen Inhalten gehindert wird, nicht jedoch derjenige, der den Zugang gezielt sucht.
Eine Filterung[2] auf Ebene der IP-Adresse ist dabei technisch eher einfach herzustellen, da die Analyse der IP-Adresse und die darauf aufbauende Entscheidung, an welchen Router die Daten weitergeleitet werden, bereits Bestandteil der Datenvermittlung im Internet (Routing) ist. Aufgrund der damit verbundenen Nachteile für Nichtbetroffene (Sperrung auch anderer Inhalte) begegnet dieses Vorgehen allerdings Bedenken.
Eine auf große Internetzugangsanbieter beschränkte Sperrung über das Domain Name System ist technisch ebenfalls einfach zu realisieren und mit geringen Kosten für die Internetprovider verbunden. Diese Art der Sperrung ist jedoch auch von wenig versierten Computernutzern leicht zu umgehen. Trotzdem ist diese Lösung zunächst vorzugswürdig, da ihre Realisierung sehr zeitnah erfolgen könnte und ein Großteil der potentiellen Nutzer allein durch den Hinweis, dass sie versuchen, auf illegale Inhalte zuzugreifen, abgeschreckt werden dürften.

---

[2] Filtern bedeutet hier eine IP-Adresse mit einer „schwarzen Liste" abzugleichen und bei Übereinstimmung den Datenverkehr abzubrechen. Routing bedeutet eine IP-Adresse mit einer Routingliste abzugleichen und die Daten an die in der Routingliste bezeichnete Netzwerkverbindung weiterzuleiten.

Unter dem Gesichtspunkt der Zielgenauigkeit ist die Sperrung über den *Uniform Resource Identifier* vorzugswürdig. Demgegenüber stehen jedoch bedeutende Investitionen der Provider, um weiterhin ausreichende Performance zu gewährleisten.