

Bundeskriminalamt

POSTANSCHRIFT **Bundskriminalamt** - 65173 Wiesbaden

Deutscher Kinderschutzbund
Landesverband Schleswig-Holstein
e.V. Beselerallee 44

24105 Kiel

HAUSANSCHRIFT Thaerstraße 11,65193 Wiesbaden

POSTANSCHRIFT 65173 Wiesbaden

TEL +49(0)61155-14676

FAX +49(0)611 55-45155

BEARBEITET VON Lob, Matthias

E-MAIL soas@bka.bund.de

AZ SO AS 207

DATUM 01.04.09

BETREFF **Access-Blocking kinderpornografischer Inhalte im Internet**

BEziG Ihr Schreiben vom 19.03.09

ZUSTFU- UND ÜEFERANSCHR1FT. BKA ThaerstraSe 11,65193 **WfcstodM** OberweiS'jngssmpfätioer.
Sundeskasse Trief

Sankverbindung: Deutsche Bundesbank
Finale Saarbrücken (3Bk
Saarbrücken) BLZ 590 0M
00 KIo* 5S0O10 20

Um den Zugriff auf bestimmte Internetinhalte zu sperren, gibt es mehrere technische Möglichkeiten. So sind „gröbere“ Sperrtechniken (z.B. anhand der IP-Adressen) recht einfach durchzuführen, jedoch weniger trennscharf, so dass die Gefahr besteht, auch zahlreiche legale Inhalte mitzuerfassen. „Feinere“ Sperrtechniken (auf Basis der „Uniform Resource Identifier“ - URI) besitzen eine größere Treffsicherheit, sind allerdings technisch und in der Folge auch finanziell aufwändiger. Die hybride Technologie verbindet in einem zweistufigen Ansatz den Vorteil der zuvor genannten Techniken. Im Rahmen der Besprechungen der Arbeitsgruppe Access-Biocking zum Abschluss eines Vertrages zwischen den einzelnen Internetservice Providern (ISP) und dem Bundeskriminalamt, einigten sich die Teilnehmer auf eine Sperrung über das Domain Name System (DNS). In Bezug auf die Trennschärfe liegt eine Sperrung über das Domain Name System zwischen der Sperrung auf Basis der IP und URL. Die Einträge im DNS-Server lassen sich dabei so verändern, dass Anfragen zu gesperrten Domains nicht zu dem Server mit der dazugehörigen IP-Adresse gelangen, sondern umgeleitet werden oder die Meldung erhalten, dass die Domain nicht gefunden wurde.

Die Sperrung soll durch die Einrichtung einer „STOPP-Seite“ ergänzt werden, auf die bei einem Zugriffsversuch automatisch umgeleitet wird. Neben dem generalpräventiven Aspekt bietet die Anzeige einer „STOPP-Seite“ ein hohes Maß an Transparenz. Neben dem dort angezeigten Grund (kinderpornografischer Inhalt im Sinne des §184 b StGB) für die Sperrung dient die Angabe einer E-Mail-Adresse des Bundeskriminalamtes einer Kontaktaufnahme, wenn der Nutzer der Auffassung ist, dass die Sperrung des Zugriffs zu Unrecht erfolgt.

Die Einrichtung einer „STOPP-Seite“ stellt somit ein essentielles Anliegen bei der Sperrung kinderpornografischer Webseiten dar.

2. *Wie und nach welchen Kriterien werden Sperrlisten erstellt? Wer erstellt sie⁹ Wie häufig müssen sie aktualisiert werden?*

Beim Bundeskriminalamt läuft eine Vielzahl von Informationen zu strafbaren Inhalten im Internet, insbesondere auch zu kinderpornografischen Inhalten, zusammen. Zum Teil gewinnt das Bundeskriminalamt seine Erkenntnisse aus eigenen Nachforschungen im Netz, teilweise erhält es aber auch Hinweise von anderen Polizeidienststellen im In- und Ausland sowie aus der Bevölkerung. Die so gewonnenen Erkenntnisse zu kinderpornografischen Inhalten im Internet wird das Bundeskriminalamt den derzeitigen Planungen nach künftig in einer „Sperrliste“ zusammenführen und den ISP als Grundlage für die von ihnen durchzuführenden Sperrmaßnahmen zur Verfügung stellen. Die Sperrung soll sich allein auf kinderpornografische Inhalte gemäß § 184b StGB beschränken. Da der Zugriff auf (kommerzielle) kinderpornografische Webseiten in der Regel nur wenige Tage möglich ist, bevor die Seiten unter einer neuen Adresse wieder zur Verfügung steht, wird eine regelmäßige Aktualisierung der Sperrliste notwendig sein.

3. Für welche Nutzergruppe stellt aus Sicht des BKA Access-Blocking von kinderporno-grafischen Inhalten eine Zugangserschwerung dar?

Die Konsumenten kinderpornografischen Materials, die sich dieses über (kommerzielle) kinderpornografische Webseiten verschaffen, sind nach hiesiger Einschätzung Personen, die diese einfache Möglichkeit nutzen, um ihr (ggf. zunächst nur latent) vorhandenes Bedürfnis zu befriedigen. Auf diese Nutzergruppe würde sich die Zugangserschwerung primär auswirken. Darüber hinaus würde der Zugriff von Internet-Nutzern, die über Spam aus Versehen auf einen entsprechenden Link geleitet wurden, abgewehrt. Die Anzahl dieser Personen dürfte eher gering sein, trotzdem stellen die Zugangserschwerungen auch für diese Personen einen erhöhten Schutz dar.

4. Gibt es Möglichkeiten, die Zugangssperren zu umgehen?

Durch den dezentralen Aufbau des Internets, der die Funktionsfähigkeit auch bei Ausfällen von Netzteilen gewährleistet, wird eine Umgehung einer Sperrung voraussichtlich immer möglich sein, so dass Access-Blocking einen Zugang nie ganz verhindern kann.

5. Welche rechtlichen Änderungen sind nötig, um Access-Blocking umzusetzen?

Bei der geplanten vertraglichen Regelung mit den Internetservice Providern sind rechtliche Änderungen nicht notwendig. Sollte in der Folgezeit zusätzlich eine gesetzliche Regelung eingeführt werden, so wäre diese aus Sicht des Bundeskriminalamtes am sinnvollsten im Telemediengesetz zu verankern.

6. Welchen finanziellen und personellen Aufwand bedeutet die Umsetzung der Sperrung?

Die Einführung von Access-Blocking führt beim Bundeskriminalamt zweifelsfrei zu einem Mehraufwand und verursacht Kosten. Wie sich diese gestalten werden, kann derzeit nicht genau beziffert werden. Der Ressourcenaufwand darf jedoch nicht über das „Ob“ von Access-Blocking entscheiden. Es geht hierbei vielmehr um den Schutz des überragend wichtigen Rechtsgutes der missbrauchten Kinder.

7. In welcher Weise stärkt diese Maßnahme den Kinderschutz? / Wie werden konkret die Kinder durch diese Maßnahme geschützt?

Gerade die Verbreitung von Kinderpornografie über kommerzielle kinderpornografische Webseiten gibt seit mehreren Jahren zunehmend Anlass zur Sorge. Kunden dieser Seiten wird der Zugriff auf tausende Darstellungen des teils schweren sexuellen Missbrauchs von Kindern gewährt und es gibt Anhaltspunkte dafür, dass Kinder zum Teil gezielt für die Erstellung des vermarkteten Bild- und Videomaterials missbraucht werden.

Insbesondere hier gilt es durch Maßnahmen wie das „Access-Blocking“ den Zugang zu erschweren, um eine Nachfragereduzierung zu erreichen und die Gewinnmargen zu minimieren.

8. Was zeigen die Erfahrungen anderer Länder, wie z.B. Schweden mit diesem Verfahren der Sperrung?

In Norwegen, wo auf Vertragsbasis zwischen polizeilicher Zentralstelle und Internetservice Providern seit 2004 Sperrungen über DNS-Server erfolgen, werden arbeitstäglich bereits 15.000 - 18.000 Zugriffsversuche auf kinderpornografische Webseiten abgewehrt.

In Dänemark erfolgt Access-Blocking kinderpornografischer Webseiten seit 2005 ebenfalls über DNS-Server.

In Großbritannien, wo eine hybride Sperrtechnik eingesetzt wird, sind nach hier vorliegenden Informationen im Jahr 2006 täglich 35.000 Zugriffe auf kinderpornografische Webseiten abgewehrt worden.

Die Erfahrungen der Staaten bezüglich der Wirksamkeit derartiger Sperren sind positiv. Nach Auskunft der norwegischen und dänischen kriminalpolizeilichen Zentraldienststellen hat es dort bislang nur in ganz vereinzelt Fällen Beschwerden gegen die vorgenommenen Sperrungen gegeben. Dies spricht für die Wirksamkeit und Akzeptanz der Sperrmaßnahmen.

9. Was kann mit Access-Blocking erreicht werden?

Das Access-Blocking soll ausschließlich zu präventiven Zwecken erfolgen.

Nach Einschätzung anerkannter Wissenschaftler kann fortgesetztes Betrachten von Kinderpornografie zu fortschreitendem Abbau von Hemmschwellen führen, an dessen Ende ein aktiver eigener Missbrauch stehen kann. Durch Access-Blocking soll der Konsum erschwert werden.

Durch die Sperrung kommerzieller Webseiten soll ferner das Angebot an Kinderpornografie nachhaltig gestört werden. Dies erschwert die Gewinnung neuer Kunden und macht darüber hinaus in der Folge durch rückläufige Kundenzahlen das Geschäft mit der Kinderpornografie weniger lukrativ.

Daneben stellt das fortgesetzte Betrachten der im Internet verfügbaren kinderpornografischen Abbildungen jedes Mal wieder einen gravierenden Eingriff in die Rechte der betroffenen Kinder dar, den es so weit möglich zu minimieren gilt.

Auch wird auf die Antwort zu Frage 7 verwiesen.

10. Welche Verantwortung übernehmen die Provider in diesem Verfahren?

Nach der geplanten vertraglichen Regelung liegt die Verantwortung der Internetservice Provider darin, die Sperrung der seitens des Bundeskriminalamtes per Liste übermittelten Webseiten innerhalb einer bestimmten Frist technisch umzusetzen. Die ISP tragen darüber hinaus die Verantwortung eines vertraulichen Umgangs mit der Liste, um ein Bekanntwerden dieser zu verhindern.

Die inhaltliche Verantwortung der Liste wird ausschließlich beim Bundeskriminalamt liegen.

//. Wie kann sichergestellt werden, dass im Rahmen der Zielrichtung Einschränkung der Verbreitung von Kinderpornografie nicht auch andere Bereiche im Internet überwacht und kontrolliert werden?

Die Sperrung soll sich allein auf Inhalte der Kinderpornografie gemäß § 184b StGB beschränken. Dabei soll die Bewertung, ob eine Webseite kinderpornografische Inhalte umfasst und damit die Festlegung der zu sperrenden Seiten durch das Bundeskriminalamt erfolgen, dem wie zu Frage 10 ausgeführt, die inhaltliche Verantwortung für die Liste obliegt. Über die Sperrung von Kinderpornografie hinausgehende Initiativen des Bundeskriminalamtes gibt es nicht.

12. Welche anderen Möglichkeiten sieht das BKA, um Nutzer —

Erwachsene und Kinder

und Jugendliche -vor der Nutzung entsprechender Seiten zu warnen?

Wie zur Frage 3 dargestellt ist die Wahrscheinlichkeit, zufällig auf kinderpornografische Webseiten im Internet zu stoßen, eher gering. Dennoch wird auch weiterhin in diesem Bereich die „klassische (polizeiliche) Präventionsarbeit“ erforderlich sein, um sowohl an die individuelle als auch die gesamtgesellschaftliche Verantwortung zu appellieren und sowohl die Folgen des Missbrauchs von Kindern als auch die strafrechtlichen Konsequenzen für die Konsumenten, Verbreiter und Hersteller aufzuzeigen.

13. Wie kann verhindert werden, dass geblockte Seiten von Kinderpornointeressenten als Wegweiser für einschlägige Seiten gebraucht werden können? Ist eine solche Gefährdung gegeben?

Um ein Bekanntwerden der Listen nach Möglichkeit zu verhindern, soll in den Verträgen zwischen Bundeskriminalamt und den Providern u. a. die Nutzung von Verschlüsselungstechniken zur Übertragung und eine Begrenzung des damit befassten Personenkreises festgeschrieben werden.

Gemäß Informationen der skandinavischen Polizei ist davon auszugehen, dass eine dort in die Öffentlichkeit gelangte Liste rückwärts generiert wurde. Zum Zeitpunkt, der Veröffentlichung war diese Liste bereits veraltet. Da die entsprechenden Inhalte in der Regel „flüchtig“ sind, also nur kurze Zeit unter einer URI vorgehalten werden, sind die Gefahren, die von der Veröffentlichung einer rückwärts generierten Liste ausgehen, somit begrenzt.

14, Sind andere Verfahren denkbar, um die Identität (die Bilder) der kindlichen Opfer im Internet auszusondern?

Nach heutigem Stand der Technik ist eine dauerhafte Entfernung einmal im Internet verbreiteter kinderpornografischer Inhalte nicht möglich. Zu dieser bedauerlichen Tatsache tragen nicht zuletzt auch die o.a. kommerziellen Webseiten bei, die tausende Konsumenten weltweit mit solchen Abbildungen bedienen. Gerade deshalb gilt es, die Verbreitung kinderpornografie -sehen Materials mit allen rechtstaatlich verfügbaren Mitteln zu bekämpfen. Dazu gehört sowohl die strafrechtliche Verfolgung der Konsumenten und Hersteller von Kinderpornografie als auch die dauerhafte Störung der Vertriebswege.

Mit freundlichen
Grüßen im Auftrag

||



Jürgen Maurer

Direktor beim Bundeskriminalamt