Universität Regensburg

Prof. Dr.-Ing. Hannes Federrath
Lehrstuhl für Wirtschaftsinformatik IV –
Management der Informationssicherheit

Federrath · Uni Regensburg · Wirtschaftsinformatik · 93040 Regensburg

An den
Landtag Nordrhein-Westfalen
Rechtsausschuss

25.02.2009

Stellungnahme zur öffentlichen Anhörung des Rechtsausschusses des Landtages Nordrhein-Westfalen am 11.3.2009 „Kinderpornographie im Internet - entschlossen und wirksam bekämpfen!" (Antrag der Fraktion der SPD, Drucksache 14/7830) in Verbindung mit „Für eine konsequente Ahndung von Erwerb und Verbreitung kinderpornografischer Dateien sowie von sexuellen Belästigungen Minderjähriger im Internet" (Entschließungsantrag der Fraktion der CDU und FDP, Drucksache 14/7907)

Den Anträgen ist insoweit uneingeschränkt zuzustimmen, dass sie auf jegliche technische Empfehlung zur Umsetzung der Sperren verzichten. Allerdings wird Bezug genommen auf die momentanen Empfehlungen und Vorschläge des BKA, das eine sog. DNS-Sperre empfehlt.

Zum technischen Hintergrund verweise ich auf meine Stellungnahme bei der Anhörung des Unterausschusses neue Medien des Deutschen Bundestages am 12. Februar 2009 (siehe Anlage 1).

Zweifellos muss der steigenden Verbreitung von kinderpornographischen Inhalten im Internet entschlossen und wirksam entgegen getreten werden. DNS-Sperren sind dies jedoch nicht. Besser geeignete Maßnahmen sind u.a. das Sperren von IP-Adressen oder das gezielte Sperren bekannter Inhalte mittels aufwändiger Hashwert-Methoden.

DNS-Sperren lassen sich faktisch problemlos umgehen. Der notwendige technische Sachverstand zum Umgehen ist gering.

Zu Demonstrationszwecken haben wir eine „Anleitung zur Einrichtung einer DNS-Sperre" erstellt (siehe Anlage 2), die praktisch demonstriert und für jeden Internet-Nutzer erkennbar macht, wie DNS-Sperren funktionieren und was deren Wirkung ist. Die durchzuführenden Schritte zur Einrichtung dieser Sperre (hier nur zu Demonstrationszwecken) unterscheiden sich nicht von denen zur Umgehung einer durch Internet Service Provider eingerichteten Sperre.

Prof. Dr. Hannes Federrath

Anlagen

ANLAGE 1

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

Anleitung zur Einrichtung einer DNS-Sperre

Hannes Federrath, 20. Februar 2009

Anlässlich einer Anhörung des Unterausschusses Neue Medien des Deutschen Bundestags am 12. Februar 2009 nahm ich Stellung zur Wirksamkeit von DNS-Sperren. Ziel dieser Sperren soll es nach dem Willen des Familienministeriums sein, den Zugang zu kinderpornographischen Inhalten signifikant zu erschweren.

In meiner Stellungnahme komme ich zu dem Ergebnis, dass DNS-Sperren kein wirksames Mittel sind, um den Zugang zu Inhalten zu erschweren. Eine DNS-Sperre verhindert die Auflösung eines Rechnernamens in seine IP-Adresse. Mit den folgenden Umgehungen gelingt es, die DNS-Sperre auszuschalten:

1. Der Anbieter eines Inhalts publiziert in Foren, Webseiten, Mails und anderswo keine Links mit DNS-Namen. So kann ganz problemlos der Inhalt unter der IP-Adresse bekannt gemacht werden. Während die URL http://www-sec.uni-regensburg.de/dns-sperre/canyouseeit.php möglicherweise geblockt wird, weil der Rechnername www-sec.uni-regensburg.de vom DNS-Server nicht in die IP-Adresse aufgelöst wird, so ist der Zugang über die URL http://132.199.128.33/dns-sperre/canyouseeit.php dennoch möglich, weil hier überhaupt keine DNS-Anfrage mehr gestellt wird.
2. Der Abrufer eines Inhalts kann anstelle des vom Internet Service Provider vorgegebenen DNS-Servers einen anderen verwenden. Im Internet existieren viele Tausend DNS-Server. An die Listen freier kommt man leicht. Es existiert sogar das Projekt OpenDNS, das sich den freien Informationszugang auf die Fahnen geschrieben hat, auf dem Anleitungen zum Umkonfigurieren des eigenen Rechners zu finden sind, aber auch Software zur Verhinderung von Internetzensur.

Im Folgenden soll gezeigt werden, wie leicht der eigene Rechner so umkonfiguriert werden kann, dass eine DNS-Sperre aktiv ist. Exakt die gleichen Schritte sind zu unternehmen, um eine existierende Sperre zu deaktivieren.

Kofiguration der DNS-Sperre

Die Adresse des DNS-Servers lautet: 132.199.128.190

Unter https://www.opendns.com/start findet man für jedes wichtige Betriebssystem die Anweisungen zum Umkonfigurieren des eigenen Rechners oder Routers (nur Step 1).

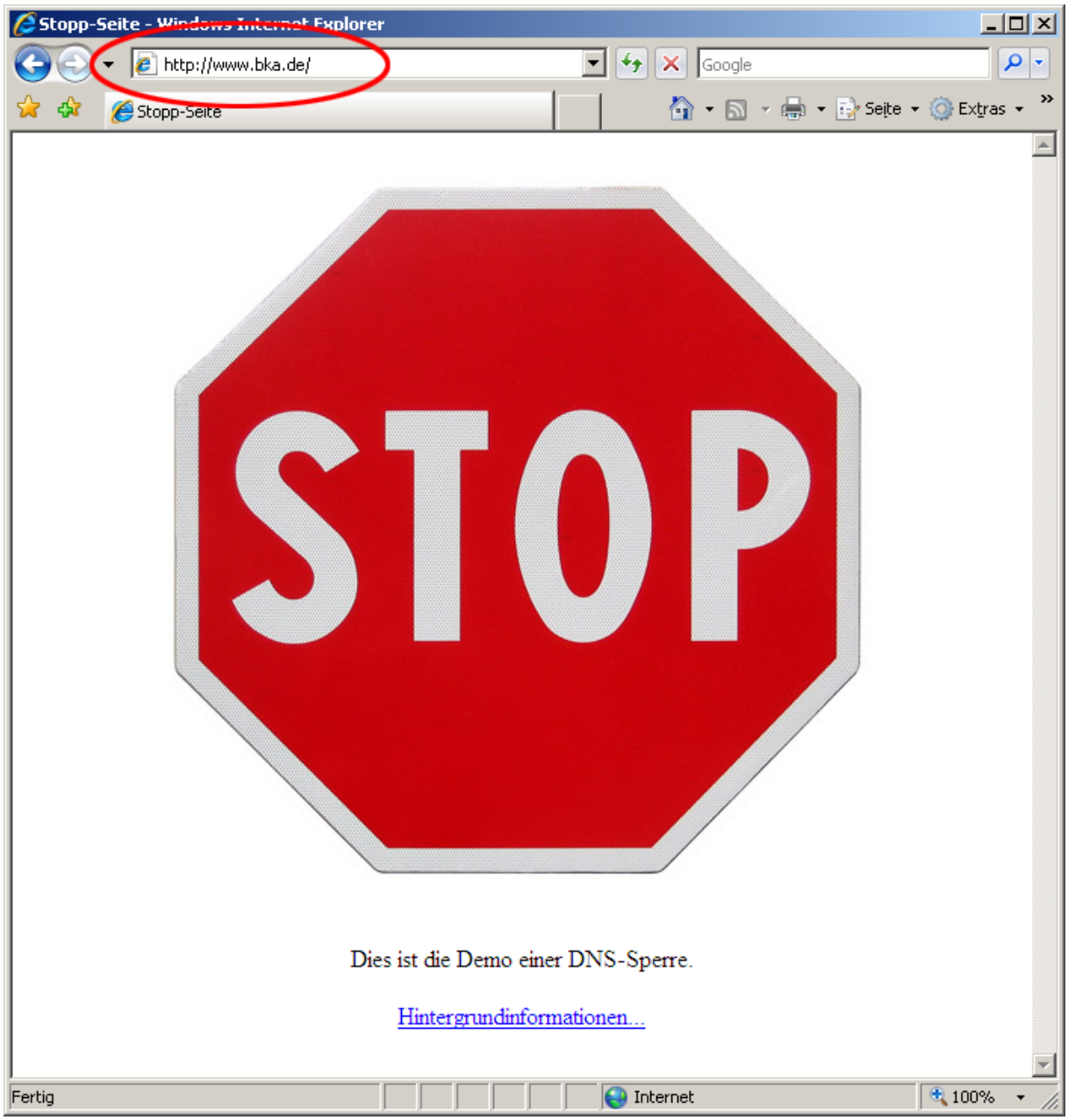
Bitte beachten Sie: Der Server 132.199.128.190 ist nicht Teil des OpenDNS-Projektes. Wir verweisen hier nur auf die Anleitung zum Umkonfigurieren. Weiterhin ist für diese Demo zu beachten, dass alle vorhandenen DNS-Server in den Internet-Einstellungen zunächst entfernt werden müssen, da sonst möglicherweise der voreingestellte DNS-Server die richtige Antwort gibt und die Sperre nicht wirksam wird.

Anmerkungen

Die hier verwendete Sperrliste enthält nur den Eintrag www.bka.de. Wird also http://www.bka.de bei aktivierter Sperre aufgerufen, landet der Besucher auf einer Stopp-Seite, die wir eingerichtet haben. Der Aufruf von http://62.156.153.38 führt dennoch zum richtigen Ziel.

Hinter einer DNS-Sperre verbirgt sich ein sog. DNS-Spoofing, d.h. der Besucher erhält eine falsche Antwort auf die DNS-Anfrage und landet somit auf dem Server mit der Stopp-Seite.

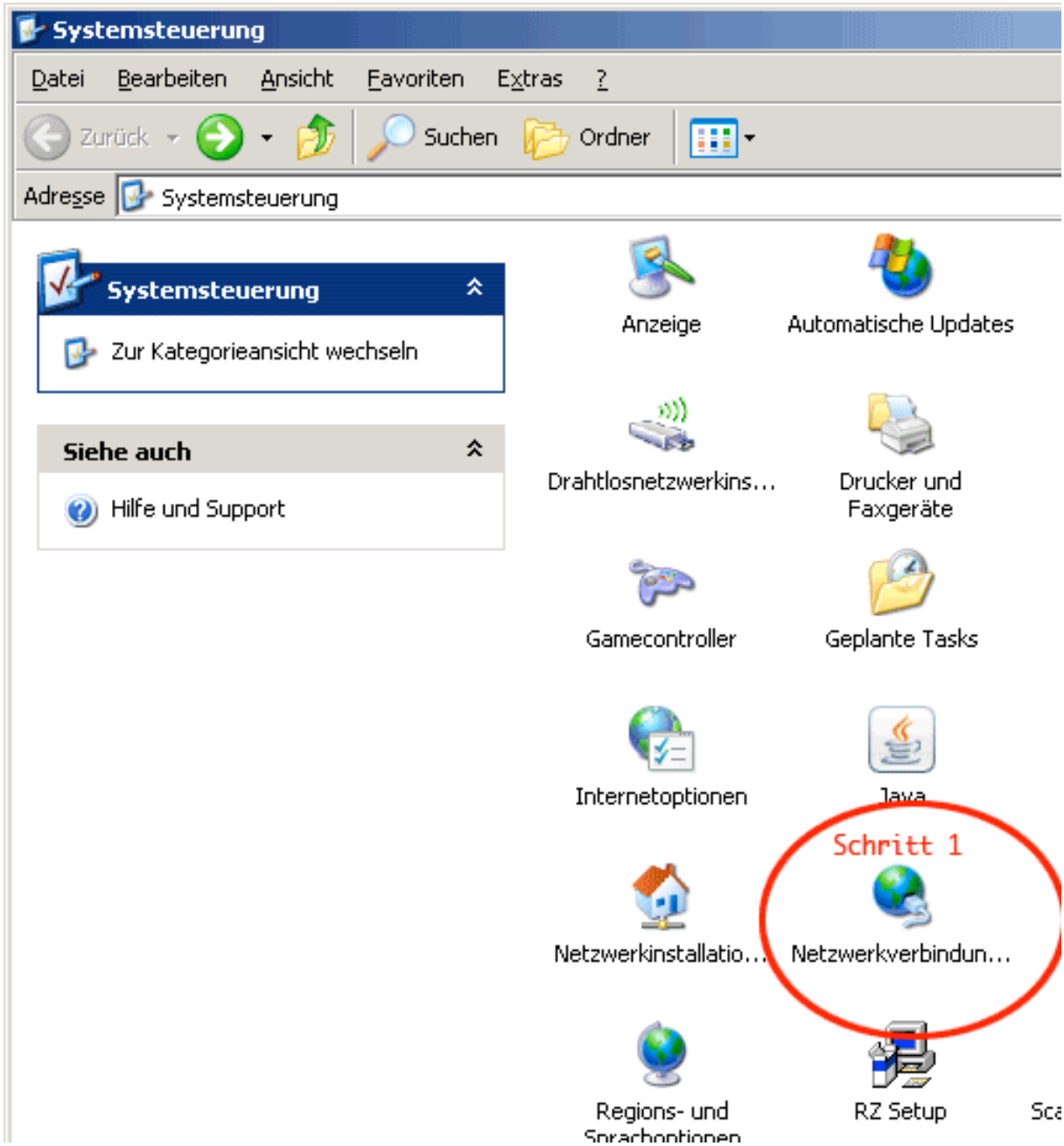
Das Umgehen durch direkte Eingabe der IP-Adresse funktioniert nicht immer. Bei virtuellen Hosts (mehrere Domains auf einem Server) kann der Rechner nicht mehr korrekt entscheiden, welche Seite tatsächlich angefragt werden sollte. Der Anbieter eines Inhalts kann jedoch sehr wahrscheinlich frei entscheiden, dass er auf virtuelle Hosts verzichtet.


Stopp-Seite - Windows Internet Explorer
http://www.bka.de/
Google
Stopp-Seite
Seite
Extras
STOP
Dies ist die Demo einer DNS-Sperre.
Hintergrundinformationen...
Fertig
Internet
100%

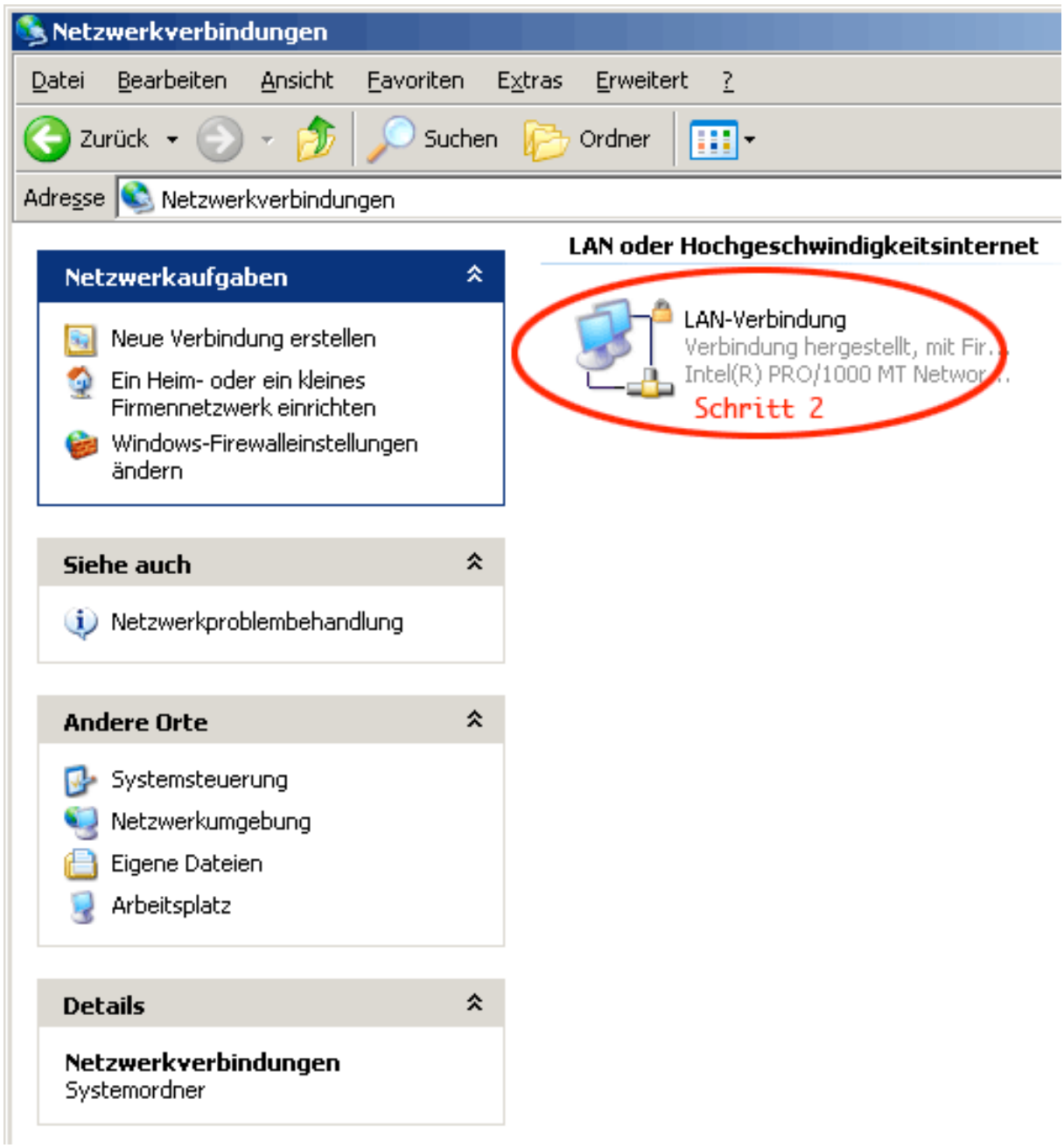

Bundeskriminalamt – Windows Internet Explorer
http://62.156.153.38/
Google
Bundeskriminalamt
Seite
Extras
Fragen&Antworten
Hinweise
Sitemap
Kontakt
Impressum
Englis
Bundeskriminalamt
www.bundeskriminalamt.de
Neu in BKAonline
Presse
Profil
Fahndungen
Berichte und Statistiken
Kriminalwissenschaften
Linksammlung
Ausbildung und Stellen
Fragen & Antworten
Bundesministerium des Innern online
bund.de
Verwaltung Online
Link zum Europa-Server
Berichte und Statistiken
Bundeskriminalamt veröffentlicht das Bundeslagebild Kc
2007
Im Jahr 2007 wurden vom BKA und den Landespolizeidienststell
Korruptionsstraftaten und damit 38 % mehr als im Vorjahr (6.8
registriert. Der Anstieg der Fallzahlen ist auf mehrere Großverfa
einer Vielzahl festgestellter Einzelstraftaten zurückzuführen.
mehr...
Personenfahndung
Die Öffentlichkeit wird um Mithilfe gebeter
Die Bundesanwaltschaft und das Bundeskrimina
seit 25.09.2008 öffentlich nach den beiden
Terrorverdächtigen Eric Breininger und Houssair
Beide Personen werden dringend verdächtigt, M
einer terroristischen Vereinigung zu sein und we
Haftbefehl gesucht.
mehr...
Personenfahndung
Öffentlichkeitsfahndung nach dem Vermissten Mathias M
Der PKW des Herrn Müller, Peugeot 306, dunkelblau, MZ-MM 12
07.10.2008 in Bad Kreuznach an der Sternwarte am Kuhberg au
Umfangreiche Suchmaßnahmen in der Gemarkung Kuhberg sow
Umfeldermittlungen blieben ergebnislos.
mehr...
Fertig
Internet
100%

Manuelle Konfiguration eines DNS-Servers unter Windows XP

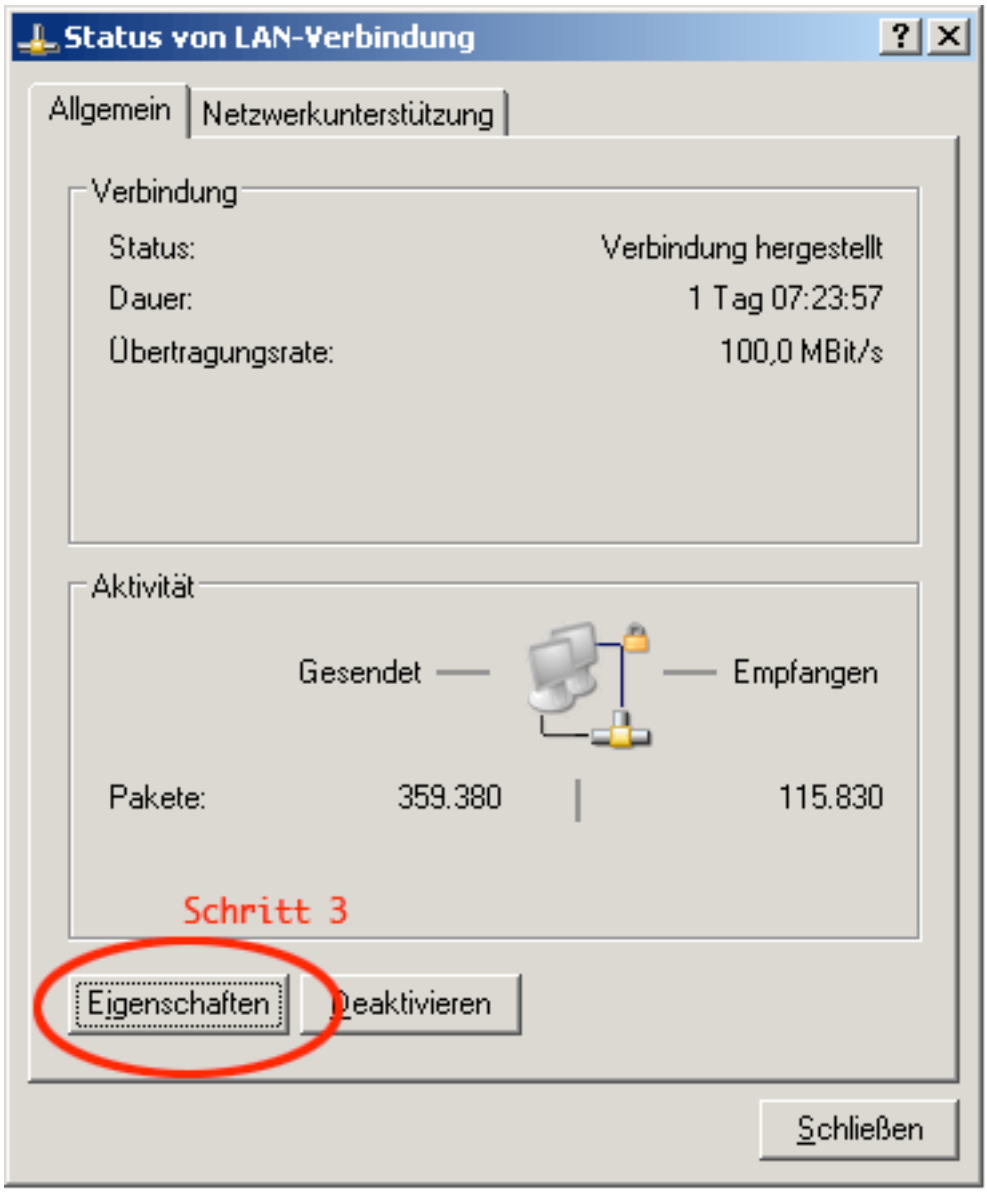
Systemsteuerung:Netzwerkverbindungen



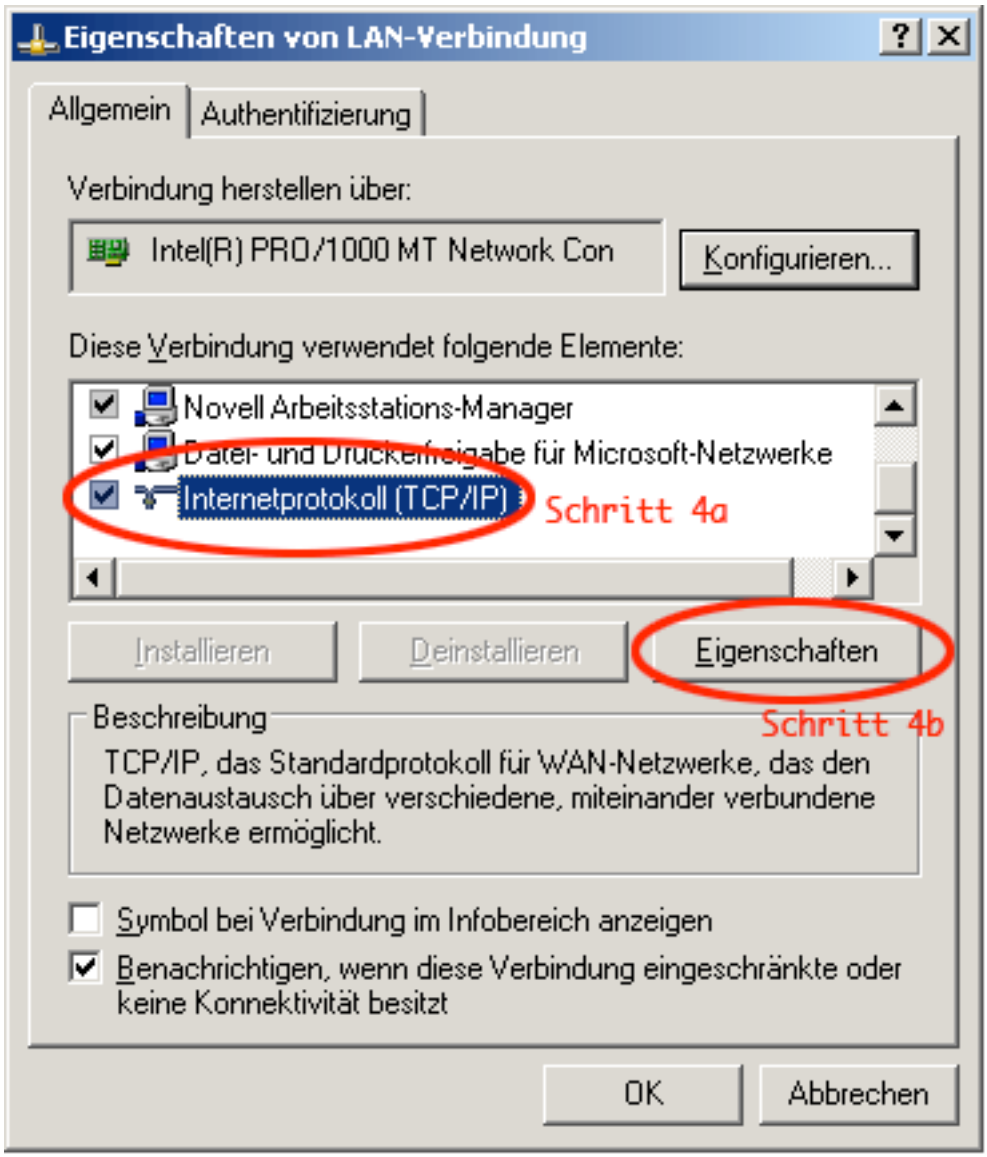
Netzwerkverbindungen:LAN-Verbindung



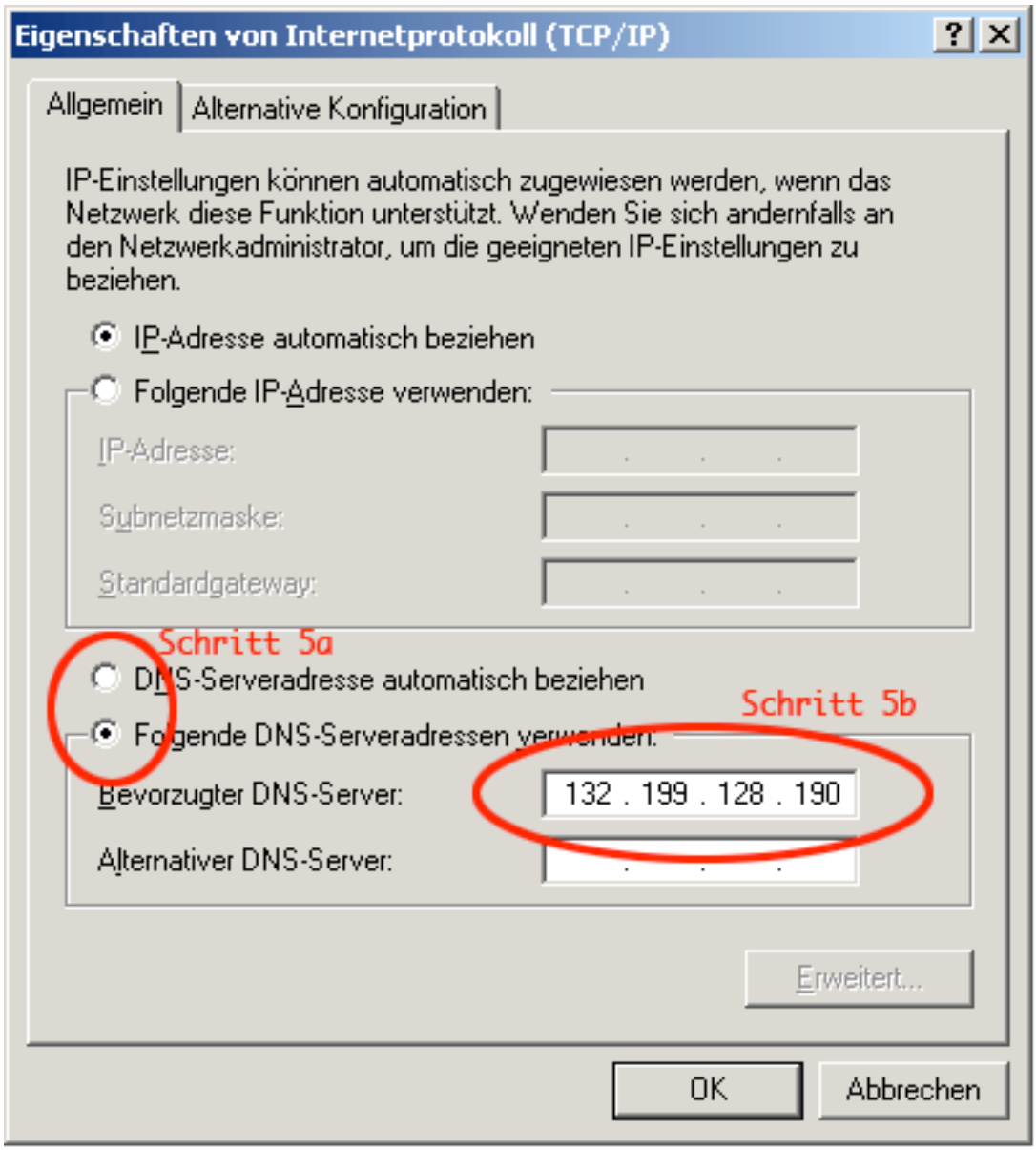
LAN-Verbindung:Eigenschaften



LAN-Verbindung:Internetprotokoll (TCP/IP):Eigenschaften



Eigenschaften von Internetprotokoll (TCP/IP):Bevorzugter DNS-Server



* * *