

# Zensur im Internet umgehen

27. Januar 2012

## Inhaltsverzeichnis

<b>1</b>	<b>Einführung der Zensur in Deutschland</b>	<b>2</b>
<b>2</b>	<b>Strafverfolgung von Kinderpornografie</b>	<b>6</b>
<b>3</b>	<b>Die Medien-Kampagne der Zensursula</b>	<b>7</b>
<b>4</b>	<b>Löschen statt Sperren ist funktioniert</b>	<b>9</b>
<b>5</b>	<b>Simple Tricks</b>	<b>10</b>
<b>6</b>	<b>Unzensierte DNS-Server nutzen</b>	<b>12</b>
6.1	WINDOWS konfigurieren . . . . .	14
6.2	Linux konfigurieren . . . . .	15
6.3	DNS-Server testen . . . . .	17

# 1 Einführung der Zensur in Deutschland

Die Zensur (Neusprech: Access-Blocking) sollte in Deutschland unter dem Deckmantel des Kampfes gegen Kinderpornografie im Internet eingeführt werden. Inzwischen hat die Zivilgesellschaft diesen Versuch gestoppt. Trotzdem wird dieser Abschnitt Bestandteil des Privacy-Handbuchs bleiben, als Beispiel für eine Kampagne und erfolgreichen Widerstand der Bürger.

Besonders verknüpft mit dem Versuch der Einführung einer Internetzensur sind Frau von der Leyen als Familienministerin, Herr Schäuble als Innenminister und Herr v. Guttenberg. Frau von der Leyen wurde dafür mit dem Big Brother geehrt. Sie wurde nicht müde zu behaupten, es gäbe einen Millionen Euro schweren Massenmarkt, der durch Sperren von Websites ausgetrocknet werden kann. Ihre Aussagen wurden überprüft und für falsch befunden.

Die Ermittler vom LKA München sind der Meinung, dass bei der Verbreitung von Kinderpornographie Geld kaum eine Rolle spielt. Es gibt selten organisierte Strukturen:

*Die überwältigende Mehrzahl der Feststellungen, die wir machen, sind kostenlose Tauschringe, oder Ringe, bei denen man gegen ein relativ geringes Entgelt Mitglied wird, wo also nicht das kommerzielle Gewinnstreben im Vordergrund steht. Von einer Kinderpornindustrie zu sprechen, wäre insofern für die Masse der Feststellungen nicht richtig. (Quelle: Süddeutsche Zeitung)*

Ermittler des LKA Niedersachsen bestätigten gegenüber Journalisten der Zeitschrift *ct* die Ansicht, dass es keinen Massenmarkt von Websites im Internet gibt. Die sogenannte "harte Ware" wird nach ihrer Einschätzung überwiegend per Post versendet. Das Internet (vor allem E-Mail) wird nur genutzt, um Kontakte anzubahnen.

Auch die *European Financial Coalition* kommt zu dem Schluss, dass es keinen Massenmarkt für Kinderpornografie gibt. In den Jahren 2009/2010 ist die Zahl der Angebote im Netz außerdem deutlich gesunken.

Kann es sein, dass diese Erkenntnisse in der Regierung nicht bekannt sind? In der Antwort auf eine parlamentarische Anfrage beweist die Regierung jedenfalls ein hohes Maß an Unkenntnis zu dem Thema:

Frage: In welchen Ländern steht Kinderpornographie bislang nicht unter Strafe?

Antwort: *Dazu liegen der Bundesregierung keine gesicherten Kenntnisse im Sinne rechtsvergleichender Studien vor.*

Frage: Über welche wissenschaftlichen Erkenntnisse verfügt die Bundesregierung im Zusammenhang mit der Verbreitung von Kinderpornographie.

Antwort: *Die Bundesregierung verfügt über keine eigenen wissenschaftlichen Erkenntnisse...*

Frage: Auf welche Datengrundlage stützt sich die Bundesregierung bei der Einschätzung des kommerziellen Marktes für Kinderpornographie in Deutschland?

Antwort: *Die Bundesregierung verfügt über keine detaillierte Einschätzung des kommerziellen Marktes für Kinderpornographie...*

Und basierend auf diesem Nicht-Wissen wird...

### **Die erste Stufe**

Am 17.04.09 unterzeichneten die fünf Provider Deutsche Telekom, Vodafone/Arcor, Hansenet/Alice, Telefonica/O2 und Kabel Deutschland freiwillig einen geheimen Vertrag mit dem BKA. Dieser Vertrag verpflichtet die Provider, eine Liste von Websites (bzw. Domains) umgehend zu sperren, die das BKA ohne rechtstaatliche Kontrolle zusammenstellt. Statt der gesperrten Website soll ein Stopp-Schild angezeigt werden. Soweit bekannt geworden ist, soll die Sperrung durch eine Kompromittierung des DNS-Systems umgesetzt werden.

### **Die zweite Stufe**

Am 18.06.09 hat der Deutsche Bundestag ein *Gesetz zur Bekämpfung der Kinderpornografie in Kommunikationsnetzen* verabschiedet. Das Gesetz ist technikoffen formuliert. Neben den (ungeeigneten) DNS-Sperren sollen auch tiefere Eingriffe in die Kommunikation zulässig und angemessen sein. Diskutiert werden IP-Adress-Sperren, kombiniert mit einer genauen Analyse des Datenverkehrs.

Das Gesetz zwingt Provider mit mehr als 10.000 Kunden dazu, die im Geheimen vom BKA erstellten Sperrlisten umzusetzen und bei Aufruf einer entsprechenden Website eine Stopp-Seite anzeigen. Die Sperrliste soll durch ein zahlloses Experten-Gremium stichprobenartig mindestens vierteljährlich überprüft werden. Diese Experten soll der Bundesdatenschutzbeauftragte berufen.

Eine Begrenzung der Sperrmaßnahmen auf kinderpornografische Angebote außerhalb der Möglichkeit der Strafverfolgung ist nicht vorgesehen. Es wurde bereits im Vorfeld die Ausweitung der Internetsperren von verschiedenen Politikern gefordert. Die Aussage von Herrn Bosbach (CDU) ist eigentlich an Eindeutigkeit nicht zu überbieten:

*Ich halte es für richtig, sich **erstmal** nur mit dem Thema Kinderpornografie zu befassen, damit die öffentliche Debatte nicht in eine Schiefelage gerät.*

Eine konsequente Umsetzung des Subsidiaritätsprinzips *Löschen vor Sperren* ist im Gesetz ebenfalls nicht vorgesehen. Es soll der Einschätzung des BKA überlassen bleiben, ob zu erwarten ist, dass der Provider ein indexiertes Angebot in angemessener Zeit vom Netz nimmt oder eine Internet-Sperre eingerichtet

wird. Es besteht keine Verpflichtung für das BKA, die Hosts der beanstandeten Websites zu kontaktieren und um Löschung der Angebote zu bitten.

### **Ein Schritt zurück**

Im Oktober 2009 hat die Regierungskoalition von CDU und FDP beschlossen, das Gesetz erst einmal nicht umzusetzen. Das BKA soll für ein Jahr keine Sperrlisten an die Provider liefern, sondern die Webseiten nach Möglichkeit löschen lassen. Nach Ablauf der Evaluierung soll das Ergebnis geprüft und über die Einführung von Sperren nochmals beraten werden.

Mit einem "Anwendungserlass" für das BKA hat die Bundesregierung ein vom Deutschen Bundestag beschlossenes Gesetz nicht umgesetzt sondern erst einmal aufgeschoben. Die Ansammlung von Adligen und Mitgliedern der Hochfinanz in unserer Regierung glaubt also, über dem Parlament zu stehen. Formal sicher eine seltsame Auffassung von Demokratie.

Im April 2011 wurde das Zugangerschwernisgesetz endültig beerdigt. Auch die Befürworter der Zensur mussten einsehen, dass ein Löschen von Bildmaterial über dokumentiertem Missbrauch durch internationale Zusammenarbeit möglich ist.

### **Umweg über die EU**

Nachdem die Zensurmaßnahmen in Deutschland nicht durchsetzbar waren, begann eine Kampagne der EU-Kommission. Alle Mitgliedsländer sollten zum Aufbau einer Sperrinfrastruktur gegen Kinderpornografie verpflichtet werden. Besonders hervorgerufen als Befürworterin einer solchen Regelung hat sich Cecilia Malmström, die EU-Kommissarin für innere Angelegenheiten.



Abbildung 1: Quelle: <http://i227.photobucket.com/albums/dd41/Scoti17/Malmstrm.jpg>

Das Vorgehen erinnert stark an die Vorratsdatenspeicherung. Der deutsche Bundestag lehnte 2001 die VDS als nicht verfassungskonform ab und kurze Zeit

später kommt eine EU-Richtlinie, die alle Mitgliedsländer zur Umsetzung der VDS verpflichten sollte. Das gleiche Spiel beim Zugangserschwerenissetzt?

### **ACTA, Urheberrecht und Glücksspiel**

Parallel zu dieser Entscheidung werden auf internationaler Ebene Abkommen vorbereitet, welche die Einführung einer Zensurinfrastruktur für Deutschland verbindlich vorschreiben sollen. In Dokumente zu den ACTA-Geheimverhandlungen wird eine Zensurinfrastruktur zur Verhinderung von Urheberrechtsverletzungen gefordert, die internationale Konferenz zum Schutz der Kinder fordert eine Zensurinfrastruktur und auch die Absicherung des staatlichen Glücksspiel Monopols soll als Vorwand für Sperren im Netz dienen.

Wie bei der Einführung der Vorratsdatenspeicherung verfolgen die Verfechter des Überwachungsstaates ihre Ziele hartnäckig und auf mehreren Wegen.

### **Die Zensur erfolgt auf vielen Ebenen**

Die Einführung der Zensur umfasst nicht nur effektive technische Sperrmaßnahmen. Sie wird auch durch juristische Schritte begleitet. Einige Beispiele:

- Das Forum *Politik global* sollte auf Betreiben des LKA Berlin im Mai 2009 wegen Volksverhetzung geschlossen werden. Das AG Tiergarten in Berlin hat der Klage stattgegeben. Das Urteil des AG Tiergarten ist uns nicht im Wortlaut bekannt. Auf der Website haben wir aber keine Nazi-Propaganda gefunden sondern Israel- und NATO-kritische Themen sowie Hinweise auf Missstände in Deutschland und International.

Die Domain wurde gelöscht. Da helfen auch keine unzensurierten DNS-Server. Die Webseite war für einige Zeit weiterhin noch unter der IP-Adresse erreichbar, da der Server nicht in Deutschland stand. Eine neue Domain wurde registriert, ist derzeit aber auch nicht mehr erreichbar.

- Am 21. Mai 2009 veröffentlichte Spiegel-Online einen Artikel über Bestechung von Politikern durch den Telekom Konzern. Dr. Klemens Joos sowie die EUTOP International GmbH wurden in dem Artikel genannt und schickten ihre Anwälte los, um den Artikel zu entfernen. Sie sahen ihre Rechte in erheblicher Weise beeinträchtigt. (Der Artikel stand bei Wikileaks weiterhin zum Download zur Verfügung.)
- Wikipedia ist immer wieder das Ziel von Zensurbemühungen. Unliebsame Artikel werden unterdrückt oder modifiziert. *Man bemühe sich um Neutralität*, sagte Gründer J. Wales bei der letzten Wikipedia-Konferenz. Aber das ist scheinbar nicht leicht umsetzbar. In der israelischen Wikipeadia fehlt jegliche kritische Bemerkung an der Politik Israels, wie der Blogger Richard Silverstein kritisch feststellte. Pakistan hat anlässlich der 2011 Balochistan International Conference Informationen über Occupation in der englischen Wikipeadia entfernen lassen und vieles andere mehr.
- Das Suchmaschinen ihre Links zensieren ist seit längerem bekannt. Die bei Wikileaks aufgetauchte Sperreliste des ehemaligen Suchdienstes Lycos

oder die Sperrlisten von Baidu sind interessant.

## 2 Strafverfolgung von Kinderpornografie

Während die Einführung von Internet-Sperren für die derzeitige Regierung “ein in vielerlei Hinsicht wichtiges Thema ist”, (v. Guttenberg), scheint die Verfolgung der Anbieter eher niedrige Priorität zu genießen.

### Wo stehen die Server?

Im scusiblog <https://scusiblog.org> findet man Analysen zu verschiedenen europäischen Filterlisten. In der Länderwertung belegt Deutschland stets einen beachtlichen vorderen Platz bei der Veröffentlichung von Material mit dokumentiertem Kindesmissbrauch. Eine Zusammenfassung der Sperrlisten der Schweiz, Dänemark, Finnland und Schweden (2008) lieferte folgende Zahlen:

Land	Anzahl der Websites
USA	3947
Australien	423
Niederlande	333
<b>Deutschland</b>	<b>321</b>
Süd-Korea	95
Kanada	88

Da diese in Deutschland gehosteten illegalen Angebote bei befreundeten Polizeien bekannt sind, stellt sich die Frage, warum sie bisher nicht entfernt und die Betreiber zur Rechenschaft gezogen wurden. Nahezu alle Provider unterstützen Maßnahmen gegen Kinderpornos. Es genügt ein Anruf, um das Angebot innerhalb weniger Stunden zu schließen. Auch die bei regierungskritischen Themen als *bullet proof* geltenden Hosters wie z.B. MediaOn und noblogs.org kennen bei KiPo kein Pardon.

Wenn das BKA kinderpornografische Websites kennt, die auf eine zukünftige Sperrliste gesetzt werden sollen, warum werden die Seiten nicht abgeschaltet und die Betreiber zur Verantwortung gezogen? Eine internationale Zusammenarbeit sollte bei diesem Thema kein Problem sein.

Zwei Jahre später war ein Teil der Webangebote noch immer online. Der AK Zensur ließ ganz ohne polizeiliche Vollmacht einige der seit zwei Jahren auf der dänischen Sperrliste stehenden Webseiten innerhalb von 30min schließen. Warum hat ds BKA zwei Jahre lang nichts unternommen?

### Der lange Dienstweg des BKA

In einer Studie der Univerität Cambridge wurde untersucht, wie lange es dauert, um strafrechtlich relevante Websites zu schließen. Phishing-Websites werden innerhalb von 4 Stunden geschlossen. Bei Websites mit dokumentierten Kindesmissbrauch dauert es im Mittel 30 Tage!

Frau Krogmann (CDU) antwortete auf eine Frage bei [abgeordnetenwatch.de](http://abgeordnetenwatch.de), dass das BKA kinderpornografische Websites nicht schneller schließen kann, weil **der Dienstweg** eingehalten werden muss.

Noch mal ganz langsam:

1. Weil das BKA den Dienstweg einhalten muss, können Websites mit dokumentierten Kindesmissbrauch nicht kurzfristig geschlossen werden?
2. Das mit dem Gesetz zur Einführung von Internet-Sperren rechtsstaatliche Prinzipien verletzt und Grundrechte eingeschränkt werden sollen (Grundgesetz Artikel 5 und 10), ist nebensächlich, wenn auch nur einem Kind damit geholfen werden kann?

Das Gutachten des Wissenschaftlichen Dienstes des Bundestages (WD 3 - 3000 - 211/09) zeigt, dass das BKA auch ohne Zensur wesentlich mehr gegen dokumentierten Kindesmissbrauch tun könnte.

Wie frustrierend dieser lange Dienstweg und die mangelhafte Unterstützung der Strafverfolger sind, zeigt Oberstaatsanwalt Peter Vogt. Die Sueddeutsche Zeitung bezeichnet ihn als Pionier der Strafverfolgung von Kinderpornografie. Ab Jan. 2010 steht Herr Vogt für diese Aufgabe nicht mehr zur Verfügung. Er hat wegen unhaltbarer Zustände in den Polizeidirektionen das Handtuch geworfen.

Interessant ist, dass das BKA eine mit hohen Kosten verbundene Sperr-Infrastruktur aufbauen möchte, selbst aber nur 6,3 (!) Planstellen für die Verfolgung von dokumentiertem Missbrauch bereitstellt.

### **Die Internet-Sperren sind kontraproduktiv**

Die geplanten Sperren von Websites mit Anzeige einer Stopp-Seite sind für die konsequente Verfolgung der Straftaten kontraproduktiv.

Mit der Anzeige der Stopp-Seite sollen die Daten des Surfers an das BKA zwecks Einleitung der Strafverfolgung übermittelt werden. Gleichzeitig wird der Konsument kinderpornografischen Materials jedoch gewarnt und kann alle Spuren beseitigen. Ohne Nachweis der Straftat ist eine rechtsstaatliche Verurteilung jedoch nicht möglich.

## **3 Die Medien-Kampagne der Zensursula**

Der Gesetzgebungsprozess wurde von einer breiten Medien-Kampagne begleitet. Die Gegner der Zensur wurden direkt und indirekt als Pädophile oder deren Helfer verunglimpft, es wurde ein Gegensatz von *“Meinungsfreiheit im Internet“* versus *“Schutz der Kinder“* konstruiert und viel mit fragwürdigem Zahlenmaterial, unwahren Behauptungen und suggestiven Umfragen argumentiert.

Das fragwürdige Zahlenmaterial für die Kampagne wurde überwiegend von Innocence in Danger geliefert. Diese Organisation unter Führung von Julia v. Weiler und Stefanie v.u.z. Guttenberg war auch wegen undurchsichtiger Geschäftsgebaren und undokumentierter Verwendung von Spendengeldern in öffentliche Kritik geraten.

In den Mainstream-Medien wurde die Argumentation der Befürworter der Zensur prominent und ohne kritische Nachfrage wiedergegeben:

*Es macht mich schon sehr betroffen, wenn pauschal der Eindruck entstehen sollte, dass es Menschen gibt, die sich gegen die Sperrung von kinderpornographischen Inhalten sträuben.* (Karl Theodor v.Guttenberg)

*Lassen Datenschützer und Internet-Freaks sich vor den Karren der Händler und Freunde von Kinderpornografie spannen? Diese Frage muss sich nicht nur Franziska Heine stellen.* (Teaser der Zeitschrift "Emma")

*Wir können es doch als Gesellschaft nicht hinnehmen, das - so wie es die Piratenpartei fordert- Jugendliche und Erwachsene ungehindert Zugang zu Kinderpornos im Internet haben können...* (S. Raabe, SPD)

Das Motto der Gegner der Zensur im Internet lautete **Löschen statt Sperren**. Das stand auch deutlich in der von Franziska Heine initiierten Petition und wurde auf dem Piraten-Parteitag ebenfalls deutlich gesagt.

Weitere Beispiele:

*Wir vermissen die Unterstützung der Internet Community, die uns sagt, wie wir dem wachsenden Problem der Kinderpornografie Herr werden können. Diese Stimmen sind bisher kaum zu hören.* (v.d.Leyen)

Heinrich Wefing, der uns schon öfter aufgefallen ist, sinniert in der *Zeit*:

*Nun könnte man die lärmende Ablehnung jeder staatlichen Regulierung vielleicht sogar als romantische Utopie belächeln, wenn die Ideologen der Freiheit gelegentlich mal selbst einen Gedanken darauf verwenden würden, wie sich der Missbrauch des Mediums eindämmen ließe.*

Die Nerds vom AK Zensur haben nicht nur Hinweise gegeben, sie haben es auch vorgemacht. **Innerhalb von 12 Stunden wurden 60 kinderpornographische Internet-Angebote gelöscht** (ganz ohne polizeiliche Vollmacht). Was wird noch erwartet. Sollen wir die Dienstanweisung für das BKA formulieren? Ein Gutachten des Wissenschaftlichen Dienstes des Bundestages zeigt, dass das BKA diesem Beispiel folgen könnte.

*Die bittere Wahrheit ist, dass bisher nur die Hälfte der Länder Kinderpornographie üchtet.* (v.d.Leyen)

Auf der *“Konferenz zum Schutz vor sexueller Gewalt gegen Kinder und Jugendliche mit Fokus auf neue Medien”* behauptet v.d.Leyen:

*Nur rund 160 Staaten haben überhaupt eine Gesetzgebung gegen die Vergewaltigung von Kindern, die von den Tätern aufgenommen und übers Netz verbreitet wird. 95 Nationen hätten keine solche Gesetze.*

Netzpolitik.org hat sich diese Zahlen genauer angesehen. 193 Staaten haben die UN-Konvention zum Schutz der Kinder ratifiziert und in geltendes Recht umgesetzt. Artikel 34 definiert den Schutz vor sexuellem Missbrauch.

Von den 95 Nationen, die lt. v.d.Leyen keine Gesetze gegen Missbrauch Minderjähriger haben sollen, verbieten 71 Pornografie generell. Das schließt dokumentiert Missbrauch ein. Weitere befinden sich im Bürgerkrieg oder in einem verfassungsgebenden Prozess nach einem Krieg. Der Rest hat keine nennenswerte Infrastruktur, um Webserver zu betreiben.

*Wer die Stoppseite zu umgehen versucht, macht sich bewusst strafbar, weil er dann aktiv nach Kinderpornografie sucht.*  
(v.d.Leyen)

Moment mal - es war im III. Reich verboten, Feindsender zu hören. Einen vergleichbaren Paragraphen sucht man im Strafgesetzbuch vergeblich. Es steht jedem Nutzer frei, vertrauenswürdige Internet-Server zu nutzen.

## 4 Löschen statt Sperren ist funktioniert

Die Aktionen des AK-Zensur haben gezeigt, dass Löschen statt Sperren möglich ist. in einer ersten Aktion wurden innerhalb von 12 Stunden 60 kinderpornografische Internet-Angebote gelöscht, ohne polizeiliche Vollmachten. In einer zweiten Aktion wurde die dänische Sperrliste analysiert. Seit 2 Jahren gesperrte Webseiten konnten innerhalb von 30min gelöscht werden. Das Beispiel zeigt, dass eine Sperrliste auch oft als Alibi dient und eine weitere Strafverfolgung nicht betrieben wird.

Der eco Verband konnte im Jahr 2010 von den gemeldeten Webseiten 99,4% entfernen. Es wurden 256 Websites mit dokumentiertem Missbrauch gemeldet. Davon wurden 448 im Wirkungsbereich von INHOPE umgehend gelöscht. 204 wurden auf ausländischen Server nach kurzem Hinweis vom Provider gelöscht. Bei zwei Meldungen handelte es sich nicht um strafbares Material.

## 5 Simple Tricks

Die besten Möglichkeiten zur Umgehung von Zensur sind *Anonymisierungsdienste* mit Anti-Censorship Funktion wie JonDonym oder Tor. Stehen diese Dienste nicht zur Verfügung, kann man es auch mit den Simple Tricks versuchen. Die *Simple Tricks* wurden bereits an der "Great Firewall" in China erprobt und sind teilweise recht erfolgreich. Das einfache Prinzip ist im Bild 2 dargestellt.

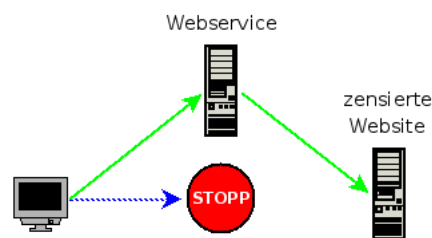


Abbildung 2: Prinzip der Simple Tricks

Wenn man auf eine Website nicht zugreifen kann (oder man befürchtet, nicht zugreifen zu können) kann man ein Webdienst im Ausland nutzen. Der Webdienst unterliegt anderen Zensurbedingungen und kann häufig auf die gewünschte Seite zugreifen und über den kleinen Umweg unzensiert liefern.

**Hinweis:** Es ist ratsam, Web-Services zu nutzen, die eine SSL-Verschlüsselung des Datenverkehrs anbieten. Wer Anonymisierungsdienst wie Tor oder JonDonym nutzen kann, sollte diese Möglichkeit bevorzugen.

Einige Vorschläge für Webdienste:

1. **RSS-Aggregatoren:** sind geeignet, um regelmäßig eine Website zu lesen, die RSS-Feeds anbietet, bspw. Blogs. Man kann sich selbst seine Feeds auf einem Web-Aggregator wie [www.bloglines.com](http://www.bloglines.com) zusammenstellen oder nutzt fertig, themenspezifische Aggregatoren wie z.B. den Palestine Blog Aggregator über den Gaza-Krieg.
2. **SSL-Web-Proxys** bieten ein Formular für die Eingabe einer URL. Die Website wird von dem Proxy geholt und an den Surfer geliefert. Dabei werden alle Links der Webseite vom Proxy umgeschrieben, so dass bei einem Klick die folgende Website ebenfalls über den Proxy geholt wird. Flüssiges Surfen ist möglich. Um die Filterung des Datenverkehr nach gesperrten Wörtern zu verhindern, sollte man SSL-verschlüsselte Web-Proxys nutzen. Eine Liste von Web-Proxys mit SSL-Verschlüsselung findet man bei [Proxy.org](http://Proxy.org) oder [mamproxy.com](http://mamproxy.com) oder [www.privax.us/](http://www.privax.us/).

Web-Proxies sind keine Anonymisierungsdienste! Die Admins könnten den gesamten Traffic mitlesen, auch bei SSL-verschlüsselten Websites. Sie sind ungeeignet für Webangebote, die ein Login mit Passwort erfordern. Viele

Web-Proxys speichern die Daten und geben sie auch an Behörden weiter, wie der Sahara-Palin-Hack zeigte. Außerdem können Webmaster die meisten Web-Proxys austricksen, um Nutzer zu deanonymisieren.

3. **Übersetzungsdienste:** Man fordert bei einem Web-Translator die Übersetzung einer Website von einer willkürlichen Sprache (z.B. koreanisch) in die Originalsprache des Dokumentes an. Der Web-Translator ändert praktisch nichts. Man kann <http://babelfish.yahoo.com> oder <http://translate.google.com> nutzen.
4. **Low-Bandwidth-Filter:** bereiten Websites für Internetzugänge mit geringer Bandbreite auf. Sie entfernen Werbung, reduzieren die Auflösung von Bildern usw. und senden die bearbeitete Website an den Surfer. Man kann sie auch mit High-Speed-DSL nutzen. Steht ein solcher Server im Ausland, hat er häufig die Möglichkeit, die gewünschte Seite zu liefern, z.B. <http://loband.org>.
5. **Cache der Suchmaschinen:** Die großen Suchmaschinen indexieren Webseiten nicht nur, sie speichern die Seiten auch in einem Cache. Da man Google, Yahoo usw. fast immer erreichen kann: einfach auf den unscheinbaren Link *cache* neben dem Suchergebnis klicken.
6. **E-Mail Dienste:** sind etwas umständlicher nutzbar. Sie stellen die gewünschte Website per Mail zu. Ein Surfen über mehrere Seiten ist damit natürlich nicht möglich. Sie sind aber gut geeignet, unauffällig einen Blick auf eine gesperrte Website zu werfen. Dem E-Mail Dienst [pagegetter.com](http://pagegetter.com) kann man eine Mail mit der gewünschten URL der Website im Betreff senden und man erhält umgehend eine Antwort-Mail mit der Website. Der Dienst bietet folgende Adresse:
  - [web@pagegetter.com](http://web@pagegetter.com) für einfache Webseiten.
  - [frames@pagegetter.com](http://frames@pagegetter.com) für Webseiten die aus mehreren Framen bestehen.
  - [HTML@pagegetter.com](http://HTML@pagegetter.com) liefert die Webseite ohne grafische Elemente aus.

## 6 Unzensierte DNS-Server nutzen



### WIR FILTERN DAS NETZ.

Am 17.04.09 unterzeichneten diese Provider einen geheimen Vertrag mit dem BKA, in welchem sie sich verpflichteten, den Zugriff auf eine vom BKA bereitgestellte Liste von Websites zu sperren. Soweit bekannt wurde, soll die Sperrung hauptsächlich durch Kompromittierung des DNS-Systems erfolgen.

**Hinweis:** Diese leicht zu umgehende Sperre ist im internationalen Vergleich die Ausnahme. Lediglich Australien hat einen vergleichbaren Weg gewählt. Die folgenden Hinweise zur Umgehung der Zensur durch Nutzung unzensierter DNS-Server können nicht auf andere Länder mit technisch hochgerüsteter Zensur-Infrastruktur übertragen werden.

Bevor man als Kunde dieser Provider ernsthaft über die Nutzung alternativer DNS-Server nachdenkt, sollte man die Möglichkeit eines **Provider-Wechsels** prüfen. Das hat folgende Vorteile:

1. Man unterstützt Provider, die sich gegen die Einschränkung der Grundrechte wehren, und übt Druck auf die Zensur-Provider aus.
2. Es ist auf für IT-Laien eine sichere Lösung, unzensierte DNS-Server zu nutzen, da möglicherweise Zensur-Provider den Datenverkehr auf eigene, zensierte DNS-Server umlenken, ohne dass man es als Nutzer bemerkt. So leitet Vodafone bspw. bereits seit Juli 09 im UMTS-Netz DNS-Anfragen auf die eigenen Server um. Im DFN Forschungsnetz soll die Nutzung unzensierter DNS-Server durch Sperrung des Port 53 unterbunden werden.

Die deutschen Provider Manitu (<http://www.manitu.de>) und SNAFU (<http://www.snafu.de>) lehnten die Sperren ab und werden sie auch nicht umsetzen. SNAFU bietet seinen Kunden an, via Webinterface alternative, unzensierte DNS-Server für den eigenen Account zu konfigurieren. Damit entfallen die im folgenden beschriebenen Spielereien am privaten Rechner und man hat mit Sicherheit einen unzensierten Zugang zum Web.

## Was ist ein DNS-Server

1. Der Surfer gibt den Namen einer Website in der Adressleiste des Browsers ein. (z.B. *https://www.awxcnx.de*)
2. Daraufhin fragt der Browser bei einem DNS-Server nach der IP-Adresse des Webservers, der die gewünschte Seite liefern kann.
3. Der DNS-Server sendet eine Antwort, wenn er einen passenden Eintrag findet. (z.B. *62.75.219.7*) oder NIXDOMAIN, wenn man sich vertippt hat.
4. Dann sendet der Browser seine Anfrage an den entsprechenden Webserver und erhält als Antwort die gewünschte Website.

Ein kompromittierter DNS-Server sendet bei Anfrage nach einer indexierten Website nicht die korrekte IP-Adresse des Webservers an den Browser, sondern eine manipulierte IP-Adresse, welche den Surfer zu einer Stop-Seite führen soll.

Die Anzeige der Stop-Seite bietet die Möglichkeit, die IP-Adresse des Surfers zusammen mit der gewünschten, aber nicht angezeigten Webseite zu loggen. Mit den Daten der Vorratsdatenspeicherung könnte diese Information personalisiert werden.

(Diese Darstellung ist sehr vereinfacht, sie soll nur das Prinzip zeigen. Praktische Versuche, das DNS-System zu manipulieren, haben meist zu komplexen Problemen geführt.)

## Nicht-kompromittierte DNS-Server

Statt der kompromittierten DNS-Server der Provider kann man sehr einfach unzensurierte Server nutzen. Einige DNS-Server können auch auf Port 110 (TCP-Protokoll) angefragt werden, falls einige Provider den DNS-Traffic auf Port 53 zum eigenen Server umleiten oder behindern. Wir gehen bei der Konfiguration für Windows und Linux darauf näher ein.

Die GPF betreibt einige unzensurierte DNS-Server.

87.118.100.175 (DNS-Ports: 53, 110)

94.75.228.29 (DNS-Ports: 53, 110)

Die Swiss Privacy Foundation stellt folgende unzensurierten DNS-Server:

62.141.58.13 (DNS-Ports: 53, 110)

87.118.104.203 (DNS-Ports: 53, 110)

87.118.109.2 (DNS-Ports: 53, 110)

Der Server awxcnx.de bietet auch unzensurierten DNS:

62.75.219.7 (DNS-Ports: 53, 110)

Der FoeBud bietet einen unzensurierten DNS-Server:

85.214.20.141

Und der CCC hat natürlich auch einen Unzensurierten:

213.73.91.35

## 6.1 WINDOWS konfigurieren

Wir bezweifeln, das es zur Umgehung der Zensur ausreicht, einfach einen unzensierten DNS-Server zu nutzen. Das am 18.06.09 verabschiedete Gesetz zur Einführung der Zensur ist ausdrücklich technik-offen formuliert. Es sieht vor, dass die DSL-Provider alle nötigen Maßnahmen ergreifen, um den Zugriff auf indexierte Webseiten effektiv zu sperren. Die Nutzung unzensierter DNS-Server kann relativ einfach unterbunden werden. Vodafone leitet im UMTS-Netz bereits alle Anfragen auf eigene DNS-Server um, die Pläne des DFN Forschungsnetzes sehen eine Sperrung von Port 53 vor.

Eine Möglichkeit bietet die Verwendung eines nicht üblichen TCP-Ports für DNS-Anfragen. Die DNS-Server der GPF können neben dem üblichen Port 53 auch auf Port 110 angefragt werden. Da WINDOWS die Konfiguration vom Standard abweichender Einstellungen nicht ermöglicht, ist etwas mehr Aufwand nötig, als die bekannten 27sec.

### bind9 installieren

Der Nameserver *bind9* steht auch für WINDOWS beim ISC unter der Adresse <https://www.isc.org/download/software/current> zum Download bereit. Nach dem Entpacken des ZIP-Archives ruft man *BINDInstall.exe* als Administrator auf. Als Target-Directory für die Installation wählt man am besten *C:/bind* und nicht die Voreinstellung.

Nach der Installation sind auf der Kommandozeile noch ein paar Nacharbeiten als Administrator nötig:

```
c:
cd \bind\bin
rndc-confgen -a
mkdir c:\bind\zone
mkdir c:\bind\log
cacls c:\bind /T /E /C /G named:F
```

Im Verzeichnis *C:/bind/zone* müssen die drei Dateien angelegt werden:

#### 1. localhost.zone

```
$TTL 86400
@ IN SOA @ root ( 1 ; serial
3H ; refresh
15M ; retry
1W ; expiry
1D ) ; minimum

IN NS @
IN A 127.0.0.1
IN AAAA ::1
```

#### 2. localhost.rev

```

$TTL 86400
@ IN SOA localhost. root.localhost. ( 1 ; Serial
3H ; Refresh
15M ; Retry
1W ; Expire
1D ) ; Minimum

IN NS localhost.
1 IN PTR localhost.

```

3. Die Datei *db.cache* lädt man von <ftp://ftp.internic.net/domain/db.cache> und speichert sie in dem Verzeichnis *C:/bind/zone*. Diese Datei enthält die Informationen zu den DNS-Root-Servern.

Abschließend konfiguriert man in der Datei *named.conf* in der Sektion *options* die für die Weiterleitung genutzten DNS-Server als *forwarders*, welche auch auf Port 110 angefragt werden können, ein Beispiel:

```

options {
    directory "C:\bind\zone";
    allow-query { localhost; };
    max-cache-size 16M;
    cleaning-interval 60;
    listen-on { 127.0.0.1; };

    forwarders {
        87.118.100.175 port 110;
        94.75.228.29 port 110;
    };
};

```

Wenn die Konfiguration fertig ist, kann man den Dienst mit dem Befehl *net start named* auf der Kommandozeile starten oder über die Taskleiste unter *Start - Systemsteuerung - Verwaltung - Dienste* hochfahren.

## Einstellungen der Internetverbindungen anpassen

In den Einstellungen der Internetverbindungen wird der lokale bind9 als DNS-Server konfiguriert. In der *Systemsteuerung* ist die Liste der Netzwerkverbindungen zu öffnen. Ein Klick mit der rechten Maustaste öffnet das Kontext-Menü, wo man den Eintrag *Eigenschaften* wählt. Der in Bild 3 gezeigte Dialog öffnet sich.

Hier wählt man die *TCP-Verbindung* und klickt auf *Eigenschaften*. In dem folgenden Dialog kann man eigene DNS-Server konfigurieren. In dem folgenden Dialog kann man den lokalen bind9 als DNS-Server konfigurieren, indem man als *Bevorzugten DNS-Server* die Adresse *127.0.0.1* eingibt.

## 6.2 Linux konfigurieren

Unter Linux sind nichts-standardmäßige Einstellungen leichter realisierbar. Es ist auch relativ einfach, einen lokalen DNS-Cache zu nutzen, um die zensurfreien

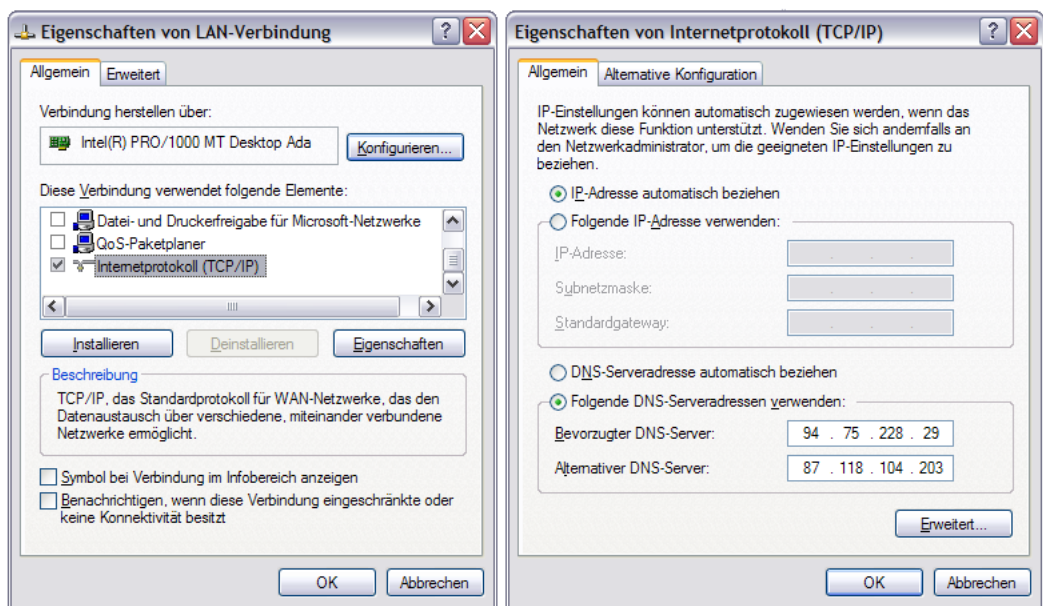


Abbildung 3: Konfiguration der DNS-Server (WINDOWS)

DNS-Server nicht übermäßig zu belasten.

### pdnsd und resolvconf verwenden

Der *pdnsd* ist ein leichtgewichtiger DNS-Cache-Daemon. Er steht auf allen Linux-Distributionen zur Verfügung. Unter Debian und Ubuntu installiert man ihn zusammen mit *resolvconf*:

```
> sudo aptitude install resolvconf pdnsd
```

Bei der Installation des *pdnsd* wird man gefragt, wie die Namensauflösung erfolgen soll. Wählen sie zuerst einmal recursive. Laden sie die vorbereitete Konfigurationsdatei <https://www.awxcnx.de/download/pdnsd-gpfserver.conf> herunter und speichern sie die Datei im Verzeichnis */usr/share/pdnsd*.

Anschließend in der Datei */etc/default/pdnsd* den *AUTO\_MODE* anpassen:

```
START_DAEMON=yes
AUTO_MODE=gpfserver
OPTIONS=
```

Den Eigentümer der Config-Datei auf *root* setzen und den Daemon neu starten:

```
sudo chown root:root /usr/share/pdnsd/pdnsd-gpfserver.conf
sudo invoke-rc.d pdnsd restart
```

Der DNS-Traffic geht via TCP-Protokoll auf Port 110 zu den unzensurierten DNS-Servern. Es ist schwer zu erkennen, dass es sich DNS-Traffic handelt und eine

Umleitung auf DNS-Server der Provider ist wenig wahrscheinlich. Zur Sicherheit gelegentlich testen.

### **bind9 und resolvconf verwenden**

Die Pakete *bind9* und *resolvconf* sind in allen Distributionen fertig konfiguriert vorhanden und bietet einen vollständigen DNS-Nameserver. Nach der Installation mit der Paketverwaltung läuft der Nameserver und ist unter der Adresse 127.0.0.1 erreichbar. Die Tools aus dem Paket *resolvconf* sorgen für die automatische Umkonfiguration, wenn *bind9* gestartet und gestoppt wird. Für Debian und Ubuntu können die Pakete mit *aptitude* installiert werden:

```
> sudo aptitude install resolvconf bind9
```

Die unzensierten DNS-Server sind in der Datei */etc/bind/named.conf.options* einzutragen. Die Datei enthält bereits ein Muster. Dabei kann optional auch ein nicht üblicher Port angegeben werden:

```
forwarders {
    94.75.228.29 port 110;
    62.75.219.7  port 110;
};
listen-on { 127.0.0.1; };
```

(Standardmäßig lauscht der Daemon an allen Schnittstellen, auch an externen. Die Option *listen-on* reduziert das auf den lokalen Rechner.)

Wer etwas ratlos ist, mit welchem Editor man eine Konfigurationsdatei anpasst, könnte *“kdesu kwrite /etc/bind/named.conf.options”* oder *“gksu gedit /etc/bind/named.conf.options”* probieren.

Nach der Anpassung der Konfiguration ist *bind9* mitzuteilen, das er die Konfigurationsdateien neu laden soll:

```
> sudo invoke-rc.d bind9 reload
```

### **6.3 DNS-Server testen**

Wir haben uns Gedanken gemacht, wie man möglichst einfach feststellen kann, ob man bei der Konfiguration der DNS-Server alles richtig gemacht hat. Möglicherweise hat man zwar alles richtig gemacht, aber der DSL-Provider leitet den DNS-Traffic auf Port 53 zu den eigenen Servern um, wie es z.B. Vodafone im UMTS-Netz macht. Der einfachen Nutzer wird diese Umleitung in der Regel nicht bemerken.

Die DNS-Server der German Privacy Foundation und der Swiss Privacy Foundation können die Test-Adresse [welcome.gpf](http://welcome.gpf) auflösen und sind auf Port 53 und Port 110 erreichbar:

```
87.118.100.175
62.141.58.13
62.75.219.7
```

94.75.228.29  
87.118.104.203  
87.118.109.2

Hat man zwei dieser Server als DNS-Server ausgewählt, so kann man recht einfach testen, ob auch wirklich diese Server genutzt werden. Einfach im Browser die Adresse <http://welcome.gpf> aufrufen. Wenn man unsere Welcome-Seite sieht, ist alles Ok.

### **Congratulation**

You are using a censorship free DNS server!

Auf der Kommandozeile kann man *nslookup* nutzen. Die IP-Adresse in der Antwort muss 62.75.217.76 sein.

```
> nslookup welcome.gpf
```

```
Non-authoritative answer:  
Name:    welcome.gpf  
Address: 62.75.217.76
```

Sollte im Webbrowser nicht unsere Welcome-Seite angezeigt werden oder *nslookup* eine andere IP-Adresse liefern, so wurde keiner der oben genannten DNS-Server genutzt. Es ist die Konfiguration zu prüfen oder .... hmmm.