

# Werbeblocker

## Werbefirmen auf der Schwarzen Liste

**Andreas Beck**

### **Zusammenfassung**

Vermeidung der Belästigung und Ablenkung durch Werbung beim Surfen im Internet, durch gezieltes Blocken bekannter Werbeserver an Hand einer Schwarzen Liste in der betriebssystemeigenen Hosts-Datei. Die Methode ist kostenlos, erfordert keinerlei Softwareinstallation und ist betriebssystemunabhängig.

*Schlüsselwörter:* Ads, Adv, Anti-Werbung, Hosts, Linux, MacOS, UNIX, Werbebanner, Werbung, Werbeblocker, Werbefilter, Windows

## Einleitung

Prinzipiell ist gegen Werbung nichts einzuwenden, da sie der Bekanntmachung und dem Verkauf von Produkten dient. Allerdings wird ein Großteil der Werbung jeglicher Art inzwischen mehr als Belästigung, denn als Bereicherung empfunden, da sie zu aufdringlich ist oder mit unlauteren Methoden arbeitet und man sich ihr praktisch nicht entziehen kann. Einige Webseiten sind derart mit Werbebannern zugepflastert, daß der eigentliche Inhalt verloren geht. Andere wiederum benutzen Werbebanner die wie Warnmeldungen von Windows aussehen, teilweise auch mit dem gewollten Effekt der Schreckwirkung, wieder andere wollen möglichst durch bewegte Bilder mit grellen Farben auffallen.

Einige besonders impertinente Firmen versuchen gezielt Benutzerprofile durch Zusammenführung der Daten zu erstellen. Besonders einfach wird es dann, wenn im Browser das beliebige Setzen von Cookies durch die besuchte Webseite erlaubt ist. Wird unter diesen Bedingungen jetzt noch eine Online-Bestellung vom Benutzer vorgenommen, läßt sich einem Benutzerprofil auch eine konkrete Person zuordnen.

Sich über solche Methoden zu beschweren hat wenig Sinn, ebenso wie der gezielte Nicht-Kauf derart beworbener Produkte wohl kaum zu einer Rücknahme der Banner führt. Insofern ist wieder einmal der mündige Bürger zur Selbsthilfe aufgerufen. In diesem Falle ist es recht einfach, da jedes relevante Betriebssystem schon von Haus aus die technischen Möglichkeiten zum Abblocken von Werbung mitbringt, einzig ein gewisses Verständnis für die Abläufe beim Surfen im Internet ist notwendig. Die hier beschriebene Methode ist äußerst effektiv und darüberhinaus ..

- legal,
- kostenlos,
- flexibel, den individuellen Bedürfnissen jederzeit anpassbar
- erfordert keine zusätzliche Software,
- erfolgt mit Bordmitteln der Betriebssysteme,
- browserunabhängig,
- betriebssystemweit, d.h. die Filterung erfolgt bei allen Zugriffen ins Internet, egal welches Programm oder Protokoll eingesetzt wird,

und bei allen relevanten Betriebssystemen (BeOS,

MacOS, UNIX(e), Windows) anwendbar.

## Technischer Hintergrund

Alle am Internet hängenden Computer kommunizieren über ihre einmalige TCP/IP-Adresse in der Form xyz.xyz.xyz.xyz, wobei xyz jeder der vier Blöcke die Zahl 0 - 255 annehmen kann (z. B. 62.134.70.60). Von den möglichen Adressen sind einige für spezielle Zwecke reserviert worden, u.a. die 127.0.0.1 die immer (**sic!**) und ausschließlich auf den jeweils eigenen Rechner („localhost“) weist, unabhängig davon ob man Windows, Linux oder MacOS benutzt.

Da sich Menschen Zahlenfolgen wesentlich schwerer merken können, als aussagefähige („sprechende“) Buchstabenkombinationen, wurde das Domain Name System (DNS) geschaffen, in dem die Webadressen den TCP/IP-Nummern zugeordnet werden. Beim Anfordern einer Webseite durch Eintippen einer URL (bspw. <http://WWW.Pruefziffemberechnung.DE/>) erfolgt zuerst eine Anfrage beim zuständigen DNS-Server nach der TCP/IP-Nummer des Servers *WWW.Pruefziffemberechnung.DE*. Erst nachdem das System diese Nummer erhalten hat (im Beispiel wäre das 212.227.119.73), kann der eigentliche Vorgang, nämlich die Anforderung der Webseite gestartet werden. Von diesem Frage-Antwort-Spiel merkt man normalerweise nichts, aber das Wissen um Dieses kann man sich zu Nutze machen um unerwünschte Verbindungen zu blockieren. Das Abfragen der TCP/IP-Nummer erfolgt für jeden Server einzeln und unter Umständen für jede Webseite etliche Male, da die Informationen (Bilder, Banner, Texte, Multimedia) einer Seite nicht zwangsläufig auf demselben Server liegen müssen. Bei jedem Betriebssystem hat man nun die Möglichkeit häufig benutzte Servernamen mit ihren dazugehörigen TCP/IP-Nummern in einer lokalen Text-Datei — namentlich Hosts — abzuliegen, also im Prinzip ein kleines, lokales DNS zu führen.

## Hosts-Datei

Der Trick des Abblockens besteht darin, den Servernamen auf denen bekanntermaßen viele Werbebanner abgelegt sind in der Hosts-Datei die TCP/IP-Nummer des eigenen Rechners zuzuweisen. Erfolgt eine Anfrage nach einer TCP/IP-Nummer wird zuerst die lokale Host-Datei konsultiert. Ist kein Eintrag des Servernamens in der Hosts-Datei vorhanden, wird die Anfrage wie gehabt an

das DNS im Internet weitergereicht. Ist hingegen der Servername mit einer TCP/IP-Nummer vorhanden, ist die Anfrage erledigt und der andere Rechner wird sofort mit der in der Hosts-Datei gefundenen TCP/IP-Nummer angesprochen, unabhängig davon was im DNS steht. Da in der Hosts-Datei eine beliebige TCP/IP-Nummer für jeden Server eingetragen werden kann, nimmt man zum Blocken zweckmäßigerweise die TCP/IP-Nummer des eigenen Rechners, also die 127.0.0.1. Da aber auf dem eigenen Rechner die angeforderten Dateien nicht existieren, meldet das System dem Browser sehr schnell nur „Datei nicht gefunden“ zurück. Bei Bildern (also eben auch bei Werbebannern), bleibt dann in der Ansicht der Webseite eine Lücke in der Größe des Bildes.

Auf allen Systemen muß eine funktionierende Hosts-Datei eine einfache Textdatei ohne Extension sein. Eine solche läßt sich mit jedem x-beliebigen Texteditor (Notepad, Text-Edit) bearbeiten bzw. erstellen. Oft wird auch bei der Installation ein leere oder eine Beispieldatei mit installiert. Am besten einfach mal nach dem Dateinamen Host\* suchen (Hosts.sam ist eine Beispieldatei [sam = sample hosts file]). Je nach Betriebssystem unterscheiden sich Ablageort und Struktur der Hosts-Datei (Tabelle 1).

Um die zu blockenden Servernamen zu ermitteln, surft man ganz normal die Webseiten an und wartet bis der Seitenaufbau abgeschlossen ist. Fährt man jetzt mit dem Mauszeiger über die einzelnen Werbebanner (nicht draufklicken !) kann man in der Statuszeile des Browsers oft den Pfad ablesen unter dem bspw. das Bild abgelegt ist. Das funktioniert leider nicht immer. Dann muß man sich merken was man gelesen hat und über den Menübefehl *Quelltext ansehen* direkt im Quellcode der HTML-Datei danach suchen. Der Bannerlink wird in einer Struktur wie etwa `` eingebettet sein. Jetzt trägt man den Servernamen (alles zwischen `src="http://` bis zum ersten Schrägstrich, im

Beispiel also [banner.adcompany.com](http://banner.adcompany.com)) in die Hosts-Datei zusammen mit der jetzt „neuen“ TCP/IP-Adresse 127.0.0.1 ein. Dies wiederholt man für alle Elemente die einen stören. Allerdings sollte man darauf achten, daß man wirklich nur Werbeserver ausschließt, denn treibt man es zu weit, sieht man nur noch eine leere Seite und das wäre doch der Selbstzensur zuviel. Einige kommerzielle Produkte arbeiten genau nach diesem Prinzip um unerwünschte Zugriffe, sei es auf Werbebanner oder ganze Webangebote, zu unterbinden.

## Werbeserverlisten

Das Zusammenstellen der Werbeserver hört sich nach viel Arbeit an, aber einerseits erkennt man recht schnell eine gewisse Systematik in der Vergabe der Servernamen (ad. ..., ads. ..., banner. ..., werbung. ...), so daß man weiß wonach man zu suchen hat. Andererseits kann man bereits auf fertige Serverlisten zurückgreifen, die nur noch in die Hosts-Datei kopiert und ggf. um einige wenige Einträge ergänzt werden müssen. Beispielsweise finden sich auf der Webseite des Autors für die verschiedenen Betriebssysteme fertig vorkonfigurierte Dateien.[1] Abgesehen von der unterschiedlichen Formatierung sind beide Dateien inhaltlich identisch und enthalten derzeit mehr als 1.000 Einträge (< 40 kByte).

Die angebotenen Serverlisten enthalten auch Servernamen aus HTML-Werbemails („Spam“; extrahiert aus mehreren Tausend Textkörpern der Mails) in denen u.a. versucht wird durch Links im HTML-Code eine vom Empfänger unbemerkte Rückmeldung darüber zu erhalten, ob die Mail gelesen wurde.[2]

Wohlgemerkt, diese Listen erheben weder den Anspruch auf Vollständigkeit noch auf immerwährende Gültigkeit, auch wenn alle paar Monate alle Einträge anhand eines vorhandenen DNS-Eintrages und erfolgreichen Pings auf Existenz überprüft werden. Die Wirksamkeit der Liste

hängt neben den Surfgewohnheiten des Einzelnen auch von der Anzahl der Anwender ab, die diese Liste benutzen und ggf. mit aktuellen Daten bestücken. Das Internet ist ein flexibles Medium und dementsprechend dienen die Serverlisten mehr als

Tabelle 1: Ablageorte und Struktur der Hosts-Datei

Betriebssystem	Pfad	Struktur
BeOS	/boot/beos/etc/Hosts	127.0.0.1 Domänenname.de
Linux	/etc/hosts	127.0.0.1 Domänenname.de
MacOS 8-9	Systemordner:Preferences:Hosts	Domänenname.de CNAME 127.0.0.1
MacOS X [3]	/etc/hosts	127.0.0.1 Domänenname.de
Windows 3.x und 9x	c:\windows\hosts	127.0.0.1 Domänenname.de
Windows NT	c:\winnt\system32\drivers\etc\hosts	127.0.0.1 Domänenname.de
Windows 2000	c:\windows\system32\drivers\etc\hosts	127.0.0.1 Domänenname.de

Ausgangspunkt. Wer also weitere Server oder Fehler in der Liste findet, sende den Servernamen mit einem dazugehörigen Link zum Ausprobieren an den Autor, damit die Listen auf dem aktuellen Stand gehalten werden können.

## Weitergehende Maßnahmen

Wer seine Hosts-Datei entsprechend angepasst hat, wird feststellen, daß immer noch reichlich Werbung erscheint, die aber von Servern kommt, die man nicht einfach komplett ausfiltern kann. An diesem Punkt sollte man wirklich darüber nachdenken, ob es nicht wirklich an der Zeit ist, seinen Browser zu wechseln. Die meisten Surfer benutzen artig, wie von Microsoft vorgesehen, den Internet Explorer (IE). Warum eigentlich? Es gibt brauchbare Alternativen, die sich darüberhinaus besser den Wünschen des Anwenders unterordnen, die eben z.B. auch das gezielte Ausblenden von Bildern anhand des Pfades oder der Größe erlauben. Jeder sollte sich auch wirklich Gedanken darüber machen, ob eine Webseite, die beim Besuch mit einem anderen Browser als mit dem IE meldet „*Diese Seite kann*

*mit Ihrem Browser nicht dargestellt werden. Sie können den aktuellen IE hier herunterladen.*“ wirklich einen Besuch wert ist. Der Besucher ist immer noch der Kunde! Ein Anbieter der sich nicht auf seine Kunden einstellen kann taugt nichts! Seien Sie konsequent, meiden Sie solche Webseiten, auch wenn es manchmal schwer fällt, aber das Internet bietet sicherlich eine brauchbare Alternative. Nutzen Sie Ihre Möglichkeiten, denn Vielfalt ist besser Einfalt.

## Referenzen

1. <http://WWW.Anmibe.DE/Tipps & Tricks/Werbeblocker.shtml>
2. <http://WWW.Pruefziffernberechnung.DE/Datenspuren.shtml#WebBeacons>
3. AppleCare Knowledge Base Document #88158  
Mac OS X 10.0: How to Add Hosts to Local NetInfo  
<http://docs.info.apple.com/article.html?artnum=88158>

---

Copyright © 2002 Attraktor

Alle Rechte vorbehalten. Jegliche teilweise oder ganze Weiterverbreitung und Weiterverarbeitung in jedwedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung. Für die in den hier veröffentlichten Inhalten, Daten oder Programmen möglicherweise enthaltenen Fehler und den daraus resultierenden Schäden wird keine Haftung übernommen. Auch wird keine Verantwortung für die Inhalte von Seiten, auf die hier verwiesen wird („Verlinkung“) übernommen.