

# DNS-Cache Beobachtungen

## Analyse des DNS-Caching diverser ISPs

September 2006

Christian Dietrich <[dietch@internet-sicherheit.de](mailto:dietch@internet-sicherheit.de)>



### Was war der Anlass?

Jeder Internetuser, der bereits einen Wechsel des Webhosters (z.B. einen Website-Umzug) mitgemacht hat, kennt das Problem: Der IP-Adresse, die hinter dem Domain-Namen steckt wird im Domain Name System geändert und es gibt für eine gewisse Übergangszeit mitunter merkwürdige Resultate, wenn man die Webseite aufruft. Ein mögliches Szenario ist folgendes: Zeitweise erhält man auf DNS-Anfragen zur entsprechenden Domain die "alte" IP-Adresse als Antwort, zu anderen Zeitpunkten gibt ein DNS-Server die "neue" IP-Adresse zurück.

### Wie entstehen solche divergierenden Antworten?

Der Umstand, dass nicht jeder DNS-Server nach der Änderung der DNS-Konfiguration die aktuellen Daten zurückliefert liegt im sog. Caching, d.h. Zwischenspeichern von DNS-Antworten begründet. DNS-Caching ist eine übliche Vorgehensweise im Internet, die dazu dient, DNS-Abfragen performanter zu gestalten. Für weitere Erläuterungen zu DNS-Caching siehe <http://de.wikipedia.org/wiki/DNS-Caching>.

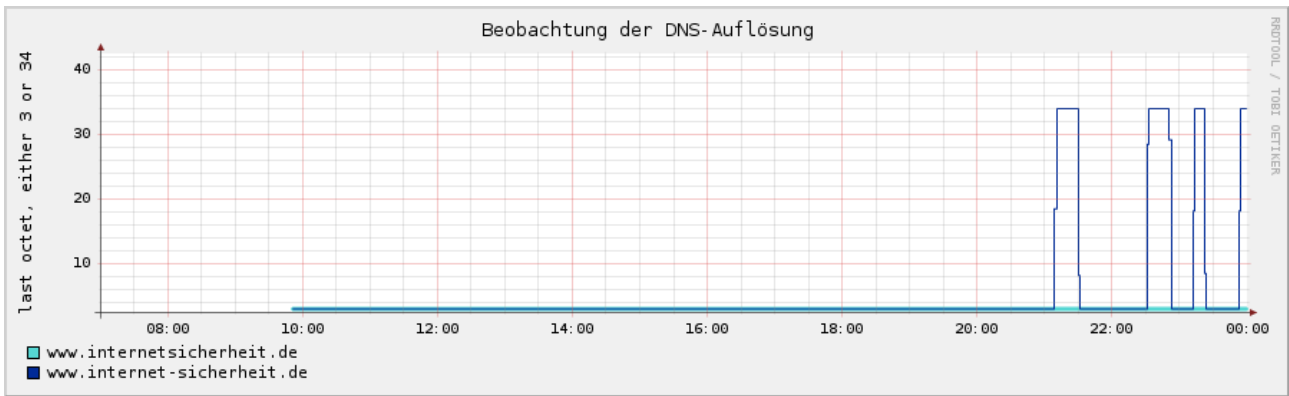
Am 8. September 2006 haben wir die IP-Adresse unseres Webservers [www.internet-sicherheit.de](http://www.internet-sicherheit.de) umgestellt. Wir nutzten die Gelegenheit, um das Caching von DNS-Antworten diverser Internet Service Provider in Deutschland zu untersuchen. Es handelt sich hierbei keinesfalls um eine repräsentative Untersuchung, sondern lediglich um ein Experiment, das oberflächlich einige der Probleme, die DNS-Caching mit sich bringen kann erkennen lässt.

### Wie wurde experimentiert?

Mit Hilfe von Sonden, die über diverse Internet-Anschlüsse verschiedener ISPs mit dem Internet verbunden waren, wurden über einen definierten Zeitraum hinweg die DNS-Antworten protokolliert. Die DNS-Queries wurden an die DNS-Server des jeweiligen ISPs gerichtet.

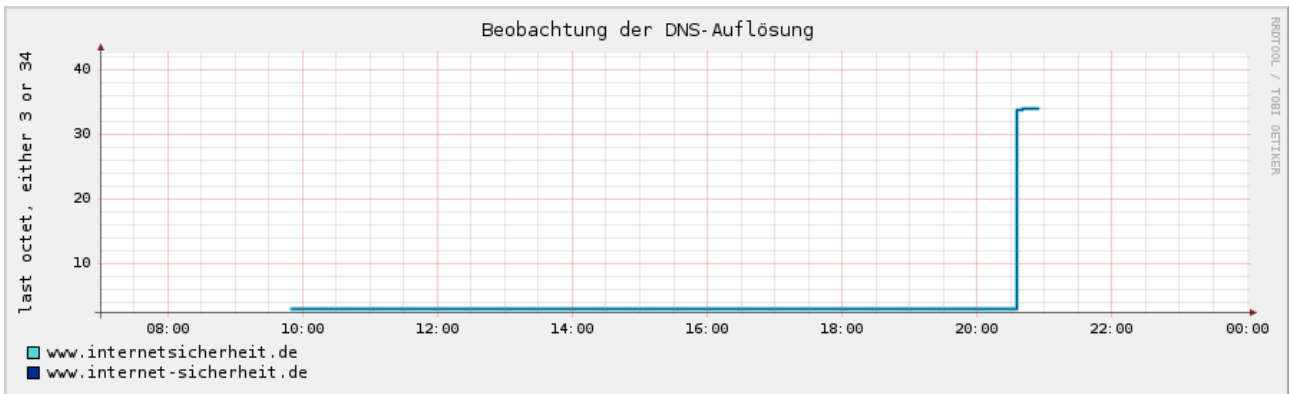
### Was sind die Beobachtungen?

Einige Beobachtungen der Sonden sind in den folgenden Graphen dargestellt.



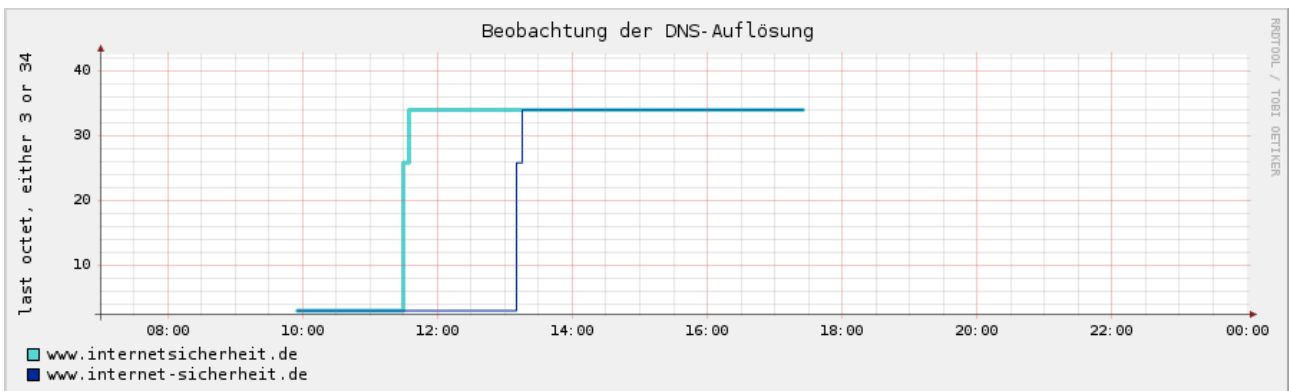
**Abbildung 1: Beobachtung der DNS-Auflösung am 08.09.2006, Provider 1**

Die x-Achse stellt die Zeit zwischen 08.09.2006, 7.00 Uhr und 09.09.2006, 0.00 Uhr dar. Auf der y-Achse wird der Wert des letzten Oktetts der IP-Adresse dargestellt (entweder 3 oder 34).<sup>1</sup> Der Wechsel der IP-Adresse fand lediglich im letzten Oktett statt. Der Wert 3 entspricht somit der bisherigen IP-Adresse 194.94.127.3, der Wert 34 entspricht der IP-Adresse nach der Umstellung (194.94.127.34).



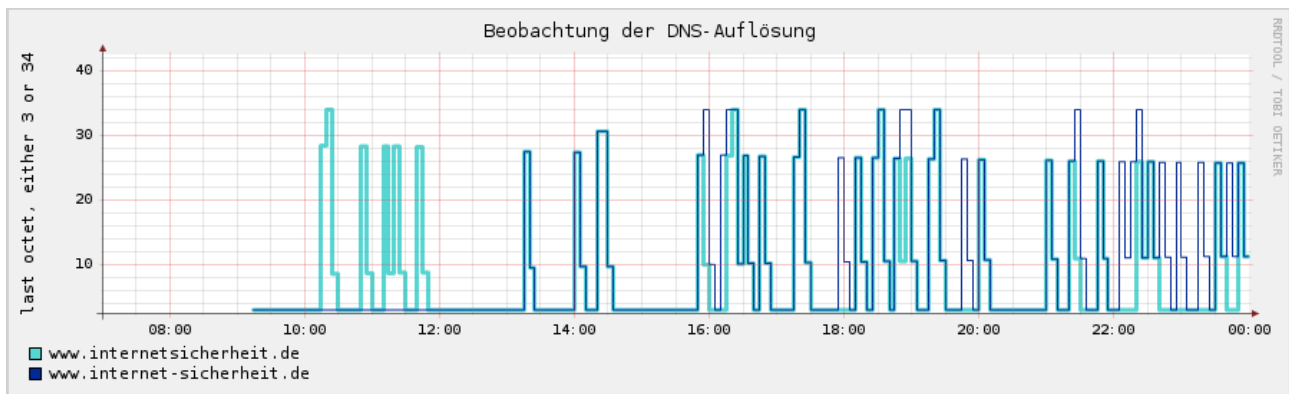
**Abbildung 2: Beobachtung der DNS-Auflösung am 08.09.2006, Provider 2**

In Abbildung 2 ist zu sehen, dass sich die Änderung beider Hosts zum gleichen Zeitpunkt (etwa 20:30 Uhr) ausgewirkt hat.



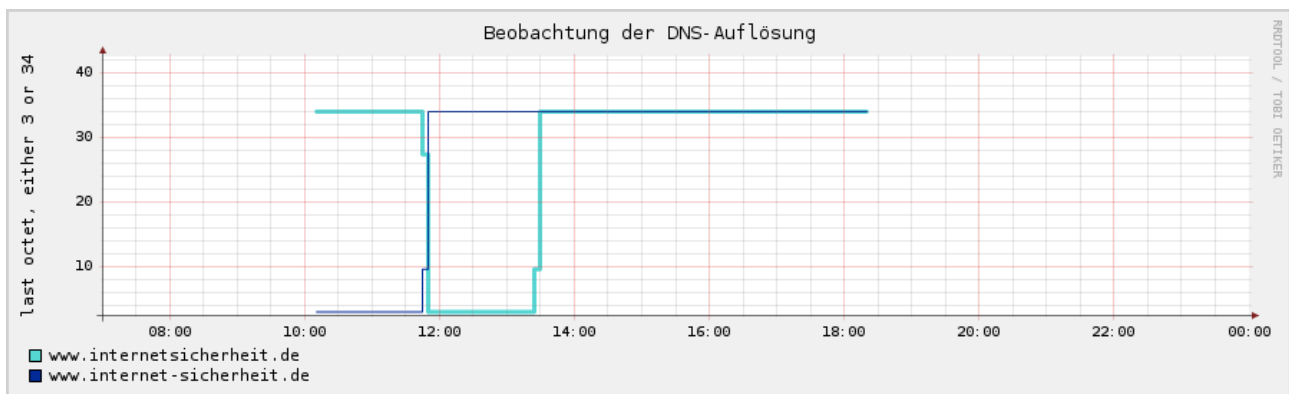
**Abbildung 3: Beobachtung der DNS-Auflösung am 08.09.2006, Provider 3**

<sup>1</sup> Da rrdtool die Ergebnisse interpoliert sind die Zwischenwerte ( $3 < y < 34$ ) der Flanken nicht bedeutend, sondern es handelt sich entweder um den Wert 3 oder 34. [Anmerkung: Dies ist kein Manko des rrdtools, sondern liegt an der Zweckentfremdung des rrdtool. Wir haben es auf Grund der Visualisierungsfunktionalität eingesetzt.]



**Abbildung 4: Beobachtung der DNS-Auflösung am 08.09.2006, Provider 4**

Bereits auf den ersten Blick ist erkennbar, dass sich die Messwerte zwischen allen Providern deutlich unterscheiden. Selbst bei ISPs, die von der Unternehmensstruktur her verwandt sind, lassen sich kaum Gemeinsamkeiten feststellen. Ein auffälliges Resultat ist in Abbildung 4 zu erkennen. Hierbei handelt es sich um eine häufigen wechselnde DNS-Antwort, wie in der Einleitung beispielhaft beschrieben.



**Abbildung 5: Beobachtung der DNS-Auflösung am 08.09.2006, Provider 5**

Darüber hinaus fällt auf, dass sich die zurückgelieferten IP-Adressen der beiden Domänen internet-sicherheit.de und internetsicherheit.de – obwohl von einem DNS-Server betreut und zur selben Zeit umgestellt – zu gewissen Zeitpunkten unterscheiden.

So zeigt beispielsweise Abbildung 3 divergierende DNS-Antworten der beiden Domains zwischen ca. 11:30 und ca. 13:15 Uhr. Ein ähnliches Muster ist in Abbildung 5 erkennbar.

### Weiterführende Informationen

- <http://www.internet-sicherheit.de/glossar.html?title=Domain+Name+System>  
Begriff 'DNS' im Glossar des Instituts für Internet-Sicherheit
- <http://de.wikipedia.org/wiki/DNS-Caching>  
Wikipedia-Eintrag zum DNS-Caching
- <http://www.internet-sicherheit.de/strukturelle-analyse.html>  
Themenkomplex strukturelle Internet-Analyse im Institut für Internet-Sicherheit