

DNS-Resolver Quad9 wegen Urheberrechtsverletzung verurteilt

Das Landgericht Leipzig macht Quad9 zum Täter von Urheberrechtsverletzungen. Müssen DNS-Betreiber jetzt mit hohen Geld- oder Haftstrafen rechnen?



Markt + Trends | IT-Recht & Datenschutz

DNS-Server lösen Namen zu IP-Adressen auf und sind essenziell fürs Surfen. Wer nicht die Standard-Server der Provider nutzt, surft schneller und ohne Blockaden.

Durch eine viel beachtete Entscheidung des Landgerichts Leipzig hat der nicht kommerzielle DNS-Resolver Quad9 erneut

eine juristische Niederlage erlitten. Das Urteil erging auf eine Klage von Sony auf Sperrung des Zugangs zu Webseiten, auf denen sich urheberrechtswidrige Downloads befinden. Das Brisante an dem Urteil ist, dass Quad9 als Täter und nicht lediglich als Störer in die Verantwortung genommen wurde. Quad9 hat mit Unterstützung der Gesellschaft für Freiheitsrechte (GFF) Berufung gegen die Entscheidung angekündigt.

Der Rechtsstreit zwischen Sony und Quad9 läuft bereits seit 2021 und hatte seinen Anfang in einem einstweiligen Verfügungsverfahren vor dem Landgericht Hamburg. Dort unterlag Quad9 in erster Instanz. Das Berufungsverfahren vor dem Hanseatischen Oberlandesgericht ist noch nicht abgeschlossen. Das jetzige Urteil des Landgerichts Leipzig erging im Hauptsacheverfahren. Dreh- und Angelpunkt der Rechtsstreitigkeiten ist, ob sich ein DNS-Resolver auf die Haftungsprivilegierungen für Zugangsprovider berufen kann.

Die Leipziger Richter lehnten es ab, Quad9 überhaupt als Zugangsprovider einzustufen. Daher griffen die allgemeinen urheberrechtlichen Bestimmungen. Durch die Auflösung von Namen in IP-Adressen greift damit eine Haftung als Täter, wenn sich hinter den IP-Adressen urheberrechtswidrige Inhalte zum Download befinden, so die Richter. Ein Rechtsgutachten der Bayreuther Juraprofessorin Ruth Janal kommt zu einem anderen Ergebnis. Danach sei ein offener DNS-Resolver von einer Urheberrechtsverletzung weiter entfernt als ein Zugangsprovider.

Das Urteil stößt auf Kritik und dürfte die Gerichte noch über Jahre hinweg beschäftigen. Moniert wird, dass damit die urheberrechtliche Haftung völlig neutraler Infrastrukturdienste wie Quad9 sogar strenger als die sozialer Netzwerke wäre. Zudem gelte nach dem jüngst in Kraft getretenen Digital Services Act die Haftungsprivilegierung für Internetzugangsanbieter eindeutig auch für DNS-Resolver. Quad9 will das Urteil anfechten. *Tobias Haar* (fo@ix.de)

Schneller und ohne Sperren: Alternative DNS-Server einsetzen

DNS-Server lösen Namen zu IP-Adressen auf und sind essenziell fürs Surfen. Wer nicht die Standard-Server der Provider nutzt, surft schneller und ohne Blockaden.



Schneller und ohne Sperren: Alternative DNS-Server einsetzen

DNS-Server lösen Namen zu IP-Adressen auf und sind essenziell fürs Surfen. Wer nicht die Standard-Server der Provider nutzt, surft schneller und ohne Blockaden.

Bevor ein Browser eine Internetseite anfragen kann, muss er die Adresse, die der Nutzer eingetippt hat, erst auflösen – über das Domain Name System, kurz DNS. Ein DNS-Server funktioniert wie ein Adressbuch, in dem ein Name wie heise.de einer IP-Adresse zugeordnet ist. Ohne zügige Namensauflösung ist zügiges Surfen also nicht möglich.

In einem typischen Heimnetzwerk ist der primäre DNS-Server für die Geräte der Router – doch der kennt nicht alle IP-Adressen der Welt. Bekommt er eine Frage, die er nicht beantworten kann, reicht er die Frage an einen öffentlichen DNS weiter. Wer nichts weiter unternimmt und den Router nach Anweisungen seines Internetanbieters eingerichtet hat, nutzt als öffentlichen DNS-Server einen Dienst des Providers. Doch es gibt Alternativen und gute Gründe, einen anderen DNS-Server als den des Providers einzutragen.

Netzsperrern

Die DNS-Server von deutschen Providern liefern nicht immer die Wahrheit, die im DNS hinterlegt ist. Bei Internetseiten, deren hauptsächliches Ziel es ist, urheberrechtlich geschütztes Material widerrechtlich zu verbreiten (vor allem Filme, Livesport und Musik), leiten die DNS-Server die Anfragen auf eine Seite der [„Clearingstelle Urheberrecht im Internet“ \(CUII\)](#) um. Die Juristen der CUII nennen solche Seiten „strukturell urheberrechtsverletzend“. Kritiker befürchten seit der Einführung solcher Netzsperrern, dass sie auch für Zensur unliebsamer Inhalte genutzt werden könnten. Die Seiten sind aber gar nicht wirklich gesperrt – der Provider-DNS verrät nur einfach nicht die richtige Adresse.

Ende März 2023 bewies Provider 1&1, wie gefährlich Manipulationen am DNS sein können. Durch einen technischen Fehler landete die Adresse [heise.de bei einigen Nutzern auf der Liste für CUII-Sperrern](#). Statt des Newstickers sahen sie eine Sperrseite. Der Fehler wurde schnell beseitigt, beweist aber, dass fälschliche Sperrern kein theoretisches Problem

sind.

Wer mit solchen Sperren und potenzieller Zensur nichts zu tun haben will, greift zu einem alternativen DNS-Anbieter aus dem Ausland, dort hat die CUII keinen Einfluss. Doch es geht auch andersherum: Einige alternative DNS-Server haben bewusst eigene Netzsperrungen eingebaut. Sie filtern zum Beispiel für Kinder ungeeignete Inhalte oder Adressen, die im Zusammenhang mit Schadsoftware aufgefallen sind. In Umgebungen mit Kindern (zu Hause oder zum Beispiel in der Schule) kann das sinnvoll sein. Welcher Anbieter für Sie infrage kommt, lesen Sie im Abschnitt „Alternativen“.

Geschwindigkeit

Die Namensauflösung per DNS ist für die gefühlte Internetgeschwindigkeit mindestens so wichtig wie die Auslieferung der Daten selbst. Eine Gedenksekunde vorm Besuchen einer Website braucht niemand. Und bei der Geschwindigkeit sind die Provider-DNS-Server nicht gerade Spitzenklasse. Zwar sind Messungen von DNS-Geschwindigkeiten immer mit Vorsicht zu genießen und fast jeder der alternativen Anbieter sagt über sich, dass er am schnellsten auflösen kann. Die Erfahrung zeigt aber: DNS-Anbieter wie Google, Quad9 und Cloudflare (dazu später mehr) lösen im Schnitt schneller auf als die Server der Provider. Besonders in Stoßzeiten holt man mit einem solchen Anbieter etwas Geschwindigkeit heraus.

So geht es

Den DNS-Anbieter fürs eigene Netz zu wechseln, ist in wenigen Minuten erledigt und funktioniert fast in jedem Router gleich. Suchen müssen Sie nach einem Punkt, der Interneteinstellungen heißt. Dort gibt es meist einen Haken, um die Standard-Server des Providers zu nutzen, darunter zwei Felder für eigene IP-Adressen. Der Hintergrund: Fällt mal ein Server aus, greift der Router zum zweiten. Sie bekommen davon gar nichts mit. Eine sinnvolle Strategie kann es sein, als zweiten Server eine

Adresse eines anderen Anbieters zu nutzen. Das reduziert die Wahrscheinlichkeit für Ausfälle ungemein.

In der in Deutschland verbreiteten Fritzbox finden Sie die Einstellung unter dem Menüpunkt Internet/Zugangsdaten/DNS-Server.

The screenshot shows the 'Internet > Zugangsdaten' (Internet > Access Data) configuration page in a Fritzbox. The 'DNS-Server' tab is selected. A help icon (?) is visible in the top right. Below the navigation tabs, a text block explains that DNS is used for resolving internet addresses and that users can choose between the provider's servers or other DNS servers. The 'DNSv4-Server' section has two radio buttons: 'Vom Internetanbieter zugewiesene DNSv4-Server verwenden (empfohlen)' (selected) and 'Andere DNSv4-Server verwenden'. Below are input fields for 'Bevorzugter DNSv4-Server' (8 . 8 . 8 . 8) and 'Alternativer DNSv4-Server' (1 . 1 . 1 . 1). The 'DNSv6-Server' section also has two radio buttons: 'Vom Internetanbieter zugewiesene DNSv6-Server verwenden (empfohlen)' and 'Andere DNSv6-Server verwenden'. Below are input fields for 'Bevorzugter DNSv6-Server' (2001:4860:4860::8888) and 'Alternativer DNSv6-Server' (2606:4700:4700::1111).

Schnell geändert: In der Fritzbox stellt man den DNS-Server für das Heimnetz unter Internet/Zugangsdaten/DNS-Server um.

Alternativen

Den Markt mit alternativen DNS-Servern aufgemischt hat Google, indem das Unternehmen die sehr leicht zu merkenden Adressen 8.8.8.8 und 8.8.4.4 für DNS-Server eingesetzt haben. Wie immer bei Google gilt: Das Angebot ist solide und sehr schnell, im Gegenzug muss man aber damit leben, dass Google die Nutzung protokolliert und analysiert.

Nach Google stieg ein anderes US-Unternehmen ins Rennen ein: Cloudflare bietet für Unternehmen zahlreiche kommerzielle Dienstleistungen im Netz an, kostenlos sind seine DNS-Server unter den Adressen 1.1.1.1 und 1.0.0.1. Cloudflare selbst gibt an, dass es keine Logs anfertigt, wer welche Seiten aufgelöst hat. Von Cloudflare gibt es noch zwei weitere Angebote: 1.1.1.2 (und 1.0.0.2 als Reserve) filtern Malware-verbreitende

Seiten. 1.1.1.3 (und 1.0.0.3) filtern Malware und Erwachseneninhalte.

Eine europäische Alternative ist Quad9, betrieben von einer Stiftung aus der Schweiz. Deren IP-Adresse lautet 9.9.9.9 (und 149.112.112.112 als Reserve). Ebenfalls aus Europa kommt das Projekt DNS.Watch mit der IP-Adresse 84.200.69.80 (und 84.200.70.40 als Reserve). Eine Rechtsform hat das Projekt nicht, auch die Macher treten nicht in Erscheinung – offenbar Schutzmaßnahmen, um nicht zu Sperrern wie die durch die CUII gezwungen werden zu können.

Anbieter	Sitz	Erste IPv4	Alternative IPv4	Erste IPv6	Alternative IPv6
Cloudflare	USA	1.1.1.1	1.0.0.1	2606:4700:4700::1111	2606:4700:4700::1001
Google	USA	8.8.8.8	8.8.4.4	2001:4860:4860::8888	2001:4860:4860::8844
Quad9	Schweiz	9.9.9.9	149.112.112.112	2620:fe::fe	2620:fe::9
DNS.WATCH	Deutschland	84.200.69.80	84.200.70.40	2001:1608:10:25::1c04:b12f	2001:1608:10:25::9249:d69b

In der Tabelle sehen Sie die Adressen der DNS-Anbieter in der Übersicht. Wenn Sie per IPv6 surfen und Ihr Router auch Felder für IPv6-DNS-Server hat, finden Sie die passenden Adressen in den letzten beiden Spalten.