Fefes Blog - DNS 1.1.1.1

Originalartikel

Backup

<html> [l] Old and busted: 8.8.8.8. New hotness: 1.1.1.1 Von der Performance her nehmen die sich nicht viel, beide antworten viel schneller als übliche DNS-Resolver von Internet-Providern. Aber lasst euch mal nicht von dem „privacy-first“-Blablah täuschen. Das ist eine Behauptung, ein Versprechen. Google verspricht Ähnliches für 8.8.8.8. Der DNS-Server kann alles sehen, was ihr an Anfragen ins Netz stellt, und sieht damit, was man seit Snowden bei Telefonen „die Metadaten“ nennt. Wer seine DNS-Daten ohne Not in fremde Hand gibt, gibt damit seine Privatsphäre weitgehend auf. Ich rate also entschieden davon ab, irgendeinen (gar zu einer ausländischen Organisation gehörende) DNS-Server zu verwenden — schon gar nicht aus Five-Eyes-Staaten. OK, was sind die Alternativen? Den ISP-DNS benutzen. Das hat den Nachteil, dass die oft langsam sind, gerne mal ausfallen, und dass man möglicherweise auch nicht will, dass die Daten beim ISP anfallen. Letzteres kann man nur mit einem VPN verhindern (wobei dann der VPN-Endpunkt alle Daten sieht und zuordnen kann; auch nicht besser!) oder einem Anonymisierungsdienst wie Tor verhindern. Ich persönlich betreibe einen eigenen Resolver in meinem Netz. Man muss sich aber im Klaren sein, dass auch am Anfang einer TLS-Verbindung noch der Name der Site im Klartext dransteht, d.h. auch ohne DNS kann jemand, der den Traffic sieht, sehen, mit welchem Host du zu reden versuchst, selbst wenn hinter der IP ganz viele Sites hängen. Besserung war glaube ich für TLS 1.3 geplant, hier ist ein aktueller Draft dazu, aber scheint es nicht in den Standard geschafft zu haben…? Und das hat auch andere Probleme, wenn man das zumacht. Im Moment kann man einen Load Balancer bauen, der den TLS durchreicht, und der das richtige Backend am SNI erkennt (wo der gewünschte Servername steht), und dann wird der TLS im Backend terminiert. Das ist viel besser als wenn man den TLS im Load-Balancer terminiert und dann zum Backend unverschlüsselt kommuniziert. Ein Angreifer, der den Load Balancer übernimmt, kann dann alle Anfragen sehen. Wenn man das beibehalten will, muss man sich ziemlich verbiegen. Ihr könnt ja selber man kurz in den Draft gucken. Also, kurz gefasst: Seine DNS-Anfragen über irgendeine amerikanische Cloud-Klitsche routen, ist eine sehr schlechte Idee für eure Privatsphäre. Aber es selber zu machen hilft leider auch nicht so viel, wie man hoffen würde. Ich finde bei sowas immer, dass man NSA und co ja nicht noch freiwillig entgegenkommen muss. Oh und richtig geil wäre das erst, wenn DNS verschlüsselt wäre. Es gibt da was mit TLS für DNS, aber das ist hochkomplex, eine riesige Angriffsoberfläche und erhöht die Netzwerklatenz deutlich. Cloudflare bietet das an. Aber das würde halt nur den Weg von euch zu Cloudflare schützen. Bei Cloudflare könnte die NSA immer noch alles abgreifen. Update: Leser berichten, dass einzelne ISPs gar keinen DNS-Resolver mehr betreiben sondern ihren Kundern per DHCP 8.8.8.8 setzen. Das ist aus meiner Sicht ein starker Anreiz, sich schnell einen anderen ISP zu suchen. </html>