Experimentelles Internetprotokoll DNS over HTTPS

Verriegelt

Monika Ermert

Das uralte Domain Name System (DNS) erfüllt die Anforderungen an Sicherheit und Datenschutz nicht mehr. Abhilfe schafft es, DNS-Anfragen mit TLS zu verschlüsseln oder in HTTPS zu verpacken.

Die Idee ist nicht neu: Als das von der damaligen Familienministerin Ursula von der Leyen mit Nachdruck vorangetriebene Zugangserschwerungsgesetz 2010 verabschiedet worden war, schlugen dessen Gegner vor, DNS-Anfragen via HTTPS zu tunneln (DNS over HTTPS, DoH), um Zugriffsbeschränkungen à la von der Leyen zu entgehen. Dabei fanden DNS-Abfragen einfach über den Port 443 statt – eine zulässige Nutzung des Webtransportprotokolls.

Idee von Google und Mozilla

Der DNS-Verkehr läuft in diesem Fall per HTTPS-verschlüsselter Verbindung über einen Webserver zu unzensierten DNS-Servern. Die Aktivisten nahmen an, dass ein Knacken der HTTPS-Verschlüsselung die Möglichkeiten staatlicher Organe übersteigt. Der Gesetzgeber hätte folglich sämtliche unliebsamen Webangebote beseitigen lassen müssen und nicht nur die DNS-Referenzen darauf.

Ursula von der Leyens Gesetz, vielfach auf spöttische Weise mit einem Stoppschild verglichen, verschwand jedoch schnell wieder in der Versenkung. Es wurde 2011 offiziell rückabgewickelt und auch um DoH kehrte wieder Ruhe ein – bis Google im Jahr 2016 einen eigenen Vorschlag einbrachte.

Für die Nutzung von DNS-Erweiterungen wie DANE (DNS-based Authentication of Named Entities, eine DNS-basierte Alternative zur Herstellung und Hinterlegung von Zertifikaten für die Transportverschlüsselung) oder DNS-basierte Services Discovery (DNSSD) müssen Web-Apps heute auf Browsererweiterungen zurückgreifen. Alles, was über das reine Umsetzen von Domainnamen zu IPv4- oder IPv6-Adressen hinausgeht, lässt Applikationen immer wieder stolpern.

Mit dem Verpacken von DNS-Abfragen in HTTP-Pakete hätten die Webentwickler dagegen einfachen Zugriff auf die neueren DNS-Entwicklungen, erklärt Paul Hoffman von der Internet Corporation for Assigned Names and Numbers (ICANN). Hoffman hat zusammen mit Patrick McManus von Mozilla die Spezifikation geschrieben, die bei der Internet Engineering Task Force (IETF) zur Standardisierung ansteht.

Hoffmans und McManus' Entwurf geht über das schlichte Tunneln von DNS-Verkehr via HTTPS hinaus. Die DNS-Anfrage wird vielmehr zur URL und die Antwort zu einem Webobjekt, gegebenenfalls im Cache. Der Browser wirkt also praktisch als DNS-Resolver. Auch andere HTTP-Features wie Redirection, Proxying, Authentifizierung und Kompression ermöglicht das DoH-Konzept. HTTP wird das neue Transportprotokoll für DNS, für klassischen DNS-Verkehr genauso wie für Apps, die das DNS benötigen.

Die Arbeitsgruppe diskutierte zuletzt, wie sich die DNS-Anfragen „einpacken" lassen sollten (per GET oder POST), doch war man sich dabei schnell einig: Server müssen beides implementieren, um den Standard zu erfüllen – Clients können wählen.

```
:method = GET
:scheme = https
:authority = dnsserver.example.net
:path = /dns-query?dns= ⤷
   AAABAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB
accept = application/dns-message
:method = POST :scheme = https :authority = ⤷
dnsserver.example.net :path = /dns-query accept = ⤷
application/dns-message content-type = ⤷
application/dns-message content-length = 33
```

Nicht einmal ein Jahr Zeit hat sich die IETF-Arbeitsgruppe zum Abstimmen der Details genommen. Nun folgt die bei der IETF übliche Begutachtung durch die Internet Engineering Steering Group und noch 2018 dürfte das Dokument eine RFC-Nummer erhalten. Für IETF-Verhältnisse ist das ziemlich schnell und es verdeutlicht das große Interesse etlicher Anwender.

Fünf DoH-Server gibt es bereits, etwa von Google und Mozilla, berichtete der französische DNS-Experte Stéphane Bortzmeyer von AFNIC auf dem 101. Treffen der IETF im Frühjahr 2018 in London. Drei davon sind schon online und alle arbeiten mit unterschiedlicher DNS-Software. Vier von fünf basieren auf Open-Source-Software – im DNS-Bereich typisch. So schnell werden neue Implementierungen selten realisiert.

Mit einem weiteren Pfund wuchern die Befürworter, darunter Mozilla und Google, noch mehr als mit dem Interesse der Webwelt: Wie Frau von der Leyens Gegner streichen sie vor allem das Datenschutzargument heraus. HTTP in seiner mit TLS abgesicherten Form, die der Standard vorschreibt, kann den DNS-Verkehr vertraulicher machen.

Mehr Vertraulichkeit für das DNS und diverse andere Protokolle genießt bei der IETF seit den Enthüllungen von Edward Snowden hohe Priorität. Bereits seit 2016 ist eine TLS-gesicherte DNS-Variante standardisiert (DNS over Trans-

port Layer Security, RFCs 7858 und 8310 – kurz DoT), die ebenso wie DoH die Verbindung zwischen dem Rechner des Nutzers – genauer gesagt dem Stub Resolver – und dem DNS-Service TLS-verschlüsselt. Gängige DNS-Software beherrscht das schon.

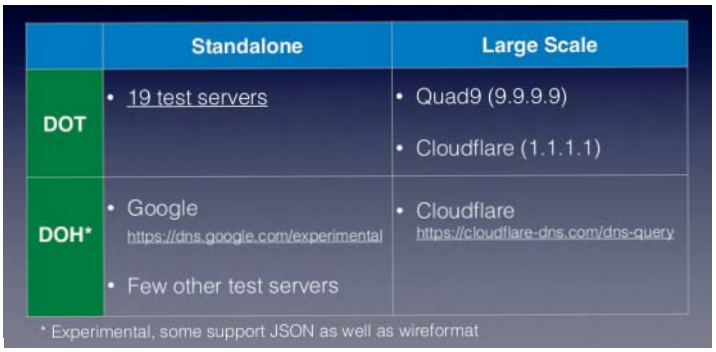
Stiftet die Parallelentwicklung DoH da nicht Verwirrung? Geoff Huston, Forscher bei APNIC, der IP-Adressvergabestelle für Asien und Australien, zeigt sich skeptisch gegenüber den Vorzügen des nachgeschobenen DoH. „Wo ist der Gewinn?“, fragte Huston in einem Blogbeitrag. TLS bringe eh Sicherheit und mehr Vertraulichkeit. Die zusätzliche Verpackung in HTTP sei „unnötige Kosmetik“. Bis auf den schieren „Thrill“, ein Protokoll in einem anderen zu verstecken, sieht er keine Vorteile von DoH.

Ist eines der beiden Protokolle besser in puncto Vertraulichkeit? Grundsätzlich verbergen beide Standards die Inhalte von DNS-Anfragen und -Antworten auf dem Weg durchs Netz vor den Augen neugieriger Dritter, sagt Sara Dickinson, Chefentwicklerin des DoT-Clients „Stubby“. Auch das Sammeln von Informationen beim Anbieter der Anwendung kann datensparsam sein, urteilt Dickinson: Wenn App oder Browser ohnehin auch die DNS-Anfragen abwickeln, müssen diese nicht noch über einen weiteren Anbieter laufen. Praktisch gesprochen: Da Twitter sowieso weiß, welchen Inhalt man abruft, kann der Anbieter die zugehörigen DNS-Anfragen gleich mit erledigen.

Wenn Twitter die DNS-Anfragen zu Links in den Beiträgen seiner Anwender selbst auflöst, tut das also aus Datenschutzsicht nicht weh. Implementierungen wie diejenigen im Firefox, die DoH-Anfragen nicht selbst auflösen, sondern vielmehr zu einem voreingestellten externen DNS-Server senden, etwa Google oder – wie im Fall Mozilla – Cloudflare, machten diesen Vorteil aber wieder zunichte.

Trotzdem könnte DoH am Ende das Rennen machen. Es bietet nämlich einen praktischen und marktrelevanten Vorteil: DoH lässt sich von gewöhnlichem HTTPS-Webverkehr auf Port 443 nicht unterscheiden, also nicht so leicht blockieren wie DoT, das durch den Port 853 auf sich aufmerksam macht und leicht an darauf angesetzten Filtern oder konservativ konfigurierten Routern scheitern kann. Für DoT müssen zudem die Endgeräte eigens angepasst werden.

Einen prominenten Abnehmer auf Endgeräteseite hat DoT mit Android zwar schon gefunden. Mitte April bestätigte Google-Entwickler Eric Kline die seit Längerem laufenden Vorarbeiten und kündigte an, dass Android-Geräte künftig standardmäßig auf DNS over TLS umschalten werden, wenn der verwendete DNS-Server die verschlüsselten DNS-Anfragen beantworten kann.



Quelle: Sara Dickinson, Sinodun

Neben DNS over TLS (DoT), Internetstandard seit 2016, schickt sich nun DNS over HTTPS (DoH) an, DNS-Verkehr vor Zugriffen Dritter zu schützen.

Doch an Clients für macOS, Windows und Linux arbeitet zurzeit nur die hartnäckige Entwicklergruppe rund um Dickinsons kleine Softwarefirma Sinodun, samt deren niederländischem Sponsor nlNet Labs. Bis zum massenhaften Einsatz von „Stubby“ könnte es also noch dauern. Wenn die großen Browseranbieter Google und Mozilla DoH einschalten, bleibt für DoT wohl allenfalls eine Nische.

Die eigentliche Frage lautet für Experten wie Dickinson, wie DoH das zur Internetinfrastruktur gehörende DNS verändern wird. Die Übergabe der DNS-Auflösung an die App oder den Browser macht die Sache für die Anwender recht intransparent. Statt dass sie selbst einen datenschutzfreundlichen DNS-Provider – etwa das neue Quad9 – aussuchen können, entscheidet die jeweilige Anwendung. Und je nach Browser oder App kommen unterschiedliche DNS-Dienste zum Einsatz.

Die HTTP-Verpackung der DNS-Anfragen verlagert damit eine zentrale Gerätefunktion weiter in die Anwendungen – mit all den Nachteilen für die Administrierbarkeit. So sieht es Peter Koch, DNS-Experte der DENIC eG. Die Kontrolle darüber, was eigentlich noch im eigenen Endgerät passiert und was die Anwendung an sich gezogen hat, wird fast unmöglich. Die reine Lehre von der Trennung der Protokollebenen gilt nicht mehr. Allein schon die Fehlersuche, mahnt Koch, könnte angesichts der gewachsenen Komplexität zur Herausforderung werden.

Auch eine fortschreitende Konzentration des DNS bei wenigen großen Anbietern, ähnlich zur Entwicklung im E-Mail-Markt, ist aus Sicht der Experten eine fast unweigerliche Folge. „Natürlich“, antwortet Huston, „indem man DNS dem verschlüsselten Webverkehr beimischt, stellt man den ISP als klassischen DNS-Provider außer Dienst.“ Im Hinblick auf den Datenschutz wirkt die Konzentration auch nicht eben fortschrittlich. Google als Browser-, App- und nun auch DNS-Server-Betreiber sammelt dann nur noch mehr Daten. Schon jetzt nutzen laut Hustons Zahlen rund 40 Prozent aller Anwender Googles DNS.

Kein Ende des DNS in Sicht

Das Ende des DNS scheint trotzdem noch nicht gekommen. Die Root, die autoritativen Nameserver und die Anfragen quer durch die Hierarchie bleiben ohne jede Verschlüsselung. Auch grundsätzliche Überlegungen zu einem DNS-Nachfolger, wie sie kürzlich der ehemalige Vorsitzende des Internet Architecture Board und langjährige IETF-Teilnehmer John Klensin forderte, sind vorerst eher ein Ausdruck von Unbehagen gegenüber der wachsenden Unübersichtlichkeit des DNS als ein wirklicher Neuanfang.

Zumindest könnte eine fortschreitende Konzentration im Markt der DNS-Anbieter Überlegungen anstoßen, die Strecken zwischen den DNS-Resolvern und den autoritativen Nameservern respektive Root-Servern sicherer zu gestalten. Wenn es nur noch so wenige zentrale DNS-Abnehmer gibt, ließen sich beispielsweise auch diese Strecken leichter verschlüsseln.

Auf eines müssen sich die DoH-Implementierer jedenfalls einstellen: Nicht nur von der Leyens ehemalige Gegner haben erkannt, dass sich verschlüsselter DNS-Verkehr einer lokalen Filterung entzieht. Beim IETF-Treffen in London wurde wie in der großen Debatte um Nachschlüssel für TLS bereits angemahnt, dass man die DNS-Firewall vielleicht doch retten müsse. (un@ix.de)

Monika Ermert

ist freie Journalistin mit dem Schwerpunkt Internet-Politik.

Alle Links: ix.de/ix1807096