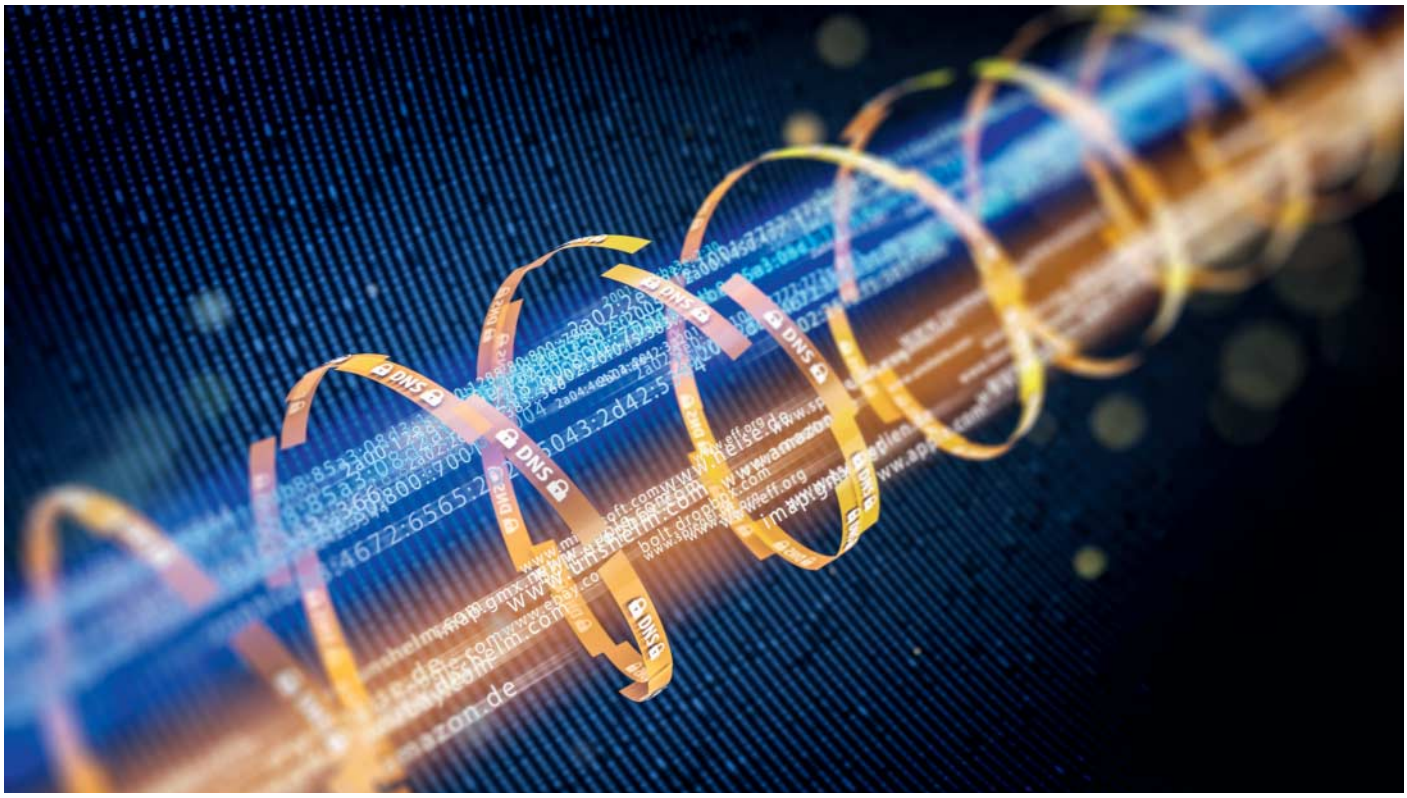


Private Auskunft

DNS mit Privacy und Security vor dem Durchbruch

Wer sich mal richtig gruseln will, befasst sich mit den Missbrauchsmöglichkeiten von DNS. Das Telefonbuch des Internet stammt nämlich aus der Zeit, als dort jeder jedem vertraute. Jetzt steht endlich die längst überfällige Grunderneuerung an: Neue Standards sollen Privatsphäre und Sicherheit verbessern und werden in Rekordzeit umgesetzt.

Von Carsten Strotmann und Jürgen Schmidt

Das Domain Name System (DNS) ist ein ganz zentrales Element des Internet und in Sachen Sicherheit und Privatsphäre absolut kritisch. Wer DNS-Kommunikation mitlesen kann, sieht unter anderem, welche Internet-Dienste ich nutze. Und wer sie manipulieren kann, ist in der Lage, beliebige Internet-Zugriffe umzuleiten, also mich etwa beim Zugriff auf die Webseite meiner Bank auf eine Phishing-Seite zu schicken, die meine Zugangsdaten zum Online-Banking abgreift.

Das ist erschreckend einfach und passiert ganz real. Sowohl beim Angriff auf die virtuelle Krypto-Geldbörse myethereumwallet.com im April 2018 als auch beim BGP-Hijacking des Cloudflare Resolver 1.1.1.1 im Mai 2018 missbrauchten Angreifer das DNS. 2016 erlangten Kriminelle für mehrere Tage die Kontrolle über die Online-Banking-Seiten einer brasilianischen Bank, indem sie deren DNS-Einträge manipulierten.

Und natürlich werden die öffentlich einsehbaren DNS-Abrufe in großem Stil auf Vorrat gespeichert. Viele Terabyte-große Datenbanken im Besitz diverser Nachrichtendienste und Sicherheitsfirmen dokumentieren minutiös, wer wann welche Internet-Adressen abgerufen hat.

Das ist die direkte Folge dessen, dass DNS in Sachen Sicherheit über Jahrzehnte hinweg als ungeliebtes Stiefkind behandelt wurde. Zwar gibt es eine Sicherheitserweiterung namens DNSSEC. Doch die hat sich nach mehr als zehn Jahren immer noch nicht flächendeckend durchgesetzt. Das liegt daran, dass sie zum einen als kompliziert verschrien ist und zum anderen längst nicht alle drängenden Probleme des Namensdienstes löst.

Doch jetzt tut sich endlich etwas Entscheidendes bei DNS und Sicherheit. Mit „DNS over TLS“ und „DNS over HTTPS“ werden derzeit zwei neue Standards durch die Standardisierungsgremien gepeitscht und parallel dazu auch schon aktiv eingesetzt. Ihre absehbar größere Verbreitung schon in den kommenden Monaten bringt endlich deutliche Verbesserungen in Sachen Privatsphäre und Sicherheit.

Oldtimer DNSSEC

Die Domain Name System Security Extensions, kurz DNSSEC, sind der älteste Versuch, das DNS abzusichern. Die Anfänge reichen zurück bis in das Jahr 1990 und seit etwa 2006 wird DNSSEC aktiv im Internet eingesetzt. Das Prinzip ist einfach: Kryptografische Signaturen schützen die DNS-Daten vor Manipulationen. Hat ein DNS-Administrator seine Zone signiert, können alle DNSSEC-Nutzer die

Echtheit einer DNS-Auskunft verifizieren. Der Empfänger prüft die Signaturen und benutzt die Daten nur, wenn die Signatur mit den Daten übereinstimmt. Dabei ist es nicht relevant, auf welchem Weg er diese DNS-Informationen bekommen hat – eine Eigenschaft, die sich neuere Standards zunutze machen.

DNSSEC verbessert allerdings die Privatsphäre der Internet-Nutzer nicht. Alle DNS-Daten werden weiterhin unverschlüsselt versendet und können unterwegs mitgelesen und auch archiviert werden. Auch die Möglichkeit zur Manipulation von DNS-Daten schafft DNSSEC nicht völlig aus der Welt.

Denn in aller Regel werden die DNS-Daten bestenfalls auf dem sogenannten Resolver geprüft. Bestenfalls deshalb, weil die meisten Anwender dafür einfach den Nameserver ihres Internet-Providers benutzen und etwa Telekom und Kabel Deutschland immer noch keine DNSSEC-Validierung durchführen. Ob Ihr Provider DNS-Daten validiert, können Sie etwa beim „Connection Test“ auf https://internet.nl prüfen.

Doch selbst wenn der genutzte Nameserver DNSSEC einsetzt: Da kaum ein Betriebssystem (mit der lobenswerten Ausnahme von Fedora Linux mit Unbound) DNSSEC unterstützt und auch die typischen Router dies nicht anbieten, bleibt die letzte Meile der Internet-Verbindung ungesichert. Wer als Man-in-the-Middle im Provider-Netz zwischen dem Nameserver und dem Browser des Anwenders Daten manipulieren kann, kann nach wie vor falsche DNS-Einträge einschleusen.

Trotz der langen Vorlaufzeit ist der Verbreitungsgrad von DNSSEC nicht gerade berauschend. So sind zwar mittlerweile die DNS-Root-Zone und auch die meisten Top-Level-Domains DNSSEC-signiert. Bei den letztlich entscheidenden Second-Level-Domains wie „heise.de“ liegt die Quote immer noch nur im niedrigen einstelligen Prozentbereich.

Das liegt vor allem am schlechten Ruf des DNSSEC: „Zu kompliziert und kleine Fehler können zum Totalausfall des DNS führen“, lautet das Verdikt. Das war 2006 durchaus gerechtfertigt; doch mit aktuellen DNS-Servern braucht eigentlich kein Admin mehr Angst vor dem Einsatz von DNSSEC zu haben. Und wer DNSSEC nicht selbst betreiben will, kann sich an DNS-Hoster wie IronDNS oder Cloudflare wenden.

DNS over TLS

Der noch recht junge Standard DNS over TLS (DoT, RFC 7858) soll drei Probleme von DNS und DNSSEC lösen: Es soll die Privatsphäre der Anwender gegen Lauscher schützen, das Einschleusen manipulierter DNS-Informationen verhindern und nebenbei auch noch den Denial-of-Service-Attacken via DNS ein Ende setzen.

Das Prinzip von DoT ist einfach: Statt wie bisher über völlig ungesicherte UDP-Kommunikation ruft der Client des Anwenders die DNS-Informationen über eine TCP-Verbindung zum Resolver ab, die via Transport Layer Security authentifiziert und verschlüsselt ist. So kann der Client (hoffentlich) DNSSEC-validierte Daten vom Nameserver beziehen, ohne dass Dritte mitlesen; DoT und DNSSEC ergänzen sich dabei also.

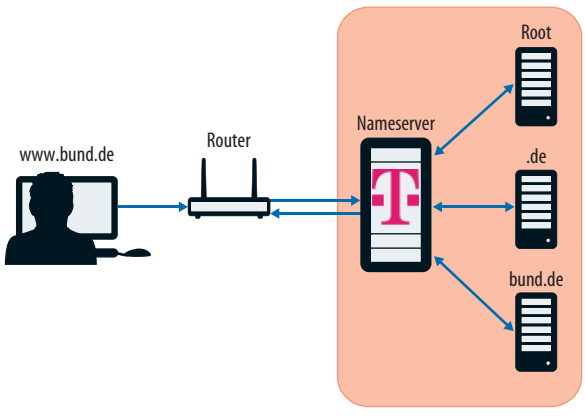
Dass die Namensauflösung des Resolvers im Klartext erfolgt, stört dabei nur wenig, weil der Urheber der Anfragen nicht mehr ersichtlich ist. Dass etwa irgendein Telekom-Kunde die Webseite der Deutschen Aids-Hilfe besuchen wollte, ist nicht mehr Privacy-relevant. Trotzdem gibt es auch bereits Pläne, die Kommunikation zwischen DNS-Resolvern und zuständigen DNS-Servern via DoT zu sichern.

Konkret läuft DoT über den TCP-Port 853; DoT-fähige Clients versuchen zuerst, die DNS-Namensauflösung darüber. Ist dieser Dienst nicht verfügbar, benutzen sie – abhängig von den Sicherheitseinstellungen des Systems – in aller Regel das klassische, unsichere DNS auf UDP-Port 53.

In der Praxis hat DoT mit zwei Handicaps zu kämpfen: Man kann sich nicht darauf verlassen, dass TCP-Verbindungen auf Port 853 das Netz ungehindert passieren. Firmen-Firewalls, aber auch Port-Filter in Hotels oder an öffentlichen Hotspots dürften diesen noch recht unbekannten Port häufig blockieren. Dann bleibt nichts anderes übrig, als auf herkömmliches, ungesichertes DNS via UDP-Port 53 zurückzufallen. Außerdem bringt TCP, noch dazu in Kombination mit TLS, einiges an Verwaltungs-Overhead mit sich, der die für zügiges Surfen elementare Namensauflösung einbremst.

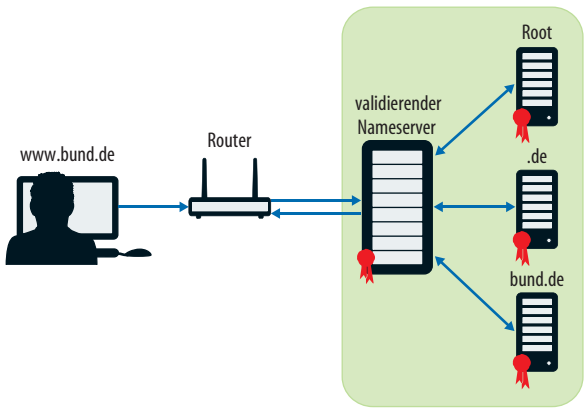
DNS

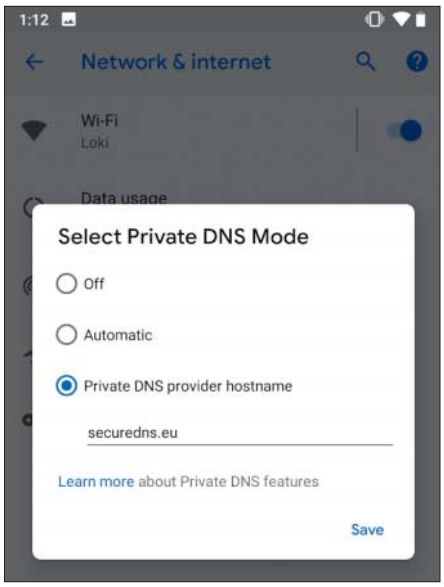
Beim herkömmlichen Domain Name System gehen alle Daten im Klartext über das Netz. Sie sind leicht zu überwachen und zu fälschen.



DNSSec

Bei DNSSec sind die DNS-Daten immerhin digital signiert, aber immer noch im Klartext. „Die letzte Meile“ vom Name Server des Providers zu dessen Kunden bleibt völlig ungesichert.





Das für August erwartete Android P beherrscht bereits von Haus aus DNS over TLS.

Um diesen Effekt zu reduzieren, werden über eine einmal geöffnete DoT-Verbindung möglichst viele DNS-Abfragen abgewickelt. So fällt der „teure“ Verbindungsaufbau von TCP und TLS nicht mehr so sehr ins Gewicht. Mit der aktuellen TLS-Version 1.2 verbleiben dennoch messbare Performance-Einbußen. Doch die im März von der IETF verabschiedete TLS-Version 1.3 bringt neue Optimierungen (0-RTT, asynchrone Kanäle), welche DoT nahe an die Geschwindigkeit des klassischen DNS heranbringen.

Das Beste an DoT: Man kann es bereits benutzen. Eine ganze Reihe großer DNS-Resolver wie die von Cloudflare (1.1.1.1) und Quad9 (9.9.9.9) bieten öffentliche Namensauflösung via DNS over TLS an und validieren die DNS-Informationen auch via DNSSEC. Cloudflare nutzt die dabei anfallenden Daten, um sein Content Distribution Network zu optimieren und die Inhalte möglichst dort zu platzieren, wo sie oft benötigt werden. Wer seine Surf-Daten lieber nicht bei einem großen amerikanischen Konzern abliefern möchte, findet über den Link am Ende des Artikels beim DNS-Privacy-Project eine Liste kleinerer, offener DoT-Server mit „no logging“-Policy.

Auch auf der Anwenderseite sieht es gar nicht schlecht aus. So enthält die für August erwartete Android-Version P einen „Private DNS Mode“; dahinter verbirgt sich nichts anderes als DNS over TLS. In der Standardeinstellung des aktuellen Previews testet Android den Nameserver und verwendet DoT, sofern er es anbietet. Auch die zukünftige Version des DNS-Resolvers in Linux-Systemd (Systemd-Resolved) kann DoT nutzen. Und wer vor ein bisschen Bastelei nicht zurückschreckt, dem erklärt der Artikel im nächsten Heft, wie man dem DNS-Filter Pi-Hole auf dem Raspberry Pi privatsphärenfreundliches DoT beibringt. Prinzipiell kann man auf dem dort beschriebenen Weg sogar ein Windows auf DoT umstellen.

DNS over HTTPS

Parallel zu DoT nimmt eine zweite DNS-Erweiterung namens DNS over HTTPS (DoH) Fahrt auf. Auf den ersten Blick erscheint das sehr ähnlich. Denn auch hier sichert Transport Layer Security (TLS) die Verbindung zwischen Client und Resolver; dass Frage und Antwort im Webseiten-Protokoll HTTP verpackt sind, erscheint nebensächlich. Es ermöglicht Anfragen wie

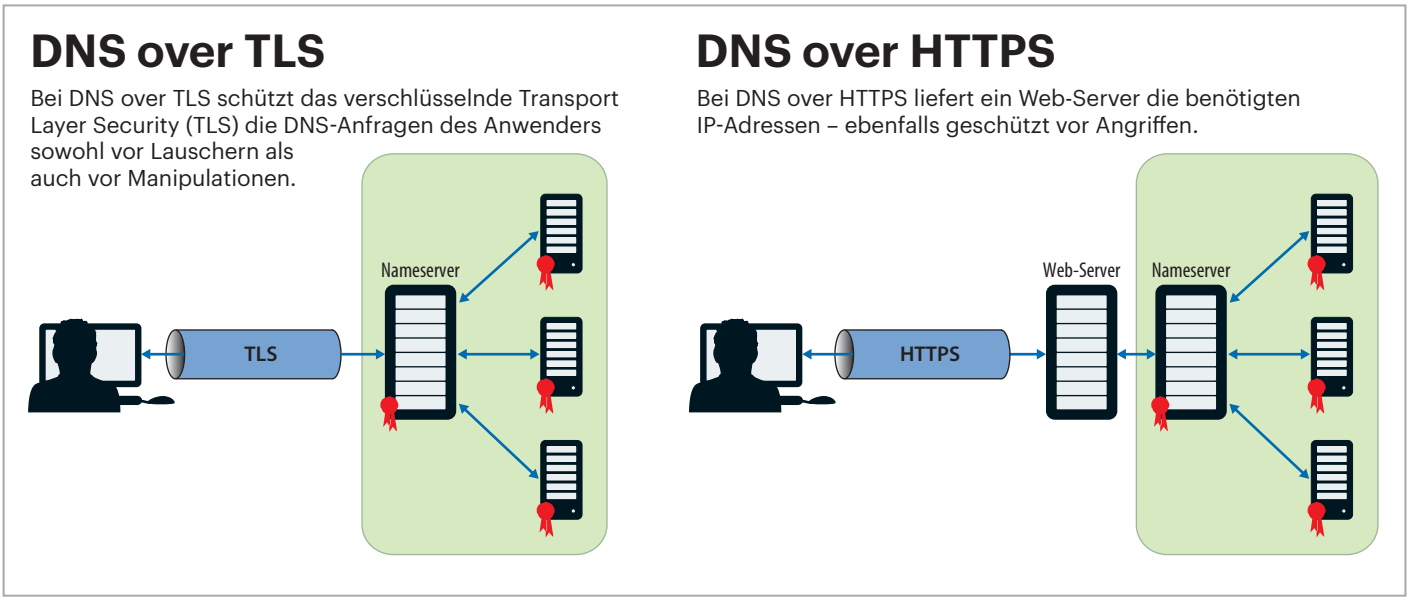
```
curl 'https://cloudflare-dns.com/
↳dns-query?ct=application/dns-json&
↳name=www.heise.de'
```

was die kompletten DNS-Infos des Heise-Webservers im JSON-Format anliefert.

Doch bei genauer Betrachtung krempelt DoH das gesamte DNS um. Die Idee dahinter ist, dass ein Webserver wie www.heise.de mit der eigentlichen Seite auch gleich alle für deren Aufbau benötigten IP-Adressen liefert. Der Vorteil liegt auf der Hand: Selbst das Laden komplexer Webseiten erfordert nur noch eine einzige DNS-Anfrage.

Herkömmliches DNS ist außerdem auf Systemebene umgesetzt. Der Browser fragt also das Betriebssystem nach der IP-Adresse für www.heise.de. DoH hingegen funktioniert auf Anwendungsebene; es läuft direkt im Browser oder in webbasierten Apps, die direkt mit dem Webserver-Resolver sprechen. Für andere Anwendungen gibt es Resolver-Dienste wie den Dnscrypt-Proxy und Cloudflared, welche zwischen klassischem DNS und DoS vermitteln (siehe ct.de/ys82).

Ein DNS-Client kann von einem DoH-fähigen Webserver natürlich auch – sofern es der Admin erlaubt – beliebige DNS-Daten abrufen. Dies verwandelt in Zukunft jeden Webserver in einen potenziellen DNS-Resolver. Damit sieht die Na-



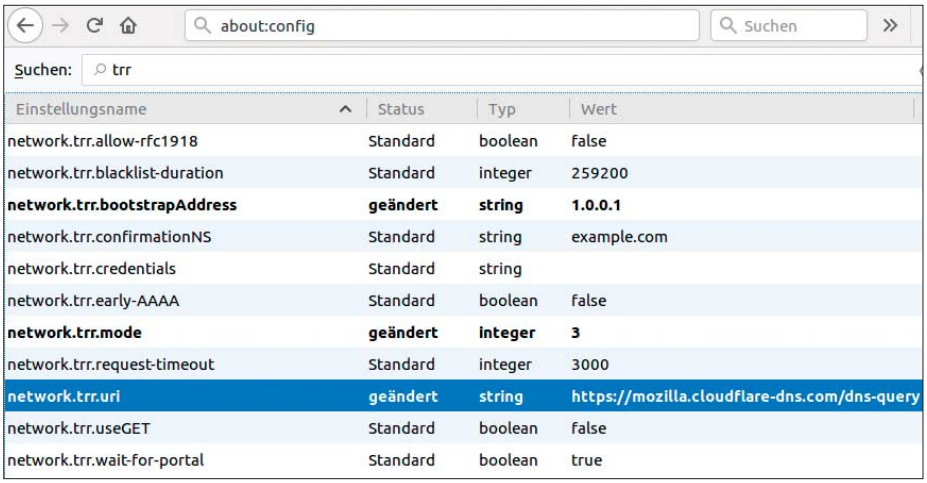
mensauflösung im Internet genauso aus wie normaler Web-Traffic und wird für Lauscher quasi unsichtbar. Anders als bei DoT kann ein Netzbetreiber DNS over HTTPS praktisch nicht blockieren, um einen Rückfall auf unverschlüsseltes DNS zu erzwingen. Auch selektive, DNS-basierte Internet-Zensur wird ineffizient, wenn jeder Webserver die benötigten Adressen liefern könnte. Und durch die Verteilung der Namensauflösung über viele Webserver fallen nicht mehr wie bisher personalisierte Surf-Profile etwa beim Nameserver des Providers an.

DNS over HTTPS ist noch sehr jung. Trotzdem oder gerade deshalb generiert diese Technologie einen ungeheuren Schwung, der Ideen, neue Software und Protokollerweiterungen hervorbringt. Die IETF hat den DoH-Draft in der rekordverdächtigen Zeit von weniger als einem Jahr zum Abschluss gebracht und wird ihn wahrscheinlich noch diesen Sommer als RFC verabschieden.

Auch der praktische Einsatz von DoH ist keineswegs Zukunftsmusik. Cloudflare und Google bieten bereits öffentliche DoH-Resolver-Webserver an. Und auch Mozilla ist vorne mit dabei: Wer möchte, kann DoH schon heute mit Firefox ab Version 60 ausprobieren. Dazu muss man im Dialog „about:config“ die Werte für „network.trr“ anpassen (Trusted Recursive Resolver). Die Option „network.trr.mode“ bestimmt, ob und wie DoH benutzt wird. Der Standardwert ist 0 (ausgeschaltet), 1 aktiviert DoH zusätzlich zum und 2 vor dem normalen DNS. Wer nur DoH benutzen möchte, trägt hier den Wert 3 ein.

Der Konfigurationsparameter „network.trr.uri“ legt die URI des zentralen DoH-Servers fest. Für den Dienst auf „https://mozilla.cloudflare-dns.com/dns-query“ hat Mozilla eine spezielle Vereinbarung abgeschlossen, die Cloudflares Nutzung der anfallenden Daten stark einschränkt. Weitere DoH-URIs finden Sie über ct.de/ys82

Ob das funktioniert, kann man einfach checken. Gibt man im Firefox in der URL-Zeile „about:networking“ an, bekommt man eine (interne) Webseite mit Informationen zu den Firefox-Netzwerkfunktionen. Unter dem Menüpunkt „DNS“ finden sich die zuletzt von Firefox aufgelösten DNS-Namen und die dazugehörigen IPv6- und IPv4-Adressen. Die Spalte „TRR“ zeigt an, welche dieser Informationen über einen vertrauenswürdigen Resolver (derzeit nur DNS over HTTPS) bezogen wurden. Bonus: Unter dem Menüpunkt „DNS Lookup“ können beliebige DNS-Anfragen angestoßen werden.



Seit Firefox 60 beherrscht der Mozilla-Browser DNS over HTTPS. Wenige Handgriffe schalten es ein.

DNS over QUIC und mehr

Quick UDP Internet Connections (QUIC) ist ein neues von Google entwickeltes Internet-Protokoll. Es soll eine leichtgewichtigere Alternative zu TCP/TLS bieten und setzt dazu auf UDP auf. Google verwendet QUIC bereits für Verbindungen zwischen den eigenen Servern (Suchmaschine und YouTube) und dem Chrome-Browser und Google-Android-Apps (YouTube). Parallel wird es auch bei der IETF standardisiert.

Mit DNS over Quic will die IETF die Vorteile von DNS over TLS mit der Geschwindigkeit von regulärem, UDP-basiertem DNS kombinieren. Derzeit gibt es allerdings nur eine Test-Bibliothek für Protokollentwickler, aber noch keine offenen Anwendungen.

DNSCurve und DNSCrypt sind zwei ältere Ansätze für sicheres DNS, die es nie in den Rang eines Internet-Standards geschafft haben. Der Dienstleister OpenDNS bietet beide an. Die Weiterentwicklung von DNSCurve wurde offenbar eingestellt und auch DNSCrypt ist wohl keine große Zukunft mehr beschieden.

Finale

So viel steht fest: Das Internet bekommt endlich eine sichere Namensauflösung, die dieses Attribut auch verdient. Und DNS als Internet-Dienst wird sich dabei grundlegend ändern. Insbesondere DNS over HTTPS hat das Potenzial, die Regeln des Spiels stärker zu verändern, als bisher absehbar ist. Wenn jeder Webserver auch Namensauflösung macht und webbasierte Apps auf Mobiltelefonen überhaupt nicht mehr auf herkömmliches DNS angewiesen sind, ändert sich das Gesamtgefüge.

Insbesondere Security-Profis sehen das mit einem lachenden und einem weinenden Auge. Denn die ersten, die diese Techniken in großem Stil einsetzen, werden Kriminelle sein. Denen ist durchaus bewusst, dass etwa DNS-Anfragen für den Namen eines Command&Control-Servers schon manchen Einbruch in Firmennetze auffliegen ließ. Die Chance, ihre verräterische Namensauflösung als harmlosen und dennoch unlesbaren HTTPS-Verkehr zu verschleiern, lassen die sich sicher nicht entgehen.

Die Leidtragenden des verschlüsselnden DNS sind somit Incident Response Teams und Forensiker, die etwa Einbrüche in Netze aufdecken und analysieren müssen. Für sie versiegen wichtige Informationsquellen wie Passive DNS und DNS-basierte Intrusion Detection Systeme. Deren Funktion beruht genau darauf, dass man DNS-Verkehr erkennen und auswerten kann (mehr dazu erläutert ein Hintergrund-Artikel zu „DNS als Sicherheitswerkzeug“, ct.de/ys82).

Doch ein Internet, das Zensurversuchen widerstehen kann und die Privatsphäre seiner Nutzer vor dem Zugriff durch autoritäre Staaten, übergriffige Geheimdienste und datenhungrige Konzerne schützt, ist dieses Opfer allemal wert. Denn jeder hat etwas zu verbergen.

(ju@ct.de) c't

DNSSEC-Test, offene DoT- und DoH-Server: ***ct.de/ys82***