FAQ

Verschlüsselte DNS-Anfragen

In der Standardkonfiguration kommunizieren alle Netzwerkgeräte unverschlüsselt mit dem Domain Name System. Deshalb klafft ein Loch im Privatsphärenschutz. Das lässt sich mit verschlüsselten oder gar anonymen DNS-Anfragen stopfen.

Von Dušan Živadinović

Warum befragen alle internetfähigen Geräte das Domain Name System?

Dafür gibt es viele Gründe. Zunächst einmal bietet kein Internetgerät der Welt genügend Kapazität, um ein Verzeichnissystem aller Internetserver der Erde vorzuhalten. Auch braucht nicht jedes Gerät die komplette Datenbank, sondern nur einen kleinen Teil davon.

Das Domain Name System (DNS) ist eine auf weltweit sehr viele Server verteilte Datenbank, die genau den Domainnamen zu seiner IP-Adresse übersetzt, den man gerade ansteuern will. So müssen sich Menschen keine IP-Adressen wie 193.99.144.80 oder 2a02:2e0:3fe:1001:302:: merken, sondern nur Domainnamen wie ct.de. Auch kann man so neue Server oder neue Dienste einfach mit ihren Domainnamen bekannt machen.

Zudem ist das DNS als Abstraktionsschicht nützlich, weil es mehr Flexibilität ermöglicht als IP-Adressen allein. Zum Beispiel kann ein Internetdienst auch während Wartungsarbeiten weiterlaufen, die das Abschalten der Serverhardware erfordern: Dafür ändert der Serveradministrator im DNS die IP-Adresse im laufenden Betrieb so, dass das DNS die Nutzeranfragen an die IP-Adresse eines Ersatzservers lenkt. Ist der Hauptserver wieder einsatzbereit, stellt der Admin im DNS wieder die ursprüngliche IP-Adresse ein. Ein weiteres Beispiel: Content Delivery Networks nutzen das DNS, um Anfragen von Nutzern zu einem Rechenzentrum in ihrer Nähe zu lenken. So wird derselbe Domainname in unterschiedlichen Regionen der Welt zu verschiedenen IP-Adressen aufgelöst.

Was ist so schlecht an üblichen DNS-Anfragen?

Das DNS wurde 1983 zu einer Zeit konzipiert, als der Privatsphärenschutz keine Rolle spielte. Deshalb senden die allermeisten DNS-Clients ihre Anfragen im Klartext. Diese Kommunikation lässt sich im lokalen Netz und im Providernetz leicht aufzeichnen und sie enthält so gut wie alle Internetziele, die von einer Nutzer-IP-Adresse angesteuert wurden.

Manche Provider außerhalb Europas nutzen sie, um Benutzerprofile etwa für Werbung anzulegen. Spione können damit Abhörattacken vorbereiten und Angreifer falsche DNS-Antworten einschleusen. Außerdem lassen sich DNS-Anfragen für Zensurzwecke filtern; Provider können dann DNS-Antworten auf unerwünschte Domains unterdrücken.

Woher weiß ein Internetgerät, wohin es seine DNS-Anfragen schicken soll?

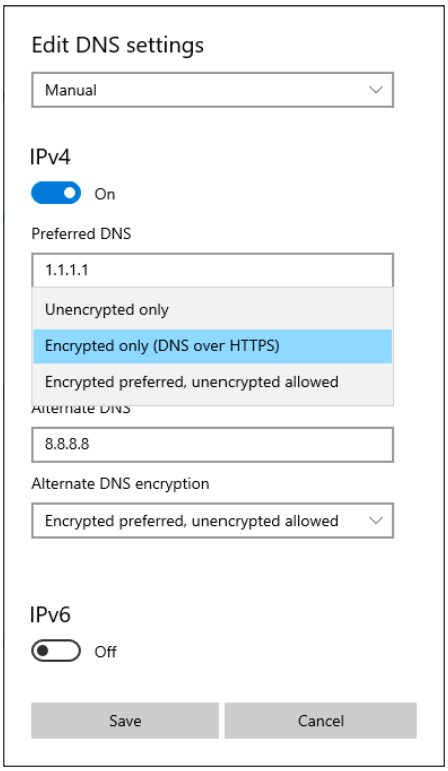
Ein Mobilfunkgerät wie ein Tablet oder ein Smartphone, das sich ins Mobilfunknetz einwählt, bezieht seine DNS-Einstellungen normalerweise vom jeweiligen Mobilfunkprovider. Wenn es die nutzt, schickt es seine DNS-Anfragen unverschlüsselt zum DNS-Resolver (DNS-Server) des Providers. Der DNS-Resolver löst dann die Anfrage für den Client auf und sendet ihm die Antwort.

Geräte, die sich in ein Heim-, ein Firmennetz oder einen Hotspot einbuchen, senden ihre DNS-Anfragen unverschlüsselt an den Router des jeweiligen Netzwerks. Der darin eingebaute DNS-Proxy leitet die Anfragen an den DNS-Resolver weiter, den ihm der jeweilige Provider bei seiner Einwahl mitgeteilt hat.

Wie schützt die verschlüsselte DNS-Kommunikation meine Privatsphäre?

Seit einigen Jahren entwickeln unterschiedliche Gruppen verschlüsselnde DNS-Protokolle. Zu den verbreiteten gehören DNSCrypt, DNS-over-TLS (DoT) und DNS-over-HTTPS (DoH). Neu dabei ist Oblivious DNS-over-HTTPS (ODoH) für anonyme DNS-Anfragen.

Um eines davon zu nutzen, braucht man spezielle DNS-Clients. Gegenüber dem Betriebssystem verhält sich ein solcher Client wie ein lokaler Resolver, der unverschlüsselte DNS-Anfragen entgegennimmt. Dann baut er eine chiffrierte Verbindung zu einem der konfigurierten verschlüsselnden Resolver auf und sendet ihm die DNS-Anfrage.



In Vorschauversionen von Windows 10 und Windows 11 lässt sich der Privatsphärenschutz per Mausklick verbessern. Bis die Funktion in öffentlichen Windows-Versionen erhältlich wird, kann man auf Windows Aufrüstungen wie Stubby oder DNSCrypt-Proxy nutzen.

? Was ist der Unterschied zwischen verschlüsselter DNS-Kommunikation und DNSSEC?

! DNSSEC einerseits und DoH, DoT und DNSCrypt andererseits sind verschiedene Methoden, die die DNS-Information auf unterschiedlichen Teilstücken des Übertragungswegs absichern. Deshalb ist es empfehlenswert, beide zu nutzen, sowohl DNSSEC als auch eine der verschlüsselnden Methoden.

Vereinfacht dargestellt kann man sich die Übertragungsstrecke der DNS-Kommunikation als zwei Teilstücke vorstellen: Der erste Teil verläuft vom Client zum Resolver, der zweite vom Resolver zum autoritativen DNS-Server, der für die gerade angefragte Domain zuständig ist. DoT, DoH oder DNSCrypt verschlüsseln die DNS-Kommunikation auf dem ersten Teilstück. Auf dem Teil vom autoritativen Server zum Resolver ist der DNS-Verkehr unverschlüsselt und kann manipuliert werden. Dagegen hilft DNSSEC, indem es die DNS-Antworten des autoritativen Servers signiert. Anhand der Signaturen können Resolver prüfen, ob die erhaltenen DNS-Antworten unverfälscht und die Sender der Antworten vertrauenswürdig sind.

? Wie findet man verschlüsselnde DNS-Resolver?

! Eine Übersicht mit zahlreichen offenen Resolvern finden Sie über ct.de/ya2r. Erste Provider bieten solche Dienste immerhin im Probebetrieb an, darunter die Deutsche Telekom.

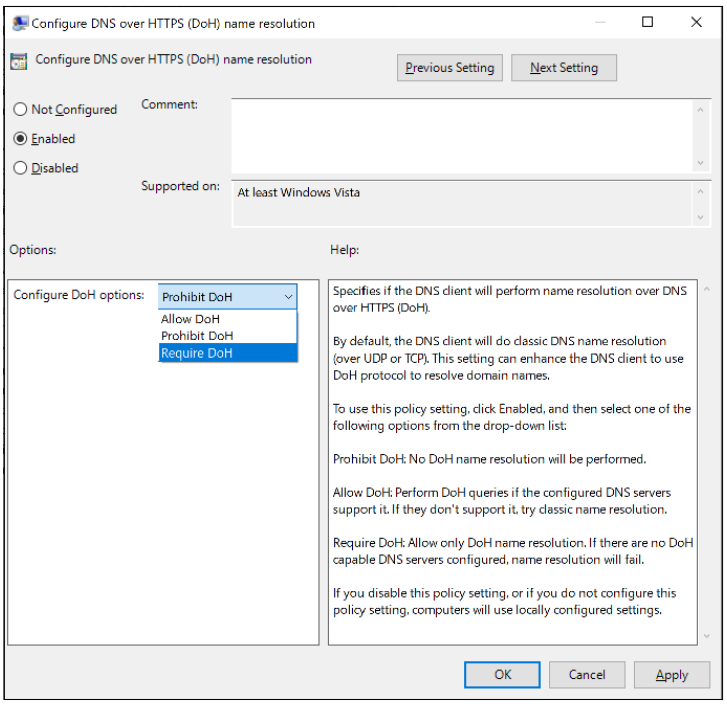
? Weshalb braucht man zusätzliche Software für verschlüsselte DNS-Anfragen?

! Die Betriebssysteme der allermeisten Geräte sind nur für unverschlüsselte DNS-Anfragen ausgelegt.

? Wie verbreitet sind Techniken zur verschlüsselnden DNS-Kommunikation?

! Zu Beginn der Entwicklung entstanden einige verschlüsselnde Resolver (hauptsächlich für Linux) und Clients für gängige Desktop- und Mobilbetriebssysteme. Dann lernten Webbrowser ihre eigenen DNS-Anfragen selbstständig zu verschlüsseln und seit einer Weile eignen sich auch gängige Betriebssysteme ab Werk für die verschlüsselte DNS-Kommunikation.

Microsoft hat DNS-over-HTTPS bereits im Windows Server 2022 implementiert. Damit können Administratoren für Windows-Plattformen netzwerkweit unter anderem bestimmen, ob die Technik verpflichtend oder nur optional zum Einsatz kommt.



Wenn die Technik im Router steckt, kann man sie gleich im ganzen LAN nutzen. Bisher bringen aber nur Fritzboxen und OpenWrt-basierte Router DoT mit. Die Telekom erwägt, DoT oder DoH in Speedport-Router einbauen zu lassen, die Huawei fertigt. Ersatzweise kann man einen Raspi mit einem verschlüsselnden DNS-Client ausrüsten und alle DNS-Anfragen vom Router zum Raspi umlenken (DNS-Einstellungen im DHCP-Bereich).

? Welche Browser eignen sich zur verschlüsselnden DNS-Kommunikation?

! Einige Browser können ihre eigenen DNS-Anfragen verschlüsseln. Wenn diese Funktion aktiviert ist, ignorieren sie die Einstellungen des Betriebssystems und kommunizieren selbst mit chiffrierenden Resolvern. Dazu gehören Google Chrome, Microsoft Edge, Mozilla Firefox und Opera.

? Welche Betriebssysteme eignen sich zur verschlüsselnden DNS-Kommunikation?

! Android ab Version 9 (Pie), iOS ab Version 14 und macOS ab Version 11.0 eignen sich ab Werk für verschlüsselnde Kommunikation.

Microsoft hat DoH in den Windows Server 2022 eingebaut. Für Administratoren gibt es unter anderem ein Group Policy Object zur netzwerkweiten Konfiguration der DoH-Einstellungen.

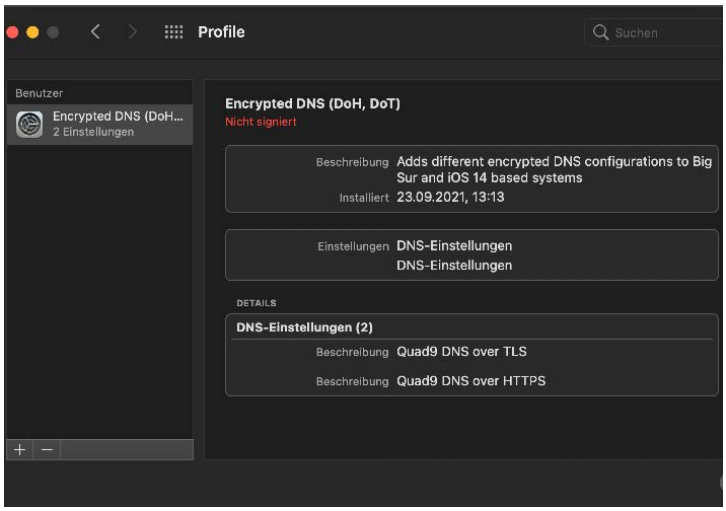
Im Rahmen des Programms „Windows Insider“ für Windows 10 kann man DoH ab dem Build 19628 testen. Ab dem Windows-Insider-Build 20185 gibt es ein grafisches User-Interface. Einzelheiten dazu sowie zum Entwicklungsstand finden Sie über ct.de/ya2r.

Um DoT oder DoH auf macOS oder iOS zu nutzen, braucht man eine spezielle Konfigurationsdatei, die sich einfach per Doppelklick installieren lässt. Apple beschreibt zwar für Entwickler, wie man eine solche .plist-Datei erzeugt, aber einige Nutzer bieten fertige Konfigurationsprofile zum kostenlosen Download an (siehe ct.de/ya2r).

Es gibt auch Webseiten zum automatischen Erstellen eigener Profile. Unter anderem kann man die DNS-Verschlüsselung in bestimmten WLAN-Netzen abschalten. Das bietet sich für Netzwerke mit internen Servern an, die externe Resolver natürlich nicht kennen. Im Heimnetz kann das zum Beispiel das private NAS-Gerät sein, in der Firma ein interner Webserver.

? Welche Software gibt es zum Nachrüsten?

! Das Angebot ist mittlerweile schwer überschaubar. Zu den prominenten Beispielen zählen Stubby, das für Windows, Linux und macOS erhältlich ist, und DNSCrypt-Proxy (siehe c’t 21/2021, S. 110). Für Apples iPhones kann man



Apple hat DNS-over-TLS und DNS-over-HTTPS zwar seit längerem in iOS und macOS eingebaut, aber ein einfaches User-Interface fehlt. Stattdessen aktiviert man die Technik mittels speziellen Konfigurationsdateien.

DNS-Cloak (to cloak = tarnen) verwenden, das sich für DoH und DNSCrypt eignet.

? Wie kann ich verschlüsseltes DNS auf Geräten nutzen, die sich nicht nachrüsten lassen?

! Webcams, Smart-TVs, Drucker und IoT-Geräte sind nicht zum Nachrüsten ausgelegt und kommunizieren mit dem DNS im Klartext. Abhilfe schaffen Router oder zentral im Heimnetz installierte DNS-Resolver. Sie nehmen unverschlüsselte DNS-Anfragen entgegen und kommunizieren selbst verschlüsselt mit einem externen Resolver. Die DNS-Antworten geben sie wiederum im Klartext an das Netzwerkgerät zurück, das die Anfrage gestartet hat. So sind die DNS-Daten nur noch innerhalb des Heim- oder Firmennetzwerks ungeschützt.

? Welche Nachteile sind mit verschlüsselnden Resolvern verbunden?

! Die übliche unverschlüsselte Methode nutzt einfache UDP-Konversationen zur DNS-Auflösung. Die verschlüsselnden Methoden gründen hingegen auf TCP-Verbindungen (Drei-Wege-Handshake) und TLS-Verschlüsselungen, deren Aushandlungen einige Millisekunden länger dauern. Komplexe Webseiten, die viele DNS-Anfragen erfordern, bauen sich daher spürbar langsamer auf. Es gibt aber Methoden, die eine verschlüsselte Verbindung zu einem Resolver für weitere DNS-Anfragen nutzen und so Zeit sparen.

Ein Problem erwächst auch daraus, dass externe Resolver die internen Server nicht kennen. Deshalb können beispielsweise im Heimnetz Zugriffe auf das eigene NAS-Gerät und in der Firma auf interne Webserver scheitern. Die einfachste Lösung besteht darin, die ursprüngliche DNS-Einstellung wiederherzustellen. Es sind aber auch Techniken in Entwicklung, die das automatisch erledigen sollen. Und natürlich können Administratoren das Problem ausräumen, indem sie in ihrem Netz eigene verschlüsselnde Resolver installieren.

Bei Apple- und Linux-Geräten kommt dieses Problem seltener vor, weil sie zur Namensauflösung im lokalen Netz zusätzlich Multicast-DNS verwenden (Bonjour auf iOS und macOS, Avahi auf Linux).

Resolver-Betreiber können die Anfragen prinzipiell protokollieren und auswerten. Die meisten sichern zwar in den Richtlinien zu, keine Protokolle anzulegen (also auch die US-Anbieter Google oder Cloudflare), aber auf staatliche Weisung müssten sie das dennoch tun. Deshalb sind Methoden zur anonymen DNS-Kommunikation empfehlenswert.

? Was sind anonyme DNS-Anfragen?

! Die DNS-Verschlüsselung verhindert unerwünschtes Mitlesen auf dem Übertragungsweg vom Client zum Resolver. Sie verhindert aber nicht, dass der Resolverbetreiber die Anfragen protokolliert und die im Internet besuchten Ziele den IP-Adressen der Nutzer zuordnet. Das lässt sich mit Techniken zur anonymen DNS-Kommunikation unterbinden.

Dabei senden spezielle Clients ihre Anfragen an Relays, die keine Schlüssel zum Dechiffrieren besitzen. Sie leiten die Anfragen an spezielle Resolver von unabhängigen Institutionen weiter (z. B. in einem anderen Land). Diese können die Nachrichten zwar entschlüsseln, aber sie kennen die IP-Adressen der Clients nicht. Deshalb verfügen solche Resolver schon technisch über keine privaten Surf-Daten und sind daher für Angreifer oder Staatsschützer uninteressant.

? Wie kann ich anonyme DNS-Anfragen senden?

! Apple, Cloudflare und Fastly entwickeln unter dem Dach der Internet Engineering Task Force das Protokoll Oblivious DNS-over-HTTPS (ODoH). Diese drei Unternehmen bieten auch die ersten ODoH-Implementierungen. Apple erprobt die Technik im Rahmen des kostenpflichtigen Angebots iCloud+. Voraussetzung ist entweder iOS 15 oder macOS 12.

Außerdem hat die Gruppe, die das DNSCrypt-Protokoll entwickelt, eine eigene Erweiterung zur anonymen DNS-Kommunikation entwickelt. Man kann sie mit verschiedenen Clients nutzen, unter anderem mit dem quelloffenen DNSCrypt-Proxy ab Version 2.10. Eine Anleitung für macOS, Linux und Windows finden Sie in c't 21/2021 auf Seite 110.

? DNSCrypt-Proxy klemmt – was tun?

! Wenn DNSCrypt-Proxy auf Windows beim Start meldet: „listen udp 127.0.0.1:53: bind: permission denied", dann nutzen Sie vermutlich eine PowerShell mit User-Rechten. Starten Sie das Programm aus einer PowerShell mit Administratorrechten.

Wenn das Programm beim Start meldet „bare keys cannot contain '\n'" enthält die Konfiguration vermutlich einen Syntaxfehler. Das kommt bei Vertippern vor oder wenn man Schlüsselwörter außerhalb des vorgesehenen Konfigurationsbereichs verwendet. Um solchen Fehlerchen auf die Spur zu kommen, empfiehlt es sich, von der mitgelieferten Konfigurationsdatei dnscrypt-proxy.example auszugehen und alle Änderungen mit Datum und Notizen zu markieren. Dann kann man eine Änderung nach der anderen auskommentieren, bis der Fehler verschwindet. Alternativ können Sie unsere über ct.de/ya2r erhältliche Beispielkonfiguration an Ihre Anforderungen anpassen. *(dz@ct.de)*

Konfigurationsdateien und Hinweise:
ct.de/ya2r