Alles verschlüsselt und abgesichert?

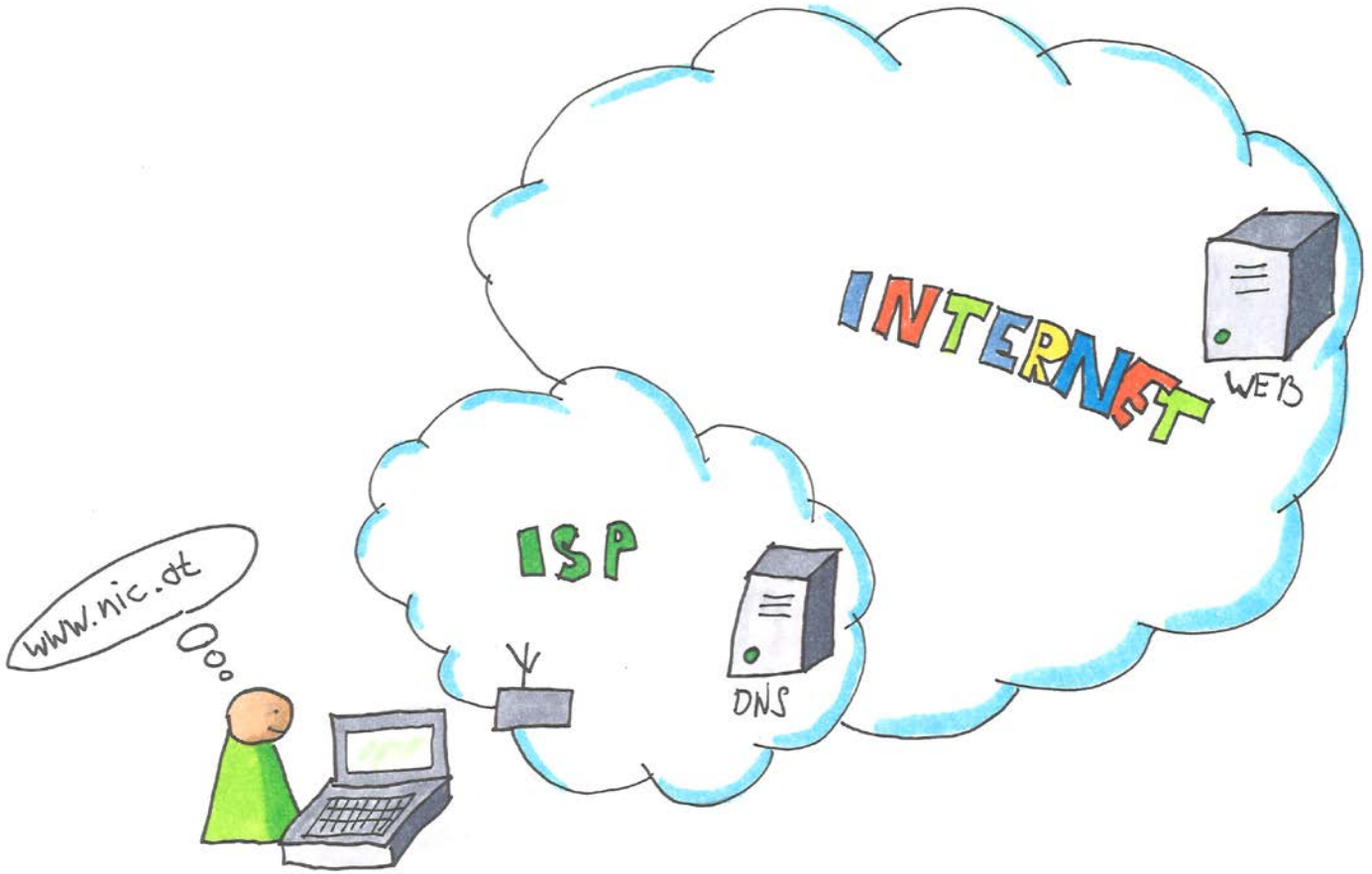
Was das Domain Name System über Sie verrät

2019- · Alex Mayrhofer · Head of Research & Development

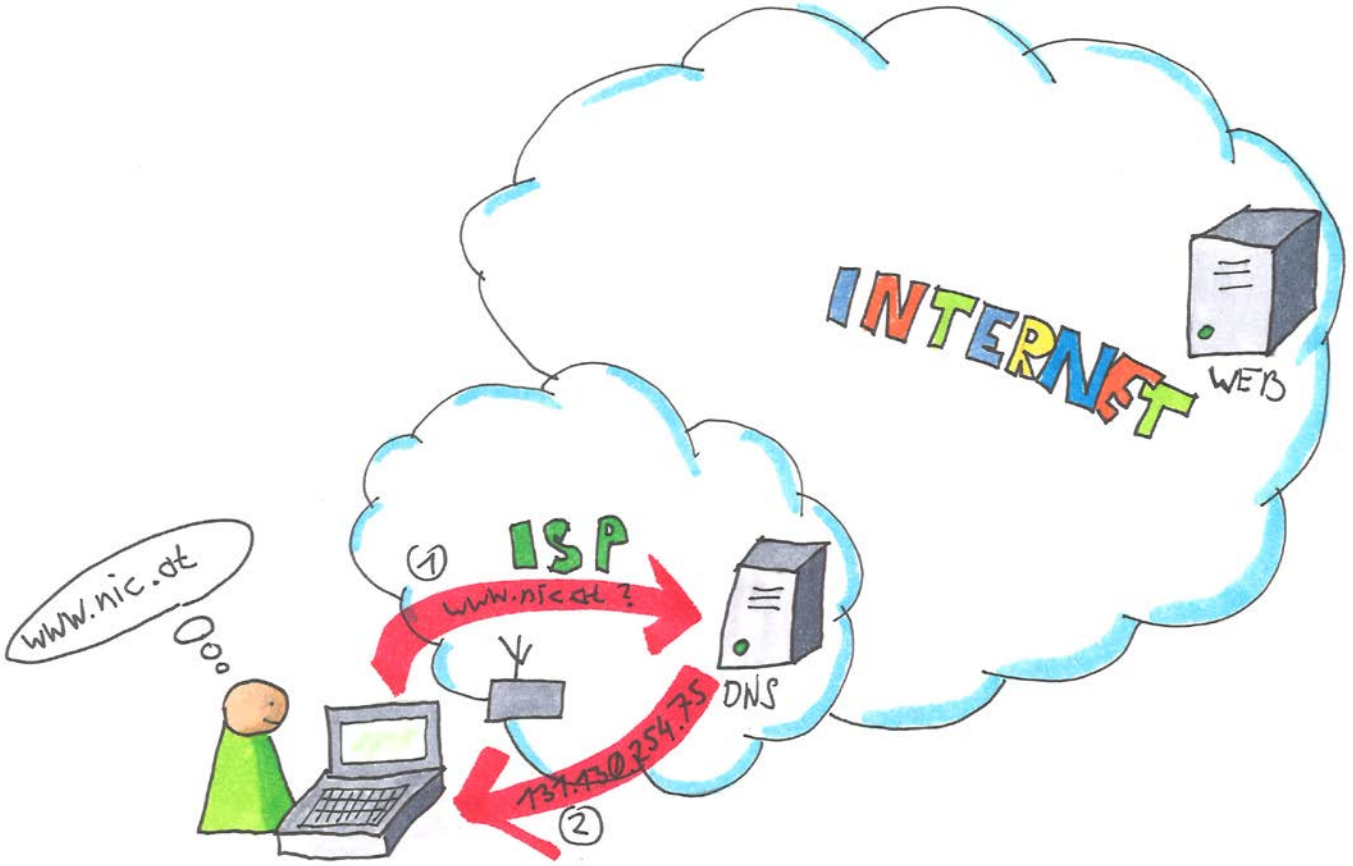
Das Domain Name System

Die Auflösung von Namen im Internet

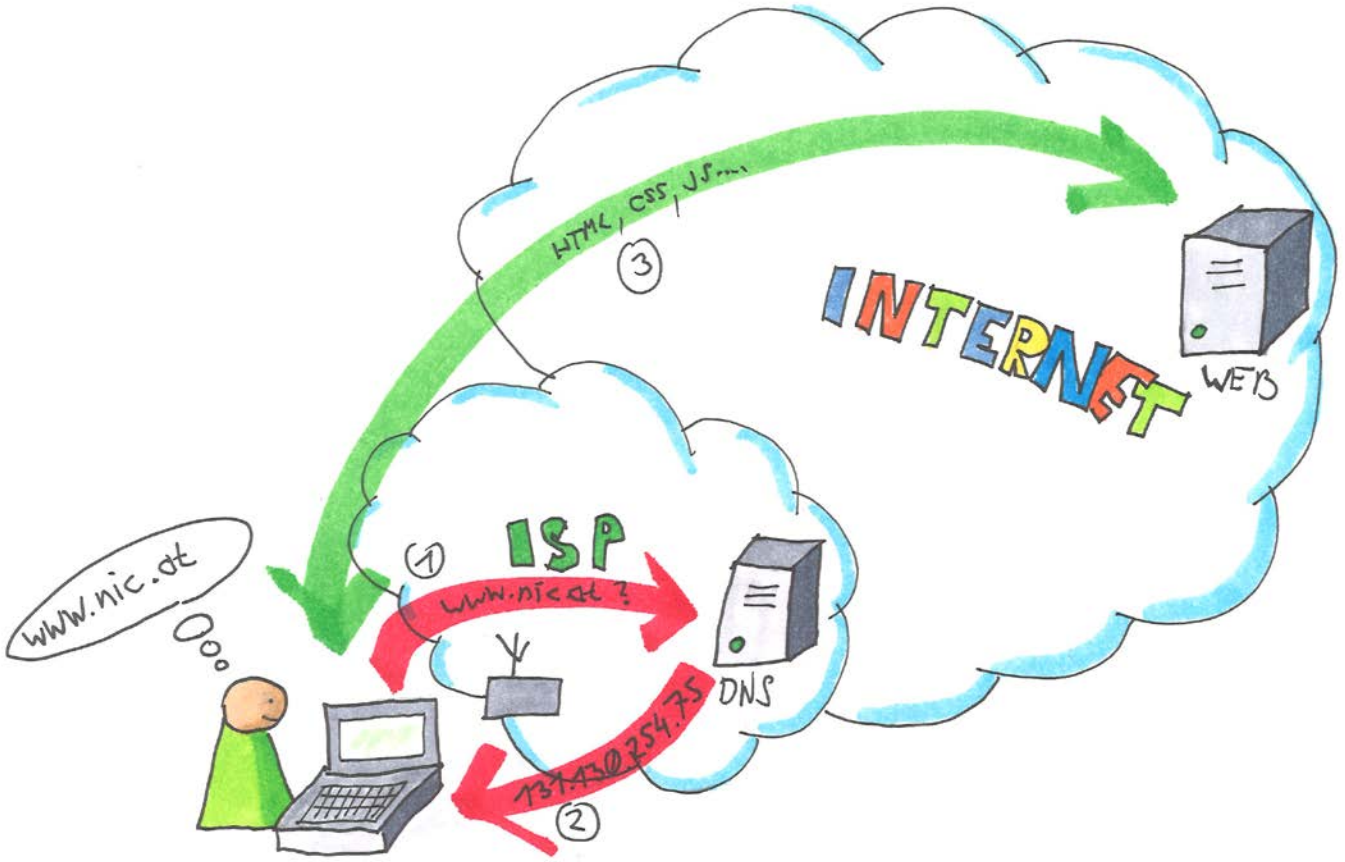
Beispiel: Aufruf einer Website



Zuerst die DNS-Abfrage



… und dann zur Website



Was heisst das für meine Privacy?

- Fast jede Transaktion im Internet beginnt mit einer (oder mehreren) DNS-Abfragen?
- Der DNS-Betreiber (und alle dazwischen) bekommen einen wunderschönen „Aktivitätsverlauf“
- Auch wenn die Kommunikation mit dem Ziel verschlüsselt ist!

„Das DNS braucht Verschlüsselung!“

Aber warum erst jetzt?

Das DNS anno circa 2012

- Sensationelle Erfolgsgeschichte
  - 25 Jahre alt, Grundzüge identisch
- Heute: Ohne DNS „geht gar nichts“
- Klartext. Alles.
  - „DNS ist ja ohnehin öffentlich?“
- DNSSEC? Macht eh alles sicher, oder!!?!
  - „Signiert“ nur, aber immer noch Klartext
- 2013: „Snowden“ Veröffentlichungen
  - NSA: „Klartext PII Daten … mmmmm…“
  - IETF: „Oh! Wir hatten nicht diesen Umfang erwartet“

Photo by Simone Acquaroli on Unsplash

„Pervasive Monitoring is an Attack“

- RFC 7258 – „**Pervasive Monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible**“

- Konsequenz: Review aller wichtigen Prokolle
- DNS – Es gibt nicht einmal eine *option* zur Verschlüsselung
- Noch schlimmer – enthält Mechanismen, die Privacy verschlechtern
  - Vollständiger „Query Name“ geht an „Unbetroffene“
  - EDNS(0) Client Subnet
- Quelle für Meta-Daten -> Fingerprinting
  - Re-Identifikation über Netzwerke hinweg

Photo by Kote Puerto on Unsplash

„DNS ist eh öffentlich“

- Nope. Abfragen lassen Rückschlüsse zu.
  - Website der anonymen Alkoholiker ist öffentlich
  - Die Information dass jemand diese besucht ist privat
  - „apothekepilledanachsamstag.at“ u.ä.
- Muster an Abfragen lassen Re-Identifikation zu
  - Laptop aufklappen -> Muster an DNS-Abfragen
  - Laptop im Hotel aufklappen -> Gleiches Muster

Photo by Andre Guerra on Unsplash

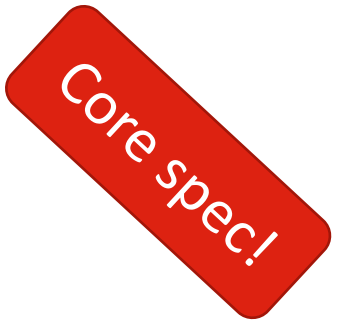
Das verschlüsselte DNS

DNS over TLS / DNS over HTTPS

DNS over TLS - Relevante RFCs

- RFC 7626 – DNS Privacy Considerations (DPRIVE) Read this!
- RFC 7766 – TCP Transport for DNS (DNSOP)
- RFC 7816 – QNAME Minimization (DNSOP)
- RFC 7828 – EDNS keepalive (DNSOP)
- RFC 7858 – DNS over TLS (DPRIVE) Core Spec
- RFC 8094 – DNS over DTLS (DPRIVE)
- RFC 7830 (+RFC 8467) – DNS Padding (DPRIVE)
- RFC 8310 – Usage Profiles
- RFC 8446 – TLS 1.3 (TLS)

RFC 7858 – DNS over TLS (DoT)

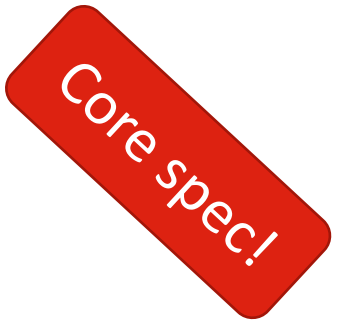


- New Port 853 / TCP
- „On the wire“ Protokoll ist identisch
- Authentifizierung: Zertifikate usw? -> RFC 8310
  - „Opportunistic“ vs. „Strict“
  - Chicken/Egg Problem -> Wie finde ich den DoT server?
- Ändert nicht den „Pfad“ der DNS Nachricht
  - Bestehende Nameserver schaffen einfach einen zusätzlichen, verschlüsselten Kanal
  - (In etwa wie http:// und https:// am selben Server)

Browser Hersteller – DNS over HTTPS

- (a) Browser machen sehr viele DNS-Abfragen
  - Websites + assets (JS, Ads, Statistiken…), CDNs
  - Zertifikat Validierung (OCSP), SafeBrowsing-Listen, updates, …
  - Wollen mehr / direktere Kontroller über das DNS API
- (b) Geschwindigkeit und Verfügbarkeit ist kritisch
  - „Happy Eyeballs“ – Langsame oder schlechte (lokale) DNS server erzeugen mieses Benutzererlebnis
  - „Mieses hotel WLAN“ is oft „Mieses Hotel DNS“…
- (c) DNS wird für Zensur benutzt
  - Das Umgehen von lokalen (zensurierenden) Nameservern schützt „Freedom of Speech“
  - Z.B. das Google „Jigsaw“ Projekt

DNS over HTTPS Spezifikation



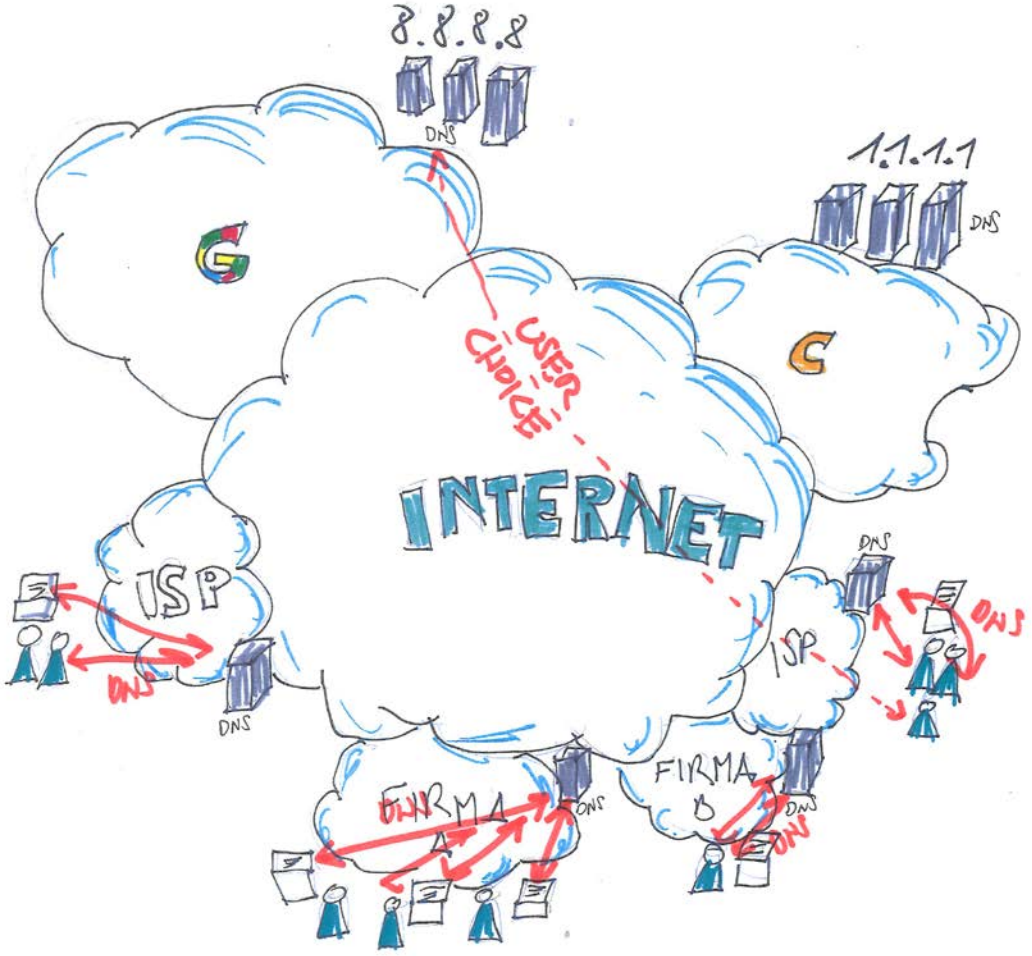
- Gruppe 2017 gegründet
- 2018: RFC 8484
  - GET or POST
  - URI Templates (https://dnsserver.example.net/dns-query{?dns})
  - Wire-Format: application/dns-message (identical zu „normal“ DNS), oder JSON
  - HTTP Response-Code always 2xx (if successful), no matter which DNS response code

*https://datatracker.ietf.org/wg/doh/about/

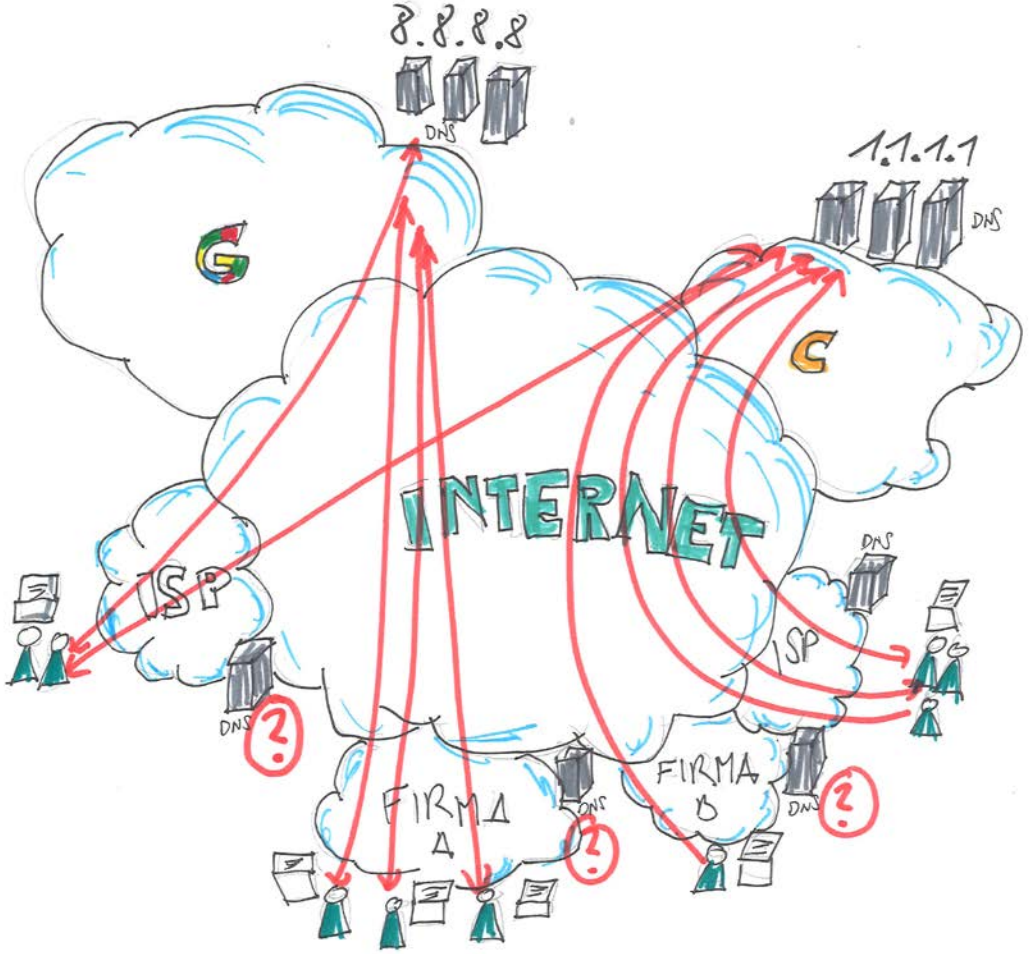
Die DNS Landschaft ändert sich.

Operative Auswirkungen der neuen Protokolle

DNS heute (und auch mit TLS)



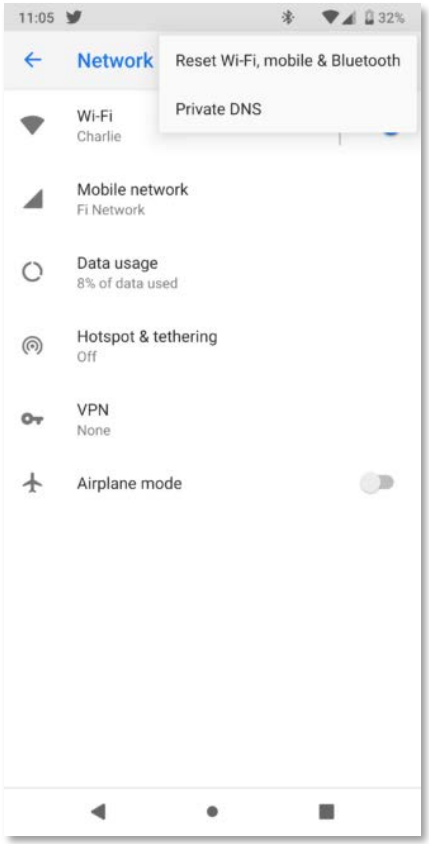
Die Landschaft von „DNS over Cloud“

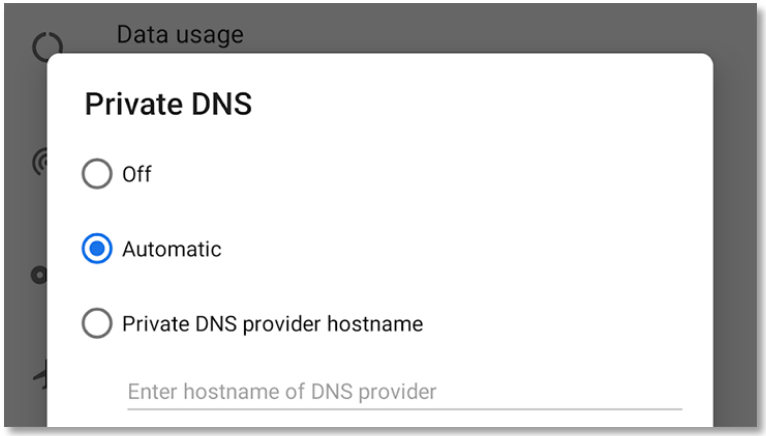


Bedenken zu DNS over HTTPS

- Eigentlich „DNS over Cloud“
- Es gibt 4 große Browser-Hersteller
- Es gibt wenige Betreiber großer öffentlicher DNS-Server (1.1.1.1, 8.8.8.8, 9.9.9.9)
- Marktkonzentration / Kontrolle?
  - Vorkonfigurierte Resolver-Adressen
  - Beispiel: Mozilla / Cloudflare Diskussion
- User Choice??
- Medienecho
  - https://Heise.de/-4203225.html („Die DNS Gruft gehört ausgelüftet“)
  - https://heise.de/-4205380.html („Vom DNS, aktuellen Hypes, Überwachung und Zensur“)
- Browser-Hersteller haben reagiert
  - Google: „Keine Aktion ohne Zustimmung des Benutzers“

Android 9 – DNS over TLS





- Verwendet DNS over TLS als default!
  - Versuche „tcpdump –n port 853“ auf dem recursive DNS-Server.
- Verwendet „unverschlüsseltes“ DNS falls TLS nicht verfügbar

Aktivitäten nic.at + Umfeld

- Mitarbeit an der Standardisierung
  - RFC 7830 + RFC 8467: EDNS(0) Padding
  - RFC 8484 (DNS over HTTPs): Review und Text
- Öffentlichkeitsarbeit / Awareness
  - Vortrag ISPA + EuroISPA
  - DNSheads Vienna Veranstaltung „Encrypted DNS“
  - IT Security Stammtisch
  - Registrar Roundtable
  - IT Business Talk
- AcoNET
  - Test-Server für DNS over HTTPS und DNS over TLS

Zusammenfassung

- Verschlüsseltes DNS ist jetzt möglich, entweder TLS oder HTTPS
- DNS über HTTPS ist eventuell mehr „disruptiv“
  - Das liegt aber nicht am Protokoll, sondern an der Anwendung
  - „DNS over Cloud“
- Öffentliche Recursor haben beides implementiert
  - Nur wenige Access-Betreiber haben nachgezogen (siehe unten :-/)
- Browser Hersteller haben DNS over HTTPS eingebaut
  - Policy-Diskussionen um Auswahl des DNS-Servers im Gange
  - „User Choice“ ist der Schlüssel
- Android 9 verwendet DNS over TLS *vorkonfiguriert*
  - Verwendet es automatisch, wenn verfügbar (siehe oben :-/)
  - Google empfiehlt/schlägt vor, „dns.google“ zu verwenden
- Windows / MacOS: Noch keine Lösungen auf OS-Ebene

nic.at GmbH

Jakob-Haringer-Str. 8/V · 5020 Salzburg · Austria

T +43 662 4669 -34 · F -29

alexander.mayrhofer@nic.at · **www.nic.at**