Von DNS-Streit und Adressverbrennung

DNS over HTTPS im Browser könnte für eine weitere Zentralisierung des Internets sorgen und das unbedachte Zweckentfremden von IPv6-Adressbits eine verfrühte Verknappung einleiten, lauteten zwei wesentliche Warnungen auf dem Kongress RIPE77.

Der Browserhersteller Mozilla (Firefox) und der Content-Delivery-Dienstleister Cloudflare wollen DNS over HTTPS (DoH) etablieren. In den Browser integriert soll DoH **Adressanfragen für Domains auf dem Transportweg vor Schnüfflern schützen**. Vertreter von Cloudflare bezeichneten den Schritt auf dem RIPE77-Treffen der europäischen Adressverwaltung RIPE als Verzweiflungstat, weil sich die Internetgemeinde mit der Einführung der alternativen Technik DoT (DNS over TLS) zu viel Zeit gelassen habe.

Sollte Google mit seinem Chrome-Browser einsteigen und ab Werk DoH mit den eigenen DNS-Servern als voreingestellter Gegenstelle sprechen, könnte das zu einer weitergehenden, ungesunden Zentralisierung des DNS-Verkehrs führen. Die DoT-Verfechter mahnten ferner, dass sich Firmen-Admins gewahr werden müssten, dass DoH ihre internen DNS-Resolver umgeht, die Zugriffe auf eigene Dienste aus dem internen Netz auf interne Adressen anstelle der öffentlichen umlenken.

Auch bei IPv6 gibt es Reibereien: Die enorm große Zahl möglicher Adressen – 2^{128}, ausgeschrieben 340 282 366 920 938 463 463 374 607 431 768 211 456 – verleitet die internationalen Adressverwalter zu großzügiger Zuteilung. Das wiederum inspiriert die Empfänger, Teile der Adressen für andere Dinge als das essenzielle Routing zu missbrauchen, beispielsweise zum Kodieren von Hierarchieebenen oder Telefonnummernplänen.

Davor warnte der IPv6-Experte Benedikt Stockebrand: „Die vielen IPv6-Adressen zu verbrennen, dauert. Bits verbrennen geht dagegen schnell“ (siehe ct.de/ygbq). Jedes einzelne nicht zur Adressierung verwendete Bit halbiert das nutzbare Adressvolumen, 8 Info-Bits lassen es folglich auf ein 256stel oder mickrige 0,39 Prozent zusammenschrumpfen. In einem vermeintlich harmlosen, kleinen Schritt verdampft ein IPv6-Netzbetreiber so gleich enorme 99,6 Prozent des ihm zugeteilten Adressraums. Das wiederum würde ihn nötigen, schneller als geplant weitere Zuteilungen zu beantragen.

So könnte eine Adressknappheit wie bei IPv4 bei IPv6 schon in 40 statt 80 Jahren eintreten. Stockebrand rät zu flacheren Hierarchien in den Adressierungskonzepten und zum Verzicht darauf, nichts fürs Routing unverzichtbare in der IPv6-Adresse zu kodieren.

(Monika Ermert/ea@ct.de)

DoH vs. DoT, IPv6-Adressverbrennung: ***ct.de/ygbq***

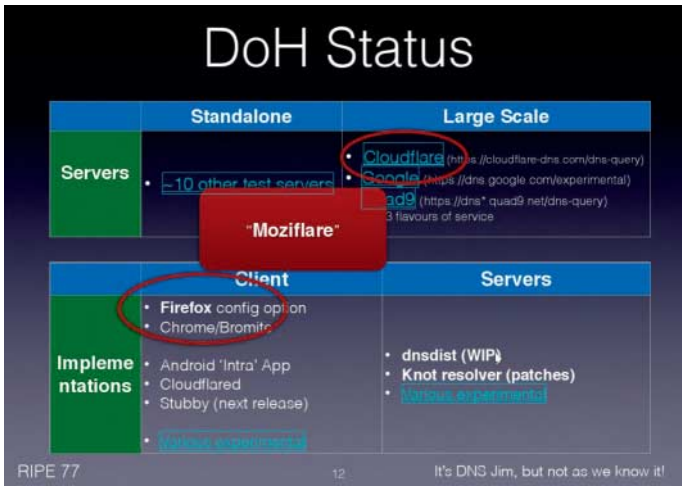

Bild: Sara Dickinson, Sinodun, ct.de/ygbq

DNS over HTTPS im Browser soll Domain-Adressanfragen vor dem Ausspähen auf dem Transportweg zwischen PC und DNS-Server schützen.

Kurz & knapp: Netze

Lancom Systems führt **mit LCOS 10.20 die verbesserte WLAN-Verschlüsselung WPA3** ein. Außerdem hat die jetzt für „alle aktuellen Access-Points und WLAN-Router“ bereitstehende Firmware das Routing-Protokoll LISP gelernt (c’t 3/2017, S. 136).

Der Chiphersteller Qualcomm hat die ersten **Bausteine für 60-GHz-WLAN** nach dem kommenden IEEE-Standard 802.11ay vorgestellt: Zwei Chips (QCA6438 und 6428) sollen in Basen Dienst tun, die Geschwister QCA6421 und 6431 in Mobilgeräten. Die Bausteine funken nach einem Entwurf, denn 802.11ay wird voraussichtlich erst im Herbst 2019 als Norm ratifiziert.

Auf www.traccar.org ist die **Version 4.1 des Tracking-Servers Traccar** erschienen (c’t 6/2018, S. 112). Sie verbessert die Kompatibilität mit MySQL, bringt Push-Nachrichten per Firebase mit und hat neue GPS-Protokolle gelernt (Wristband, MilesMate, Anytrek, SmartSole, ITS).

Synology stellt seinem Breitband-Router RT2600ac (Test in c’t 9/2017, S. 53) den 135 Euro teuren Kompagnon MR2200ac zur Seite. Mit der frisch erschienenen Firmware SRM 1.2 arbeitet ein Gespann aus RT2600ac und einem oder mehreren MR2200ac als **Mesh-WLAN-System**, sogar schon mit Unterstützung der verbesserten WLAN-Verschlüsselung WPA3.