Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Minister van Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
2888775

Datum 3 juli 2020
Onderwerp Kamerbrief gevolgen versleuteling DNS-verkeer

Hierbij bied ik, mede namens de staatssecretaris van Economische Zaken en Klimaat, uw Kamer een brief aan over de gevolgen van het voornemen van onder andere Mozilla om DNS-verkeer van hun internetbrowser, Firefox, te gaan versleutelen. Met deze brief geef ik uitvoering aan de toezegging die ik tijdens het AO digitalisering op 11 maart 2020 aan het lid Buitenweg heb gedaan. Zij vroeg in dit AO onder andere om een brief van het kabinet aan de hand waarvan verder gepraat kan worden over deze gevolgen en die ingaat op de impact van verdere concentratie van macht en data bij bepaalde partijen.

Versleuteling van DNS-verkeer
Alvorens op de mogelijke gevolgen van de versleuteling van DNS-verkeer in te gaan, is het goed om te weten wat dit precies inhoudt. Het Domain Name System (DNS) is een van de belangrijkste protocollen van het internet. Wanneer een gebruiker in een webbrowser wil navigeren naar een bestemming, bijvoorbeeld de website van de Rijksoverheid, dan typt hij niet het IP-adres van de Rijksoverheid in, maar www.rijksoverheid.nl. Op het moment dat via de webbrowser het 'verzoek' wordt ingediend om naar dat adres te navigeren, dient de webbrowser doorgaans via het besturingssysteem een DNS-verzoek in bij de internet service provider (internetprovider, hierna: ISP) om deze te laten vertellen welk IP-adres bij het opgevraagde domein hoort. Dit DNS-verzoek geschiedt doorgaans onversleuteld, waardoor apparaten die tussen de gebruiker en de ISP zitten, kunnen zien naar welke domeinnaam wordt gevraagd.

Standaardisatie DNS-verkeer protocol
Toegenomen zorgen in o.a. de Verenigde Staten (VS) over monitoring van DNS-verkeer door ISP's en tussenliggende partijen heeft geleid tot de standaardisatie van moderne DNS-transportprotocollen die gebruik maken van versleuteling.[1] De moderne DNS-transportprotocollen dragen bij aan de doelstelling om het DNS-verkeer op transportniveau beter te beveiligen en geeft de gebruiker een betere bescherming tegen ongeautoriseerde toegang tot het DNS-verkeer tijdens transport. Bij versleuteld DNS-verkeer dient de internetbrowser een verzoek in bij de door de ontwikkelaar van de browser ingestelde DNS-omgeving, bijvoorbeeld die van Cloudflare. Deze DNS-servers geven het antwoord terug aan de browser, die vervolgens naar het IP-adres dat bij het domein hoort, navigeert. Dit verzoek gaat daarmee dus niet meer onversleuteld langs de ISP. Het bekendste voorbeeld

[1] Deze ontwikkeling wordt ook wel aangeduid met de namen van deze moderne DNS-transportprotocollen, DoH (DNS over HTTPS) en DoT (DNS over TLS).

van deze ontwikkeling is dat Mozilla sinds februari dit jaar in de VS de Firefoxbrowser standaard zo instelt dat DNS-verzoeken van Amerikaanse gebruikers naar DNS-servers van Cloudflare worden verzonden. De leveranciers van internetbrowser laten op dit moment overigens wel de mogelijkheid open voor gebruikers om handmatig in te stellen dat het verkeer naar andere DNS-servers wordt gestuurd.

Blokkeren toegang tot gezochte informatie via DNS
In Europa is de netneutraliteitsverordening[2] van kracht. ISP's mogen het internetverkeer niet blokkeren, vertragen, wijzigen of beperken. Ook mogen ISP's het internetverkeer niet degraderen van, interfereren met of discrimineren tussen specifieke inhoud, toepassingen of diensten, of specifieke categorieën daarvan. In voorkomende gevallen kan DNS-verkeer in Europa echter wel op basis van nationale wetgeving of een rechterlijke uitspraak worden gebruikt als instrument om toegang tot –bepaalde benoemde– websites en omgevingen te blokkeren. In Nederland betreft dit op dit moment de door de rechter opgedragen blokkade van de site van The Pirate Bay. Niet alle landen buiten Europa passen het beginsel van netneutraliteit toe.

Gevolgen van versleuteling van DNS-verkeer
Naast gevolgen voor de mogelijkheid om toegang tot bepaalde websites te kunnen blokkeren, heeft de versleuteling van DNS-verkeer ook gevolgen voor de beveiliging van bedrijfsnetwerken. Het NCSC heeft in oktober vorig jaar een factsheet gepubliceerd die specifiek ingaat op deze gevolgen voor de beveiliging.[3]

Voor alle netwerken geldt dat het filteren en blokkeren van websites op basis van DNS-verkeer lastiger wordt als dit versleuteld is. Nationale opsporingsautoriteiten zullen op dit punt eveneens een effect hiervan ondervinden. Aan de ene kant door de versleuteling, maar ook doordat in toenemende mate verkeer op basis van versleuteld DNS-verkeer niet meer door de ISP als onderdeel van de internet toegangsdienst behandeld wordt, maar door derden. Waar tot op heden het afhandelen van DNS-verkeer een onderdeel van de dienstverlening van ISP's richting hun klanten is, verschuift deze rol naar derde partijen buiten de controle van de ISP's. In de praktijk lijkt het erop neer te komen dat het aantal partijen waaraan DNS-verzoeken gesteld worden, wereldwijd beperkt wordt tot maar een klein aantal partijen. Kijkend naar het wereldwijde aandeel van de betrokken leveranciers van internetbrowsers zou een centralisatie en concentratie van DNS-verkeer het gevolg kunnen zijn.

Het is lastig om nu al een inschatting van de werkelijke impact van versleuteld DNS-verkeer te maken. Dat is in de eerste plaats zo, omdat versleuteld DNS als standaard optie zich vooralsnog lijkt te beperken tot gebruikers in de Verenigde Staten als het om Firefox gaat en het gebruik bij Chrome beperkt is tot bepaalde gevallen. Voor andere internetbrowsers is het voorts onbekend of hun ontwikkelaars van plan zijn om te gaan experimenteren met versleuteld DNS-verkeer.

Versleuteld DNS-verkeer tegenhouden lijkt geen reële optie en de toepassing van versleuteling van DNS-verkeer heeft ook duidelijke voordelen. Waar het

[2] VERORDENING (EU) 2015/2120 VAN HET EUROPEES PARLEMENT EN DE RAAD van 25 november 2015 tot vaststelling van maatregelen betreffende open-internettoegang en tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en –diensten en Verordening (EU) nr. 531/2012 betreffende roaming op openbare mobielecommunicatienetwerken binnen de Unie.
[3] https://www.ncsc.nl/actueel/nieuws/2019/oktober/2/wees-voorbereid-op-dot-en-doh

uiteindelijk om gaat is hoe de leveranciers van internetbrowsers hun standaardinstellingen gaan bepalen, naar welke DNS-servers ze gaan verwijzen en door wie deze beheerd worden. Om binnen het huidige Europese regelgevende kader te blijven, zouden de leveranciers ervoor kunnen kiezen om het DNS-verkeer naar de ISP's en netwerkbeheerders te sturen, die ook nu het huidige DNS-verkeer afhandelen. Het is nog de vraag of de leveranciers van internetbrowsers hiertoe genegen zijn en of de condities die door de internetbrowsers worden gesteld zodanig zijn dat ISP's en netwerkbeheerders op verantwoorde wijze investeringsbeslissingen kunnen nemen ten aanzien van het implementeren van versleuteld DNS-verkeer binnen hun systemen. Voor de Nederlandse en Europese situatie is van cruciaal belang toe te kunnen werken naar een verwerking van het DNS-verkeer dat is gebaseerd op de Europese condities en de daar van toepassing zijnde regelgeving.

De staatssecretaris van Economische Zaken en Klimaat is in gesprek met Nederlandse partijen over de versleuteling van DNS-verkeer en de gevolgen daarvan, waaronder die voor de routering van het internetverkeer en de impact van mogelijke concentratie van data bij browserpartijen. De uitkomst zal (bijvoorbeeld in de vorm van een *position paper*) in Brussel worden geagendeerd en uw Kamer wordt geïnformeerd over relevante ontwikkelingen op dit gebied.

Tot slot
In het AO van 11 maart jl. werd ook verzocht om meer te horen over op welke wijze Nederland betrokken is bij het Internet Engineering Taskforce (IETF) en hoe gewaarborgd kan worden dat de standaarden van het internet en hoe daarmee omgegaan wordt, in lijn is met de mensenrechtenverdragen. De Internet Engineering Task Force is een grote, open, internationale gemeenschap van netwerkontwerpers, -operators, -leveranciers en -onderzoekers die zich bezighoudt met de evolutie van de internetarchitectuur en de soepele werking van het internet. Deelname staat open voor alle geïnteresseerde individuen.[4] De Nederlandse overheid als zodanig is geen deelnemer aan de IETF. Wel volgt Nederland de ontwikkelingen in deze en vergelijkbare werkgroepen op de voet en neemt Nederland deel aan diverse andere internationale overleggen over dit onderwerp en aanverwante onderwerpen.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

[4] https://www.ietf.org/