Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

DNS-versleuteling

De nieuwe standaard voor DNS-verkeer

Deze factsheet bevat relevante informatie voor systeem- en netwerkbeheerders, IT-managers en functionarissen op het gebied van informatiebeveiliging.

Factsheet FS-2023-237 | 2.2 | februari 2023

Moderne, versleutelde DNS-transportprotocollen maken het lastig om DNS-verkeer te monitoren en te onderscheppen voor detectie- en beschermingsdoeleinden. Enerzijds levert dit uitdagingen op voor systeem- en netwerkbeheerders. Anderzijds biedt het voordelen voor de veiligheid van eindgebruikers en organisaties. DNS-versleuteling maakt de cirkel rond voor een van de laatste, veelgebruikte onversleutelde protocollen. Het NCSC adviseert organisaties zich vertrouwd te maken met versleutelde DNS, zich te oriënteren op een overgang naar versleutelde DNS-infrastructuur en eindpoints zo in te stellen dat ze DNS-resolvers expliciet configureren.

Achtergrond

Het Domain Name System (DNS) is een van de belangrijkste internetprotocollen, want het is een fundamenteel onderdeel voor de start van de meeste internetsessies. DNS is het telefoonboek van het internet. Mensen krijgen op digitale apparaten toegang tot informatie via domeinnamen, die worden vertaald van door mensen leesbare tekst naar technische IP-adressen voor het omleiden van netwerkpakketten.

Het DNS-protocol communiceert van oudsher via UDP-poort 53. In de oorspronkelijke opzet worden geen authenticiteits- of integriteitstests uitgevoerd en is het verkeer onversleuteld.

Steeds vaker veranderen eindgebruikers handmatig hun voorkeurs-DNS-server in die van een derde partij, buiten hun eigen interne netwerk en het netwerk van hun internetprovider. In eerste instantie werd dit vooral gedaan om de prestaties te verbeteren, aangezien externe DNS-providers hun diensten adverteerden op basis van betere lookup-tijden, die tot een wezenlijk snellere surfervaring leiden. Meer recentelijk is versleuteling toegevoegd aan de lijst van voordelen van het kiezen van een externe DNS-provider.

De voordelen van DNS-versleuteling kunnen een verschil maken voor eindgebruikers en hun organisaties. Dit geldt vooral voor bedrijfsomgevingen waar vertrouwelijkheid van groot belang is, of in samenlevingen waar de vrijheid van meningsuiting beperkt is en internetgebruikers in de gaten worden gehouden door de overheid.

Daarom zijn softwareontwikkelaars van applicaties en besturingssystemen DNS-versleuteling breed gaan inzetten, zowel in de protocol-stack van besturingssystemen als in softwareapplicaties zoals webbrowsers. Vooral dat laatste, waarbij een webbrowser een versleutelde externe DNS-provider kiest, kan een uitdaging vormen voor IT-teams van organisaties die proberen schadelijke DNS-activiteit op hun netwerken te monitoren en detecteren.

Naast andere maatregelen om DNS betrouwbaarder te maken, zoals DNSSEC, adviseert het NCSC organisaties zich te oriënteren op een overgang naar versleutelde DNS.

Belangrijke feiten

1. Leveranciers van internetbrowsers en ontwikkelaars van de belangrijkste besturingssystemen voeren automatische DNS-switching in. Als een onversleutelde DNS-server wordt toegewezen aan het besturingssysteem, kunnen browsers of andere applicaties overschakelen naar een externe versleutelde DNS-server.

2. Als dit automatische overschakelgedrag niet door netwerk- of systeembeheerders wordt gemodereerd, kunnen nadelige effecten optreden, zoals verbindingsproblemen, datalekken of gegevensexfiltratie.

Wat is er aan de hand?

Versleuteld DNS-transport zal de norm worden voor moderne besturingssystemen, webbrowsers en smartphones.

Nederlandse internetproviders werken aan oplossingen om hun klanten in het midden- en kleinbedrijf-segment rechtstreeks te voorzien van versleutelde DNS-resolvers. Deze klanten gebruiken internetrouters die soms nog gebruikmaken van een lokale onversleutelde DNS-server voor endpoint-communicatie. Het ontbreken van DNS-versleuteling lijkt minder urgent, aangezien het lokale netwerk wordt gezien als een vertrouwde zone. Datzelfde kan worden gezegd over de internetverbinding: die is niet versleuteld, maar het netwerksegment naar de DNS-server wordt door de gebruiker en de internetprovider afdoende vertrouwd.

Grotere organisaties implementeren en beheren doorgaans hun eigen DNS-resolvers en wijzen deze toe aan hun eindgebruikers en servers. Deze worden gebruikt om zowel openbare als interne DNS-records te publiceren, voor toegang tot interne systemen. Dit soort implementaties zijn nog steeds grotendeels onversleuteld om dezelfde reden dat particulieren en kleine bedrijven geen versleuteling toepassen op hun lokale DNS: hun netwerk wordt gezien als een vertrouwde zone. Vaak is er aanvullende netwerksegmentatie en monitoring om ervoor te zorgen dat dit ook zo is.

De architectuur die wordt gebruikt om moderne apparatuur en software te ontwerpen en te ontwikkelen, gaat uit van een onvertrouwde omgeving. Hierbij wordt elk deel van de infrastructuur, ook lokaal, als onveilig gezien en worden extra beveiligingselementen toegevoegd om de integriteit, vertrouwelijkheid en geldigheid van informatie te waarborgen.

Deze nieuwe ontwerptrend moet als waardevol worden gezien. Het NCSC adviseert softwareontwikkelaars en -architecten dan ook om hun systemen te ontwerpen uitgaande van een onvertrouwde omgeving. Onversleutelde DNS-servers kunnen gevoelig zijn voor interventie, manipulatie en afluisteren door een kwaadwillende partij binnen het netwerk.

Voor de korte termijn adviseert het NCSC netwerk- en systeembeheerders allereerst te anticiperen op afwijkend DNS-gedrag op endpoints en netwerken die onder hun beheer vallen. Elke webbrowserleverancier kan een iets andere roadmap hanteren voor het implementeren van DNS, met andere beleidsvormen waaruit beheerders kunnen kiezen, maar uiteindelijk wordt gestreefd naar volledig versleutelde DNS. Deze strategie is te vergelijken met de overgang van HTTP naar HTTPS, waarbij onversleutelde HTTP-verbindingen door moderne browsers resoluut worden geweigerd.

Gevolgen van versleutelde DNS

Technische achtergrond

Versleutelde DNS is al een aantal jaren in ontwikkeling. RFC7578 *DNS over TLS* (DoT) dateert van mei 2016, RFC8484 *DNS over HTTPS* (DoH) van oktober 2018 en de meest recente ontwikkeling, RFC9250 *DNS over dedicated QUIC* (DoH3 of DoQ), kwam uit in mei 2022. Al deze varianten pakken in wezen

het DNS-verkeer over TCP in met versleuteling, met behulp van verschillende transportvarianten. DoT gebruikt tcp/853, DoH en DoQ gebruiken allebei tcp/443. DNS over HTTPS lijkt op dit moment de meest gebruikte standaard te zijn.

DNS verschuift naar de toepassingslaag

Softwareontwikkelaars kunnen gebruik maken van de softwarebibliotheken van besturingssystemen om DNS-aanvragen uit te voeren. Er gaat een signaal naar het besturingssysteem, dat de aanvraag zelf afhandelt en de resultaten naar de applicatie stuurt. Veel applicaties die onder één besturingssysteem draaien, gebruiken dan ook één enkele DNS-stub-resolver voor al hun DNS-verkeer.

In moderne softwaretoepassingen hebben ontwikkelaars diverse opties tot hun beschikking om te valideren welk type DNS-server het besturingssysteem aanbiedt. Ze kunnen beoordelen of hun applicatie deze wel of niet moet gebruiken op basis van door de ontwikkelaar ingestelde criteria.

Alle IT-bedrijven die besturingssystemen en tools voor softwareontwikkeling leveren, zoals Apple, Google en Microsoft, bieden tegenwoordig een uitgebreide toolkit en richtlijnen voor het gebruik van versleutelde DNS op applicatieniveau. Hiermee worden de instellingen van het besturingssysteem effectief omzeild.

Versleutelde DNS in specifieke webbrowsers

Mozilla Firefox, Google Chrome en afgeleiden van Chromium, zoals Microsoft Edge, bieden allemaal vergelijkbare evaluaties van DNS-versleuteling. Ze kunnen hun eigen externe versleutelde DNS-provider kiezen, meestal Cloudflare of Google, als het besturingssysteem is voorzien van niet-versleutelde DNS-servers. Browsers kunnen proberen de lokaal verstrekte DNS-verbinding te upgraden naar een versleutelde variant. Als dat niet lukt, kunnen ze proberen verbinding te maken met een externe provider.

De meeste browsers houden rekening met lokaal geïnstalleerde CA-certificaten, bijvoorbeeld specifieke organisatiecertificaten, en schakelen hun evaluatie van DNS-versleuteling helemaal uit als deze zijn geïnstalleerd. Hun evaluatie is ook afhankelijk van de geografische locatie: Firefox detecteert bijvoorbeeld of de browser wordt gebruikt in de Verenigde Staten of in een land dat op een specifieke lijst van onderdrukkende regimes staat. Voor die regio's selecteert de browser een externe DNS-provider als er geen andere DNS-versleuteling beschikbaar is. In Europa schakelt Firefox echter niet automatisch over naar een versleutelde provider, maar gebruikt het elke onversleutelde DNS-server die het besturingssysteem levert.

Dat gedrag zou kunnen veranderen. De verwachting is dat versleutelde DNS verplicht zal worden gesteld, na een zeer geleidelijk pad van log-notificatie, eindgebruikersnotificatie en uiteindelijk het blokkeren van onversleuteld DNS-verkeer. Dit pad kan vergelijkbaar zijn met de uitfasering van HTTP en vele jaren in beslag nemen.

DNS in de applicatielaag kan onvoorspelbaar blijken voor systeem- en netwerkbeheerders

De manier waarop DNS in de toepassingslaag wordt geïmplementeerd varieert. Het feit dat alle gebruikelijke webbrowsers en besturingssystemen op dit moment versleutelde DNS ondersteunen, biedt infrastructuur-beheerders de mogelijkheid om proactief over te schakelen naar de versleutelde DNS-infrastructuur die hun voorkeur heeft. Op die manier zijn zij voorbereid op softwareaanpassingen met betrekking tot DNS-versleuteling.

DNS-infrastructuur aanpassen gaat niet in één keer en vereist veel voorbereiding, want het is van invloed op de gehele IT-infrastructuur. Een proactieve, programmatische aanpak is daarom aan te bevelen.

Als laatste adviseert het NCSC beheerders na te denken over de huidige oplossingen voor

DNS-monitoring. DNS-verkeer wordt vaak gemonitord door zowel parsen van de DNS-serverlogs als packet monitoring van DNS-netwerkverkeer. Dat laatste werkt niet meer als het verkeer versleuteld is. In het geval dat uitgaand verkeer op poort 443 ongefilterd wordt toegestaan, kan dat een risico vormen, omdat hier ook DoH(3) verkeer tussen kan zitten. DNS is bruikbaar voor data-exfiltratie, waardoor alertheid op dergelijk verkeer is geboden.

DoT of DoH?

Afzonderlijke netwerkstromen komen netwerksegmentatie ten goede

Als we het netwerkbeheer vanuit technisch oogpunt bekijken, kan DNS over TLS (DoT) beter bij de behoefte passen dan DNS over HTTPS (DoH). DoT wordt uitgevoerd via een aparte poort, 853, en is dus eenvoudiger te segmenteren en isoleren in een bestaande netwerkarchitectuur. Tenzij er een HTTPS-proxy met certificaatinjectie wordt gebruikt, of HTTPS-verkeer helemaal verboden wordt, kan DoH lastig te segmenteren en te onderscheppen zijn.

Maatregelen

- Zorg dat kennis en inzicht op niveau zijn met betrekking tot de technologie achter DNS-versleuteling en het mechanisme waarmee kerntoepassingen, zoals webbrowsers, DNS-servers evalueren.
- Blijf op de hoogte, want de roadmaps voor volledige DNS-versleuteling in browsers zijn nog niet definitief.
- Dwing voorkeurs-DNS-servers af voor eindpunten en blokkeer ongewenst gedrag zoals automatisch overschakelen naar een externe DNS-server.
- Bereid een programma voor waarmee de IT-organisatie op termijn kan overschakelen naar versleutelde DNS.
- Evalueer DNS-monitoring en verzeker je ervan dat die aan gestelde detectievereisten voldoet.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl

Februari 2023