dialogic
innovatie • interactie

Inventarisatie aanbieders van DNS-diensten in Nederland

In opdracht van:
Ministerie van Economische Zaken en Klimaat

Project:
2020.154

Publicatienummer:
2020.154.2034 v1.4

Datum:
Utrecht, 16 februari 2021

Auteurs:
ir. Tommy van der Vorst
ir. Wazir Sahebali

Inhoudsopgave

Citeren als: Dialogic, van der Vorst, T., Sahebali, W. (2020). *Inventarisatie aanbieders van DNS-diensten in Nederland*. Ministerie van Economische Zaken en Klimaat, Den Haag.

Woordenlijst

ccTLD	*Country Code Top Level Domain.* Een TLD die tevens een landcode is, bijvoorbeeld ".nl" of ".de".
DNS	*Domain Name System.* Verwijst ofwel naar het wereldwijde systeem waarin informatie over domeinnamen is opgeslagen, ofwel naar de onderliggende technologie (het 'DNS-protocol').
FQDN	*Fully Qualified Domain Name*. Een volledige domeinnaam, die zijn oorsprong kent in de 'root'. Eindigt formeel met een punt: "www.dialogic.nl.".
NS	*Name Server*. Gegeven in het DNS dat bepaalt welke naamserver(s) verantwoordelijk is/zijn voor DNS-gegevens voor een bepaalde *zone*.
Root	Oorsprong van de domeinnaamruimte op het internet. Direct onder de 'root' vallen de TLD's, welke vanuit de root worden gedelegeerd.
RR	*Resource Record*. Een gegeven in het DNS dat hoort bij een bepaalde domeinnaam.
SLD	*Second Level Domain*. Een domeinnaam in de zone van een TLD. Zo is "dialogic.nl" een SLD onder de ".nl"-TLD.
SOA	*Start Of Authority.* Gegeven in het DNS dat bepaalt welke naamserver ultiem verantwoordelijk is voor de DNS-gegevens voor een bepaalde *zone*.
TLD	*Top Level Domain*. Het laatste achtervoegsel van een volledige domeinnaam (FQDN); bijvoorbeeld ".com" of ".nl".
TTL	*Time To Live*. Houdbaarheidsindicatie van een DNS-*record*.
Zone	Een afgebakend onderdeel van de 'domeinnaamruimte'.

1 Introductie

1.1 Aanleiding

De Europese Netwerk en Informatiebeveiliging (NIB)-richtlijn[1] benoemt DNS-diensten als essentiële dienst binnen de sector digitale infrastructuur. Het is aan de lidstaten van de EU om de richtlijn te implementeren en specifieke aanbieders te identificeren. In Nederland is de NIB-richtlijn geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (Wbni). Onder de Wbni zijn momenteel beheerders van een topleveldomein (vanaf een miljoen domeinnamen) aangewezen als aanbieder van een essentiële DNS-dienst [1]. Er zijn echter meer soorten DNS-dienstverleners. Het ministerie van Economische Zaken en Klimaat heeft Dialogic gevraagd om onderzoek te doen. Het voorliggende onderzoek legt de focus op aanbieders van *authoritative* DNS-diensten.

1.2 Onderzoeksvragen

In dit onderzoek staan de volgende vragen centraal:

1. Welke soorten DNS-diensten kunnen vanuit technisch perspectief worden onderscheiden? Wat zijn mogelijke gevolgen van verstoring (ook buiten de sector) van deze diensten?
2. Om welke (soorten) aanbieders en gebruikers gaat het?
3. Wat zijn de voornaamste in Nederland gevestigde aanbieders?

Bij de laatste onderzoeksvraag wordt een overzicht van in Nederland gevestigde partijen verwacht, zowel Nederlandse als buitenlandse met een vestiging in Nederland. Daarnaast is een gedetailleerd overzicht van de voornaamste aanbieders gevraagd. Per aanbieder wordt het marktaandeel beschreven, in ieder geval in termen van aantallen domeinen en gebruikers.

Bij deze onderzoeksvragen merken we het volgende op:

- We richten ons op (verleners van) *authoritative* DNS-diensten. We laten hierbij de (dienstverleners voor de) top-leveldomeinen daarbij buiten beschouwing.
- Het DNS is een wereldwijd systeem. Dat betekent dat een DNS-server in Nederland verantwoordelijk kan zijn voor de domeinnamen die horen bij een dienst die voornamelijk relevant is voor gebruikers *buiten* Nederland. Andersom is uiteraard ook mogelijk. In het kader van de NIB zou de duiding van marktaandelen en aantallen ons inziens dus moeten worden gericht op *voor Nederland (en/of de EU) relevante diensten*. Dit geldt zeer waarschijnlijk voor ".nl"-domeinen,[2] maar mogelijk ook voor

[1] [eur-lex.europa.eu]. De NIB-richtlijn verplicht landen in de Europese Unie om de weerbaarheid van netwerk- en informatiesystemen te vergroten. Daarbij valt te denken aan een gedegen risicomanagement, organisatorische en technische beveiligingsmaatregelen en het melden van incidenten.

[2] Dit is niet noodzakelijk zo voor alle landspecifieke top-leveldomeinen (ccTLD's). Zo wordt de extensie van het eiland Tonga (.to) voornamelijk buiten Tonga gebruikt in domeinen als "go.to", "cr.yp.to", "p.ota.to", et cetera. Voor het ".nl"-domein achten we dergelijke buitenlandse interesse beperkt.

andere extensies, waarbij de kans groot is dat de eigenaren van de domeinen hiervoor DNS-diensten in Nederland afnemen.

- Veel grotere hostingpartijen zijn in meerdere Europese landen actief; denk aan de Amerikaanse partijen Amazon, Google en de grotere Europese hosters OVH en Strato. Het marktaandeel van deze partijen is wereldwijd groot, maar in dit onderzoek gaat het om het voor Nederland specifiek relevante aandeel.

Om een onderbouwd antwoord te kunnen geven op deze vragen is gekozen voor een kwantitatieve onderzoeksmethode op basis van feitelijke informatie uit het DNS zélf. De resultaten daarvan worden vervolgens kwalitatief beoordeeld en waar nodig aangevuld.

1.3 Verantwoording

In dit onderzoek is primair gebruik gemaakt van een kwantitatieve meetmethode, waarmee een objectief beeld ontstaat. In het rapport gaan we in op de beperkingen van de methode. De kwantitatieve resultaten worden kwalitatief geduid, waarmee een (wat ons betreft) realistisch en waarheidsgetrouw beeld ontstaat.

Bij de start van het onderzoek zijn de drie grootste ISP's (voor wat betreft marktaandeel in Nederland) benaderd met de vraag of zij aanvullende informatie zouden kunnen bijdragen aan dit onderzoek (vanuit hun rol als leverancier van DNS-resolverdiensten aan klanten). Van deze mogelijkheid hebben de ISP's geen gebruik gemaakt.

In de loop van het onderzoek is de gehanteerde methode voorgelegd aan SIDN. Daarnaast hebben we SIDN verzocht om gegevens op te leveren. SIDN heeft constructief meegedacht en enkele eigen bevinden en kengetallen met ons gedeeld. Tot slot heeft SIDN een check uitgevoerd, waarbij onze resultaten zijn vergeleken met een analyse op niveau van *registrar*. Verschillen in deze resultaten zijn vervolgens nagetrokken.

1.4 Leeswijzer

In hoofdstuk 2 wordt allereerst een achtergrond geschetst rondom DNS. Daarbij komen de belangrijkste begrippen aan bod die nodig zijn om het vervolg van het rapport te kunnen begrijpen. In hoofdstuk 3 beschrijven we de onderzoeksmethode. In hoofdstuk 4 geven we de resultaten van de meting en duiding hierbij. In hoofdstuk 5 beantwoorden we de onderzoeksvragen.

2 Achtergrond

2.1 Het Domain Name System (DNS)

Domeinnamen worden gebruikt voor allerhande toepassingen op het internet; het ontwerpdocument voor het DNS geeft de volgende omschrijving:

> *The goal of domain names is to provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations. [2]*

Het Domain Name System (DNS) is een wereldwijd systeem dat voorziet in informatie over domeinnamen. Voor iedere domeinnaam kunnen in het DNS verschillende soorten gegevens, ook wel *records* genoemd, worden opgeslagen. Vanaf het eerste ontwerp van het DNS is rekening gehouden met deze potentiële veelheid aan toepassingen. [3] DNS-records worden vandaag de dag voor verschillende toepassingen gebruikt:

- Een besturingssysteem zoekt een 'A' of 'AAAA'-record op in het DNS om te weten te komen welk IP-adres hoort bij een bepaalde domeinnaam. Deze informatie is nodig tijdens het surfen op internet. Communicatie op internet (en dus ook met de bedoelde website) vindt immers plaats op basis van IP-adressen.

- Een e-mailserver zoekt een 'MX'-record op in het DNS om te bepalen aan welke andere e-mailserver e-mail voor een bepaald domein moet worden afgeleverd. Speciale 'TXT'-records worden gebruikt om te verifiëren of een server namens een bepaald domein e-mail mag zenden.

- Een uitgever van certificaten die worden gebruikt om websites te beveiligen, controleert in het DNS (via 'CAA'-records) of het wel gemachtigd is om een certificaat uit te geven voor het domein.

- Een VoIP-telefoon zoekt in het DNS (via 'SRV'-records) op met welke VoIP-server verbonden moet worden voor een bepaald domein.

- In het DNS kan ook 'andersom' worden gezocht en informatie worden ingewonnen over IP-adressen.

Zoals in het eerste ontwerp van DNS al werd voorzien, is het DNS een gedistribueerde database. Dat betekent dat de informatie voor verschillende groepen van domeinnamen door verschillende partijen wordt beheerd, terwijl het DNS als geheel een consistent beeld geeft van alle domeininformatie via een consistente 'ingang'. [3]

2.1.1 Domeinnamen

Het DNS is hiërarchisch opgebouwd en kent een soort 'boomstructuur'. Aan de basis van het DNS staat de *root* zone. De root zone wordt gekenmerkt met de 'lege' domeinnaam ".". In de *root zone* kunnen verschillende *top-level domains* of *TLD*'s worden gedefinieerd. Voorbeelden van TLD's zijn ".com", ".nl" en ".de". Op moment van schrijven zijn er circa 1500 TLD's gedefinieerd door het ICANN [4]. De TLD's zijn in te delen in verschillende categorieën: [5]

- **Country-code top-level domain (ccTLD).** Dit zijn TLD's als ".nl" en ".de", verwijzend naar een specifiek land, en in de praktijk vaak ook gericht op publiek in dat land. Registratie geschiedt via een specifieke instantie per land, waarbij aanvullende eisen kunnen worden gesteld (in sommige landen dient de aanvrager ook daadwerkelijk gevestigd te zijn in het betreffende land, bijvoorbeeld).

- **Generic top-level domain (gTLD).** Dit zijn TLD's als ".com", ".net" en ".org". Het beheer van deze TLD's ligt over het algemeen bij private organisaties. Domeinen onder deze TLD's zijn in principe voor iedereen te registreren. Uitzondering vormen de zogenaamde *restricted* gTLD's (grTLD's), waarbij aanvullende eisen worden gesteld (zo is ".pro" alleen te registreren door "gecertificeerde professionals"). Het overige beleid van ICANN voor registratie is hierbij onverminderd van toepassing.

- **Sponsored top-level domain (sTLD).** Dit zijn TLD's als ".aero" en ".museum". Ze zijn gericht op een specifieke sector. Anders dan bij de gTLD's geldt het standaardbeleid van ICANN niet voor deze domeinen.

- **Infrastructure top-level domain (ARPA).** Dit betreft alleen de ".arpa" TLD, welke is bedoeld voor infrastructurele zaken, zoals reverse DNS-lookup en identificatie van telefoonnummers (E.164) in DNS.

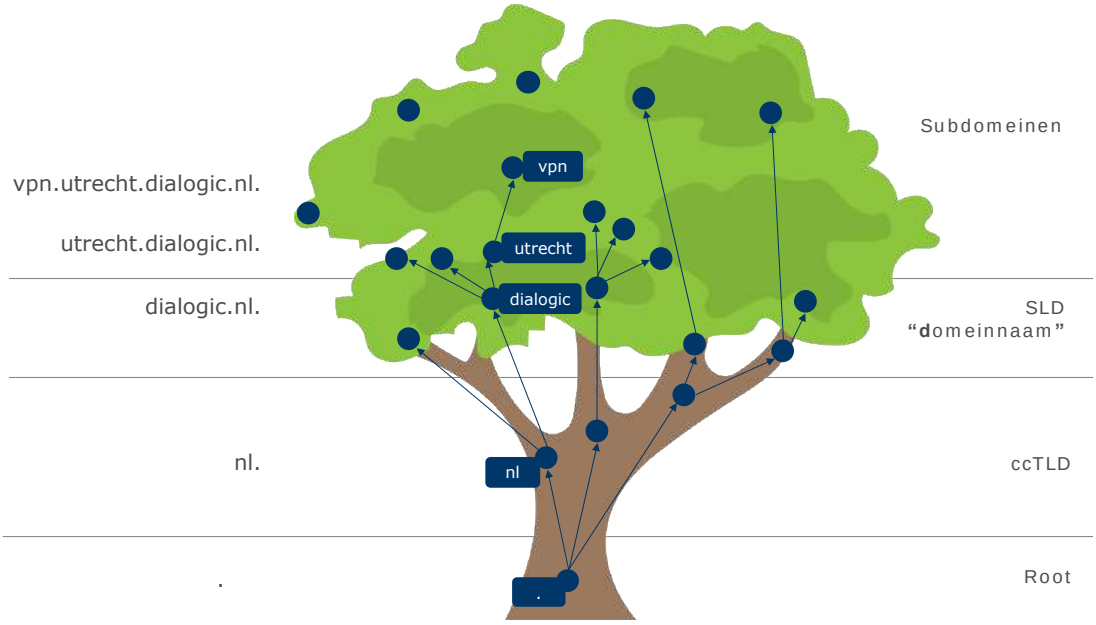
- **Test top-level domain (tTLD).** Dit betreft ".test" en enkele TLD's in niet-Latijns schrift, bedoeld voor het testen van software.

- **Gereserveerde TLD's.** Sommige TLD's mogen nooit worden gebruikt, omdat ze buiten het openbare DNS een specifieke rol vervullen. Zo wordt ".local" gebruikt door mDNS, een variant van DNS voor lokale netwerken. [6] Hetzelfde geldt onder andere voor ".invalid", ".onion" [7] en ".localhost".

Een TLD is te zien als een 'subdomein' onder het rootniveau en vormt op zichzelf een nieuwe *zone* waarbinnen subdomeinen kunnen worden gedefinieerd. Een subdomein onder een TLD wordt een *second-level domain* genoemd.[3] Deze SLD's zijn wat in de volksmond "domeinnamen" worden genoemd; voorbeelden zijn "dialogic.nl" en "minezk.nl". Onder een SLD kunnen opnieuw (en zelfs zolang totdat de lengte van de volledige naam onder de 255 tekens blijft) subdomeinen worden gedefinieerd.

In een volledige domeinnaam zijn de verschillende niveaus aangegeven met een ".". Het adres "www.dialogic.nl" betreft dus het subdomein 'www' onder de SLD 'dialogic' binnen de TLD 'nl' onder de root. Om twijfel te voorkomen over of een bepaalde naam een subdomein betreft of een absolute, volledige domeinnaam (een *FQDN*) wordt bij volledige domeinnamen vaak een punt toegevoegd aan het einde, om aan te geven dat de naam vanaf de root dient te worden gelezen: "www.dialogic.nl.". Figuur 1 illustreert deze hiërarchie schematisch.

[3] In sommige landen is hiertussen een extra tussenniveau aangebracht; zo is het TLD '.uk' onderverdeeld in '.co.uk' en '.gov.uk'. Bedrijven kunnen alleen binnen de '.co.uk'-zone een domeinnaam aanvragen.



Figuur 1 Schematische weergave van de hiërarchie in het DNS. Links een voorbeeld-van de volledige domeinnaam die per niveau wordt geregistreerd, rechts de term voor een domeinnaam op dat niveau.

Dankzij de hiërarchische opbouw is er steeds maar één organisatie verantwoordelijk voor de DNS-informatie binnen een bepaalde ‘tak’ (*zone*).[4] Toch is het denkbaar dat het DNS aan verschillende gebruikers verschillende informatie verstrekt. Dit kan gebeuren in de volgende scenario’s:

- Een DNS-server geeft aan verschillende gebruikers verschillende antwoorden, afhankelijk van (bijvoorbeeld) het afzender-IP-adres van de gebruiker. Dit wordt toegepast om verkeer te spreiden over meerdere IP-adressen of om gebruikers te laten verbinden met een IP-adres waarmee door de gebruiker het snelst kan worden gecommuniceerd.

- Grotere organisaties hebben binnen hun eigen netwerk vaak eigen DNS-servers ingericht die een eigen TLD toevoegen voor intern gebruik. Zo worden namen onder “.local” of “.internal” of “.bedrijfsnaam” gedefinieerd die alleen binnen het netwerk geldig zijn.

- De TLD “.local” wordt gebruikt voor mDNS, waarmee binnen een thuisnetwerk apparaten op naam kunnen worden geïdentificeerd. De namen zijn alleen binnen het thuisnetwerk te vinden en daarbuiten niet geldig.

- Sommige ISP’s of andere resolvers maskeren bepaalde informatie in het DNS, bijvoorbeeld om ongepaste of onveilige websites te blokkeren voor hun gebruikers.

- Zogenaamde “alternate roots” bieden gebruikers als het ware een volledig alternatieve invulling van domeinnamen.

[4] Merk op dat de verantwoordelijkheid voor de *informatie* niet hoeft samen te vallen met verantwoordelijkheid voor de bijbehorende DNS-servers die in de informatie voorzien. Een domeinnaamhouder kan dit ‘uitbesteden’ aan een DNS-aanbieder.

2.1.2 Werking

Om informatie in het DNS op te zoeken kan een verzoek worden gericht aan een *DNS-server*. Een DNS-server verwerkt vragen en retourneert de gevraagde informatie via het *DNS-protocol*.

Authoritative DNS

Een zogenaamde *authoritative* DNS-server is verantwoordelijk voor het verstrekken van informatie voor een of meerdere specifieke *zones*. Een authoritative DNS-server krijgt deze verantwoordelijkheid door een vermelding op het direct bovenliggende niveau in DNS. Om bijvoorbeeld te bepalen wat de authoritative DNS-server voor "dialogic.nl." is, dient allereerst aan de server verantwoordelijk voor de *root zone* te worden opgevraagd welke DNS-server verantwoordelijk is voor de ".nl."-zone. Bij deze server kan vervolgens worden opgevraagd welke DNS-server verantwoordelijk is voor "dialogic.nl.". Deze werkwijze heet 'delegatie' en de bijbehorende gegevens in het DNS heten 'NS-records'.

NS-records worden beheerd door de beheerder van de betreffende zone. Voor het ".nl"-domein is SIDN (*Stichting Internet Domeinregistratie Nederland*) aangewezen als beheerder. Het 'registreren van het domein' betekent vanuit DNS-perspectief dus het aanvragen van een NS-record in de ".nl."-zone.

Omwille van redundantie kan een zone worden gedelegeerd naar meer dan één DNS-server, door het maken van meerdere NS-records.[5] Voor vrijwel alle TLD's en SLD's zijn meerdere DNS-servers aangegeven in het DNS. Omdat deze redundante DNS-servers in principe onderling geen verschillende informatie zouden moeten verstrekken, wordt in het DNS één DNS-server aangewezen als ultieme autoriteit, middels een zogenaamd *SOA-record*.

Omdat het rootniveau het allerhoogste niveau is in het DNS kan voor dit niveau niet worden opgezocht in DNS welke DNS-server verantwoordelijk is. De root-servers en bijbehorende IP-adressen zijn daarom meestal voorgeprogrammeerd in alle software die het DNS bevraagt (in het bijzonder in besturingssystemen als Windows en macOS). De root-servers zijn verspreid over de wereld en worden geïdentificeerd met dertien 'letters' ("a.root-servers.net" t/m "m.root-servers.net") en dertien bijbehorende IP-adressen; in werkelijkheid gaat achter iedere letter een groter aantal servers schuil (die het IP-adres dus delen middels een techniek die "anycast" heet).[6]

Resolving

Om informatie over een domeinnaam op te zoeken dienen DNS-servers op verschillende niveaus te worden bevraagd. Het opzoeken van informatie wordt "to resolve" genoemd en wanneer daarbij inderdaad de hiërarchie wordt afgelopen spreken we van "recursive resolving".

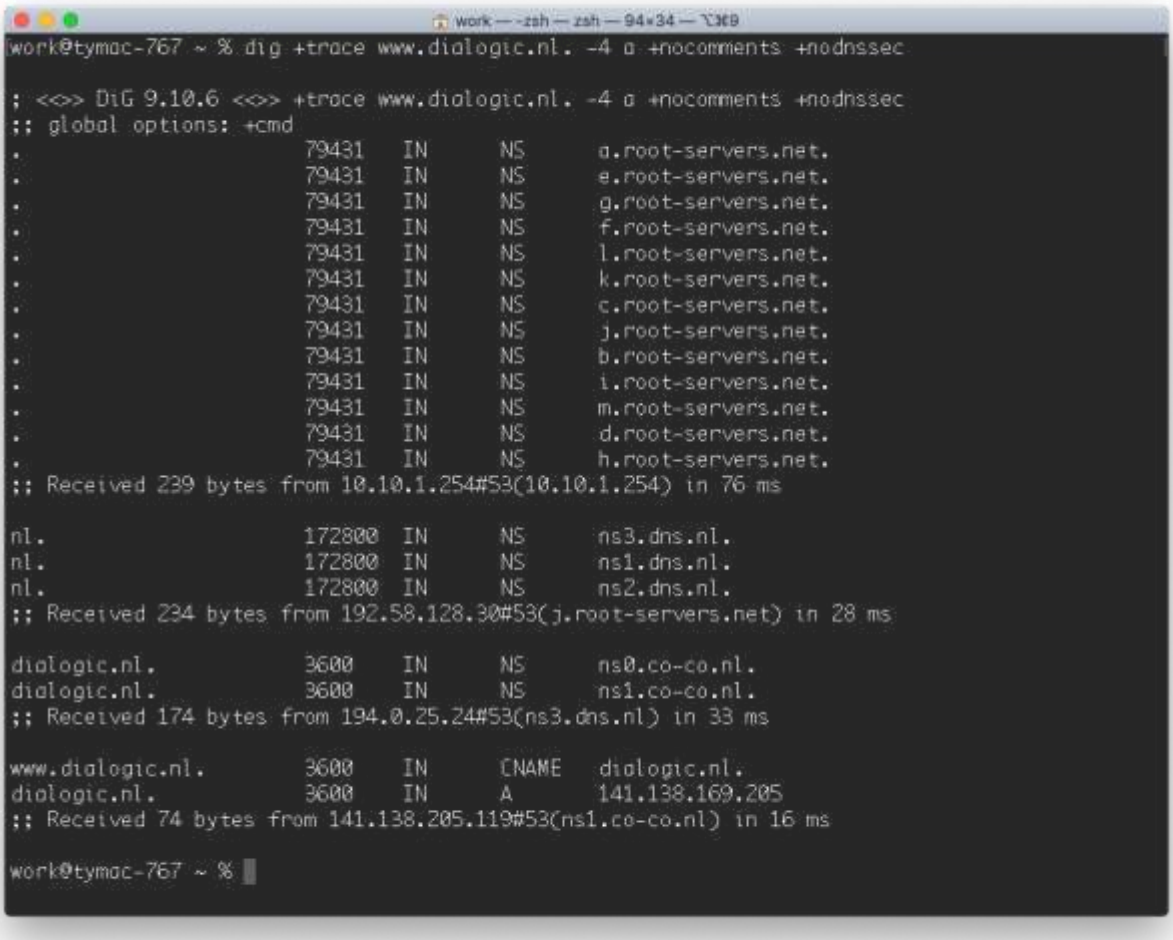
Onderstaande Figuur 2 toont het resultaat van een *recursive resolve* van het adres (A-record) behorend bij de domeinnaam 'www.dialogic.nl.'. In de figuur is te zien dat allereerst de 'root servers' worden geraadpleegd. Een van de root servers (*j.root-servers.net.* in dit geval) geeft vervolgens informatie over de ".nl."-zone: hiervoor moeten we bij "ns1.dns.nl." (of een van de andere genoemde nameservers) zijn. De resolver kiest voor "ns3.dns.nl" en vraagt daar

---

[5] Technisch gezien wijst het NS-record een naam en (via A/AAAA- en glue records) een IP-adres aan voor een (logische) DNS-server. Het is denkbaar dat dit IP-adres naar verschillende fysieke servers verwijst (*anycast*).

[6] Een ISP of organisatie kan voor het eigen netwerk eventueel ook zélf een root-server opereren, op basis van de door ICANN gepubliceerde root zone. [29]

informatie op over "dialogic.nl.". Omdat Dialogic haar webhosting heeft uitbesteed verwijst de server van SIDN hier door naar "ns1.co-co.nl.". In de laatste stap wordt aan deze server gevraagd wat het adres is dat hoort bij het subdomein "www" onder "dialogic.nl." en komen we uit bij "141.138.169.205", het antwoord op de vraag.

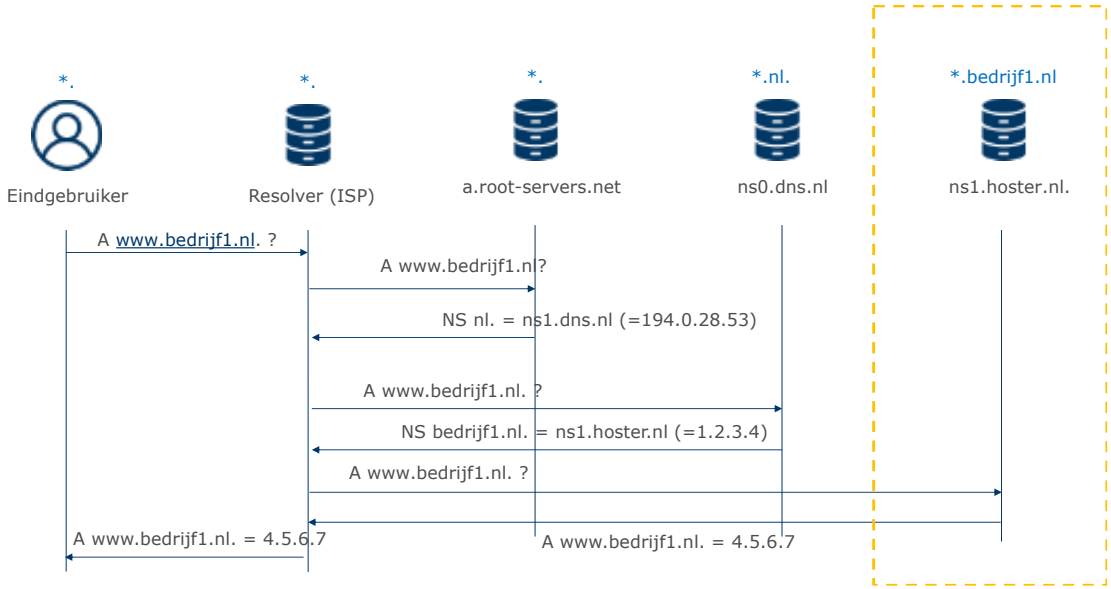


Figuur 2 Het recursief opzoeken van informatie over een domein (hier "www.dialogic.nl.") in het DNS

Wat opvalt in bovenstaande is dat (in dit voorbeeld) maar liefst vier verzoeken nodig zijn aan verschillende DNS-servers om tot het adres voor een domeinnaam te komen. In totaal kost de operatie 153 milliseconden. Dat lijkt weinig, maar met de hedendaagse internetsnelheden had de hele website van Dialogic in die tijd al geladen kunnen zijn. Informatie uit het DNS wordt daarom op verschillende plaatsen 'gecached': onthouden zolang deze nog geldig is. In het DNS is per record aangegeven hoe lang het antwoord mag worden onthouden (de *time to live* of 'TTL'-waarde). Gedurende deze tijd onthoudt het besturingssysteem en/of de browser het record, zodat het niet voor iedere webpagina de domeinnaam opnieuw hoeft te worden opgezocht.

Naast deze *caching* kan ook gebruik worden gemaakt van een *resolving server* of 'resolver'.[7] Een *resolver* is een DNS-server die antwoord geeft op *alle* DNS-vragen die worden gesteld, door het antwoord eventueel zelf op te zoeken middels *recursive resolving* bij de authoritative bronnen. Een *resolver* is dus zelf niet 'authoritative'. Internetproviders bieden aan klanten in vrijwel alle gevallen toegang tot een resolver. Doordat veel klanten dezelfde resolver gebruiken kan deze resolver efficiënt DNS-antwoorden onthouden en wordt het opzoeken van domeinnamen voor alle klanten sneller.

Onderstaand Figuur 3 toont het proces schematisch voor een situatie waarin een eindgebruiker een DNS-resolver van een ISP gebruikt. Wanneer de resolver beschikt over een actuele kopie van het gevraagde record, dan worden alleen de stappen tussen eindgebruiker en de resolver uitgevoerd (de resolver antwoordt uit het 'eigen geheugen'). Wanneer dit niet het geval is wordt het recursieve proces doorlopen (deel van de interacties rechts van de resolver). De meest rechtse DNS-server is de (voor dit domein) authoritative DNS-server.



Figuur 3 Schematische weergave van het proces van het 'resolven' van het adres voor een domeinnaam in DNS

2.2 DNS-dienstverlening

In bovenstaande is besproken welke verschillende functies het DNS vervult. De functies kunnen in de praktijk door verschillende partijen worden uitgevoerd. Omdat we in dit onderzoek inventariseren welke partijen essentiële DNS-diensten leveren, is van belang om deze modellen te bekijken.

2.2.1 DNS-resolver-diensten

Zoals hierboven is toegelicht wordt met "to resolve" het opzoeken van informatie in DNS bedoeld. Om dit proces te versnellen bieden de meeste ISP's en grotere organisaties aan

[7] De term 'resolver' wordt breder gebruikt dan voor resolving servers; in feite is ieder stuk software dat het DNS bevraagt een 'resolver'.

hun gebruikers toegang[8] tot een "DNS resolver" – een DNS-server die informatie verstrekt voor domeinen waar het zelf niet de authoritative bron voor is. De resolver zoekt de informatie op bij de authoritative bron en 'onthoudt' deze gedurende een bepaalde tijd.

Gebruikers van DNS-resolvers zijn in de regel eindgebruikers: klanten van ISP's (consumenten, kleinzakelijke gebruikers, en in sommige gevallen grotere organisaties). Daarnaast betreft het gebruikers binnen (meestal grotere) organisaties. Ook aan de aanbiedende kant is het gebruik van DNS-resolvers gemeengoed; ook webapplicaties en dergelijke zullen af en toe behoefte hebben aan informatie uit het DNS, en daarvoor de resolver van de webhoster raadplegen. Een ander voorbeeld zijn e-mailservers.

2.2.2 Authoritative DNS-diensten

Onder authoritative DNS valt alle DNS-dienstverlening die authoritative is voor een bepaalde DNS-zone. Zo zijn de root-servers authoritative voor de root-zone; deze servers geven antwoorden voor informatieverzoeken over de root-zone, maar niet over andere zones. Hetzelfde geldt voor de zones op TLD-niveau en 'lager'. Op root- en TLD-niveau is over het algemeen steeds één organisatie verantwoordelijk voor het realiseren van de authoritative DNS-dienst (voor het .nl-domein is dat SIDN). Veelal is het aantal domeinen groot genoeg om investering in eigen infrastructuur te rechtvaardigen. Een organisatie als SIDN beheert dan ook de eigen DNS-dienst.

Anders wordt het op de lagere niveaus. Veel domeinhouders (eigenaren van een SLD) zullen zelf geen interesse (noch expertise) hebben in het draaiend houden van een eigen authoritative DNS-server. Voor hen is weliswaar belangrijk dat de informatie over het eigen domein beschikbaar blijft, maar spelen er geen aanvullende eisen of beperkingen die maken dat er een eigen DNS-server nodig is. Het overgrote deel van de domeinhouders zal het realiseren van authoritative DNS uit handen geven aan een gespecialiseerde partij – veelal de partij waarbij de domeinnaam werd geregistreerd. Van deze partijen zijn verschillende soorten te identificeren:

- **Full-service webhosters.** Dit zijn vaak wat grotere partijen die naast domeinregistratie ook authoritative DNS, webhosting, e-mail en aanverwante diensten levert. De domeinhouder kan bij één partij terecht voor alle 'basisdiensten' die nodig zijn voor een website en eigen e-maildomein.

- **Reseller webhosters**. Dit zijn partijen die gebruik maken van infrastructuur van een **wholesale (whitelabel) webhoster**. Zij richten zich specifiek op een bepaalde markt of soort gebruiker, en bieden daarbij bijvoorbeeld aanvullende ondersteuning of specifieke functionaliteit (denk bijvoorbeeld aan webwinkelsoftware). Het registreren van de domeinnaam en de DNS-dienstverlening worden overgelaten aan de wholesale-leverancier.

- **ISP's.** Voorheen was het gebruikelijk dat ook ISP's deze diensten leverden – tegenwoordig doen feitelijk alleen de op de zakelijke markt gerichtte ISP's dit nog.

In het resultatenhoofdstuk zoomen we nader in op de organisaties die wél zelf eigen authoritative DNS realiseren. Wanneer de domeinhouder zélf zijn authoritative DNS realiseert kan dit op verschillende manieren worden gedaan:

---

[8] Binnen grotere organisaties zullen gebruikers typisch verplicht worden de eigen DNS-resolver te gebruiken, omdat ook interne namen worden gedefinieerd via deze DNS-server, en om toegang tot bepaalde DNS-informatie te kunnen blokkeren.

- **Middels een eigen server ('co-located', 'dedicated' of 'virtueel' bij een hoster).** De domeinhouder draait op deze server(s) DNS-software en vraagt de registrar om de NS-records te laten verwijzen naar deze server(s). Typische gebruikers zijn bedrijven die specifieke eisen aan DNS-stellen (denk aan VoIP-aanbieders) of diensten aan hun klanten leveren (kleine en middelgrote ICT-leveranciers, bijvoorbeeld).

- **Middels een eigen server in het eigen netwerk (eigen AS).** Grotere organisaties hebben een eigen AS (logisch netwerk dat aan het internet is verbonden) en realiseren hun DNS-server middels een server binnen dit AS. Zij zijn als zodanig te herkennen doordat een NS-record verwijst naar een IP-adres binnen het eigen AS. Domeinregistratie wordt vaak uitbesteed aan een gespecialiseerde registrar (die geen webhosting levert, maar bijvoorbeeld wel domeinen kan registreren in een groot aantal TLD's, en wellicht ook andere vormen van merkbeheer doet; een voorbeeld van een wereldwijde speler op dit vlak is Markmonitor).

- **Middels een separate DNS-dienst.** De domeinhouder neemt bij een hoster een losse DNS-dienst af en vraagt de registrar om de NS-records naar deze partij te laten verwijzen. Het beheer van de informatie geschiedt vervolgens via een (web)interface bij deze partij. Dergelijke diensten bieden vaak meerwaarde in de vorm van 'load balancing' (het verspreiden van gebruikers over servers), DDoS-preventie, et cetera. Een voorbeeld is 'Route 53' van Amazon [8] en de dienstverlening van CloudFlare. Gebruikers zijn typisch de wat populairdere websites. De DNS-server is specifiek ingericht om gebruikers over bepaalde IP-adressen te verdelen.

Een praktijk die tot slot veel wordt toegepast is "DNS fronting" – hierbij is een DNS-dienst van een derde partij aangewezen als authoritative middels NS-records. Deze DNS-dienst betrekt zijn informatie echter uit een achterliggende DNS-server. In sommige gevallen is een dergelijke constructie te identificeren aan de hand van het SOA-record. Een voorbeeld is "ah.nl" (Albert Heijn). De NS-records verwijzen naar servers van Akamai, maar het SOA-record verwijst naar een server van Ahold zelf.

2.3 Impact van verstoring en uitval

Wanneer het DNS niet kan worden bevraagd, werken veel diensten niet meer naar behoren. Zo kunnen websites niet meer worden bezocht, omdat het niet mogelijk is om te achterhalen met welk IP-adres er moet worden gecommuniceerd. E-mailbezorging valt stil, omdat een e-mailserver niet meer kan opzoeken welke server de mail in ontvangst kan nemen voor een bepaald domein. Naast deze diensten zijn er talloze andere diensten voor welke DNS essentieel is.

Omdat het DNS zo belangrijk is, zijn er verschillende maatregelen genomen om zowel de kans als de impact van uitval te verkleinen:

- Voor een zone kunnen meerdere DNS-servers worden aangewezen als 'authoritative'. Eerder zagen we dat voor de ".nl."-zone wordt verwezen naar "ns1.dns.nl.", "ns2.dns.nl." en "ns3.dns.nl.". Een resolver kiest willekeurig één van de servers en bevraagt de volgende als de gekozen server niet beschikbaar is. De verschillende nameservers worden meestal in verschillende datacenters en in verschillende

netwerken geplaatst, zodat uitval van een locatie niet leidt tot uitval van authoritative DNS voor de zone.[9]

- De *time-to-live* (TTL)-waarde bepaalt dat informatie een bepaalde tijd mag worden onthouden. Deze periode varieert typisch van een seconde tot enkele dagen. Voor informatie die nauwelijks verandert wordt vaak een hogere TTL-waarde ingesteld. Dit stelt *resolver*s in staat om de gegevens te onthouden, zodat bij uitval van de authoritative DNS-servers er nog enige tijd een kopie beschikbaar is bij de resolver. Wie de resolver gebruikt merkt gedurende die tijd niets van uitval, zolang de resolver de gezochte gegevens kort daarvoor wel heeft kunnen opvragen.

- Het DNS is hiërarchisch opgebouwd, en het beheer van de verschillende zones ligt bij verschillende partijen. Uitval van authoritative DNS-informatie is dus specifiek voor bepaalde zones. Uitval van de root servers zou leiden tot uitval van het volledige DNS. De root servers zijn echter zeer redundant uitgevoerd. Daarnaast is de kans dat een DNS-resolver beschikt over de informatie die de root servers verstrekken zeer groot, omdat deze informatie voor het opzoeken van *alle* domeinnamen nodig is.

2.3.1 Impact van uitval en verstoring

Kijken we naar de gevolgen van uitval en verstoring, dan is het eerder besproken 'model' waarmee authoritative DNS wordt gerealiseerd bepalend voor de impact:

- Wanneer een DNS-server wordt verstoord van een grotere organisatie die zijn eigen DNS heeft gerealiseerd (in eigen AS of ten minste op een eigen server) dan zullen over het algemeen alleen de diensten van deze partij onbereikbaar worden voor eindgebruikers. Het is ook denkbaar dat in dat geval zaken als VPN- of e-mail voor eigen medewerkers niet meer beschikbaar zijn. Omdat er vaak meerdere redundante DNS-servers zijn ingericht dienen echter wel alle (als NS genoemde) servers te worden verstoord om tot grootschalige uitval te leiden. Missiekritische processen zullen over het algemeen niet afhankelijk zijn van een openbaar bereikbare server.

- Wanneer de DNS-servers worden verstoord van een partij die diensten voor anderen aanbiedt, kunnen alle klanten van deze partij bovengenoemde problemen ondervinden. Merk op dat klanten in theorie wel zouden kunnen 'spreiden' over meerdere aanbieders (al lijkt dit, gezien de resultaten uit de steekproef, niet gangbaar).

- Wanneer de DNS-resolvers worden verstoord zullen alle klanten van de betreffende ISP, of alle gebruikers binnen de organisatie, hier last van hebben. In sommige gevallen is een 'alternatieve' resolver ingesteld, zodat beiden zouden moeten worden verstoord om tot volledige uitval te leiden. Ook kunnen klanten van een ISP vaak zelf een andere DNS-resolver uitkiezen.

[9] Of een van de NS-servers ook is ingesteld als SOA heeft hier geen invloed. Wel zou verstoring van de SOA-server kunnen leiden tot het later of niet (goed) bijwerken van informatie op de andere (niet-SOA) NS-servers.

2.3.2 Aantasting van de integriteit van DNS-informatie

Wanneer een kwaadwillende informatie in het DNS kan wijzigen, kan dat nadelige gevolgen hebben. Naast de DNS-server zijn ook omliggende systemen van DNS-aanbieders en beheerders van TLD-zones hiervoor gevoelig. Via deze omliggende systemen is het immers mogelijk de informatie in DNS te wijzigen. Mogelijke gevolgen van aantasting van de integriteit van DNS-informatie zijn (niet-uitputtend):

- Het verkeer gericht aan een bepaald domein kan worden 'omgeleid' naar een ander adres. Wanneer op de applicatielaag geen authenticatie plaatsvindt van de dienst, kan een gebruiker nietsvermoedend verbinding maken met de aanvaller en bijvoorbeeld wachtwoorden prijsgeven.

- Door het aanpassen van 'MX'-records kan e-mailverkeer worden omgeleid naar een andere server.

- Door het aanpasen van SPF- en 'domain key' records in DNS kan een aanvaller e-mail versturen (vanaf eigen server) namens het domein.

- Door het aanpassen van bepaalde TXT-records kan een aanvaller toegang krijgen tot systemen (bijvoorbeeld analytics-systemen) of zelfs SSL-certificaten registreren namens het domein.

Een dergelijke aanval is op verschillende manieren te realiseren (niet-uitputtend):

- Een kwaadwillende zou toegang kunnen krijgen tot de systemen van een registrar of zelfs de registry (SIDN), en zo volledige controle over de authoritative informatie van een domeinnaam kunnen krijgen. Ook het hacken van DNS-servers is denkbaar.

- Een aanvaller zou ongemerkt een 'eigen' DNS-resolver kunnen instellen voor een nietsvermoedende eindgebruiker. Deze resolver kan onjuiste informatie verstrekken. Deze tactiek is in het verleden ook gebruikt om advertenties te injecteren op webpagina's.

- Een aanvaller zou DNS-verkeer kunnen onderscheppen en dit kunnen wijzigen. Hiervoor is toegang vereist tot apparatuur tussen de eindgebruiker en het internet (bijvoorbeeld de firewall of router). Grotere organisaties en ISP's gebruiken deze methode om toegang tot bepaalde websites te beperken.

- Een kwaadwillende kan een domeinnaam registreren die sterk lijkt op een legitieme domeinnaam ("lng.nl" in plaats van "ing.nl"). Deze techniek ('domain squatting') maakt gebruik van typfouten en onoplettendheid van eindgebruikers. Een variant is het gebruik van subdomeinen als ware het top-leveldomeinen ("abnamro.nl.lang.domein.van.de.aanvaller.com" – de gebruiker ziet alleen het eerste deel).

Tegen bovenstaande aanvallen zijn diverse mitigaties ontwikkeld. Deze technieken maken vooral het DNS-systeem zélf beter bestendig, en niet de omliggende systemen. Zo biedt DNSSEC aan resolvers de mogelijkheid om te verifiëren of informatie in het DNS daadwerkelijk door de geautoriseerde beheerder ervan is geplaatst, of dat deze is gefalsifieerd. Via technieken als DNS-over-HTTPS (DoH) en DNS-over-TLS (DoT) kan worden voorkomen dat DNS-verkeer onderweg kan worden ingezien en gemanipuleerd. Technieken als 'Oblivious DoH' (ODoH) voorkomen tot slot dat aanbieders van DNS-resolvers uit DNS-verzoeken informatie kunnen afleiden over hun gebruikers. Op de applicatielaag vinden we technieken als HTTPS en 'STARTTLS' voor SMTP, waarmee gebruikers een melding krijgen bij het

'omleiden' van een website en waarbij omleiding van e-mailverkeer niet zonder meer mogelijk is. Tot slot zou (op basis van bijvoorbeeld Certificate Transparency) actief kunnen worden gemonitord op het gebruik van phishingdomeinen.

Voor wat betreft scope van impact geldt in principe hetzelfde als in voorgaande paragraaf beschreven: wanneer een ISP geen DNSSEC aanbiedt, zijn de klanten van deze ISP (die niet zelf een DNS-resolver hebben ingesteld die wél DNSSEC aanbiedt) in principe niet beschermd en vatbaar voor bepaalde aanvallen.

3 Onderzoeksmethode

3.1 Aanpak

In het onderzoek hanteren we een combinatie van kwalitatieve en kwantitatieve methoden. We verzamelen informatie uit het DNS zélf en gebruiken deze om de marktaandelen van de verschillende aanbieders te bepalen. Vervolgens identificeren we de in Nederland gevestigde aanbieders van authoritative DNS-diensten. Tot slot analyseren we de resultaten kwalitatief: worden er bijvoorbeeld ándere DNS-diensten aangeboden (zoals DDoS-preventie)?

3.2 Kwantitatieve analyse (meting)

Middels een meting beogen we tot concrete aantallen en marktaandelen te komen. Door het DNS zélf als databron te gebruiken kunnen we hiervoor de benodigde informatie verzamelen. Op hoofdlijnen werkt dit als volgt:

1. We stellen een lijst samen met een steekproef van voor Nederland relevante domeinnamen (second-level domains).
2. Voor alle domeinen in de steekproef zoeken we in het DNS (geautomatiseerd) op welke DNS-servers authoritative zijn
3. We bepalen wie de DNS-dienst aanbiedt, en of dit een in Nederland gevestigde partij is.

3.2.1 Samenstellen steekproef domeinnamen

Het achterliggende doel van de Europese NIB-richtlijn is het beschermen van maatschappij en economie tegen de impact van cyberincidenten. Hier gaat het specifiek om het vergroten van de weerbaarheid van netwerk- en informatiesystemen binnen de Europese Unie [9]. Bij het aanwijzen van aanbieders van essentiële diensten gaat het dus om diensten die van essentieel belang zijn voor de instandhouding van kritieke maatschappelijk en/of economische activiteiten.

De richtlijn wordt per lidstaat geïmplementeerd, waarbij per lidstaat essentiële aanbieders aangewezen. Het is uiteraard denkbaar dat een dienst die in de ene lidstaat waarde vertegenwoordigd, afhankelijk is van een (essentiële) dienst in een andere lidstaat. In dit onderzoek wordt uitsluitend gekeken naar de diensten die relevant zijn voor maatschappelijke/economische activiteiten in Nederland. Daarbij kunnen uiteraard DNS-aanbieders worden gevonden die zich in een andere EU-lidstaat bevinden. In dit onderzoek rapporteren we deze aanbieders specifiek, zodat deze informatie eventueel kan worden gedeeld met de betreffende lidstaten. Onderstaande Tabel 1 toont de ‘scope’ van deze studie schematisch.

Tabel 1 Overzicht afbakening onderzoek

	Afhankelijk van DNS-dienst van aanbieder gevestigd in Nederland	Afhankelijk van DNS-dienst van aanbieder gevestigd in andere EU-lidstaat	Niet afhankelijk van een DNS-dienst van een aanbieder gevestigd in een EU-lidstaat
DNS-diensten relevant voor maatschappelijke/economische activiteiten in Nederland	✓	✓	✓
DNS-diensten niet relevant voor Nederland, maar wel voor een andere lidstaat			
DNS-diensten niet relevant voor EU-lidstaat			

Concreet bestaat de set met einddiensten die relevant zijn voor Nederland (hier economische en/of maatschappelijke waarde vertegenwoordigen) in de context van DNS uit een set *domeinnamen*. Er bestaat echter geen eenduidige registratie van wat voor Nederland een relevante domeinnaam is. De volgende databronnen zijn overwogen:

- **Overzichten van 'top 1000' van in Nederland bezochte websites.** Mits een betrouwbare bron wordt gebruikt geeft dit een goed beeld voor zover het de populaire websites betreft. De populariteit van websites is echter zeer scheef verdeeld – veel economische waarde is waarschijnlijk vertegenwoordigd in een groot aantal minder populaire websites. We vermoeden (en stellen verderop vast) dat de grotere partijen de DNS voor populaire websites daarnaast anders inrichten dan de kleinere, minder populaire websites. De grotere partijen zullen vaker hun eigen DNS inrichten en/of gebruik maken van specifieke diensten, terwijl de kleinere partijen (bijvoorbeeld mkb'ers) vaker zullen inkopen bij webhosters.

- **Gegevens uit het handelsregister.** KVK houdt sinds lange tijd bij wat het webadres is van geregistreerde bedrijven. Een nadeel van deze methode is dat de data waarschijnlijk niet compleet is, nauwelijks wordt geactualiseerd (registratie bij inschrijving), slechts één domeinnaam per bedrijf bevat, en het verkrijgen van een grote steekproef kostbaar is. Een voordeel is dat een koppeling kan worden gemaakt naar sector (SBI-indeling) en er meer zekerheid bestaat over de achterliggende economische waarde.

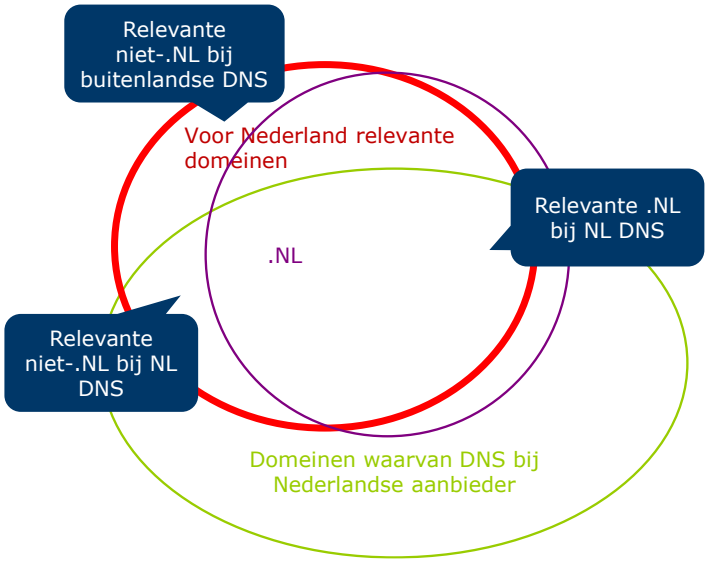
- **Het .nl-domein.** Veel Nederlandse websites maken gebruik van het .nl-domein. Het .nl-domein is een goede indicatie van 'gericht zijn op de Nederlandse markt': er is voor buitenlandse partijen nauwelijks interesse in het gebruiken van een .nl-domeinnaam[10], en veel Nederlandse bedrijven en organisaties hebben (ten minste) een .nl-

[10] SIDN geeft aan dat slechts een klein deel van de ".nl"-domeinnamen (enkele procenten) is geregistreerd door domeinhouders met een vestigingsplaats buiten Nederland. Voor andere ccTLD's, zoals ".to", ".it" en ".io", is wel veel interesse buiten het betreffende land, omdat met het achtervoegsel

domein. Hoewel er geen openbaar beschikbare lijsten bestaan van .nl-domeinnamen, is het wel mogelijk deze te verzamelen (zie verderop). Het nadeel is uiteraard dat voor Nederland relevante diensten die (uitsluitend) via een niet-.nl-domein actief zijn, niet worden gevonden. Met de juiste databron is er (door ".nl" als vertrekpunt te nemen) echter wel een zeer grote (en daarmee betrouwbare) steekproef mogelijk. Daarnaast kunnen we gebruik maken van de kennis waarover SIDN (die het .nl-domein beheert) beschikt.

In het onderzoek kiezen we voor de laatste bron als primair uitgangspunt. Daarbij verzamelen we overigens ook een set met niet-".nl"-domeinnamen, die we inzetten als 'controlegroep'. We verifiëren of in deze groep de verdeling van domeinen over de verschillende aanbieders vergelijkbaar is. Vanwege de grotere populatiegrootte versus de steekproefgrootte bij deze 'controlegroep' is de precisie van de geschatte marktaandelen hier echter een stuk beperkter dan in de ".nl"-groep.

Onderstaande Figuur 1 toont schematisch de dekking van de .nl-domeinnamen versus de voor de onderzoeksvraag relevante sets. Concreet kijken we voor een steekproef van .nl-domeinnamen (blauwe cirkel) naar het aantal diensten dat afhankelijk is van DNS-diensten van in Nederland gevestigde aanbieders (groene cirkel). Daarbij is de aanname dat het overgrote deel van de .nl-domeinen relevant is voor Nederland (rode cirkel). Daarnaast nemen we aan dat de verdeling over aanbieders binnen de (steekproef uit de) set van .nl-domeinnamen overeenkomt met de populatie (groene cirkel).



Figuur 4 Overzicht van de verschillende sets met domeinnamen en hun relevantie in dit onderzoek

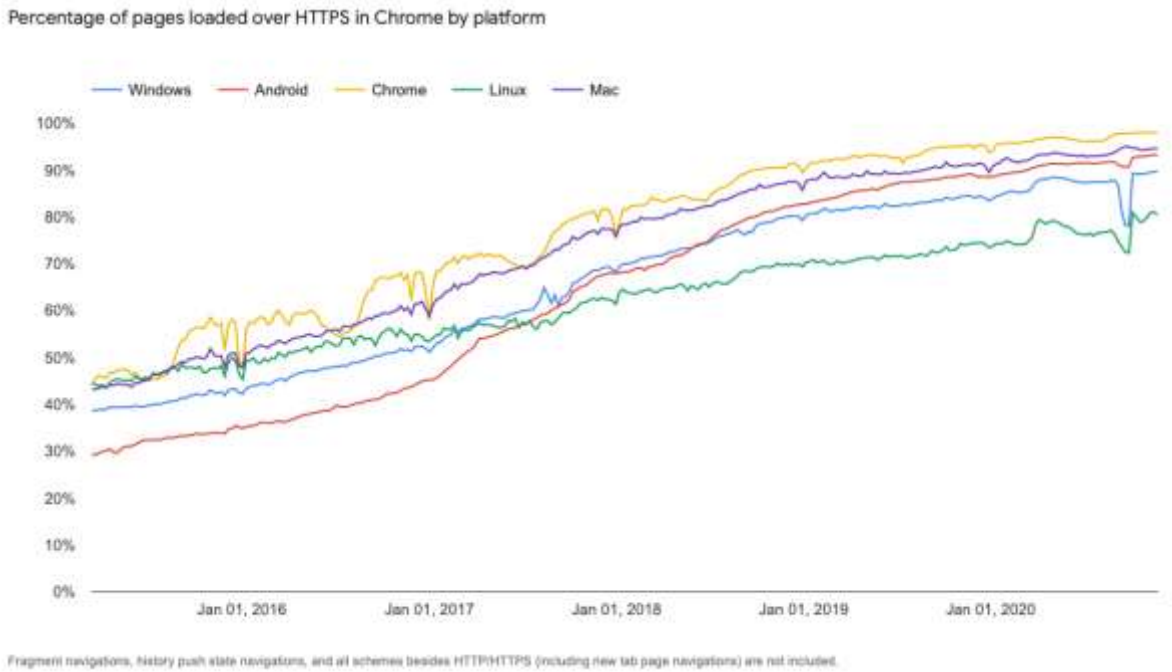
Omdat er geen openbaar beschikbare lijsten van .nl-domeinnamen beschikbaar zijn (uit officiële bron) wordt de steekproefset .nl-domeinnamen samengesteld op basis van andere bronnen. In dit onderzoek maken we gebruik van zogenaamde *certificate transparency (CT) logs*. Het CT-ecosysteem bestaat uit een aantal openbare databases, aangeboden door enkele grotere internetpartijen (o.a. Google en CloudFlare), waarin alle aanvragen voor SSL-certificaten worden geregistreerd. Deze certificaten worden gebruikt om internetverbindingen (specifiek voor het bezoeken van websites: "https") te beveiligen. Om te voorkomen dat een willekeurige certificaatautoriteit een certificaat uitgeeft voor een website die daar geen

'mooie' woorden kunnen worden gevormd: "www.go.to". Deze dynamiek speelt voor zover bekend niet voor het ".nl"-domein.

toestemming voor heeft gegeven, zijn allerlei maatregelen ingericht. Een van de maatregelen is het openbaar maken van alle registraties via de CT-logs, zodat door iedereen is te controleren welke autoriteiten voor welke domeinen certificaten uitgeven.

Iedere vermelding in het CT-log bevat de relevante informatie over de certificaatautoriteit en het certificaat (waaronder de domeinnaam en de datum waarop het certificaat werd aangevraagd). Zodoende kan uit een CT-log een set met domeinnamen worden geëxtraheerd. Vanwege de verificatie die nodig is voor het aanvragen van een certificaat gaat het daarbij in vrijwel alle gevallen om domeinen waarop daadwerkelijk een website actief is, wat voor deze steekproef een prettige bijkomstigheid is. Er zijn aanwijzingen dat zoekmachines en cybercriminelen de informatie uit CT-logs gebruiken voor 'domain discovery'. [10] De techniek kan ook gebruik worden om phishingdomeinen op te sporen. [11]

Omdat de CT-logs voor een heel ander doel zijn ingericht dan voor het nemen van aselecte steekproeven van domeinnamen is het van belang om vast te stellen of de genomen steekproef een juiste afspiegeling is van de populatie. Afgaand op diverse statistieken, waaronder van Google, blijkt dat het aantal webpagina's dat via HTTPS (en dus gebruik makend van een certificaat) wordt bezocht, intussen boven de 80% van het totaal ligt (Figuur 5). Veel browsers geven sinds enkele jaren diverse waarschuwingen wanneer geen HTTPS wordt gebruikt, en er toch wachtwoorden of creditcardgegevens worden uitgewisseld, wat de adoptie van HTTPS waarschijnlijk sterk heeft versneld. De meeste domeinen zullen dus in de set vertegenwoordigd zijn in het CT-log. De Mozilla Foundation geeft aan dat er verwacht wordt dat er in de Firefoxbrowser uiteindelijk helemaal geen ondersteuning meer zal zijn voor HTTP-only-websites. Dit is in een recente versie van de browser reeds als optie doorgevoerd [12].[11]



Figuur 5 Ontwikkeling van het aantal webpagina's dat over HTTPS wordt geladen [13]

We kunnen ons voorstellen dat de domeinen die *niet* vertegenwoordigd zijn, specifieke eigenschappen hebben. Zo zal het wellicht gaan om kleinere websites met minder gevoelige

[11] Zie [mozilla.org]

inhoud (bijvoorbeeld geen webwinkels waarbij creditcardgegevens worden uitgewisseld). Een andere vorm van bias zou kunnen worden veroorzaakt door de wijze waarop certificaten worden aangevraagd. Vaak wordt dit als dienst aangeboden door webhosters, die dit geautomatiseerd regelen voor alle klantdomeinen. Wanneer een webhoster dit (nog) niet aanbiedt, zal deze sterk ondervertegenwoordigd zijn in de steekproef.

Tot slot is van belang dat domeinen van diensten die niet zijn gericht op eindgebruikers ondervertegenwoordigd kunnen zijn in de CT-dataset. Voor deze domeinen is de kans groter dat geen of geen CT-geregistreerde (bijvoorbeeld *self-signed*) certificaten worden gebruikt. Hoewel dit in potentie een grote groep domeinen betreft met potentieel grote impact bij uitval (denk bijvoorbeeld aan M2M-toepassingen) is het de vraag of dergelijke kritieke toepassingen afhankelijk zullen zijn van openbare DNS en/of van het aanbod van de hier onderzochte (soorten) aanbieders van DNS-diensten.

3.2.2 Bepalen aanbieder authoritative DNS

Voor alle domeinen in de steekproef bepalen we, door opzoeken in DNS, welke servers (technisch gezien eveneens DNS-namen) zijn aangewezen als NS- en SOA voor het domein. Aan de hand van deze informatie wordt vervolgens bepaald door wie de DNS-dienst wordt aangeboden.

Zoals eerder toegelicht zijn per domeinnaam (zone) meestal meerdere NS-servers aangewezen, en zijn deze samen verantwoordelijk voor de adresinformatie binnen die zone ('onder' het domein). Daarbij geldt dat de NS-servers vaak zijn verspreid over locaties, netwerken en aanbieders omwille van redundantie. Om dubbeltellingen te voorkomen maken we daarom primair gebruik van het SOA-record. In veel gevallen (98,1% in onze steekproef) is de als SOA genoemde server namelijk ook één van de NS-servers. De aanname is dat dit de 'primaire' verantwoordelijke server is.

Gedurende het onderzoek is ook steeds geteld op basis van de NS-records, en zijn afwijkingen nader handmatig onderzocht. Een voorbeeld is de situatie voor het domein "ah.nl" (Albert Heijn). De SOA voor dit domein is "ns0.ahold.nl", een server die in de IP-adresruimte (AS) van "AHOLD" blijkt te staan. Voor het domein worden echter zes servers van Akamai ("aX-YY.akam.net.") aangewezen als NS-server. In dit geval levert Akamai een DNS-dienst aan Ahold (waarschijnlijk omwille van DDoS-preventie of redundantie) en levert Ahold de juiste informatie aan Akamai via een eigen DNS-server. Hoewel de server van Ahold technisch gezien authoritative is (en overigens ook benaderbaar door eindgebruikers als zodanig) zijn de facto de servers van Akamai authoritative voor dit domein in het dagelijks gebruik.

De locatie van de aanbieder van de DNS-dienst is op verschillende manieren af te leiden. Die locatie zou kunnen aangeven of een aanbieder wel of niet in Nederland gevestigd is. De volgende invalshoeken zijn onderzocht:

- **TLD van de naam van de SOA/NS-server.** DNS-servers van Nederlandse partijen hebben typisch een DNS-naam 'onder' een domeinnaam van de webhoster: "ns1.webhoster.nl". De TLD van deze naam (hier ".nl") zou een indicatie kunnen zijn van de vestigingsplaats van de aanbieder. Er zijn echter redenen voor aanbieders om ook onder andere TLD's (bijvoorbeeld van een buurland) een DNS-server in te richten. Een van de redenen is redundantie; mocht de ".nl"-zone niet meer functioneren, dan is een DNS-server buiten die zone nog wel bereikbaar.[12] Daarnaast

[12] Zij het in die situatie niet meer bruikbaar voor het volledig recursive opzoeken van informatie voor een ".nl"-domeinnaam (de ".nl"-zone is immers niet bereikbaar om de juiste NS-records op te kunnen halen), maar nog wel voor niet-".nl"-domeinnamen.

hebben sommige hosters nevenbedrijven of -locaties in andere landen, en komt de naam in dat geval waarschijnlijk overeen met het land waarin de DNS-server is geplaatst.

- **Landcode van het AS waarbinnen het IP-adres van de SOA/NS-server valt**. Het IP-adres van de DNS-server is per definitie onderdeel van een bepaald IP-adresblok, dat weer is gekoppeld aan een AS (*Autonomous System*) – een zelfstandig, via het openbare internet routeerbaar netwerk. Van AS'en is allerlei informatie bekend, waaronder de naam van de bijbehorende organisatie en een landcode, die veelal verwijst naar de vestigingsplaats. Voor Europa wordt de toewijzing van IP-adresblokken en de registratie van AS-nummers beheerd door RIPE. De door RIPE geregistreerde landcode verwijst naar de 'locatie van het netwerk' – een notie waarbij diverse vraagtekens kunnen worden gezet. RIPE is voornemens de country code 'op te schonen' en informatie te verzamelen over de juridische vestigingsplaats van de houders van AS-nummers. [14] Voor onze analyse betekent dit dat we weliswaar kunnen selecteren op de "NL"-landcode, maar dat we alle vermeldingen handmatig moeten controleren op juistheid.

- **Responstijd van de DNS-server**. Een DNS-server die binnen een bepaalde tijdsinterval reageert, moet zich vanwege fysieke beperkingen (lichtsnelheid) binnen Nederland bevinden. Het is echter niet eenvoudig om een absolute grenswaarde te bepalen (deze is immers niet alleen afhankelijk van de lichtsnelheid, maar ook van de route van de betreffende kabels, vertraging in tussenliggende apparatuur) en daarnaast is de looptijd lastig te meten (onder andere vanwege ruis door ander verkeer).

- **"Trace route"-informatie van de route naar de DNS-server.** Op basis van "trace route"-gegevens is te bepalen welke route verkeer van en naar de DNS-server volgt. Uit deze informatie kan worden afgeleid via welke AS'en en routers het verkeer loopt, wat iets zou kunnen zeggen over de locatie. Hoewel dit met handmatige inspectie goed lijkt te werken, is het lastig te automatiseren.

Merk op dat de verschillende meetmethoden relateren aan verschillende opvattingen over "vestigingsplaats". Informatie op basis van routering en AS-nummers zegt wellicht iets over de 'fysieke' locatie van een DNS-server, terwijl informatie op basis van DNS-namen wellicht eerder iets zegt over de "logische" locatie. Een voorbeeld is een Nederlandse webhoster die voor de DNS-dienst gebruik maakt van een (van origine Amerikaanse) cloudaanbieder. Het AS-nummer verwijst in dit geval naar de VS, terwijl de naam van de NS/SOA-server waarschijnlijk nog wel op ".nl" eindigt.

Voor dit onderzoek kiezen we voor een aanpak die neigt naar "false positives" (liever een aanbieder onterecht markeren als "gevestigd in Nederland" dan andersom). Vervolgens filteren we de 'false positives' handmatig uit deze lijst. In de eerste fase labelen we aanbieders als "Nederlands" indien het TLD van de SOA overeenkomt met ".nl". We verifiëren deze toewijzing door te controleren of ten minste één NS-record eindigt op ".nl" en of de server waarnaar de NS- en SOA-records verwijzen wellicht in Nederland staan.

3.2.3 Aggregatie

Bij het aggregeren van de resultaten en het 'tellen' van domeinnamen spelen diverse valkuilen.

Het tellen van domeinnamen

Bij het bepalen van marktaandelen ligt het in deze context voor de hand om domeinnamen te tellen. Logisch gezien is dit de eenheid in DNS waarmee wordt gewerkt – DNS-diensten worden typisch per domeinnaam geleverd. Hierbij spelen echter verschillende kanttekeningen:

- De notie 'domeinnaam' is niet precies gedefinieerd. Een voor de hand liggende definitie is die van "second-level domain" (SLD): de namen die worden geregistreerd onder de TLD's. Dat leidt echter niet voor alle TLD's tot de juiste resultaten. Voor sommige TLD's geldt immers dat een verdere uitsplitsing is gemaakt; een bekend voorbeeld is het ".uk"-domein. Tot 2014 was het alleen mogelijk om onder bepaalde subdomeinen hiervan een domein te registreren (waarvan ".co.uk" de bekendste is). In deze telling is alleen "co.uk" geteld. Een correctie voor dergelijke "public suffixes" is, met enige voorzichtigheid mogelijk op basis van de 'Public Suffix List'. [15] Voor .nl speelt de problematiek in principe niet; in deze analyse is daarnaast het exacte aantal SLD's in de referentieset niet bijster relevant. In deze analyse volstaan we dan ook met het tellen van SLD's.

- De waarde die een domeinnaam vertegenwoordigt in economie en maatschappij is sterk wisselend. Een enkele domeinnaam (denk aan booking.com, klm.nl, et cetera) kan verantwoordelijk zijn voor vele miljoenen omzet, terwijl er naar verwachting een veel groter aantal is dat nauwelijks waarde vertegenwoordigt. Het simpelweg tellen van domeinnamen doet hieraan geen recht. Andersom is ook het kijken naar alleen de top-domeinnamen geen juiste aanpak, omdat (zoals elders aangegeven) voor hen speelt dat DNS vaak anders is ingericht. Daarnaast vermoeden we dat er sprake is van een grote 'long tail' onder domeinnamen (veel kleinere bedrijven die opgeteld veel waarde vertegenwoordigen).

Technische afwijkingen

Een aantal andere valkuilen bij het tellen van domeinnamen zijn meer technisch van aard:

- Sommige domeinen zijn door hosting- of andere partijen 'geparkeerd': de aanbieder houdt de domeinnaam nog een tijd vast na het opzeggen door de klant. Er zijn daarnaast partijen die domeinnamen registreren zonder deze direct te gebruiken, maar met het doel om de domeinnaam door te verkopen ("domain squatting"). Deze domeinnamen zien we terug in onze steekproef wanneer voor deze domeinen een SSL-certificaat is aangevraagd (wat vaak het geval is: de domeinhouder adverteert op de domeinnaam zélf de mogelijkheid om deze te kopen). Desondanks vertegenwoordigt de domeinnaam nauwelijks maatschappelijke/economische waarde. Partijen die dit doen en daarbij zelf DNS aanbieden, zijn in de steekproef oververtegenwoordigd.

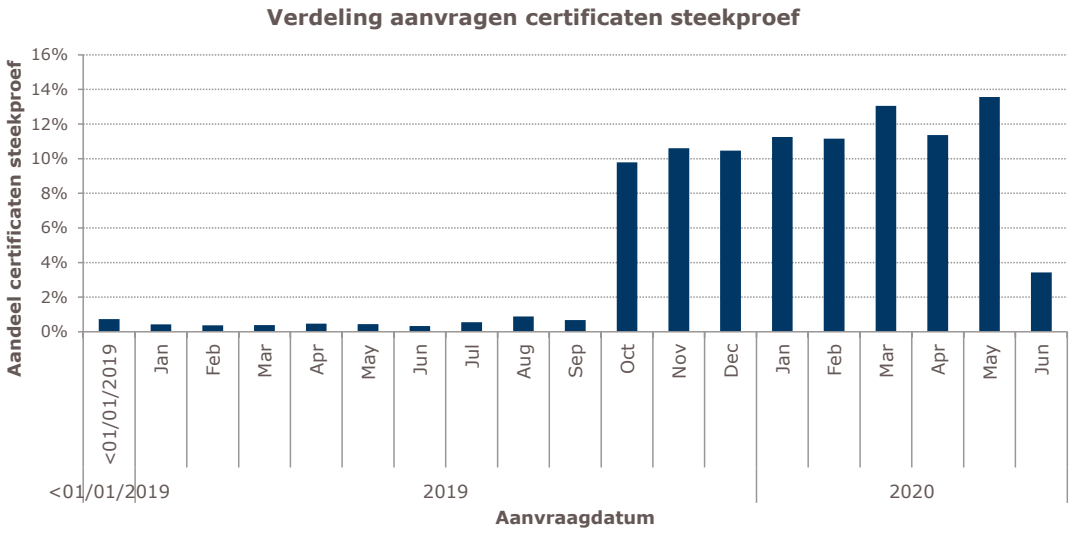
- Sommige partijen hanteren geen 'logische' naamstructuur voor de DNS-servers. Waar veel aanbieders werken met namen als "ns*.webhoster.*" zien we dat (bijvoorbeeld) Amazon werkt met namen als "aws-*-*.org". Deze namen zullen in de analyse met de hand moeten worden geaggregeerd om deze toe te kunnen rekenen aan Amazon.

4 Resultaten

4.1 Onderzochte domeinnamen

De steekproef van domeinnamen is zoals in het vorige hoofdstuk is beschreven opgesteld aan de hand van CT-logs. Specifiek is gebruik gemaakt van het "Argon2020"-log van Google. [16] De logs werden gedownload middels een door Dialogic aangepaste versie van een open-source tool voor inspectie van CT-logs. [17]

Vanwege de grootte van het CT-log is slechts een deel van het logbestand gedownload. De uiteindelijke steekproef bevatte 656.802.624 certificaataanvragen. Een certificaataanvraag betreft één of meerdere domeinnamen. Een certificaat kent in de regel een geldigheid tussen de 3 maanden en 3 jaar – in de dataset bevinden zich dan ook meerdere aanvragen voor hetzelfde domein. In Figuur 6 is te zien hoe de aanvragen van de verzamelde steekproef over tijd verdeeld zijn. Zoals de figuur toont is 99% van de aanvragen uit 2019 of later. We kunnen dus aannemen dat de domeinen in onze steekproef een recente representatie is van domeinen die in gebruik zijn. Voor de acht maanden waarin de data compleet is (oktober 2019 tot en met mei 2020) kan worden gesteld dat een goede representatie van alle domeinnamen op internet is verkregen, als ten minste het CT-log zélf daar een goede afspiegeling van is.



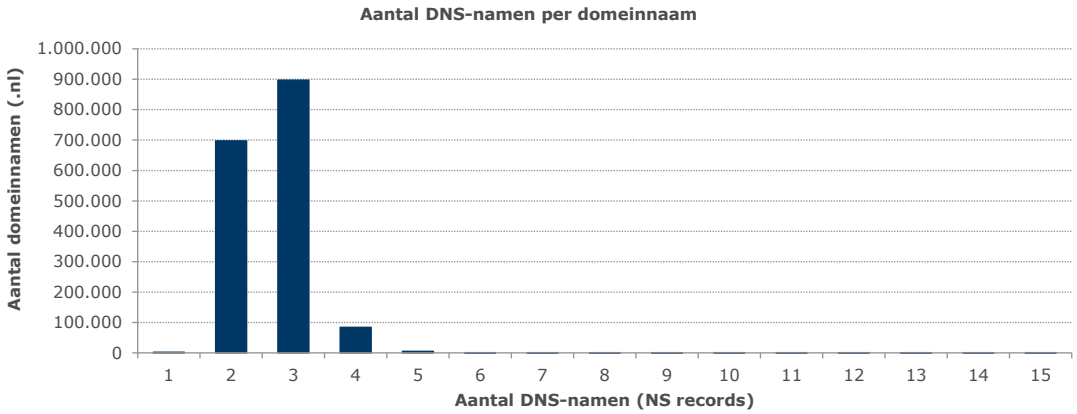
Figuur 6 Certificaataanvragen in de steekproef uit het Argon2020 CT-log naar aanvraagdatum

De steekproef bevat 1.691.381 unieke SLD's onder de ".nl" TLD. In totaal waren er op moment van schrijven 6,106,959 geregistreerde .nl-domeinnamen. [18] De steekproef betreft daarmee circa 27,7% van de populatie .nl-domeinnamen. Ter referentie hebben we uit de CT-logs voor deze analyse ook 212.812 SLD's met een niet-Nederlandse domeinnaam verwerkt (niet-.NL).

4.2 Inrichting van authoritative DNS voor .nl-domeinen

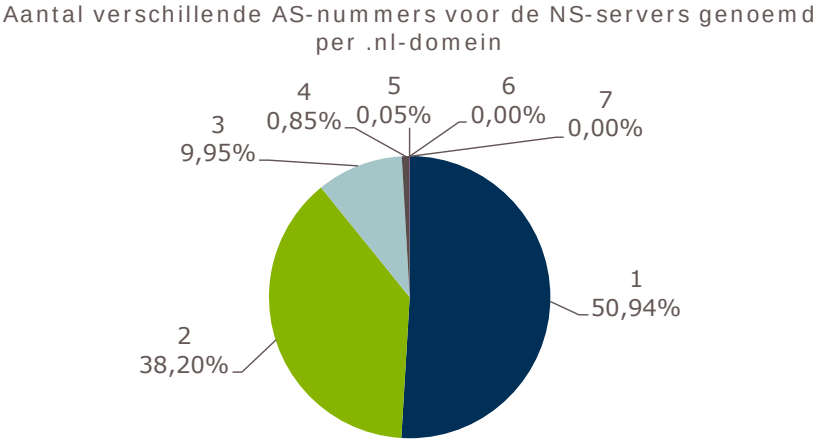
Op basis van de steekproef zijn ook enkele andere aannames te toetsen. Zo zien we in de gegevens dat er voor de overgrote meerderheid van de domeinnamen twee of drie NS-servers worden aangewezen als authoritative, wat duidt op aanwezigheid van enige vorm van

redundantie. Figuur 7 toont een histogram van het aantal NS-servers per domeinnaam binnen onze steekproef voor ".nl"-domeinnamen.



Figuur 7 Aantal DNS-namen per domeinnaam[13]

Figuur 8 toont het aantal AS-nummers dat per domeinnaam voorkomt voor de voor dat domein aangewezen NS-servers. Voor iets meer dan de helft van de .nl-domeinnamen geldt dat de NS-servers zich binnen één AS lijken te bevinden. Voor de andere helft zijn de NS-servers over twee of meer AS'en verspreid. Merk op dat de resultaten afhankelijk kunnen zijn van de locatie vanaf waar de meting werd verricht. Content Delivery Networks (CDN) maken in sommige gevallen gebruik van een techniek waarbij een DNS-server een verschillend IP-adres teruggeeft afhankelijk van de locatie van de opvrager. De meting is verricht vanuit Nederland.

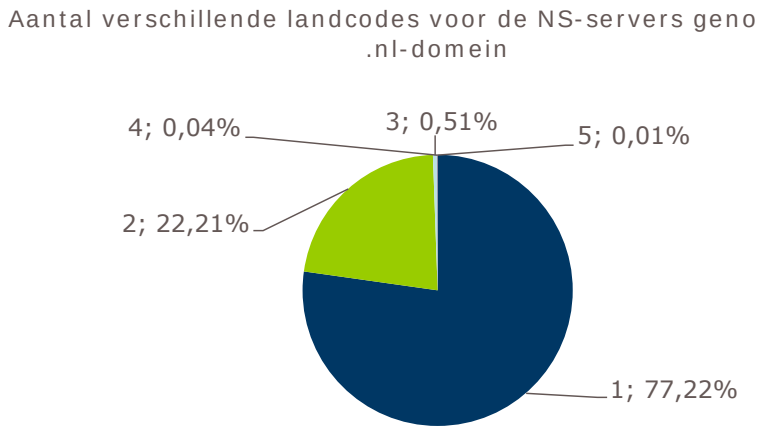


Figuur 8 Aantal verschillende AS-nummers per .nl-domeinnaam

Figuur 9 toont het aantal landcodes dat per domeinnaam voorkomt voor de voor dat domein aangewezen NS-servers. Voor 77,22% van de .nl-domeinnamen geldt dat de NS-servers zich uitsluitend in Nederlandse AS'en lijken te bevinden. Voor de andere 22,78% lijken de NS-servers verdeeld te zijn over AS'en met verschillende landcodes. Dit kan erop wijzen dat de

[13] Het gaat hier specifiek om NS-records. Meerdere NS-records kunnen echter verwijzen naar eenzelfde DNS-server.

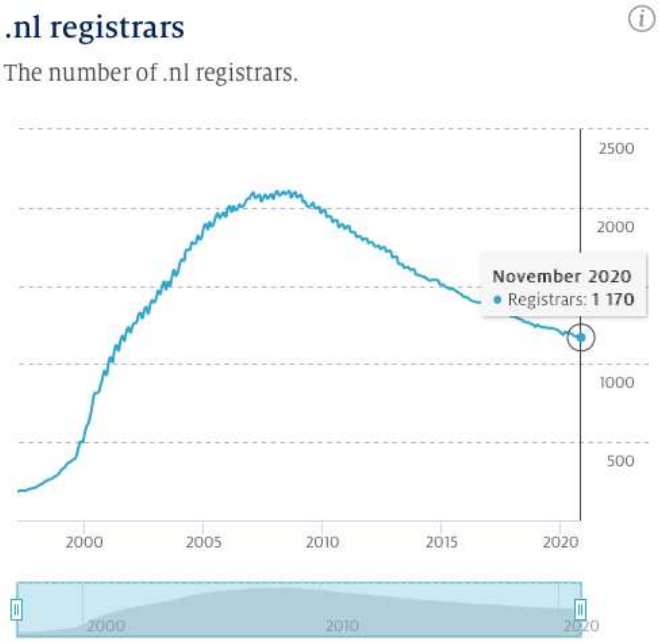
NS-servers in verschillende landen staan; waarschijnlijker is echter dat de NS-servers zijn verspreid over verschillende infrastructuren, waarvan een aantal in handen van buitenlandse partijen (denk aan Amazon, Google en CloudFlare).



Figuur 9 Aantal verschillende landcodes voor de NS-servers die voor een domein worden genoemd

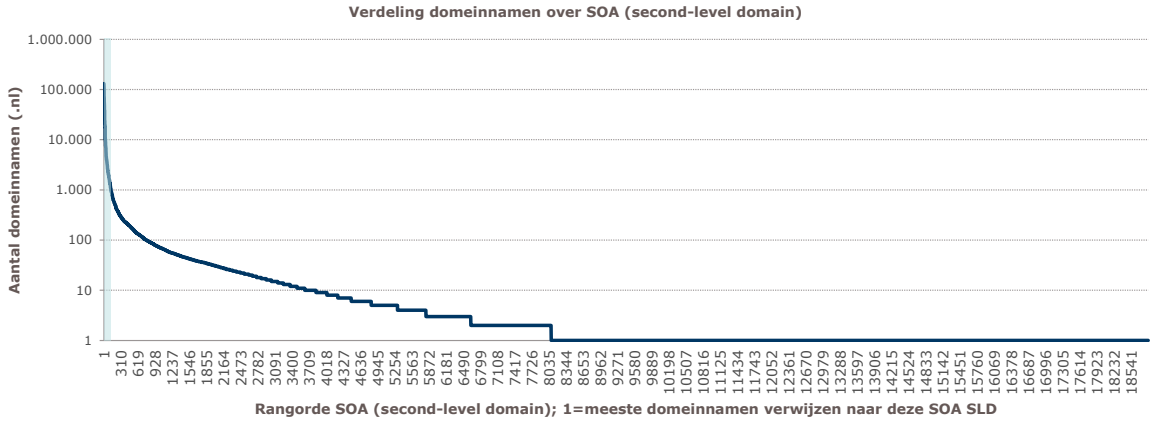
4.3 Verdeling over aanbieders

Er is een groot aantal bedrijven binnen en buiten Nederland actief op het gebied van webhosting en gerelateerde diensten. SIDN geeft aan dat er per november 2020 in totaal 1.170 partijen zijn die .nl-domeinnamen kunnen registreren, [18] waarvan het merendeel in Nederland is gevestigd (de volledige lijst: [19]). Opvallend is dat het aantal registrars vanaf ongeveer 2009 bijna is gehalveerd. Hoewel het aantal actieve .nl-domeinen gedurende die periode nog is gegroeid is de groei sterk afgenomen (voor november 2020 bedraagt deze nettogroei 26.113 domeinen per maand; in de recordmaand juli 2011 bedroeg de nettogroei 105.701 domeinnamen). Het lijkt erop dat er in de markt voor registrars in ieder geval een aanzienlijke consolidatieslag heeft plaatsgevonden.



Figuur 10 Ontwikkeling van het aantal registrars voor het .nl-domein [18]

Kijken we naar de verdeling van domeinnamen over unieke SOA-namen, dan ontstaat het beeld van Figuur 11. Van links naar rechts zijn hier de aantallen domeinnamen per SOA-naam getoond. De vijf SOA-namen die het meest voorkomen voor .nl-domeinnamen komen voor op 27,5% van de domeinnamen. De bovenste 96 SOA-namen hebben samen een aandeel van 80% van de .nl-domeinnamen. Alleen de 25 meest voorkomende SOA-namen hebben een aandeel groter dan 1%. Eenzelfde patroon is te observeren op basis van NS-records en wanneer wordt gekeken naar AS-landcodes.



Figuur 11 Verdeling van .nl-domeinnamen over SOA (SLD), gerangschikt naar aantal per SOA

Tabel 2 toont de SLD's waar door 1% of meer van de .nl-domeinnamen (in de steekproef) naar wordt verwezen als SOA. Op basis van deze lijst kan een aantal conclusies worden getrokken ten aanzien van de methodologie. Allereerst lijkt het erop dat de identificatie op basis van ofwel een SLD eindigend op ".nl", ofwel een landcode 'NL' voor het betreffende AS wijst op een Nederlandse partij. Verder zien we geen invloed van SLD's met een extra niveau in de hiërarchie (aanbieders uit de UK waren anders wellicht in de tabel getoond als één SOA

SLD "co.uk").[14] Een opvallende naam is verder 'UltraDNS', een merk van NeuStar. Dit betreft een DNS-dienst gericht op grotere afnemers (waaronder dus, zo lijkt het, hostingpartij Mijndomein). [20]

De regels voor openprovider.nl, webhostingserver.nl, metaregistrar.nl en ns0.nl zijn interessant, omdat het hier om whitelabel resellers lijkt te gaan. Zo is ns0.nl een dienst van TransIP en verraadt de AS-naam van webhostingserver.nl dat het hier in feite om Antagonist gaat. Metaregistrar is een losse entiteit die onder andere de (.nl)-domeinnamen voor Mijndomein registreert. Merk tot slot het domein sedoparking.com op; Sedo houdt ongebruikte domeinnamen aan en verdient zijn geld met advertenties op deze domeinnamen.[15]

Tabel 2 SOA-namen (gegroepeerd naar SLD) waarnaar door ≥1% van .nl-domeinnamen wordt verwezen

SOA SLD	AS van IP-adres van SOA	Landcode AS van SOA	Aantal .nl-domeinnamen dat deze SOA noemt in steekproef	
transip.net	TRANSIP-AS Amsterdam, the Netherlands	NL	130.886	7,7%
mijndomein.nl	ULTRADNS - NeuStar, Inc.	US	101.828	6,0%
cloudflare.com	CLOUDFLARENET - Cloudflare, Inc.	US	87.678	5,2%
webhostingserver.nl	ANTAGONIST-AS	NL	75.199	4,4%
zxcs.nl	AS-ZXCS	NL	69.015	4,1%
one.com	ONECOM	DK	68.475	4,0%
hostnet.nl	HOSTNET	NL	58.689	3,5%
openprovider.nl	AMAZON-02 - Amazon.com, Inc.	US	58.663	3,5%
axc.nl	ASTRALUS	NL	46.811	2,8%
undeveloped.com	AMAZON-02 - Amazon.com, Inc.	US	45.996	2,7%
rzone.de	ONEANDONE-AS Brauerstrasse 48	DE	39.197	2,3%
neostrada.nl	LEASEWEB-NL-AMS-01 Netherlands	NL	38.258	2,3%
firstfind.nl	ASTRALUS	NL	32.063	1,9%
dan.com	AMAZON-02 - Amazon.com, Inc.	US	28.773	1,7%
auroradns.eu	ASTRALUS	NL	24.540	1,5%
metaregistrar.nl	ASN-PROSERVE Amsterdam	NL	23.577	1,4%
takeaway.com	AMAZON-02 - Amazon.com, Inc.	US	20.252	1,2%
wixdns.net	GOOGLE - Google LLC	US	20.147	1,2%
vevida.net	VEVIDA	NL	19.648	1,2%
argewebhosting.eu	SENTIA	NL	18.400	1,1%
sedoparking.com	SEDO-AS	DE	17.783	1,1%
jimdo.com	CLOUDFLARENET - Cloudflare, Inc.	US	17.727	1,0%
ns0.nl	TRANSIP-AS Amsterdam, the Netherlands	NL	17.092	1,0%

[14] Specifiek voor co.uk zien we in de dataset 78 domeinnamen.

[15] Zie [sedo.com]

De lijst van SOA-namen in Tabel 2 wordt aangevoerd door Nederlandse partijen TransIP, Mijndomein en Antagonist. Nummer drie op de lijst is CloudFlare – deze partij biedt DNS-diensten aan ten behoeve van DDoS-preventie en content delivery. De aanbevolen methode bij het in gebruik nemen van CloudFlare diensten is om de NS-records te laten wijzen naar servers van CloudFlare. [21] Deze servers verwijzen vervolgens naar een CloudFlare-server als SOA.

Wat verder opvalt aan Tabel 2 is dat een aantal SOA's wordt gerealiseerd vanuit AS'en van cloudhosters (zie de regels met AMAZON als AS). Dat zou betekenen dat ofwel de cloudaanbieder een (authoritative) DNS-dienst verzorgt, ofwel dat de authoritative DNS wordt gerealiseerd op basis van infrastructuur (bijvoorbeeld een virtuele server) bij deze partijen. Binnen de steekproef zijn er 257 Nederlandse (.nl-TLD) NS-records (177 unieke IP-adressen) met Amazon, Google of Microsoft als AS. Hiervan dient 39% ook als SOA voor een .nl-domeinnaam. Voor 80.076 .nl-domeinnamen uit de steekproef loopt een DNS-dienst via de infrastructuur van één van deze cloudaanbieders.

Voor deze NS-records hebben we een *reverse DNS lookup* uitgevoerd.[16] Op die manier kan er aan de hand van de domeinnaam met enige zekerheid worden bepaald of het NS-record verwijst naar een DNS-dienst van een cloudaanbieder, of dat er enkel van de *infrastructuur* van de cloudaanbieder gebruik wordt gemaakt voor het hosten van een eigen DNS-dienst. De eerste groep is te identificeren aan de hand van reverse-DNS-namen als *awsdns-XX.com, dns.google, ns-cloud-gX.googledomains.com* en *nsX.bdm.microsoftonline.com.*

Tabel 3 laat een uitsplitsing zien voor deze NS-records. Zoals daaruit blijkt maakt maar 13% van deze NS-records gebruik van de specifieke DNS-dienst die wordt aangeboden door de cloudaanbieder. In 71% van de gevallen gaat het om een eigen DNS-dienst. Hierbij verwezen zo'n 129 NS-records naar een virtuele server op een van de clouddiensten. De overige 53 verwijzen naar de server van een hostingpartij of een andere eigen DNS-dienst. Voor 15 NS-records kwam de *reverse DNS-lookup* uit op een domeinnaam van het netwerk van de cloudaanbieders *zelf*, zoals *awsglobalaccelerator.com* (Amazon) of *1e100.net* (Google). Het is aannemelijk dat dit 'global CDN'-achtige diensten zijn die het DNS-verkeer (samen met ander verkeer) verdelen.

Tabel 3 NS-records via cloudaanbieders per type

Type dienst	Aantal NS-records	Aantal .nl-domeinen dat gebruik maakt van dit type dienst
Cloud DNS (DNS-dienst van cloudaanbieder)	33	64
Self-hosted (DNS-server op basis van server bij cloudaanbieder)	182	77.000
Accelerator (DNS-verkeer gedistribueerd door cloudaanbieder)	15	12
Onbekend[17]	27	3.001

[16] In de meeste gevallen geeft een dergelijke lookup een DNS-naam die hoort bij het gegeven IP-adres. Deze informatie is door de houder van het IP-adres zélf in te stellen en dus niet per definitie altijd juist of bruikbaar.

[17] De *reverse DNS lookup* leverde in deze gevallen geen resultaat op.

Het beeld dat uit bovenstaande naar voren komt is dat de afhankelijkheid van clouddiensten niet groot is als het gaat om de specifieke DNS-dienst. Er lijkt wel een grote afhankelijkheid te zijn van de *infrastructuur* van deze partijen bij het realiseren van authoritative DNS.

Welke domeinhouders realiseren zélf authoritative DNS?

Authoritative DNS is essentieel voor de beschikbaarheid van een online dienst. Het vraagt veel kennis en specifieke technische inrichting om authoritative DNS goed te kunnen realiseren. We verwachten dan ook dat domeinhouders die zélf authoritative DNS realiseren, daar waarschijnlijk een goede reden voor hebben. Het ligt bijvoorbeeld voor de hand dat partijen die ook andere delen van hun infrastructuur in eigen beheer hebben, DNS daar ook in meenemen. Denk hierbij bijvoorbeeld aan banken, overheden, grotere zakelijke dienstverleners en grotere onlinebedrijven. Voor sommige domeinhouders geldt dat zij domeinen of subdomeinen gebruiken ten behoeve van klanten (zo beheert thuisbezorgd.nl een groot aantal websites voor onder andere cafetaria's; iets soortgelijks zien we overigens ook bij vakantiehuisjes en makelaars).

De meetresultaten bevestigen dit beeld. In de steekproef vinden we circa 13.000 domeinen waarvoor het SOA-record dezelfde SLD-naam heeft als het domein zelf. Dit kan erop wijzen dat de DNS-server die als SOA is aangemerkt specifiek voor dit domein (deze organisatie) is ingericht (dit hoeft echter strikt genomen niet; een DNS-server kan best onder meerdere namen bekend zijn). In deze set vinden we onder andere de volgende (soorten) organisaties terug:

- Grotere onderwijsinstellingen en -instituten (surfsara.nl, kennisnet.nl, uvt.nl, tue.nl, noordhoff.nl, nhtv.nl)
- Overheden (rotterdam.nl, mindef.nl, arnhem.nl, delft.nl, brabant.nl)
- Grotere zakelijke dienstverleners (adp.nl, debeer.nl, skidata.com)
- Aanbieders van online SaaS-diensten en websitebouwers (wpcloud02.nl, typokings.nl)
- Grotere retailers (dell.com, ahold.nl)
- Media (streamgate.nl, rtvoost.nl, vpro.nl)
- ICT-dienstverleners (netfiesta.nl, nibble.nl, chipsoft.nl)
- ISP's, webhosters en cloudaanbieders (zie elders in dit stuk)

Een andere manier om deze groep in beeld te krijgen, is door te kijken naar het AS van waaruit authoritative DNS wordt gerealiseerd. In onze steekproef zien we circa 400 AS'en waarin zich een DNS-server (NS-record) bevind. Kijken we vervolgens naar de AS'en met een klein aantal bijbehorende domeinnamen, dan vinden we de volgende (soorten) organisaties:

- Media (PUBLIEKE-OMROEP-AS)
- Grotere Nederlandse bedrijven (ANWB, GOOSSENS, KLM)
- (Semi-)overheden (RDW, MINEZ-DICTU)
- Universiteiten (TUDELFT-NL, AS-TUE, UTWENTE-AS), Kennisnet (KENNISNET-AS)
- Zakelijke dienstverleners (ADYEN, BUCKAROO)
- IT-dienstverleners (CLOUDWERKT-AS, CLEVERIT, RONOIT, WORLDSTREAM)
- Telecomaanbieders, voornamelijk transit en VoIP (VOIPRO-AS, MOTTO-VOIP-AS, FUSIX-AS, DT-IT)

4.4 Classificatie van in Nederland gevestigde aanbieders

Zoals in het methodologiehoofdstuk reeds is beschreven zijn er verschillende manieren om te benaderen of een authoritative DNS-dienst wordt aangeboden door een in Nederland gevestigde partij.

Benadering op basis van landcode van AS van NS-server

Onderstaande Tabel 4 toont het percentage domeinnamen waarvoor ten minste één NS-server zich (na resolven vanaf een Nederlands netwerk[18]) in een AS bevindt met een Nederlandse landcode. De tabel is uitgesplitst naar .nl- en niet-.nl-domeinnamen, waarbij de kolommen optellen tot 100%.

Uit Tabel 4 volgt dat circa 60% van de .nl-domeinen ten minste één NS-server in een AS met Nederlandse landcode heeft. In andere woorden: 60% van de .nl-domeinen zou bij benadering worden gefaciliteerd door een in Nederland gevestigde DNS-aanbieder.

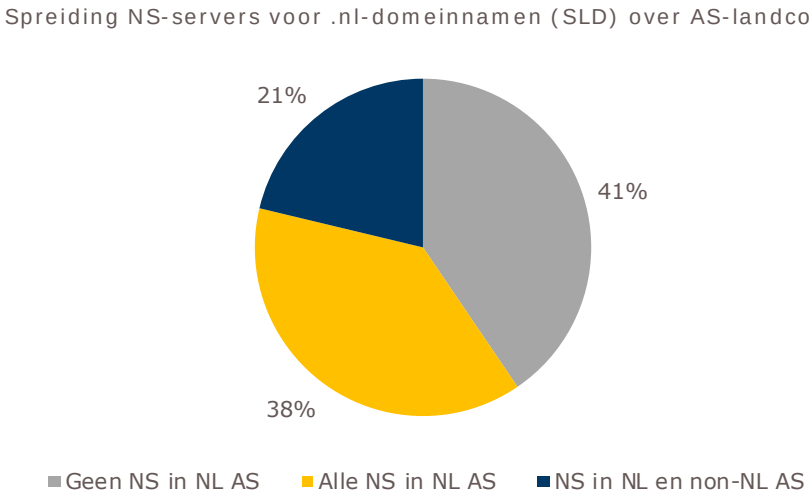
Uit het beeld dat Tabel 4 geeft wordt ook duidelijk dat Nederlandse DNS-aanbieders (zoals wellicht te verwachten) een relatief klein, maar niet te onderschatten aandeel hebben in het leveren van DNS-diensten voor niet-.nl-domeinen. We vermoeden dat een groot deel van deze niet-.nl-domeinen een Nederlandse houder heeft.

Tabel 4 Verdeling van domeinnamen over authoritative NS-servers binnen en buiten Nederland

	.NL N=1.691.381 (±27,7% van totaal)	**Niet-.NL** N=212.812
Authoritative DNS van Nederlandse aanbieder (benadering: ten minste 1 NS-server in NL AS)	59,4%	1,6%
Geen authoritative DNS van Nederlandse aanbieder (benadering: geen van de NS-servers in NL AS)	40,6%	98,4%

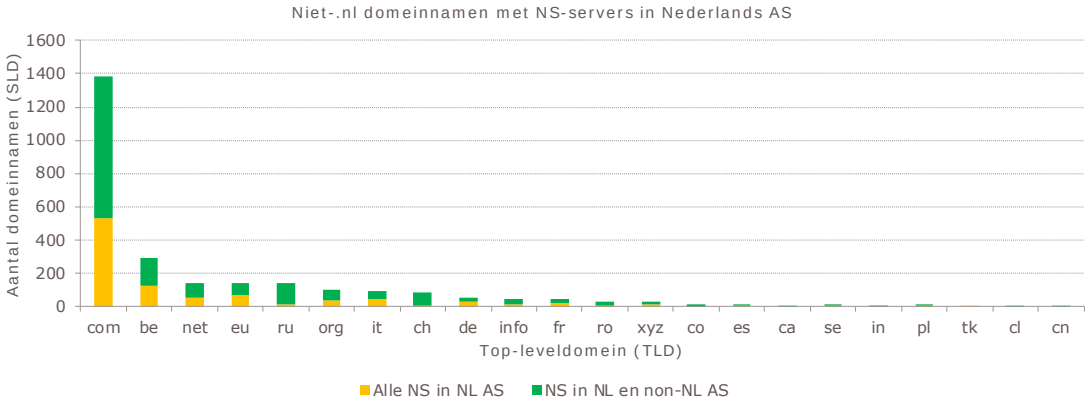
In paragraaf 4.2 werd beschreven dat de meerderheid van de domeinen twee of drie verschillende NS-servers noemt, met alle waarschijnlijkheid omwille van redundantie. Figuur 12 toont de mate waarin dit geldt voor .nl-domeinnamen, en in hoeverre deze spreiding plaatsvindt over AS'en met verschillende landcodes. Wat opvalt in de grafiek is dat een aanzienlijk deel van de ".nl"-domeinnamen, op basis van de benadering met AS-landcode, uitsluitend gebruik lijkt te maken van DNS-diensten van niet-Nederlandse aanbieders.

[18] Een domeinnaam kan, afhankelijk van de locatie, resolven naar een verschillend IP-adres. Een DNS-server 'ziet' immers het IP-adres van degene die informatie opvraagt, en kan afhankelijk van dit adres andere antwoorden geven. Deze techniek wordt onder andere gebruikt in *content delivery networks* (CDN) om gebruikers te laten verbinden met een server die zo dicht mogelijk bij de gebruiker in de buurt staat. Dit verlaagt de latency tussen gebruiker en dienst, en ook kosten voor transitverkeer tussen netwerken. Een tweede techniek is *anycast*. Daarbij wordt wel steeds hetzelfde IP-adres geretourneerd door het DNS, maar wordt het IP-adres vanaf verschillende bestemmingen gerouteerd naar verschillende eindpunten.



Figuur 12 Spreiding van NS-servers voor .nl-domeinnamen (SLD) over landcodes van bijbehorende AS'en

Figuur 13 toont deze verdeling procentueel voor verschillende andere TLD's. Uit de afbeelding kan worden afgeleid dat DNS-aanbod vanuit Nederlandse AS'en met name relevant is voor domeinen binnen de getoonde TLD's, waarbij .com veruit het grootste aantal domeinen vertegenwoordigt.



Figuur 13 Spreiding van NS-servers over AS'en met verschillende landcodes per TLD

Benadering op basis van SOA-naam

Kijken we naar de SOA-records voor domeinnamen in de steekproefset, dan tekent zich de verdeling in Tabel 5 en Tabel 6 af. De percentages liggen iets lager dan in de voorgaande exercitie, waarbij werd gekeken naar het TLD van de NS-server (ten minste één onder .nl). Kijken we naar het verschil tussen de benadering op basis van SOA-naam en het AS van de SOA-server, dan zien we dat het aandeel in de laatste categorie iets hoger ligt. In beide gevallen zou het verschil kunnen worden verklaard door het feit dat in Nederland ook veel buitenlandse aanbieders actief zijn, vanwege de goede Nederlandse infrastructuur voor hosting.

Tabel 5 Verdeling van domeinnamen over SOA-servers binnen en buiten .nl

	.NL N=1.691.381 (±27,7% van totaal)	**Niet-.NL** N=212.812
Authoritative DNS van Nederlandse aanbieder (benadering: SOA-naam in ".nl")	52,7%	0,5%
Geen authoritative DNS van Nederlandse aanbieder (benadering: SOA-naam in ".nl")	47,3%	99,5%

Tabel 6 Verdeling van domeinnamen over SOA-servers binnen en buiten NL AS

	.NL N=1.691.381 (±27,7% van totaal)	**Niet-.NL** N=212.812
Authoritative DNS van Nederlandse aanbieder (benadering: SOA in NL AS)	58,4%	1,1%
Geen authoritative DNS van Nederlandse aanbieder (benadering: SOA niet in NL AS)	41,6%	98,9%

4.5 Verdeling over Nederlandse aanbieders

In voorgaande paragraaf is gebruik gemaakt van het SLD van het SOA-record om te bepalen wie de aanbieders van de DNS-dienst is. De stap naar uitsplitsing tussen "in Nederland gevestigde" en "niet in Nederland gevestigde" aanbieder kan op verschillende manieren (automatisch) worden gemaakt. In dit onderzoek hanteren we de volgende criteria:

- **SOA TLD=.nl.** Het SOA-record eindigt op ".nl."
- **SOA NL AS.** Het SOA-record resolved naar een IP-adres in een AS met landcode "NL"
- **NS TLD=.nl.** Het NS-record eindigt op ".nl."
- **NS NL AS.** Ten minste één van de NS-records resolved naar een IP-adres in een AS met landcode "NL".

Uit onze analyse volgt dat de verschillende criteria tot verschillende classificaties komen. We combineren daarom de methoden. Onderstaande Tabel 7 toont de SOA/NS-namen die bij ten minste één van deze vier methoden in de top 20 terechtkwamen[19], en daarbij het gevonden aandeel van .nl-domeinnamen. Omdat de namen bij de methoden die gebruik maken

[19] Het aantal partijen in de kolom "NS NL AS" is lager dan 20 omdat in de top 20 meerdere NS-records voorkwamen voor dezelfde partijen als gevolg van het gebruiken van meerdere NS-records per domein. Zo komt TransIP in deze set voor met transip.nl, transip.eu en transip.net. In de "NS TLD=.nl"-kolom speelt dit niet, omdat daar in deze gevallen vaak maar één NS-server per partij wordt gevonden (alleen "transip.nl" in het voorbeeld).

van AS-landcode ook een niet-.nl-TLD kunnen hebben, kijken we hier alleen naar het SLD minus de TLD.

Tabel 7 Vergelijking van marktaandelen bij verschillende methoden voor het classificeren van een aanbieder als 'Nederlands'

SOA/NS-record	SOA TLD=.nl	SOA NL AS	NS TLD=.nl	NS NL AS	Geschat marktaandeel (.nl-domeinnamen)
transip.*		7,7%	7,9%	7,9%	7,7%-7,9%
mijndomein.*	6,0%		6,0%		6,0%
webhostingserver.*	4,4%	4,4%	4,4%	4,4%	4,4%
zxcs.*	4,1%	4,1%	4,1%	4,1%	4,1%
hostnetbv.*			3,7%	3,7%	3,7%
hostnet.*[20]	3,5%	3,5%	3,7%	3,7%	3,5%-3,7%
openprovider.*	3,5%		3,6%		3,5%-3,6%
axc.*	2,8%	2,8%	2,8%	2,8%	2,8%
neostrada.*	2,4%	2,3%	2,4%	2,4%	2,3%-2,4%
firstfind.*	1,9%	1,9%	1,9%	1,9%	1,9%
auroradns.*		1,5%	1,5%	1,5%	1,5%
metaregistrar.*	1,4%	1,4%	1,4%	1,4%	1,4%
vevida.*		1,2%		1,2%	1,2%
argewebhosting.*		1,1%	1,1%	1,1%	1,1%
ns0.*	1,0%	1,0%	1,0%		1,0%
dn-s.*	0,6%	0,6%	0,6%		0,6%
mijndnsserver.*	0,6%	0,6%	0,6%		0,6%
hosting2go.*	0,6%	0,6%	0,6%		0,6%
dnssrv.*	0,5%	0,5%	0,5%		0,5%
yourwebhoster.*			0,5%		0,5%
anony.*	0,3%		0,5%		0,3%-0,5%
xs4all.*	0,4%	0,4%			0,4%
flexwebhosting.*	0,4%	0,4%			0,4%
ixlhosting.*	0,4%	0,4%			0,4%
dds.*	0,4%	0,4%			0,4%
2is.*	0,3%				0,3%

Tabel 7 toont dat met de vier methoden samen robuust zijn ten aanzien van specifieke verschillen in de wijze waarop DNS is ingericht, en de grote partijen goed kunnen worden

[20] Hostnet gebruikt zowel *.hostnetbv.nl als *.hostnet.nl voor NS-namen. Voor 99,8% van de domeinnamen in onze dataset met 'hostnet' in de SOA-naam zien we dat beide SLD's voorkomen als NS-record. De regels voor *.hostnetbv.nl en *.hostnet.nl moeten hier dus niet worden opgeteld.

geïdentificeerd. In een enkel geval levert een methode een afwijking van 0,1 tot 0,2 procentpunt op ten aanzien van het marktaandeel.

4.6 Classificatie en groepering van aanbieders

In het algemeen geldt dat de notie "in Nederland gevestigd" zonder aannames niet eenduidig is vast te stellen. Op de verschillende lagen in de infrastructuur (cf. de 'OSI-stack') kan de infrastructuur zich immers wel, niet of gedeeltelijk in Nederland bevinden, en/of onder controle en/of eigendom zijn van een Nederlandse partij.

In de handmatige nacontrole is gekeken naar de grootste partijen in de dataset, en is onderzocht hoe de bedrijfsstructuur op hoofdlijnen in elkaar zit. Het criterium dat is gehanteerd laat zich het best formaliseren als "aanwezigheid van een Nederlandse rechtspersoon in de hiërarchie".

Nader handmatig onderzoek wijst uit dat een aantal SOA SLD's in de eerder getoonde lijst behoren tot aan elkaar gerelateerde bedrijven:

- TransIP is sinds 2019 gelieerd aan het Belgische 'Combell' (in 2019 vond een overname/fusie plaats onder de naam 'team.blue'). Voor zover door ons vast te stellen heeft TransIP na deze fusie geen substantiële wijzigingen doorgevoerd aan de manier waarop het haar DNS-diensten aanbiedt. Combell en TransIP zijn in de dataset als separate bedrijven te herkennen.
- TWS is een Europese hostinggroep (met hoofdkantoor gevestigd in Nederland). TWS heeft in de afgelopen jaren een groot aantal Nederlandse hosters overgenomen (PCExtreme, Neostrada, Argeweb, FXW). We zien alle hosters in bovenstaande dataset los terug.

Tabel 9 geeft een overzicht van geschatte marktaandelen met daarbij de relevante groepering.

4.7 Validatie en triangulatie

4.7.1 Analyse op basis van AS (Autonomous System)

Door te kijken naar het AS van waaruit een authoritative DNS-server opereert kan iets worden gezegd over de partij die de infrastructuur beheert. In onze steekproef hebben we voor alle gevonden NS-records het AS opgezocht. In deze lijst verwachten we in ieder geval de hierboven genoemde aanbieders terug te vinden. Het is echter interessant om te kijken of er zich in deze lijst ook andere partijen bevinden met grote aantallen domeinen onder zich. Het kan daarbij gaan om partijen die voor zichzelf domeinen beheren (denk bijvoorbeeld aan de NPO) maar ook om aanbieders die infrastructuur voor andere partijen verzorgen. Wanneer daarbij per klant een eigen (logische) DNS-server wordt ingericht, zouden we deze aanbieders in de hierboven beschreven analyse niet vinden.

In totaal zien we in onze steekproef 405 verschillende AS'en in Nederland van waaruit (authoritative) DNS-servers opereren (hiernaar wordt verwezen via een NS-record). Voor 125 AS'en geldt dat ze voor tien of minder domeinnamen (in de steekproef) DNS verzorgen. Voor 238 AS'en is dit 100 of minder. We zien 73 AS'en die ieder voor 1.000 of meer domeinnamen authoritative DNS verzorgen. Tabel 8 toont de AS'en van waaruit authoritative DNS-servers opereren waarnaar door 1.000 of meer domeinen wordt verwezen (exclusief de partijen die al worden genoemd in Tabel 7).

Tabel 8 AS'en met Nederlandse landcode van waaruit authoritative DNS-servers opereren met 1.000 of meer domeinnamen in de steekproef (exclusief reeds geïdentificeerde aanbieders).

AS-naam	AS-nummer	Aantal domeinen	NS-naam met meeste vermeldingen binnen dit AS	Aanbieder?
XS4ALL-NL Amsterdam	3265	37.514	ns3.argewebhosting.nl.	Ja
SENTIA	8315	21.847	ns1.argewebhosting.eu.	Ja
TRUESERVER-AS TrueServer BV	15703	14.228	ns1.exonet.nl.	Ja
CJ2-AS	39704	12.910	dns3.hosted.nl.	Ja
PREVIDER-AS	20847	11.753	ns1.shockmedia.nl.	Ja
SERVERIUS-AS	50673	10.833	ns1.gethost.nl.	Ja
KPN-INTERNEDSERVICES	15879	10.327	ns01.is.nl.	Ja
DENIT-AS Amsterdam	25542	9.636	ns1.dnstools.nl.	Ja
WEDARE wd6.NET B.V	20495	9.506	ns3.bhosted.nl.	Ja
TODAYCONCEPTS	203065	8.204	ns1.thednscompany.com.	Ja
TILAA	196752	7.974	ns1.wned-dns.eu.	Ja
SIGNET-AS	28878	7.284	ns3.dds.amsterdam.	Ja
MIHOSNET	200831	6.378	ns1.mdns.nl.	Ja
CYSO-AS	25151	6.070	ns1.yoursrs.com.	Ja
NETBASE	213192	5.954	ns11.webreus.net.	Ja
NETWORKING4ALL	42585	5.814	ns1.yourdomainprovider.net.	Ja
FUNDAMENTS-AS	20559	5.014	ns1.oxilion.nl.	Ja
INTERCONNECT Interconnect Services BV	9150	4.837	ns-3.eu.	Ja
DUOCASTBACKUP-AS	39292	4.720	ns2.duocast.net.	Ja
VXBITS VXbits Network	59545	4.650	dns2.hosted.nl.	Ja
VIVOR-AS	34942	4.547	ns4.bhosted.nl.	Ja
I3DNET	49544	3.884	ns0.co-co.nl.	Ja
IPS	202916	3.531	ns01.ips.nl.	Ja
WORLDSTREAM	49981	3.510	dns1.interip.nl.	Ja
TUXIS	197731	3.443	ns3.tiscomhosting.eu.	Ja
ZYLON-AS	8312	3.408	ns1.maxdns.nl.	Ja
GL-IX-AS	43190	3.161	ns1.tiscomhosting.nl.	Ja
COMPUKOS-AS	29028	3.114	ns2.nederhost.nl.	Ja
GREENHOST	47172	2.872	ns1.greenhost.nl.	Ja
TRANS-IX-AS	30870	2.499	ns10.foxxl.nl.	Ja
NOVOSERVE-AS	24875	2.486	ns00.skyberate.eu.	Ja
INTENTION-AS	207647	2.478	intention.ns01.nl.	Ja
SURFNET-NL	1103	2.378	ns1.surfnet.nl.	Ja*
BITENCY-AS	61029	2.345	ns2.ispdns.nl.	Ja
TNF-AS	33915	2.320	nameserver1.benfmedia.nl.	Ja
NL-SOLCON SOLCON	12414	2.280	nsauth01.solcon.nl.	Ja
INTERRACKS-AS	42093	2.194	ns1.hosting.whixx.com.	Ja
FIBERRING Amsterdam	38930	1.962	ns2.realworks.nl.	Ja*
ITCREATION	201311	1.666	ns1.pharmeon.nl.	Ja*
REDHOSTING-AS	39647	1.620	ns1.nedlook.com.	Ja
LINQHOST	59791	1.615	ns1.linqhost.nl.	Ja
PROLOCATION	41887	1.578	ns1.as41887.nl.	Ja
ASN-ROUTIT	28685	1.539	ns1.routit.net.	Ja
QWEB-AS	15922	1.440	ns1.qweb.net.	Ja

AS-naam	AS-nummer	Aantal domeinen	NS-naam met meeste vermeldingen binnen dit AS	Aanbieder?
ASN-ROUTELABEL	198203	1.432	dns1.orangelemon.nl.	Ja
RADIK-AS	30785	1.426	ns1.pansa.net.	Ja
SUPERIOR-AS	34233	1.397	ns1.hix.nl.	Ja
LITESERVER	60404	1.365	nsauth3.hostingcp.be.	Ja
NFORCE	43350	1.270	ns-canada.topdns.com.	Ja
XENOSITE Amsterdam	15426	1.260	ns3.spothost.nl.	Ja
POCOS	50522	1.246	ns1.m3is.nl.	Ja
OPENFIBER	207176	1.202	ns1.resellerdns.nl.	Ja
NL-CAVEO	24642	1.163	ns1.caveo.nl.	Ja
UNET Unet Network	29396	1.130	dns1.suilichem.com.	Nee
NETROUTING-AS	47869	1.086	ns2.serverion.eu.	Nee
INTERBOX-AS Lubbers Box Telematica BV	16298	1.056	dns-sec.box.nl.	Nee
OSSO	43366	1.014	ns1.osso.nl.	Ja*
BIP-AS BIP Backbone ASN	34343	1.002	ns1.neukserver.com.	Nee

In Tabel 8 vinden we bovenaan voornamelijk aanbieders van professionele hostingdiensten. Vergeleken met de eerdergenoemde aanbieders bieden deze partijen over het algemeen meer gespecialiseerde en professionele diensten, tot en met maatwerk. Veel van deze partijen bieden weliswaar een 'generieke' authoritative DNS-dienst (de NS-naam in het AS met de meeste gekoppelde domeinen verwijst bij deze partijen naar de AS-houder). Echter maakt slechts een relatief klein deel van de klanten hiervan gebruik. Handmatige inspectie van de dataset leert dat met name MKB-bedrijven en ZZP'ers de generieke DNS-dienst afnemen. De andere klanten maken waarschijnlijk gebruik van een *eigen* DNS-server, gehost binnen het AS van de aanbieder. Het is door ons niet vast te stellen of deze DNS-server dan ook onder *beheer* van de betreffende klant valt, of dat de hier genoemde aanbieder dit specifiek voor de klant inricht en beheert.

Onderaan Tabel 8 zien we met name partijen die zeer waarschijnlijk zelf nauwelijks DNS-diensten leveren, maar wel connectiviteit verzorgen voor klanten die zelf een DNS-server opereren. Zo is UNET het AS voor (over het algemeen zakelijke) klanten van Eurofiber. Voor BIP-AS geldt dat één NS-server (vermoedelijk van een klant van BIP/Eweka) verantwoordelijk is voor 636 domeinnamen. Deze partijen zouden dan ook niet moeten worden beschouwd als grootschalige aanbieders van authoritative DNS, maar als infrastructuuraanbieders.

Een aantal opvallende namen uit Tabel 8 is tot slot Surfnet, Osso, Pharmeon en Realworks. Vanuit deze AS'en worden steeds domeinnamen voor een bepaalde doelgroep gerealiseerd (respectievelijk onderwijsinstellingen, klusbedrijven, huisarts- en tandartspraktijken, en makelaars). Het lijkt hier te gaan om "full service" aanbieders die voor een bepaalde doelgroep een volledig dienstenpakket aanbieden, inclusief eigen domeinnaam.

Concluderend vinden we in deze exercitie een aantal namen van partijen betrokken bij authoritative DNS voor grote aantallen domeinnamen (1.000+ in onze steekproef). De dienstverlening is echter meer gespecialiseerd, waardoor het onderscheid tussen aanbieder van infrastructuur vóór de authoritative DNS versus aanbieder van de authoritative DNS-dienst zélf minder eenduidig is.

4.7.2 Analyse op registrarniveau

In de loop van het onderzoek is de gehanteerde methode voorgelegd aan SIDN. SIDN heeft vervolgens een eigen analyse uitgevoerd om de verdeling van NS-namen over registrars te bepalen. Hieruit heeft SIDN geconcludeerd dat de gehanteerde methode valide is en 'werkt' voor een groot aantal aanbieders, maar dat er tegelijkertijd een aantal aanbieders is dat (door de specifieke inrichting) zou kunnen worden onderschat in de analyse.

Een belangrijk verschil tussen de analyse van SIDN en onze analyse is dat hier wordt gekeken naar de aanbieder van de DNS-dienst, terwijl SIDN in haar analyse redeneert vanuit registrars. Dat is niet noodzakelijkerwijs (maar wel vaak) dezelfde partij als de aanbieder van authoritative DNS voor een domein. Door voor de grotere registrars bijbehorende NS-records op te zoeken, worden ook kleinere DNS-services gevonden (van de grotere klanten of resellers van deze registrars). In onze analyse wordt gestart vanuit de DNS-services en vinden we deze partijen onderaan onze lijst (en worden ze niet gekoppeld aan de registrar, omdat we dit zien als een separate DNS-dienst).

De volgende verschillen zijn opgemerkt, geanalyseerd, en blijken te verklaren:

- Een aantal registrars komt niet voor op onze lijst, omdat zij zelf geen DNS-diensten aanbieden, maar betrekken bij andere aanbieders. Dit is uiteraard de bedoeling van onze analyse.

- Een aantal partijen staat hoog in onze lijst (aantal domeinen DNS), maar laag in de lijst van SIDN (aantal domeinregistraties). De verklaring lijkt dat deze partijen DNS-diensten leveren aan zusterbedrijven of klanten die een domeinnaam 'meebrengen', en/of domeinnamen registreren via zusterbedrijven. Een vergelijkbare situatie doet zich voor bij Metaregistrar (1,4% in onze analyse) en Mijndomein (6,0%). In het registraroverzicht van SIDN komt alleen Mijndomein voor, maar navraag leert dat het hier feitelijk om Metaregistrar gaat. Metaregistrar voert dus (ook) de registraties voor Mijndomein uit. In onze analyse zien we beide namen separaat terugkomen.

- Een aantal registrars zou volgens SIDN meer domeinen onder beheer hebben dan uit onze analyse volgt. Mogelijk komt dit voort uit fusies en/of het verspreiden van DNS-diensten over meerdere NS-namen. De aanbieders die SIDN identificeert en die helemaal niet in onze resultaten voorkomen, zien wij wel terug in onze analyse op AS-niveau (zie §4.7.1).

4.7.3 Indicaties hostingpartijen

Er is in het openbaar weinig te vinden over marktaandelen van hosters en aanbieders van DNS-diensten. Een van de gevonden resultaten is een inventarisatie van webhosters.nl uit 2018, waarbij gekeken werd naar de door de hosters op hun eigen website aangegeven aantallen geregistreerde domeinen. [22] In de analyse wordt geen (goed) onderscheid tussen het totaal aantal domeinen en .nl-domeinnamen (maar worden de marktaandelen vervolgens wel bepaald ten opzichte van het totaal aantal .nl-domeinnamen). Desondanks komen in deze analyse vrijwel alle hosters terug die ook in onze analyse het meeste marktaandeel krijgen toegedicht. Opvallende afwijkingen zijn er voor Yourhosting (o.a. firstfind.* in Tabel 7) en Versio (o.a. axc.*). Deze partijen hebben volgens webhosters.nl een veel groter marktaandeel (Yourhosting zou zelfs de grootste zijn) dan uit onze analyse volgt.

Nadere controle van onze resultaten laat zien dat beide partijen desondanks goed herkend zijn in de analyse. Een mogelijke verklaring is dat HTTPS bij deze hosters niet automatisch geleverd wordt, maar door de klant moet worden geactiveerd. [23] Een andere mogelijkheid

is dat deze partijen wellicht grotendeels niet-.nl-domeinen realiseren en/of er infrastructurele wijzigingen hebben plaatsgevonden sinds de bedrijven onderdeel zijn geworden van TWS.

Een aantal hosters geeft zelf informatie over het aantal aangeboden domeinen. Mijndomein.nl rapporteert op moment van schrijven bijvoorbeeld 782.014 domeinnamen te beheren voor haar klanten. [24] Dit zou corresponderen met een marktaandeel van 8%, onder de aanname dat (1) circa 65% van de domeinnamen van in Nederland gevestigde domeinnaamhouders een .nl-domeinnaam is en (2) dat Mijndomein voornamelijk in Nederland gevestigde domeinnaamhouders bedient. In onze analyse is het (geschatte) marktaandeel lager (6%). Het verschil kan worden verklaard door de gemaakte aannames, het niet meetellen van (whitelabel) resellers, en het feit dat HTTPS niet voor alle klanten zal zijn ingeschakeld (dit gebeurt alleen voor nieuwe pakketten automatisch [25]).

De cijfers van de webhosters zijn ook om andere reden lastig te interpreteren, omdat ze betrekking lijken te hebben op *registraties* en niet direct op DNS-dienstverlening. Zo geeft Metaregistrar aan 800.000 domeinnamen te beheren (omgerekend zou dat een marktaandeel van 8,5% zijn). [26] We zien in onze analyse echter maar een marktaandeel van 1,4% van het DNS-aanbod. We vermoeden dat Metaregistrar voor andere bedrijven (specifiek Mijndomein, waar Metaregistrar uit is ontstaan) registraties uitvoert en slechts voor een deel zelf DNS realiseert.

4.7.4 Beperkingen van het onderzoek

Een belangrijke kanttekening is dat het louter tellen van domeinnamen niet per definitie een juiste indicatie geeft van de maatschappelijke/economische waarde van die domeinen (en in het verlengde, de potentiële impact bij uitval of verstoring van DNS). Desondanks constateren we dat in de resultaten wel degelijk een sterke concentratie van DNS-aanbod over een klein aantal aanbieders zichtbaar is, en dat uitval/verstoring van de DNS-dienstverlenging van een dergelijke aanbieders een zeer groot aantal gebruikers kan raken. Hoewel de *relatieve* marktaandelen c.q. relatieve 'waardeverdeling' over domeinen niet exact is vast te stellen met de hier gehanteerde methode, blijft staan dat het *absolute* aantal (potentieel) geraakte gebruikers hoog genoeg kan zijn om aanleiding te geven tot het stellen van specifieke eisen aan deze aanbieders.

5 Conclusie

5.1 Beantwoording onderzoeksvragen

Welke soorten DNS-diensten kunnen vanuit technisch perspectief worden onderscheiden? Wat zijn mogelijke gevolgen van verstoring (ook buiten de sector) van deze diensten?

Domeinnamen worden voor een groot aantal verschillende toepassingen op het internet gebruikt. Het DNS bevat de hiervoor essentiële informatie over domeinnamen. Veel gebruikte toepassingen van DNS zijn vertaling van domeinnamen naar IP-adressen, informatie over e-mailservers, spambeperking, verificatie van eigenaarschap t.b.v. clouddiensten, beveiligingsparameters en het vinden van services zoals VoIP-servers.

Alle diensten die gebruik maken van een domeinnaam kunnen verstoord raken bij het (langdurig) niet-beschikbaar of verstoord zijn van (alle) authoritative DNS-servers voor een bepaald domein en/of bovenliggende zone. Aantasting van de integriteit van informatie in het DNS kan daarnaast diverse vormen van cyberaanvallen mogelijk maken.

Authoritative DNS-servers zijn over het algemeen redundant uitgevoerd. In sommige gevallen zijn de NS-servers verspreid over verschillende netwerken (AS'en). Uitval van meerdere gescheiden systemen en/of een aanval op een centraal beheerssysteem zijn dan noodzakelijk voor uitval.

Om welke (soorten) aanbieders én gebruikers gaat het?

De meest bekende vorm van DNS-dienstverlening is het aanbieden van een resolver door een ISP aan haar klanten. Deze dienstverlening valt buiten scope van dit onderzoek maar is onverminderd van belang voor het goed functioneren van het internet.

Kijken we naar dienstverlening aan de 'DNS-informatie-verstrekkende' zijde, dan zien we verschillende soorten aanbieders:

- Aanbieders van authoritative DNS ten behoeve van actieve domeinen. Deze categorie kan worden onderverdeeld in verschillende typen partijen:
    - Webhosters die tevens, als registrar, domeinnamen namens hun klanten registreren en daarvoor de authoritative DNS realiseren. In deze groep zijn de verticaal geïntegreerde webhosters (met eigen datacenters en 'harde' infra), whitelabel-aanbieders, wholesale-gebaseerde-aanbieders (afnemers van de whitelabel-aanbieders), en resellers te onderscheiden. Veel webhosters zijn gericht op de Nederlandse markt of op een specifiek segment (bijvoorbeeld webshops).
    - De grotere cloudaanbieders, zoals Google, Amazon en Microsoft. Zij leveren authoritative DNS als onderdeel van een breed dienstenportfolio, en doen dit internationaal. Het is overigens goed denkbaar dat DNS-diensten ook (deels) fysiek vanuit Nederland geleverd worden, gezien de grootschalige aanwezigheid van deze partijen in Nederland.
- De 'website builders', zoals Wix. Dit zijn partijen die aan met name kleinere bedrijven een 'one-stop-shop' bieden voor het realiseren van een website, en als onderdeel daarvan ook een domeinnaam registreren en authoritative

DNS realiseren. Een variant zijn de 'web shop builders' en 'Magento hosts' die een soortgelijk model hanteren, maar dan gericht op (kleinere) webwinkels.

- Gespecialiseerde partijen die namens andere bedrijven in een specifieke doelgroep domeinnamen registreren en exploiteren. Een voorbeeld is Thuisbezorgd.nl, dat voor veel restaurants en café's een .nl-domeinnaam heeft geregistreerd, en laat doorverwijzen naar Thuisbezorgd. Hetzelfde zien we voor huisartspraktijken, klusbedrijven en makelaars.

- Aanbieders van onderliggende infrastructuur en maatwerkoplossingen. Denk hierbij aan hostingpartijen waar een (virtuele) server kan worden ingericht om een eigen DNS-server te draaien en de meer 'full service' ICT-dienstverleners. Mogelijk leveren deze partijen ook beheersdiensten voor de betreffende DNS-servers, maar de mate waarin is van buitenaf niet vast te stellen.

- Aanbieders van diensten t.b.v. niet-actieve domeinen. In deze groep vallen met name de 'domeinmakelaars'. Zij beheren domeinnamen voor klanten, parkeren ze eventueel (in eigen DNS) en beheren de SOA-records bij SIDN. Deze partijen werken ofwel voor grotere partijen, of zijn zelf actief in 'domeinhandel'.

- Aanbieders van *content delivery*- en beveiligingsdiensten. Denk hierbij aan partijen als CloudFlare of Akamai. Door hun eigen authoritative DNS-service in te zetten kunnen deze partijen wereldwijd de stroom van verkeer tussen dienst en eindgebruiker sturen en optimaliseren. Ook is het hiermee mogelijk om bescherming te bieden tegen DDoS-aanvallen.

Onze analyse geeft tot slot een beeld van de afhankelijkheid van buitenlandse DNS-aanbieders. Een aantal grotere aanbieders (zie Tabel 7) is ogenschijnlijk (primair) niet-Nederlands. Verder zien we een afhankelijkheid van grotere cloudaanbieders als Amazon en Google (met name, zo lijkt het, van infrastructuurdiensten op basis waarván DNS wordt gerealiseerd, en niet zozeer de specifieke DNS-diensten van deze partijen) en buitenlandse dienstverleners als Akamai en CloudFlare. De meeste grotere partijen hebben echter wel fysieke aanwezigheid in Nederland.

Wat zijn de voornaamste in Nederland gevestigde aanbieders?

Het aantal domeinnamen is zeer scheef verdeeld over aanbieders van de bijbehorende authoritative DNS. Dat betekent dat een klein aantal partijen de authoritative DNS realiseert voor een groot deel van de voor Nederland relevante domeinnamen. In onze steekproef van .nl-domeinnamen zien we dat 25% verwijst naar authoritative DNS van de vijf grootste partijen, waarbij eventuele whitelabel-activiteiten van die partijen niet zijn meegeteld. Voor 80% van de .nl-domeinnamen wordt verwezen naar 95 verschillende authoritative servers; het aantal achterliggende aanbieders is kleiner vanwege (white)labels. Het kantelpunt tussen de kleine set grotere partijen en een grote hoeveelheid kleine partijen ligt in onze steekproef rond een marktaandeel van 0,05% (waarbij de kleinste 'grote' partijen enkele duizenden .nl-domeinnamen onder zich heeft).

We merken op dat een aantal aanbieders van authoritative DNS onderdeel is van een groter concern of moederbedrijf. Wanneer op dit niveau wordt geaggregeerd zullen met name de grotere partijen in de dataset een groter marktaandeel krijgen.

Op basis van een representatieve steekproef komen we tot de volgende lijst met voornaamste *in Nederland gevestigde* aanbieders, gegroepeerd op de recordnaam in het DNS.

Tabel 9 Overzicht van geschatte marktaandelen per (Nederlandse) partij (op basis van SOA/NS-record)

SOA/NS-record	Duiding[21]	Groepering	Geschat marktaandeel (.nl-domeinnamen)
transip.*	TransIP (webhoster)	team.blue	7,7%-7,9%
mijndomein.*	Mijndomein (webhoster)	Mijndomein	6,0%
webhostingserver.*	Antagonist (whitelabel webhosting)		4,4%
zxcs.*	Vimexx (webhoster)	team.blue[22]	4,1%
hostnet(bv).*	HostNet (webhoster)		3,5%-3,7%
openprovider.*	OpenProvider (whitelabel-aanbieder)		3,5%-3,6%
axc.*	Versio (wholesale domeinregistrar)	TWS	2,8%
neostrada.*	Neostrada	TWS	2,3%-2,4%
firstfind.*	Yourhosting	TWS	1,9%
auroradns.*	Astralus / PCExtreme (webhoster)	TWS	1,5%
metaregistrar.*	Metaregistrar	Mijndomein[23]	1,4%
vevida.*	Vevida	TWS	1,2%
argewebhosting.*	Argeweb	TWS	1,1%
ns0.*	TransIP (whitelabel webhosting)	team.blue	1,0%
dn-s.*	TransIP (whitelabel webhosting)	team.blue	0,6%
mijndnsserver.*	MijnDomeinReseller (whitelabel registrar)		0,6%
hosting2go.*	Hosting2Go		0,6%
dnssrv.*	Totaaldomein (whitelabel domeinregistrar)[24]		0,5%
yourwebhoster.*	Yourwebhoster.com (whitelabel webhosting)		0,5%
anony.*	FlexWebhosting (webhoster)[25]		0,3%-0,5%
xs4all.*	XS4All (ISP/webhoster)		0,4%
flexwebhosting.*	FlexWebHosting (webhoster)		0,4%
ixlhosting.*	iXL (webhoster)		0,4%
dds.*	DDS (ISP/webhoster)		0,4%
2is.*	Integrated Internet Services (whitelabel registrar).[26]		0,3%

Kijken we naar niet in Nederland gevestigde aanbieders van authoritative DNS voor .nl-domeinnamen, dan zien we daar onder andere CloudFlare (±4,9%), Dan.com (3,9%), Strato

[21] Op basis van Whois-gegevens van SIDN en bureauonderzoek.

[22] [vimexx.eu]

[23] Metaregistrar is ontstaan uit Mijndomein, in eerste instantie als handelsnaam, maar inmiddels lijkt het om een separate rechtspersoon (Metaregistrar B.V.) te gaan. Het is niet duidelijk in hoeverre de organisaties in de praktijk gescheiden zijn. Duidelijk is wel dat Metaregistrar een deel van de domeinregistraties uitvoert voor Mijndomein.

[24] [totaaldomein.nl]

[25] [flexwebhosting.nl]

[26] [2is.nl]

(±3,5%) en One.com (±3,4%) terugkeren als aanbieders van authoritative DNS. We zien daarnaast Sedo, een partij die domeinnamen 'parkeert' (±1,2%), Takeaway.com (±1,1%) en Wix (±1,1%).

Uit onze analyse volgt tot slot een aantal meer *gespecialiseerde* aanbieders die betrokken zijn bij het leveren van authoritative DNS. De authoritative DNS verloopt voor een aanzienlijke hoeveelheid domeinnamen via infrastructuur van deze partijen. Het is echter niet vast te stellen of deze partijen de DNS-dienst ook beheren: in veel gevallen gaat het om (virtuele) servers van *klanten van* deze partijen. Het betreft:[27] Trans-IX, Greenhost, DirectVPS, Totaalnet Internet Works, Zylon, Tuxis, Worldstream, IPS, I3D, Vivor, Vixbits, Duocast, Interconnect, Fundaments/Oxilion, Networking4All, Netbase, Cyso, Mihosnet, SIGNET, Tilaa, Todayconcepts, Wedare, Denit, Hosting2Go, KPN InterNedServices, Serverius, Previder, CJ2, TrueServer, Sentia, Astralus en XS4ALL (KPN).

Beperkingen van het onderzoek

Voor dit onderzoek is gebruik gemaakt van een representatieve steekproef van actuele domeinnamen. De hierboven genoemde conclusies zijn gebaseerd op aantallen .nl-domeinnamen, onder de aanname dat deze set representatief is voor de voor Nederland relevante domeinnamen, en dat de verdeling binnen de .nl-set niet substantieel afwijkt van de verdeling buiten .nl. Er is geen weging toegepast bij het tellen van de domeinnamen, en dus geen rekening gehouden met de economische of maatschappelijke waarde van individuele domeinen.

We constateren dat in de resultaten een sterke concentratie van DNS-aanbod over een klein aantal aanbieders zichtbaar is, en dat uitval/verstoring van de DNS-dienstverlenging van een dergelijke aanbieders een zeer groot aantal gebruikers kan raken. Hoewel de *relatieve* marktaandelen c.q. relatieve 'waardeverdeling' over domeinen niet exact is vast te stellen met de hier gehanteerde methode, blijft staan dat het *absolute* aantal (potentieel) geraakte gebruikers hoog genoeg kan zijn om aanleiding te geven tot het stellen van specifieke eisen aan deze aanbieders.

[27] Genoemd worden de partijen gelieerd aan AS'en met een Nederlandse landcode waarvoor we vaststellen dat 2.500 of meer NS-records verwijzen naar IP-adressen binnen het AS, en die niet worden genoemd in de eerdere resultaattabel.

Verwijzingen

[1] Overheid (2019). *Besluit beveiliging netwerk- en informatiesystemen* [wetten.overheid.nl]

[2] Mockapetris, P. (1987). *RFC 1035: Domain names - implementation and specification* [www.ietf.org] IANA, Network Working Group.

[3] Mockapetris, P. (1987). *RFC 1034. Domain names - concepts and facilities* [tools.ietf.org] IANA. Network Working Group.

[4] ICANN (2020). *List of Top-Level Domains* [data.iana.org]

[5] ICANN (2020). *Root Zone Database* [www.iana.org]

[6] IETF (2013). *RFC6762. Multicast DNS* [tools.ietf.org]

[7] IETF (2015). *RFC7686. The ".onion" Special-Use Domain Name* [tools.ietf.org]

[8] Amazon (2020). *Amazon Route 53* [aws.amazon.com]

[9] EU (2016). *Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie* [eur-lex.europa.eu] vol. L 194/1, Brussel: Europese Commissie.

[10] Scheitle, Q., Gasser, O., Nolte, T., Amann, J., Brent, L., Carle, G., Holz, R., Schmidt, T., and Wählisch, M. (2018). *The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem* [arxiv.org] Boston, MA, USA: ACM.

[11] Marchal S., F.J. S. R. E. T. (2012). *Proactive Discovery of Phishing Related Domain Names* [link.springer.com] Springer.

[12] Mozilla (2020). *Firefox 83 introduces HTTPS-Only Mode* [blog.mozilla.org]

[13] Google (2020). *HTTPS encryption on the web* [transparencyreport.google.com]

[14] RIPE NCC (2020). *Our Plan to Fix Country Codes* [labs.ripe.net]

[15] Mozilla Foundation (2020). *Public Suffix List* [publicsuffix.org]

[16] Chromium (2017). *Issue 756818: Certificate Transparency - Google "argon2020" Log Server Inclusion Request* [bugs.chromium.org]

[17] Sears, R. (2016). *Axeman* [github.com]

[18] SIDN (2020). *.nl stats and data: Registration.* [stats.sidnlabs.nl]

[19] SIDN (2020). *Registrar List* [www.sidn.nl]

[20] Neustar (2020). *UltraDNS* [www.home.neustar]

[21] CloudFlare (2020). *Changing your domain name servers to CloudFlare* [support.cloudflare.com]

[22]Webhosters.nl (2018). *Grootste Webhosting Bedrijven in Nederland (2018)* [www.webhosters.nl]

[23]YourHosting (2020). *Gratis SSL* [www.yourhosting.nl]

[24]Mijndomein.nl (2020). *Mijndomein online* []

[25]Mijndomein. *Gratis SSL Certificaat* [www.mijndomein.nl]

[26]Metaregistrar (2020). *Over Metaregistrar. Abuse en klachtenprocedure* [www.metaregistrar.nl]

[27]ICANN. *Top-Level Domains* [archive.icann.org]

[28]ICANN (2020). *Root zone* [www.internic.net]

[29]SIDN. *Registrar listing* [www.sidn.nl]

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl