Betrouwbaarheid DNS-Infrastructuur Nederlandse Overheid bij Beschikbaarheidsproblemen

Strategisch Adviesrapport

dr. Giovane C. M. Moura[1]
Raffaele Sommese, MSc[2]
dr.ir. Mattijs Jonker[2]
1: SIDN Labs 2: Universiteit Twente

Betrouwbaarheid DNS-Infrastructuur Nederlandse Overheid bij Beschikbaarheidsproblemen

Strategisch Adviesrapport

door

dr. Giovane C. M. Moura[1]
Raffaele Sommese, MSc[2]
dr.ir. Mattijs Jonker[2]

1: SIDN Labs 2: Universiteit Twente

17 maart 2022

Inhoudsopgave

Management samenvatting

Beoogd Publiek: *Dit rapport is geschreven voor beleidsmakers bij de Nederlandse overheid alsmede besluitvormers voor vitale infrastructuur. De auteurs hebben aangenomen dat niet alle lezers een sterke technische achtergrond hebben en om deze reden zullen we, waar nodig geacht, relevante achtergrondinformatie geven.*

Nederland is een van de **wereldleiders op het gebied van digitale overheid**. Meer dan 80% van de volwassen populatie communiceert digitaal met de overheid.[1] Burgers en bedrijven kunnen gebruikmaken van verscheidene digitale diensten, wat efficiëntie ten goede komt en kosten drukt.

Om digitale diensten zo toegankelijk mogelijk te houden is het van belang dat de overheid **betrouwbare en robuuste** diensten aanbiedt die weerbaar zijn tegen een veelvoud aan digitale dreigingen die dienstverlening kunnen verstoren. Neem `DigiD` als voorbeeld: als deze dienst ongepland voor een lange periode uit de lucht ligt dan kunnen burgers niet meer bij digitale diensten, worden digitale processen verstoord, en kunnen er zelfs problemen ontstaan met fysieke infrastructuur (b.v. files naar aanleiding van verstoorde douane processen).

In dit adviesrapport leggen we de focus op een *specifiek deel* van Internet infrastructuur die van belang is voor digitale dienstverlening: het zogeheten **Domain Name System (DNS)**. Het **DNS** is een *vitale* component van het Internet en kan als een "telefoonboek" worden gezien. Stel dat een burger belastingaangifte wil doen. Het DNS zorgt ervoor dat de domeinnaam, `belastingdienst.nl`, die mensen begrijpen en kunnen onthouden, wordt vertaald naar een IP-adres, die computernetwerken vervolgens gebruiken voor communicatie. De DNS-infrastructuur die bij deze vertaling betrokken is moet betrouwbaar en robuust zijn om ervoor te zorgen dat de website van de Belastingdienst voor burgers bereikbaar is en blijft.

Het falen van het DNS kan **ernstige gevolgen** hebben en kan er uiteindelijk voor zorgen dat digitale overheidsdiensten niet meer werken. Er zijn in het buitenland notoire incidenten geweest waarin falen van het DNS ervoor heeft gezorgd dat online diensten uren tot dagen niet beschikbaar waren. Met dit in gedachte zijn de auteurs van dit rapport, van Stichting Internet Domeinregistratie Nederland Labs (SIDN Labs) en Universiteit Twente, door het NCSC gevraagd om via een meetstudie de betrouwbaarheid van de DNS-infrastructuur van de Nederlandse overheid te onderzoeken en om te evalueren of, operationeel gezien, algemeen bekende en door experts vastgelegde best practices om weerbaarheid te verhogen worden nageleefd.

Het tweeledige doel van deze studie is om de *configuratie* van de DNS-infrastructuur die wordt gebruikt voor domeinnamen van digitale overheidsdiensten te **evalueren** en om mogelijkheden te **identificeren** om weerbaarheid tegen digitale dreigingen te vergroten. Als auteurs erkennen we dat we geen experts op het gebied van beleid zijn, maar we presenteren als DNS-experts wel **aanbevelingen** om het gebruik van het DNS door overheidsdiensten te verbeteren. Tevens bespreken we de complexiteit en de naar verwachting benodigde inspanningen om deze aanbevelingen op te volgen.

[1] https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Netherlands_2019_0.pdf

Hoofdbevindingen:

Onze studie heeft uitgewezen dat de meeste domeinnamen die voor overheidsdoeleinden worden gebruikt de door experts vastgelegde en algemeen bekende best practices om weerbaarheid te verhogen naleven, wat goed nieuws is. Echter stellen we ook vast dat een significant aantal domeinnamen, gebruikt voor verscheidene overheidslagen, dit niet doen. Dit creëert onnodig risico dat, naar onze mening, in veel gevallen eenvoudig te voorkomen is.

We identificeren twee *kritische* zogeheten single points of failure (SPoF), die aanwezig zijn voor ongeveer 50% van de overheids domeinnamen. Een SPoF is een enkel punt in een systeem dat bij falen het hele systeem omverhelpt. Namelijk:

1. Ten eerste: circa de helft van de overheids domeinnamen hangen (elk) van slechts één enkele DNS-aanbieder af, wat voor onnodig risico zorgt. Een enkele aanbieder kan zijn een externe dienstverlener, alsmede een enkele DNS server in eigen beheer. Als de aanbieder het doelwit van een cyberaanval wordt en omvalt, of als netwerkstoringen optreden, dan kunnen alle afhankelijke digitale diensten vervolgens onbereikbaar worden. Dit is niet slechts hypothetisch: er zijn notoire incidenten geweest waarin cyberaanvallen op DNS-infrastructuur bij enkelvoudige afhankelijkheid voor (aanhoudende) beschikbaarheidsproblemen hebben gezorgd.
2. Ten tweede: een significant deel van domeinnamen hangen elk af van een "keten van DNS servers" die een enkel top-level domein (TLD) gebruiken (b.v. `.nl` of `.com`). De consequentie hiervan kan zijn dat falen in de DNS-infrastructuur van het TLD zich verspreid en gevolgen heeft voor bereikbaarheid van digitale diensten.

Om deze knelpunten aan te pakken doen we in Hoofdstuk 4 twee aanbevelingen:

1. Diversificeer DNS-aanbieders

   Dit kan op twee complementaire manieren worden gedaan:

   i. door overheidsinstanties op verscheidene niveaus (gemeente, provincie, enz.) aan te sporen om geen afhankelijkheid van één enkele DNS-aanbieder te hebben en (technische) ondersteuning te bieden om dit te realiseren
   ii. door een robuuste *NLDNS* dienst te ontwikkelen (of uit te besteden) die los van de primaire DNS-aanbieder (of beheerder) staat en die door overheids domeinnamen als secundaire DNS server ingesteld kan worden

2. Monitoren van DNS-infrastructuur voor problemen

   Netwerkstoringen en menselijke fouten kunnen ten alle tijden voorkomen dus het is belangrijk om de goede werking en de staat van DNS-infrastructuur vaker dan één keer (onze) te analyseren.

   - door frequente beoordelingen te doen gaat situationeel bewustzijn omhoog en kunnen de verantwoordelijke beheerders worden ingelicht en aangespoord om actie te ondernemen als zich problemen voordoen, waardoor het risico van onbereikbaarheid wordt verlaagd
   - door centraal in monitoren te voorzien doen zich schaalvoordelen op (kosten, benodigde expertise, enz.). Tevens is op lokaal niveau niet per definitie alle informatie aanwezig om specifieke configuratierisico's te kunnen beoordelen

Naar onze mening zal met het toepassen van deze aanbevelingen de weerbaarheid van de DNS-infrastructuur van de Nederlandse overheid aanzienlijk worden vergroot.

1

Introductie

Het DomeinNaam Systeem (DNS) [4] voorziet in een kernonderdeel van het Internet: vrijwel alle website-bezoeken en e-mail-interacties hangen af van het DNS. Het DNS kan gezien worden als de contactenlijst op je telefoon, die ervoor zorgt dat een "vertaling" van naam tot nummer plaatsvindt, waarna het nummer wordt gebruikt om het communicatiekanaal op te zetten. Op het Internet zorgt het DNS ervoor dat domeinnamen zoals in `https://overheid.nl` kunnen worden vertaald naar adressen die computernetwerken begrijpen en gebruiken voor communicatie.

Als het DNS faalt dan kan dat sterke gevolgen hebben voor diensten die van het DNS afhangen. Er zijn precedenten waarin menselijke fouten, netwerkstoringen, of moedwillige cyberaanvallen gebruikers de toegang tot diensten die van het DNS afhangen hebben ontkend. Als voorbeeld: in 2016 is de grote DNS dienstverlener Dyn door een distributed denial-of-service (DDoS) lamgelegd. O.a. Twitter, PayPal en Spotify maakten indertijd (enkelvoudig) gebruik van Dyn [12]. Door de aanval op de DNS-aanbieder waren voor een groot deel van een dag deze (en andere) digitale diensten voor hun gebruikers aan de oostkust van de VS en in delen van Europa niet of slecht bereikbaar. Dichter bij huis: in augustus van 2015 konden miljoenen Internet-gebruikers in Nederland niet of slecht bij het Internet dankzij een aanval op de DNS-infrastructuur van Ziggo.

Binnen de context van overheden is het hebben van betrouwbare en weerbare DNS van vitaal belang voor digitale dienstverlening. Als DNS-infrastructuur van de overheid met beschikbaarheidsproblemen kampt, dan kunnen burgers mogelijk niet meer bij digitale diensten. Als gedachtenexperiment: wat zou er gebeuren als `DigiD` ongepland, aanhoudend en tijdens drukke tijden onbereikbaar is?

Het DNS is een complex systeem. Het ontwerpen en beheren van weerbare DNS-infrastructuur vergt technische kennis en financiële middelen. Ervaren netwerkbeheerders en experts hebben *best practices* vastgelegd om, operationeel gezien, de weerbaarheid van DNS infrastuctuur te vergroten. Door deze best practices na te leven kunnen de risico's van beschikbaarheidsproblemen worden *verlaagd*. We vatten deze algemeen bekende best practices samen in [7].

Voor dit strategische adviesrapport hebben we ons gericht op de weerbaarheid van de DNS-infrastructuur die relevant is voor domeinnamen van Nederlandse overheden. Dit houdt in domeinnamen voor websites (b.v. `https://overheid.nl`) alsmede domeinnamen waar e-mail naartoe kan worden verstuurd (b.v. `*****@minjenv.nl`). Onze studie richt zich op circa 2000 domeinnamen die door overheden worden gebruikt alsmede op de DNS-infrastructuur waar deze domeinnamen gebruik van maken. De bestudeerde domeinnamen beslaan een kernset die door Forum Standardisatie is opgesteld alsmede specifieke DigiD "toegangspunten" (b.v.

	Web	**E-mail**
Namen	1460	536
Bron		
DigiD	902	0
Forum Standaardisatie	558	535
Unieke Namen	1309	536
Overheidslaag		
Gemeenten	1044	366
Uitvoerders	99	49
Rijk	84	64
Waterschappen	46	31
Provincies	30	19
Overig	6	6

Tabel 1.1: Onderzochte domeinnamen (bron samenstelling op 2021-10-01)

digitaal gemeenteloket). Het is belangrijk om op te merken dat hoewel de kernset het startpunt is van onze studie, onze resultaten ook inzichten geven in de weerbaarheid van de gebruikte DNS-infrastructuur zelf. Sommige resultaten zijn niet "gebonden" aan specifieke domeinnamen. Het gevolg hiervan is dat onze resultaten ook van toepassing zijn op *andere* domeinnamen (d.w.z. niet in de kernsset), mits deze domeinnamen van dezelfde DNS-infrastructuur afhangen. We identificeren voor circa 50% van de domeinnamen twee kritische single points of failure in de mate waarin DNS is ingericht. We presenteren deze bevindingen in Hoofdstuk 2. Daarna presenteren we nog twee belangrijke (echter niet kritische) verbeterpunten in Hoofdstuk 3. In Hoofdstuk 4 doen we aanbevelingen om DNS-weerbaarheid te verhogen. We discussiëren mogelijke stappen voor vervolgonderzoek in Hoofdstuk 5 en concluderen vervolgens.

1.1. Domeinnamen van Nederlandse overheden

Het NCSC heeft ons een lijst met te onderzoeken domeinnamen aangeleverd. Het gaat om 1309 domeinnamen die worden gebruikt voor web (d.w.z., ze leiden tot een website) en 536 domeinnamen die in e-mail worden gebruikt (d.w.z. ze komen voor achter de `@` in e-mail adressering). Deze domeinnamen vormen de input voor onze meetstudie van de betrouwbaarheid van de DNS-infrastructuur die door de Nederlandse overheid wordt gebruikt. Onze studie richt zich op domeinnamen voor digitale diensten op het **open Internet**.

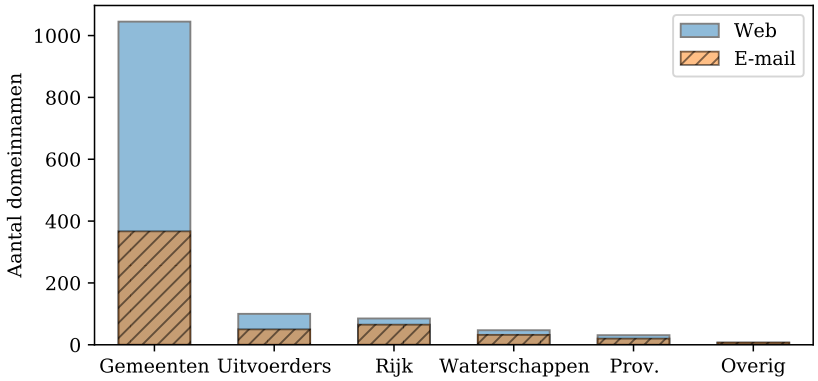
Tabel 1.1 geeft de verdeling van de namen over de categorieën weer, alvolgens de bron (Forum Standardisatie of DigiD) en de overheidslaag waar de naam bij hoort (gemeente, provincie, enz.).[1] Figuur 1.1 geeft de data van Tabel 1.1 in een staafdiagram weer. We zien dat de meerderheid van overheids domeinnamen onder de gemeente categorie vallen.

Om te onderzoeken of deze namen de vastgelegde best practices naleven (zie [7]) hebben we een Internet meetstudie uitgevoerd. In dit adviesrapport behandelen we de resultaten die opvolging vragen. We verwijzen de lezer naar het technische rapport voor verdere details.

1.2. Bereik en beperkingen van de uitgevoerde studie

Bereik: Deze studie richt zich op de DNS-infrastructuur die van belang is voor digitale dienstverlening op het open Internet. De studie zou herhaald kunnen worden op besloten netwerken zoals Diginetwerk, maar deze vielen vooralsnog buiten de scope van het onderzoek.

[1] Merk op: in een DNS-context is de term *naam* een gangbaar alternatief voor *domeinnaam* en we gebruiken deze verkorte versie veelal in dit rapport.



Figuur 1.1: Onderzochte domeinnamen Nederlandse overheden

Beperkingen: we doen kwantitatief onderzoek door metingen te verrichten op het Internet om vervolgens gebaseerd op meetdata de mate waarin best practices worden nageleefd te evalueren. De meetmethoden waar we gebruik van maken kennen beperkingen, wat niet zozeer aan de methoden zelf ligt maar aan de manier waarop het Internet werkt en is ingericht. Als voorbeeld: we kunnen (vaak) niet bepalen of twee servers letterlijk in hetzelfde datacenter hangen en een Internetverbinding gemeen hebben. We kunnen wel zien of de servers zich in dezelfde IP-adresruimte bevinden. We beschrijven niet te meten metrieken in meer detail in §3.3 in [7].

2

Kritische problemen: Single Point of Failure (SPoF)

Een goed ontwerpprincipe voor foutbestendige systemen is om zogeheten *Single Points of Failure (SPoF)* te voorkomen, wat knelpunten in een systeem zijn die bij falen ervoor zorgen dat het hele systeem omvalt. Neem als voorbeeld het Deltawerk de Maeslantkering: om te voorkomen dat bij stroomstoring het systeem niet werkt heeft de kering drie onafhankelijke stroombronnen. Zelfs als er twee falen dan kan de derde alsnog gebruikt worden om de kering te sluiten en Rotterdam, de haven en het omliggende gebied te beschermen tegen overstromingen.

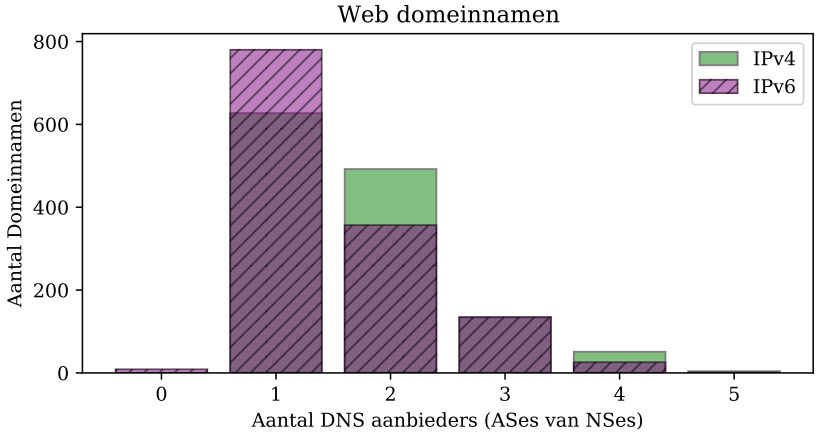
We evalueren de domeinnamen van Nederlandse overheden (Tabel 1.1) tegen tien DNS SPoF metrieken. Voor de details van deze metrieken verwijzen we naar §3.1 van [7]. We stellen vast dat de meeste domeinnamen tegen acht van de tien SPoF's beschermd zijn. De twee overgebleven en problematische SPoF's zijn: 1) de naam gebruikt een enkele DNS-aanbieder (of beheerder) (§2.1); en 2) de keten van DNS servers herleidt naar een enkele TLD (§2.2). We classificeren de urgentieniveaus respectievelijk als **hoog** en **laag**, wat we later zullen motiveren.

2.1. Afhankelijkheid van één DNS-aanbieder (of-beheerder)

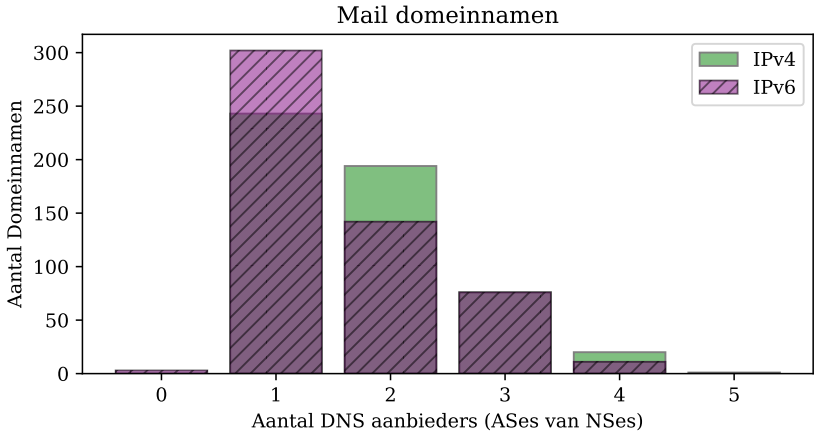
Het gebruik van een enkele DNS-aanbieder is een mogelijk single point of failure. Met aanbieder bedoelen we zowel een externe dienstverlener (b.v. commerciële partij), alsmede een enkele DNS server onder eigen beheer. De in de introductie genoemde cyberaanval op de DNS-aanbieder Dyn laat zien hoe dit is afgelopen voor bezoekers van digitale diensten (b.v. Twitter, PayPal en Spotify) die ten tijde van de aanval uitsluitend van Dyn DNS-infrastructuur gebruikmaakten [12].

Figuur 2.1 laat de aantallen van DNS-aanbieders zien waarvan zowel de te onderzoeken web en e-mail-namen gebruikmaken. We zien dat de meeste namen, voor zowel web als e-mail, elk van slechts één DNS-aanbieder gebruikmaken, wat neerkomt op een SPoF. Als deze aanbieder het doelwit van een cyberaanval wordt (b.v. een distributed denial-of-service attack) of op andere wijze netwerkstoring ondervindt, dan zullen alle domeinnamen die van de aangevallen DNS-infrastructuur afhangen niet meer bereikbaar zijn. Afhankelijk van de aanwezigheid en staat van zogeheten DNS cache mechanismes kan dit voor veel gebruikers (b.v. mensen die een website die aan de domeinnaam hangt willen bezoeken) direct of na verloop van tijd merkbaar zijn. Wegens het precedent classificeren we het urgentieniveau hier als **hoog**.

Tabel 2.1 geeft de top 3 DNS-aanbieders voor elke dataset weer. Voor de web-categorie zien



(a) Web



(b) E-mail

Figuur 2.1: Aantal DNS-aanbieders voor web en e-mail (AS staat voor Autonoom Systeem c.q. beherend netwerk)

	Web	
	IPv4	**IPv6**
TransIP-AS20857	281	281
TWS-AS48365	86	86
Quality-AS12315	73	73
Overig	182	179
	E-mail	
	IPv4	**IPv6**
Microsoft-AS8075	154	0
TransIP-AS20857	36	39
Amazon-AS16509	19	19
Overig	108	119

Tabel 2.1: Top 3 aanbieders voor domeinnamen die (elk) van slechts één DNS-aanbieder afhangen

	Web		Mail	
	IPv4	**IPv6**	**IPv4**	**IPv6**
gemeenten	533 (51.0%)	664(63.3%)	185 (50.5%)	234 (63.9%)
uitvoerders	37(37.3%)	50(50.5%)	17(34.7%)	21(42.8%)
rijk	26 (30.9%)	25(29.7%)	20 (31.2%)	19 (29.7%)
provincies	14(46.6%)	15(50.0%)	10(52.2%)	11(57.8%)
waterschappen	14(30.4%)	23 (50.0%)	8 (25.8%)	14 (45.6%)
overig	3 (50.0%)	3 (50.0%)	3 (50.0%)	3(50.0%)

Tabel 2.2: Aantal namen per categorië met afhankelijkheid van één DNS-aanbieder. Percentages zijn berekend naar het totaal aantal namen per categorie.

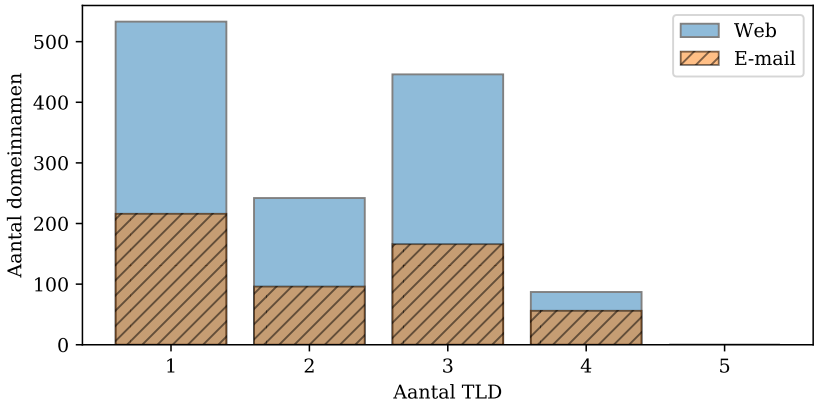
we dat TransIP de markt domineert: 281 domeinnamen hangen volledig af van TransIP als DNS-aanbieder. Voor e-mail zien we dat Microsoft domineert, wat komt omdat veel instanties Microsoft Outlook gebruiken, waar de DNS-infrastructuur van Microsoft zelf bij betrokken is.

In Tabel 2.2 zien we dat, wat betreft web namen die van slechts één DNS-aanbieder afhangen, de resultaten variëren van 30.9% tot 51% voor verschillende overheidslagen. Concreter, 533 van 1044 Gemeente web namen (dat is 51%) hebben een enkele aanbieder. De categorie Rijk heeft het laagste percentage van 30.9%, maar dit komt alsnog neer op een onnodig risico voor 26 van de 84 namen.

Onze eerste aanbeveling is om deze single points of failure te voorkomen. Dit hoeft over het algemeen niet moeilijk te zijn, wat staaft met het feit dat een groot deel van alle onderzochte Overheids domeinnamen nu al een secundaire DNS-aanbieder (of beheerder) gebruikt. Wat betreft moeite: dit probleem aanpakken kan neerkomen op het contractueren van een (tweede) commerciële partij. In §4.1 suggereren we andere en alternatieve stappen die genomen zouden kunnen worden om de ingebruikname van een secundaire DNS server te helpen en tevens om de weerbaarheid te verhogen op een manier die niet per sé afhangt van een (tweede) commerciële aanbieder.

2.2. Afhankelijkheid enkel top-level domein

Een andere (en de tweede problematische) single point of failure is het afhankelijk zijn van een "keten van DNS servers" die naar een enkel top-level domein (TLD) zijn te herleiden. Merk op dat een `.nl` domeinnaam ook van ketens gebruik kan maken die b.v. in `.eu` eindigen. Zonder hier in technische details te treden over wat we met keten bedoelen en waar deze toe dienen binnen het DNS benadrukken we dat een consequentie van het afhangen van één TLD kan zijn dat falen van



Figuur 2.2: Aantal TLDs gebruikt door web en e-mail namen

de DNS-infrastructuur van de TLD beheerder voor (te voorkomen) bereikbaarheidsproblemen van domeinnamen kan zorgen. We benadrukken dat de top-level domein beheerders (waaronder `.nl`) doorgaans wel meerdere servers in beheer hebben en dat deze met een cyberaanval platleggen minder praktisch is dan de aanbieder van b.v. `enschede.nl` lam te leggen, maar niet onmogelijk. Om deze reden classificeren we het urgentieniveau voor het niet naleven van deze metriek als **laag**.

Figuur 2.2 laat het aantal TLDs zien waartoe de server-ketens van zowel web als e-mail-namen te herleiden zijn. We zien dat veel namen afhangen van één TLD, hoewel sommigen ook van twee of drie. Als goed voorbeeld (in positieve zin) halen we `digid.nl` aan: in §A.2 laten we zien dat de "server-ketens" van deze naam naar vier TLDs te herleiden zijn (`.com`, `.nl`, `.eu`, `.org`) wat betekent dat in het (onwaarschijnlijke) geval dat de TLD server-infrastructuren van drie platgelegd worden de vierde alsnog de bereikbaarheid van `digid.nl` kan bewerkstelligen.

Onze tweede aanbeveling is om niet afhankelijk te zijn van slechts één TLD in de "keten van DNS servers" die betrokken is bij het vertalen van een gegeven domeinnaam. We merken hierbij op dat de beheerders van een TLD ook in overweging genomen moet worden. Als voorbeeld: `.net` en `.com` worden door de partij *Verisign* beheerd op dezelfde infrastructuur, waardoor ze zich qua weerbaarheid als een enkele TLD gedragen. Door onze tweede aanbeveling op te volgen zullen namen minder snel met beschikbaarheidsproblemen zitten mocht een enkele TLD beheerder (tijdelijk) met storing kampen.

3

Belangrijke problemen

In dit hoofdstuk bespreken we aanvullende problemen. Deze zijn niet zo kritisch als de single points of failure uit Hoofdstuk 2, maar ze komen weerbaarheid onnodig niet ten goede.

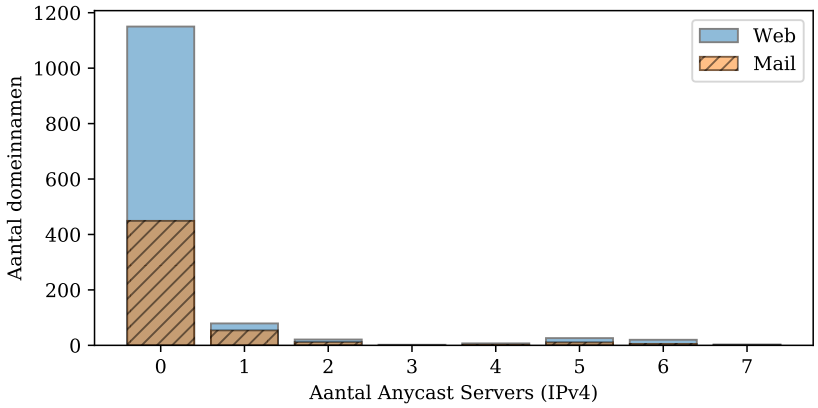
3.1. DNS-configuratiefouten

Er zijn verscheidene soorten DNS-configuratiefouten die gemaakt kunnen worden, vaak door menselijk handelen. Een mogelijke fout is het verkeerde IP adres instellen voor de DNS-server van een domeinnaam. Als voorbeeld: stel dat in het geval van `digid.nl` (Tabel A.3) de DNS server met de IP-adres verwijzing van 178.22.85.27 niet daadwerkelijk op dat adres bereikbaar is, terwijl deze wel zo is opgenomen in de DNS-configuratie van de domeinnaam. Dit verlaagt de bertrouwbaarheid omdat gebruikers niet op deze server kunnen rekenen. Dit is effectief gelijk aan één server minder hebben.

Onze resultaten hebben uitgewezen dat 17 van de web domeinnamen ten minste één niet reagerende DNS server kennen (als gebruikers het veelgebruikte IPv4 protocol gebruiken om de server te benaderen voor "vertaling") en 23 namen voor IPv6. Voor de categorie e-mail zijn de aantallen 3 en 4, respectievelijk. Deze fouten kunnen makkelijk hersteld worden door de DNS-configuratie aan te passen of de status en goede werking van de servers te checken. We classificeren het urgentieniveau als **middel** tot **hoog**.

Er zijn andere typen DNS (configuratie)fouten die kunnen plaatsvinden, wat we verder in §4 in [7] bespreken. Veel van deze fouten kunnen jaren onopgemerkt blijven terwijl ze de prestaties van DNS-infrastructuur omlaag halen. De auteurs van dit rapport hebben eerder een academische studie gepubliceerd waarmee we één van deze fouten uitlichten [14].

Om dit soort fouten te voorkomen raden we aan (in §4.2) om centraal via frequent monitoren de aanwezigheid van fouten te testen en na te lopen. Indien dat geregeld gedaan wordt kunnen DNS-beheerders ingelicht worden bij problemen om deze vervolgens zo snel mogelijk te corrigeren. Veel DNS-aanbieders monitoren hun eigen DNS-infrastructuur overigens ook, op o.a. prestaties en beschikbaarheid. Echter hebben DNS-aanbieders wegens de manier waarop het DNS werkt niet altijd voldoende informatie tot handen om alle mogelijke (configuratie)problemen voor specifieke domeinnamen te herkennen, waar het vanuit een centraal punt monitoren van vitale domeinnamen een oplossing voor biedt.



Figuur 3.1: Aantal anycast DNS servers per web en e-mail namen

3.2. Lage anycast adoptie

Een andere mogelijke maatregel om de weerbaarheid van DNS-infrastructuur te vergroten is het gebruik van zogeheten IP anycast [3, 11]. IP anycast wordt breed gebruikt door grote DNS-aanbieders. Alle DNS root servers ("het beginpunt van het globale DNS") gebruiken anycast en veel TLD beheerders doen dat ook. Anycast vergroot de weerbaarheid door servers globaal en logisch te verspreiden, in plaats van op een enkele fysieke locatie. Dit maakt het platleggen van alle infrastructuur aanzienlijk minder praktisch. Anycast wordt ook door grote DNS-aanbieders gebruikt. Het is belangrijk om op te merken dat het implementeren van IP anycast op infrastructuur onder eigen beheer specifieke operationele kennis en middelen vergt.

Figuur 3.1 laat het aantal domeinnamen zien met anycast DNS servers. We zien dat de meerderheid van de namen geen gebruik maakt van DNS-aanbieders met anycast. Hoewel veel domeinnamen geen DNS-infrastructuur met anycast gebruiken, is het gebruik aangeraden wegens de toegevoegde waarde voor weerbaarheid [6]. We classificeren het urgentieniveau als **laag**. De "makkelijkste" manier om anycast in te zetten is door een commerciële DNS-aanbieder te kiezen die het al in gebruik heeft. In §4.1 suggereren we stappen die genomen kunnen worden om de ingerbuikname van anycast te helpen op een manier die niet afhangt van een commerciële DNS aanbieder.

4

Aanbevelingen om betrouwbaarheid te vergroten

Hoewel we erkennen we dat we geen experts op het gebied van beleid zijn, geven we twee **aanbevelingen** om het gebruik van DNS-infrastructuur door Nederlandse overheidsinstanties weerbaarder te maken tegen mogelijke beschikbaarheidsproblemen.

4.1. Diversificeren van DNS-aanbieders

De belangrijkste aanbeveling die we doen is om het aantal DNS-aanbieders te verhogen en te diversificeren, ongeacht of dat nu commerciële partijen zijn of DNS-infrastructuur onder eigen beheer. Dit advies heeft met name betrekking op domeinnamen die momenteel (elk) van slechts één enkele DNS-aanbieder gebruikmaken (§2.1). We hebben in Tabel 2.2 gezien dat de percentages van namen met enkelvoudige afhankelijkheid tussen 30.9% (Rijk) en 51% (Gemeenten) rijkt. We adviseren om *ten minste* één aanvullende DNS-aanbieder toe te voegen aan elke domeinnaam, waarmee single points of failure worden voorkomen.

We zien twee manieren waarop deze diversificatie gerealiseerd kan worden, wat we nu verder toelichten:

4.1.1. Licht beheerders in en ondersteun ze bij diversificatie

Onze resultaten wijzen uit dat veel van de domeinnamen die slechts een enkele DNS-aanbieder gebruiken onder de categorie Gemeente vallen (§2.1). We nemen aan dat er variatie is in de technische kennis bij gemeenten en dat niet overal voldoende expertise en ondersteuning aanwezig is om een secundaire DNS-beheerder te kiezen en toe te voegen om betrouwbaarheid te verhogen.

Een goede keuze zou zijn om een DNS-aanbieder te kiezen die IP anycast gebruikt (§3.2) en die tevens niet uitsluitend van TLDs afhangt waar de primaire DNS-aanbieder gebruik van maakt (§2.2). Ondersteuning bij het maken van keuzes is mogelijk een behoefte waarin **centraal voorzien kan worden**, omdat dit schaalvoordelen brengt. Een eerste stap kan inlichten zijn, gevolgd door technische ondersteuning.

Benodigde inspanning: gegeven dat hogere overheidslagen (vermoedelijk) niet direct controle hebben over alle domeinnamen met slechts één enkele DNS aanbieder betekent dit (waarschijnlijk) dat elke getroffen overheidsinstanties (gemeente, provincie, enz.) benaderd moet

worden om ze in te lichten en daarna mogelijk technisch bij te staan. We stellen ons voor dat als dit centraal gedaan wordt, het probleem uitleggen, hulp bieden bij het maken van keuzes, en erop toezien dat beschikbaarheidsrisico's worden opgelost, weken tot maanden in beslag zou kunnen nemen en dat wegens het aantal kwetsbare domeinnamen c.q. overheidsinstanties hier een klein team op gezet zou moeten worden. Om te bevestigen dat de kwetsbaarheden zijn opgelost zou onze meting na verloop van tijd herhaald kunnen worden (mogelijk gericht op specifieke domeinnamen).

We willen tevens benadrukken dat dit **zorgvuldig** gedaan moet worden: als er tijdens dit proces configuratiefouten worden geïntroduceerd dan kan dit een averechts effect op betrouwbaarheid hebben en zelfs voor onbereikbaarheid zorgen.

4.1.2. Een robuuste secondaire DNS server voor overheden

Naast het aanmoedigen van overheden om een secundaire DNS-aanbieder naar keuze toe te voegen zou de overheid kunnen overwegen om een robuuste *NLDNS* dienst te ontwikkelen die los van de primaire DNS-aanbieder (of beheerder) staat en die vervolgens door instanties als secundaire DNS server ingesteld kan worden [6]. Dit idee is niet nieuw. Een vergelijkbaar idee wordt momenteel uitgevoerd door RIPE NCC, de regionale Internet registry voor o.a. Europa. RIPE NCC opereert secundaire DNS-infrastructuur voor de top-level domeinen van veel landen[1], waaronder Nepal (.np), Uruguay (.uy) en de Filipijnen (.ph). Deze dienst is echter niet beschikbaar voor overheids domeinnamen.

Met zulke robuuste DNS-infrastructuur zou elke overheidsinstantie een primaire DNS-aanbieder van eigen keuze kunnen gebruiken naast een centraal door de overheid geopereerde secundaire DNS server. Hiermee wordt vervolgens een single point of failure voorkomen. De overheid zou er tevens ook voor kunnen kiezen om deze infrastructuur over meerdere strategische punten in het open Internet in Nederland te verspreiden zodat de effecten van eventuele storingen in specifieke netwerken op betrouwbaarheid beperkt kunnen worden. Voorbeelden van strategische punten zijn Internet Service Providers (ISPs) en Internet Exchange Points (IXPs) zoals AMS-IX. Een bijkomend voordeel van het gebruiken van een *NLDNS* secundaire server is dat eventuele nevenschade van het afhangen van een (veelgebruikte) commerciële DNS-aanbieder die onder vuur komt te liggen wordt uitgesloten. Als voorbeeld de in de introductie genoemde cyberaanval op Dyn: hoewel PayPal en Twitter niet het doelwit van die aanval waren ondervonden de diensten en hun gebruikers wel de gevolgen. Het gebruik van toegewijde overheidsinfrastructuur zou het ondervinden van nevenschade bij aanvallen op commerciële DNS-aanbieders kunnen voorkomen, tenzij de overheidsinfrastructuur zelf natuurlijk het doelwit wordt (in welk geval de primaire DNS-aanbieder voor bereikbaarheid kan zorgen). Zulke infrastructuur biedt ook een kans om IP anycast in te zetten. Herinnering aan §3.2: anycast vergt specifieke operationele kennis en middelen.

Een alternatief voor het zelf beheren en aanbieden van een secundaire DNS server voor overheden is om dit uit te besteden aan een commerciële partij. Er zijn verschillende commerciële aanbieders die ook IP anycast inzetten. Sommige hiervan opereren in de Europese unie, wat met oog op privacy vraagstukken mogelijk voordelen met zich meebrengt. Het uitbesteden zou voor snelle implementatie en inzet kunnen zorgen en operationele inspanningen kunnen verlichten. Echter, verhoogt het mogelijk weer het raakvlak voor nevenschade, omdat de onderliggende netwerkinfrastructuur mogelijk ingezet wordt om DNS-infrastructuur voor meerdere afnemers in te richten. Tevens verkleint het mogelijk de controle over waar servers geplaatst worden (b.v. strategisch in bepaalde Nederlandse ISPs). Het is aan te raden voor beleidsmakers om de voor- en nadelen van opties af te wegen om vervolgens de beste oplossing te kiezen.

[1] https://www.ripe.net/publications/docs/ripe-663

Benodigde inspanning: evenals voor de aanbeveling in §4.1.1 zullen overheidsinstanties benaderd moeten worden, wat tijd zal vergen.

Tevens zal uitgedacht moeten worden hoe geautoriseerde personen van overheidsinstanties (b.v. een gemeente) wijzigingen in DNS-configuratie kunnen doorvoeren. Het is belangrijk om dit consistent door te voeren in zowel primaire als secundaire infrastructuur, wat bij het ontvangen van wijzigingen duidelijk aangegeven zou kunnen worden. We raden aan dat hier goed wordt over nagedacht, o.a. door DNS-experts, systeemarchitecten, en mensen die (bestaande) communicatiekanalen en processen tussen overheden kennen.

Als de overheid haar eigen secundaire DNS server met IP anycast wilt opereren dan zal dit een aanzienlijke investering in ontwerpen, implementatie en operatie kosten. Dit zal een klein team aan mensen vergen en heeft als voordeel volledige controle, b.v. door infrastructuur in elke omvangrijke en willende ISP in Nederland te plaatsen. Het nadeel is echter de verantwoordelijkheid voor dienstverlening. Het aantal benodigde servers zal afhangen van het aantal strategische punten en netwerken waarin de infrastructuur gewenst is. Het voorbeeld van `digid.nl` (Tabel A.3) laat zien dat de benodigde kennis al aanwezig is binnen de Rijksoverheid (of dat ze diensten heeft afgenomen van een partij waar de kennis aanwezig is), wat het implementeren van deze aanbeveling ten goede zal komen.

4.2. Monitoren van het DNS

Analoog aan hoe Rijkswaterstaat de staat van dijken in Nederland in de gaten houdt, stellen wij dat het continu monitoren van het DNS van cruciaal belang is om betrouwbaarheid te waarborgen en beschikbaarheid te testen. Open netwerken kunnen op vrijwel elk moment het doel van een cyberaanval worden. Netwerken kunnen storingen ondervinden, servers kunnen falen en configuratieproblemen kunnen worden geïntroduceerd. Om deze reden is het belangrijk om DNS-infrastructuur continu te monitoren. Door geregeld de responsiviteit, configuratie en weerbaarheid van DNS-infrastructuur en domeinnamen te testen kunnen problemen vroegtijdig worden opgemerkt en actie worden ondernomen. De tests zouden geautomatiseerd kunnen worden en b.v. meerdere keren per dag kunnen lopen.

Er zijn verscheidene commerciële aanbieders van netwerk meetdiensten die afnemers de mogelijkhed bieden om hun eigen infrastructuur aan tests te onderwerpen, bijvoorbeeld voor beschikbaarheid en prestaties, vanuit globale gebruikersperspectieven. Deze diensten kunnen duur zijn en zijn niet per definitie NL of zelfs EU gebaseerd. Een bijkomend probleem is dat, gegeven hoe het DNS werkt, DNS-aanbieders niet per definitie alle informatie (kunnen) weten om specifieke problemen van domeinnamen te herkennen.[2] We vermoeden dat het monitoren de DNS-infrastructuur waar overheden van afhangen met een op maat gemaakte oplossing kan worden uitgevoerd, die voornamelijk op breed beschikbare open-source software en tools gebaseerd kan worden, maar wel integratie door een systeemontwikkelaar en vervolgens een operator en beheerder vereist. We stellen ons voor dat dit iets is dat centraal gebeurt (o.a. wegens schaalvoordelen) en mogelijk geïntegreerd kan worden met ontwikkel- en operatorteams die al op andere vitale (digitale) infrastructuur toezien.

Benodigde inspanning: we kunnen aannemen dat taken als monitoren en analyse en interpretatie van resultaten door een aantal analysten in deeltijd uitgevoerd kunnen worden. Dit is ongetwijfeld makkelijker dan toegewijde secundaire DNS-infrastructuur voor Nederlandse overheden ontwikkelen en beheren, maar vergt ook precisie en nauwkeurigheid.

Om zaken makkelijker te maken kan het monitoren centraal gedaan worden om vervolgens in het geval van mogelijke problemen contact op te nemen met de domeinnaam beheerders van

[2] Om een voorbeeld te noemen: als een domeinnaam twee DNS-aanbieders gebruikt dan weten de aanbieders dat niet per sé van elkaar terwijl die informatie wel nodig is om DNS-configuratie problemen te kunnen herkennen.

de betrokken overheidsinstantie. Er zijn verscheidene open-source tools die bij monitoren (lees: meten) en automatisering kunnen helpen en die ook kunnen worden ingesteld om notificaties te generenen.

5

Conclusies en vervolgonderzoek

De hoofdconclusie die met dit rapport gepaard gaat is dat acht van tien door experts vastgelegde best practices voor DNS-weerbaarheid worden nageleefd voor domeinnamen van Nederlandse overheden. Echter, op twee kritische punten wordt voor grote aantallen namen (circa 50%) niet goed gescoord, waardoor de digitale diensten waarvoor ze gebruikt worden een risico lopen en onnodig kwetsbaar zijn voor cyberaanvallen of andere netwerkstoringen bij DNS-aanbieders. Zo'n situatie hoeft zich niet per sé voor te doen, maar voorkomen is beter dan genezen, zeker als voorkomen in veel gevallen relatief eenvoudig kan zijn.

Onze onderzoeksresultaten suggeren dat er een grote mate van vrijheid is binnen bepaalde overheidsinstanties om DNS-aanbieders te kiezen, wat o.a. voor concentratie op commerciële lokale DNS-aanbieders heeft gezorgd (b.v. TransIP). Inachtnemende het belang van digitale dienstverlening stellen wij dat de overheid stappen zou kunnen nemen om gemeenten, provincies, e.d. te helpen bij het robuuster en betrouwbaarder maken van de DNS-infrastructuur waar ze gebruik van maken. Op deze manier zullen eventuele incidenten minder waarschijnlijk een negatief en merkbaar effect op burgers en digitale dienstverlening hebben.

Als mogelijk vervolgonderzoek stellen we voor om deze studie te herhalen en te testen of er significante wijzigingen zijn doorgevoerd waardoor de cyberweerbaarheid van overheids domeinnamen over tijd is verbeterd.

Auteurs

dr. Giovane C. M. Moura is datawetenschapper bij SIDN Labs, de onderzoeksarm van de .nl top-level domein beheerder Stichting Internet Domeinregistratie Nederland (SIDN). Zijn onderzoek richt zich op het brengen van academische precisie naar netwerk operaties om de prestaties, beveiliging en stabiliteit van netwerksystemen te verbeteren. Giovane is tevens gast onderzoeker in TU Delft's CyberSecurity groep. Giovane heeft zijn Ph.D. in 2013 behaald aan de Universiteit Twente.

Raffaele Sommese, MSc is Ph.D.-kandidaat aan Universiteit Twente. Zijn doctorale onderzoek richt zich op het analyseren en karakteriseren van DNS kwetsbaarheden en misconfiguratie om de weerbaarheid van DNS-infrastructuur tegen denial-of-service aanvallen te vehoren. Raffaele heeft zijn Master of Science in Computer Science in 2018 behaald aan Politecnico di Torino, Italië.

dr.ir. Mattijs Jonker is assistent professor en onderzoekswetenschapper aan de Universiteit Twente. Zijn onderzoek richt zich op netwerkbeveiliging in brede zin en maakt extensief gebruik van Internetmetingen en data analysemethoden. Hij is tevens data architect binnen het bekroonde OpenINTEL project, wat het domeinnaam systeem op grote schaal meet voor onderzoeksdoeleinden. Mattijs heeft zijn Ph.D. in 2019 cum laude behaald aan Universiteit Twente en heeft tevens een M.Sc. met een CyberSecurity specialisatie.

A

Bijlagen

A.1. Tabel van DNS-aanbieders

Tabel A.1 en Tabel A.2 tonen het aantal DNS-aanbieders voor respectievelijk web- en maildomeinen. Zij zijn de cijfers erachter Figuur 2.1.

A.2. Referentievoorbeelden

Vervolgens laten we twee domeinnamen uit de dataset zien die zich aan de andere kant van DNS-veerkracht bevinden: `digid.nl` and `slachtofferportaal.nl`. Tabel A.3 toont de DNS-configuraties voor de eerste, en Tabel A.4 voor de tweede.

Vervolgens berekenen we de *critical* beste metrieken die we hebben gedefinieerd in ons best-practices document [7]. We tonen de resultaten voor de kritische best practices beide domeinen in Tabel A.5, terwijl Tabel A.5 de aanbevolen best practices-scores toont. Rode cellen geven aan waar een domein niet voldoet aan de vereisten voor best practices.

Grote problemen kritische metrics: het grootste probleem met `slachtofferportaal.nl` is dat het een enkele AS (29311), een enkele IPv4 en een enkele IPv6 prefix heeft. Als er dus iets zou gebeuren met deze routeaankondigingen op dit specifieke AS, zou `slachtofferportaal.nl` *onbereikbaar* worden. Een oplossing zou zijn om een tweede AS toe te voegen, die een extra laag redundantie kan toevoegen. `digid.nl` wordt bijvoorbeeld aangekondigd door drie verschillende AS'en.

Grote problemen aanbevolen metrieken: we zien in Tabel A.6 dat `slachtofferportaal.nl` slechts één TLD in zijn NS-records heeft. Als er iets met het TLD zou gebeuren, zou dit domein onbereikbaar worden.

Aanbieders	**IPv4**	**IPv6**
0	0 (0.0%)	9 (0.6%)
1	627(47.9%)	780 (59.6%)
2	492(37.6%)	357 (27.3%)
3	134(10.2%)	135(10.3%)
4	51(3.9%)	26(2.0%)
5	4(0.3%)	1(0.1%)
Totaal	1308	1308

Tabel A.1: DNS-aanbieders distributie voor web domeinnamen

.

Aanbieders	IPv4	IPv6
0	0(0.0%)	3(0.56%)
1	243(45.34%)	302(56.34%)
2	194(36.19%)	142(26.49%)
3	76(14.18%)	76(14.18%)
4	20(3.73%)	11(2.05%)
5	1(0.19%)	0(0.0%)
Totaal	534	534

Tabel A.2: DNS-aanbieders distributie voor e-mail domeinnamen

NS	IPv4	Prefix	IPv6	Prefix	AS IPv4	AS IPv6
ns0.rijksoverheidnl.com	185.136.96.82	185.136.96.0/24	2a06:fb00:1:0:0:0:1:82	2a06:fb00:1::/48	203391	203391
ns1.rijksoverheidnl.nl.	178.22.85.27	178.22.84.0/22	2a00:d00:3:6:0:0:0:130	2a00:d00::/32	41887	41887
ns2.rijksoverheidnl.eu	94.228.142.136	94.228.142.0/23	2a00:d01:3:1:0:0:0:20	2a00:d01::/32	41887	41887
ns3.rijksoverheidnl.org	145.100.177.67	145.100.0.0/15	2001:610:188:203:3:1:0:67	2001:610::/29	1103	1103

Tabel A.3: `digid.nl` DNS-configuratie

NS	IPv4	Prefix	IPv6	Prefix	AS IPv4	AS IPv6
ns1.minvenj.nl	159.46.194.11	159.46.192.0/22	2a04:9a04:18ad:8a04:0:0:2:0	2a04:9a04::/32	29311	29311
ns2.minvenj.nl	159.46.194.12	159.46.192.0/22	2a04:9a04:18ad:8a04:0:0:3:0	2a04:9a04::/32	29311	29311

Tabel A.4: `slachtofferportaal.nl` DNS-configuratie

Metric	Description/Reference	Reference	digid.nl	slachtofferportaal.nl
nNSes	Number of NS records for a zone/[5]	>=2	4	2
nIP(NSv4)	Number of Unique IP addresses for NSes (IPv4) [5]	>=2	4	2
nIP(NSv6)	Number of Unique IP addresses for NSes (IPv6) [5]	>=2	4	2
ResponsiveNSesV4	All authoritative servers are responsive for the domain/[13]	True	True	True
ResponsiveNSesV6	All authoritative servers are responsive for the domain/[13]	True	True	True
nPrefixes(NSv4)	Number of unique BGP prefixes for NSes (IPv4/[2])	>=2	4	1
nPrefixes(NSv6)	Number of unique BGP prefixes for NSes (IPv6)/[2])	>=2	3	1
nAses(NSv4)	Number of unique ASes for NSes (IPv4) [1]	>=2	3	1
nASes(NSv6)	Number of unique ASes for NSes (IPv6) [1]	>=2	3	1
nGeoDiverseNSes	Number of NS distinct geographical locations [2]	>=2		

Tabel A.5: Critical metrics scores

Metric	Description/Ref.	Value	digid.nl	slachtofferportaal.nl
nTLDs	Use more than one TLD for NS records/[1]	2	3	1
NS TTL	TTL values of NS records/[6, 9, 10]	>=3600s	3600	3600
A(NS) TTL	TTL values for A (NS) records[6, 9, 10]	>=1800s	14400	3600
AAAA(NS) TTL	TTL values for AAAA (NS) records[6, 9, 10]	>=1800s	14400	3600
nAnycastIPv4	Number of Anycast Auth Servers IPv4/[8]	>=1		
nAnycastIPv6	Number of Anycast Auth Servers IPv6/[8]	>=1		

Tabel A.6: Recommended Best Practices Metrics

Referenties

[1] Mark Allman. "Comments on DNS Robustness". In: *Proceedings of the Internet Measurement Conference 2018*. IMC '18. Boston, MA, USA: Association for Computing Machinery, 2018, p. 84–90. ISBN: 9781450356190. URL: https://doi.org/10.1145/3278532.3278541.

[2] R. Elz e.a. *Selection and Operation of Secondary DNS Servers*. RFC 2182. IETF, jul 1997. URL: http://tools.ietf.org/rfc/rfc2182.txt.

[3] D. McPherson e.a. *Architectural Considerations of IP Anycast*. RFC 7094. IETF, jan 2014. URL: http://tools.ietf.org/rfc/rfc7094.txt.

[4] P.V. Mockapetris. *Domain names - concepts and facilities*. RFC 1034. IETF, nov 1987. URL: http://tools.ietf.org/rfc/rfc1034.txt.

[5] P.V. Mockapetris. *Domain names - implementation and specification*. RFC 1035. IETF, nov 1987. URL: http://tools.ietf.org/rfc/rfc1035.txt.

[6] G. Moura e.a. *Considerations for Large Authoritative DNS Server Operators*. RFC 9199. IETF, mrt 2022. URL: http://tools.ietf.org/rfc/rfc9199.txt.

[7] Giovane C. M. Moura, Raffaele Sommese en Mattijs Jonker. *Best Practices of Resilience of Authoritative DNS Servers*. Tech. rap. Arnhem, The Netherlands: Dino Project Deliverable, 2022.

[8] Giovane C. M. Moura e.a. "Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event". In: *Proceedings of the ACM Internet Measurement Conference*. Santa Monica, California, USA: ACM, nov 2016, p. 255–270. DOI: http://dx.doi.org/10.1145/2987443.2987446. URL: https://www.isi.edu/%7ejohnh/PAPERS/Moura16b.html.

[9] Giovane C. M. Moura e.a. "When the Dike Breaks: Dissecting DNS Defenses During DDoS". In: *Proceedings of the ACM Internet Measurement Conference*. Boston, MA, USA: ACM, okt 2018, p. 8–21. DOI: https://doi.org/10.1145/3278532.3278534. URL: https://www.isi.edu/%7ejohnh/PAPERS/Moura18b.html.

[10] Giovane C. M. Moura e.a. "Cache Me If You Can: Effects of DNS Time-to-Live". In: *Proceedings of the ACM Internet Measurement Conference*. Amsterdam, the Netherlands: ACM, okt 2019, p. 101–115. DOI: https://doi.org/10.1145/3355369.3355568. URL: https://www.isi.edu/%7ejohnh/PAPERS/Moura19b.html.

[11] C. Partridge, T. Mendez en W. Milliken. *Host Anycasting Service*. RFC 1546. IETF, nov 1993. URL: http://tools.ietf.org/rfc/rfc1546.txt.

[12] Nicole Perlroth. "Hackers Used New Weapons to Disrupt Major Websites Across U.S." In: *New York Times* (okt 2016), A1. URL: http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

[13] A. Romao. *Tools for DNS debugging*. RFC 1713. IETF, nov 1994. URL: http://tools.ietf.org/rfc/rfc1713.txt.

[14] Raffaele Sommese e.a. "When Parents and Children Disagree: Diving into DNS Delegation Inconsistency". In: *Passive and Active Measurement*. Cham: Springer International Publishing, 2020, p. 175–189.