Een privacyraamwerk voor 'DNS big data'-toepassingen

Cristian Hesselman, Jelte Jansen, Maarten Wullink, Karin Vink en Maarten Simon
SIDN*
Contactpersoon: Jelte.Jansen@sidn.nl

In dit artikel bespreken we ons privacyraamwerk voor toepassingen die de veiligheid en stabiliteit van het .nl-domein verder verhogen op basis van 'DNS big data', bijvoorbeeld om daarmee automatisch botnets te detecteren in DNS-verkeer. Ons raamwerk is uniek omdat het (1) privacybeheer toepast op DNS-data en (2) omdat het juridische, organisatorische en technische aspecten van privacybeheer daarvoor integraal combineert. We gaan het raamwerk 'by design' inbouwen in het ENTRADA-platform, het technische systeem voor DNS big data-toepassingen dat we ontwikkelen bij SIDN Labs.

I. Introductie

Als beheerder van de internetextensie van Nederland (.nl) zoeken we bij SIDN voortdurend naar nieuwe mogelijkheden om de veiligheid en stabiliteit van het .nl-domein verder te vergroten. Dat doen we bijvoorbeeld door DNSSEC grootschalig in te voeren voor .nl-domeinnamen [23], door onze bijdrage aan AbuseHUB [19] en door onderzoek en ontwikkeling op dit gebied via ons R&D-team, SIDN Labs [18].

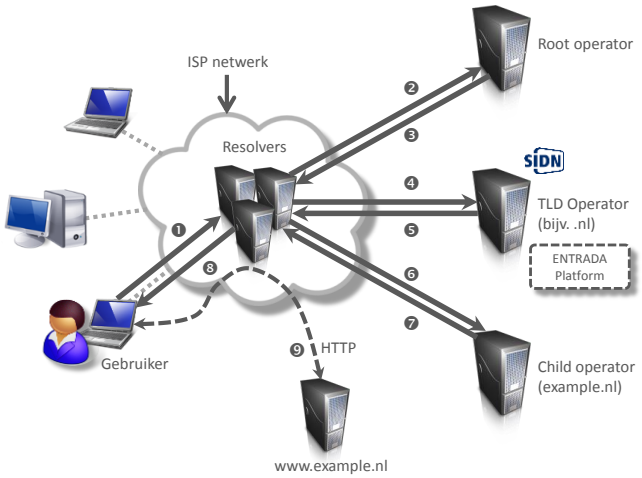
Een andere kans die we zien om de veiligheid en stabiliteit van .nl verder te vergroten is door de DNS-data die wij dagelijks verwerken op te slaan en daar door automatische analyses vroegtijdig bedreigingen en onregelmatigheden in te signaleren. Het DNS (Domain Name System) [20][21] is het systeem dat domeinnamen zoals www.example.nl omzet naar een IP-adres waarop de bijbehorende website draait. Deze vertaalslag is nodig omdat het internet informatie tussen computers verstuurt op basis van IP-adressen terwijl mensen meestal werken met domeinnamen.

**SIDN (www.sidn.nl) beheert de internetextensie van Nederland, .nl. Als nationale registry zorgen wij ervoor dat internetgebruikers altijd en overal op een veilige manier .nl-domeinnamen kunnen gebruiken en bereiken. Hiervoor runnen wij de .nl-zone van het Domain Name System (DNS). We handelen dagelijks meer dan een miljard DNS-berichten af voor de meer dan vijfenhalf miljoen geregistreerde .nl-domeinnamen. Daarvan zijn er ruim 1,8 miljoen beveiligd met 'secure DNS' (DNSSEC), waarmee .nl wereldwijd koploper is. SIDN Labs (www.sidnlabs.nl) is het research- en developmentteam van SIDN. Het team werkt onder andere aan nieuwe internettechnieken en –systemen voor het verder verhogen van de stabiliteit en veiligheid van het DNS.*

Voorbeelden van DNS-datatoepassingen die we voorzien, zijn de automatische detectie van botnets die gebruik maken van het DNS (bijv. Feederbot [1] of Cutwail [2]), een automatische koppeling met AbuseHUB om botnetinfecties samen met ISP's onschadelijk te maken, autoconfiguratie-toepassingen die zelfstandig nameservers opnieuw instellen bij een afwijking in het DNS-verkeer (bijv. als gevolg van een DNS-reflectieaanval [3][4][5] of een plotselinge verkeerspiek), het meten van de securityperformance van topleveldomeinen en van de distributie van .nl-nameservers (vgl. [6]), geavanceerde dashboards voor DNS-beheerders en open data toepassingen.

Dit soort toepassingen wordt mogelijk door nieuwe technologieën zoals Hadoop [7], die om kunnen gaan met 'big data', een paradigma dat draait om het analyseren en verrijken van zeer grote datastromen (orde petabytes) met complexe relaties die snel verwerkt moeten kunnen worden [8] (de drie V's van big data: Volume, Velocity en Variability). Traditionele dataverwerkingsmethoden zoals relationele databases zijn hiervoor ontoereikend, vooral als het gaat om verwerkingssnelheid en data-analyse [8].

Een uitdaging voor toepassingen van 'DNS big data' is dat een deel van het DNS-verkeer dat de .nl-nameservers verwerken uit persoonsgegevens bestaat, in het bijzonder IP-adressen en domeinnamen waarvoor gebruikers het overeenkomstige IP-adres zoeken. We hebben daarom een privacyraamwerk ontwikkeld waarmee we per toepassing een privacypolicy kunnen instellen. De doelen van het raamwerk zijn (1) ons in staat te stellen op een gestructureerde manier een afweging te kunnen maken tussen de bijdrage van een DNS big data-toepassing aan de stabiliteit en veiligheid van .nl aan de ene kant en de privacy van .nl-gebruikers aan de andere kant en (2) het technische systeem zo te kunnen configureren dat het de privacypolicy's afdwingt. Het raamwerk is uniek omdat het privacybeheer toepast op DNS-data en omdat het juridische, organisatorische en technische aspecten van privacybeheer daarvoor integraal combineert. We gaan het raamwerk 'by design' inbouwen in het ENTRADA-platform ('ENhanced Top-level domain Resilience through Advanced Data Analysis'), het technische systeem voor DNS big data-



Figuur 1. DNS-resolving.

toepassingen dat op dit moment in ontwikkeling is bij SIDN Labs.

Als beheerder van .nl vinden we een gedegen privacyraamwerk bijzonder belangrijk, omdat het cruciaal is voor het vertrouwen in het Nederlandse domein en in SIDN als beheerder daarvan. Daarnaast zien we het als onze verantwoordelijkheid om hier proactief en transparant actie te ondernemen, omdat we een publieke dienst leveren met een kritische functie voor de Nederlandse economie en samenleving.

In de rest van dit artikel geven we een overzicht van het ENTRADA-privacyraamwerk. We beginnen met een meer gedetailleerde uitleg over de werking van het DNS (Sectie II). Daarna bespreken we hoe en onder welke omstandigheden de IP-adressen en domeinnamen in het DNS-verkeer persoonsgegevens zijn (Sectie III). We vervolgen met het privacyraamwerk zelf (Sectie IV) en de realisatie daarvan (Sectie V). We sluiten af met een korte discussie van vergelijkbaar werk (Sectie VI) en conclusies en onderwerpen voor verder onderzoek (Sectie VII).

II. DNS-RESOLVING

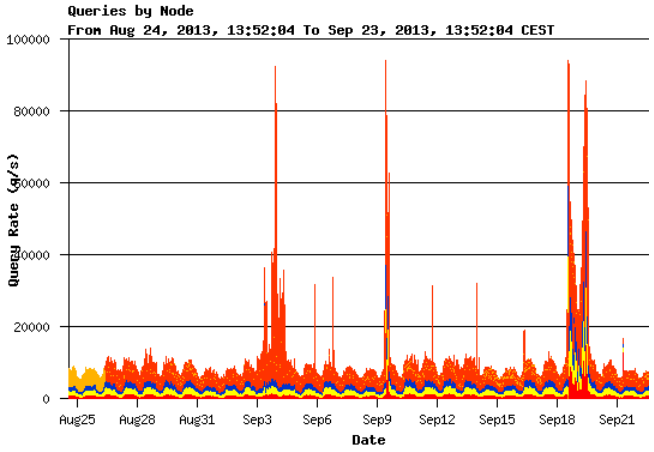
Als beheerder van .nl verwerkt SIDN berichten om het IP-adres op te zoeken van een domeinnaam, zoals 192.0.2.189 voor www.example.nl. Deze vertaalslag is nodig omdat het internet informatie tussen machines verstuurt op basis van IP-adressen terwijl mensen juist werken met domeinnamen. De vertaalslag van domeinnaam naar IP-adres heet 'resolving' en verloopt via het Domain Name System (DNS) [20][21], een wereldwijde infrastructuur van servers waarvan SIDN het .nl-deel beheert.

Figuur 1 laat zien hoe DNS-resolving typisch werkt. Een gebruiker vult allereerst een url in in zijn browser (of klikt erop), bijvoorbeeld http://www.example.nl/. Het deel tussen de slashes (www.example.nl) is de domeinnaam van het adres en verwijst naar de server waar de site op draait.

Om de domeinnaam te vertalen naar het IP-adres van de server stuurt de machine van de gebruiker een DNS-bericht naar een zogenaamde 'resolver' (stap 1 in Figuur 1), een machine die meestal van de ISP is waar de gebruiker zijn internetaansluiting bij afneemt. Deze resolver zoekt voor de browser de domeinnaam op in het mondiale DNS, te beginnen bij een vaste groep van zogenaamde 'rootservers' (stap 2). Deze rootservers verwijzen in het geval van www.example.nl de resolver door naar de nameservers van .nl (stap 3). De resolver neemt vervolgens contact op met een .nl-nameserver (stap 4), die de resolver op zijn beurt doorverwijst naar de nameservers van example.nl (stap 5). De resolver stuurt daarop een DNS-bericht naar de nameserver van example.nl (stap 6), die uiteindelijk het IP-adres van www.example.nl kent en dat terugstuurt naar de resolver (stap 7). Tot slot antwoordt de resolver met het IP-adres van www.example.nl naar de browser (stap 8), waarna de browser via HTTP de webpagina ophaalt van www.example.nl (stap 9).

Om de schaalbaarheid van het DNS te maximaliseren maken resolvers gebruik van caching. Dit betekent dat een resolver een antwoord een tijd lang in zijn cache opslaat en vragen van andere clients voor het IP-adres van dezelfde domeinnaam uit de cache beantwoordt zonder opnieuw contact op te nemen met de nameservers in het DNS (de resolver slaat dan stappen 2 t/m 7 over). De zogenaamde 'time-to-live' (TTL) van de domeinnaam bepaalt hoe lang een resolver een vraag voor een domeinnaam cacht. Per TTL zal elke resolver dezelfde vraag in principe maar eenmaal naar de .nl-nameservers sturen. Als .nl-registry adviseert SIDN een TTL van 2 uur. Resolvers zijn vrij om een kortere TTL te gebruiken, maar geen langere.

Gemiddeld verwerken de .nl-nameservers gezamenlijk (unicast en anycast) ongeveer 15.000 query's per seconde, wat neerkomt op 39 miljard query's (en responses) per maand. Als we deze data op zouden slaan (inclusief IP- en



Figuur 2. DNS-query's op een van SIDN's unicast-nameservers.

ethernetheaders), dan gaat het onder normale omstandigheden om ongeveer 60 gigabyte per dag per nameserver. Figuur 2 toont ter indicatie de hoeveelheid verkeer die een van SIDN's unicast-nameservers over een maand te verwerken krijgt (augustus 2013).

III. PERSOONSGEGEVENS

Het IP-adres van een resolver en de gezochte domeinnaam in een DNS-query zijn in specifieke gevallen persoonsgegevens. In deze sectie analyseren we waarom dit volgens de Wet Bescherming Persoonsgegevens zo is en bespreken hoe we voldoen aan de relevant eisen die de wet stelt (Sectie III.A). Ook schatten we op basis van operationele .nl-data in hoe vaak we persoonsgegevens verwerken voor IP-adressen (Sectie III.B) en voor de domeinnaam waarop een gebruiker zoekt (Sectie III.C).

A. WBP-analyse

De Wet Bescherming Persoonsgegevens (WBP) [15] definieert een persoonsgegeven als 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon' en de verwerking daarvan als 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, (…) of vernietigen van gegevens' (art. 1, sub a). Op basis van deze definitie zijn wij van mening dat het IP-adres van een resolver en de gezocht domeinnaam in een DNS-bericht (zie Sectie II) in specifieke gevallen mogelijk een persoonsgegeven is.

Andere gegevens in een DNS-query die de .nl-nameservers verwerken zijn in die gevallen naar onze mening ook persoonsgegevens, omdat ze daaraan te koppelen zijn. Voorbeelden zijn het tijdstip van een query, 'protocol-flags' in DNS-query's die informatie geven over de resolver, 'vluchtige' data zoals transactienummers voor de query zelf (query ID, source port) en netwerkgegevens van de resolver, zoals de afstand tot de .nl-server (netwerkhops).

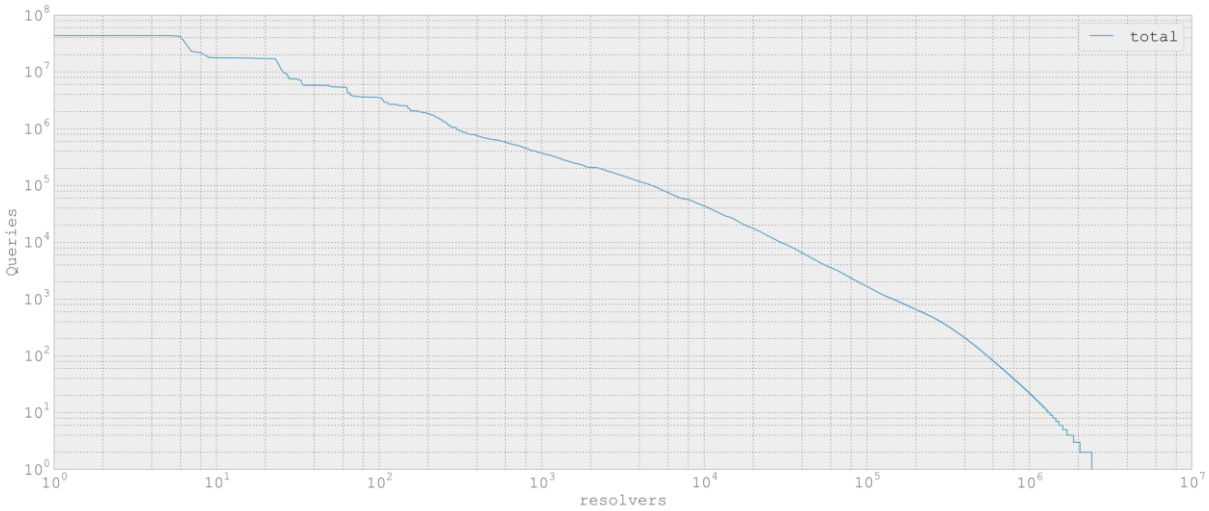
Als registry van .nl zijn wij van mening dat we deze gegevens voor het ENTRADA-platform mogen verwerken, omdat we voldoen aan de relevante eisen die de WBP stelt (doelbinding, legitieme grondslag, voorwaarden verwerking bijzondere persoonsgegevens en informatieverstrekking).

Doelbinding: persoonsgegevens mogen alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (art. 7) en verwerking mag niet plaatsvinden op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (art. 9). Voor het ENTRADA-platform en haar toepassingen is het doel van de gegevensverwerking het bestrijden van fraude en misbruik en het verder verbeteren van de stabiliteit van het .nl-domein en het Internet in de breedte. Wij gebruiken de gegevens niet voor andere doeleinden, zoals commerciële doeleinden.

Legitieme grondslag: vervolgens stelt de WBP dat we gegevens slechts mogen verwerken als hiervoor een legitieme grondslag is. In het kader van ENTRADA is deze grondslag art. 8 sub f, behartiging van een gerechtvaardigd belang. Met het bestrijden van fraude en misbruik en het verder verbeteren van de stabiliteit van het internet behartigen we daarmee allereerst een gerechtvaardigd belang van SIDN, namelijk (het bevorderen van) een zo veilig en betrouwbaar mogelijk .nl-domein en van geval tot geval het gerechtvaardigde belang van de partijen aan wie wij de data beschikbaar stellen. Dit laatste kan bijvoorbeeld gaan om het belang van de houder van een geïnfecteerde computer die wij via zijn provider informeren over de besmetting of het belang van een instelling die onder een DDOS-aanval ligt om informatie te ontvangen om deze af te slaan. Kenmerk van het verwerken van persoonsgegevens op grond van artikel 8 onder f van de WBP is dat verwerking niet mag plaatsvinden indien 'het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op de bescherming van de persoonlijke levenssfeer, prevaleert'. Hier moeten wij daarom per ENTRADA-toepassing een afweging maken.

Bijzondere persoonsgegevens: de WBP verbiedt in beginsel het verwerken van bijzondere persoonsgegevens, zoals iemands godsdienst of levensovertuiging (art. 16). Artikel 23 lid 2 heft dit verbod echter op als deze gegevens worden verwerkt in het kader van wetenschappelijk onderzoek of statistiek voor zover het onderzoek een algemeen belang dient, de verwerking voor het betreffende onderzoek of de betreffende statistiek noodzakelijk is, het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Het ENTRADA-platform verwerkt in zeer uitzonderlijke situaties mogelijk bijzondere persoonsgegevens (Sectie III.C), maar deze gegevens koppelen wij in geen geval aan een persoon. We berokkenen zo geen schade aan de persoonlijke levenssfeer en voldoen zo aan art. 23 lid 2.

Informatieverstrekking aan de betrokkene: gezien de manier waarop het DNS werkt (zie Sectie II), zien wij geen praktische mogelijkheid om eindgebruikers te informeren via de dienstverlening zelf. Omdat DNS-resolutie in de internetinfrastructuur ('onder water') plaats vindt bestaat er voor ons geen mogelijkheid om interactief om toestemming te vragen, zoals dat bijvoorbeeld wel kan bij het openen van een website. Op grond van artikel 34 lid 4 is onze interpretatie dat we kunnen volstaan met het vastleggen van de herkomst van de gegevens.



Figuur 3. Gemiddeld aantal query's per dag (juni 2014).

B. IP-adressen

De IP-adressen van resolvers in de DNS-query's die wij op onze nameservers verwerken zijn persoonsgegevens als ze zijn te herleiden tot een natuurlijk persoon. We onderscheiden hierbij twee gevallen: (1) een resolver bedient een klein aantal gebruikers (één of meer) en (2) een resolver bedient een groot aantal gebruikers. We achten het hierbij respectievelijk waarschijnlijk en onwaarschijnlijk dat het IP-adres van een resolver een persoonsgegeven is. We volgen hiermee de huidige WBP en laten de discussie of een IP-adres niet onder alle omstandigheden een persoonsgegeven is [9] buiten beschouwing tot dit in de wet is vastgelegd.

In het eerste geval is het IP-adres van de resolver voor de nameserver *waarschijnlijk* een persoonsgegeven in combinatie met de domeinnamen waarop een specifieke gebruiker zoekt. De nameserver ziet dan het IP-adres van de resolver en niet die van de eindgebruiker, maar door het kleine aantal gebruikers raadpleegt de resolver waarschijnlijk relatief vaker de nameservers (cache misses) waardoor die relatief meer gezochte domeinnamen van die resolver voorbij zien komen. Dit kan bijvoorbeeld het geval zijn bij een huishouden waar een lokale resolver draait.

Het IP-adres van een resolver is ook waarschijnlijk een persoonsgegeven als het IP-adres van de gebruiker en die van de resolver gelijk zijn. Deze situatie treedt bijvoorbeeld op bij botnets die een eigen resolver aan boord hebben om het botnet te besturen. De machine van een besmette eindgebruiker maakt dan gebruik van die resolver en niet langer van de normale resolver die bijvoorbeeld de ISP van de gebruiker heeft ingesteld. Voorbeelden van dit soort botnets zijn het Feederbot [1] en het Cutwail-botnet [2]. Dezelfde situatie treedt ook op bij besturingssystemen die (expertgebruikers) de mogelijkheid bieden om lokaal een resolver te draaien, zoals FreeBSD10 [11] en DNSSEC Trigger [12].

In het tweede geval (resolver die een groot aantal gebruikers bedient) is het *onwaarschijnlijk* dat het IP-adres een persoonsgegeven is. De nameservers zien ook dan alleen het IP-adres van de resolver en daarnaast ook slechts een beperkt aantal domeinnamen waarop gebruikers zoeken. Dit laatste komt doordat de resolver door het grote aantal gebruikers relatief veel vragen uit zijn cache kan beantwoorden (zonder de interacties 2 t/m 7 uit Figuur 1), in ieder geval voor de populairste domeinnamen. Hierdoor komen van individuele gebruikers typisch slechts een klein deel van de DNS-vragen op de nameservers uit. Een individuele gebruiker die grote aantallen unieke domeinnamen bezoekt die andere gebruikers achter dezelfde resolver niet gebruiken is mogelijk te zien op de nameservers, maar het is onwaarschijnlijk dat die gebruiker te identificeren is op basis van een IP-adres.

We hebben een eerste onderzoek uitgevoerd naar de verdeling van het aantal resolvers met een klein en een groot aantal gebruikers die de .nl-nameservers bevragen. Dit is relevant omdat het aantal resolvers met een klein aantal gebruikers medebepalend is voor het ontwerp van ons privacyraamwerk, bijvoorbeeld met betrekking tot de datafilters in het ENTRADA-platform (zie Sectie IV). We merken daarbij op dat we alleen een schatting kunnen geven van het aantal gebruikers achter een resolver, omdat nameservers alleen het extern observeerbare gedrag van een resolver zien (interacties 4 en 5 in Figuur 1).

Als indicator voor het aantal gebruikers achter een resolver hebben we het aantal query's gebruikt dat we van die resolver ontvangen. Onderzoek naar andere indicatoren is onderdeel van toekomstig werk (zie Sectie VII). Voorbeelden hiervan zijn de verdeling van domeinnamen waarop de eindgebruikers zoeken die achter de resolver

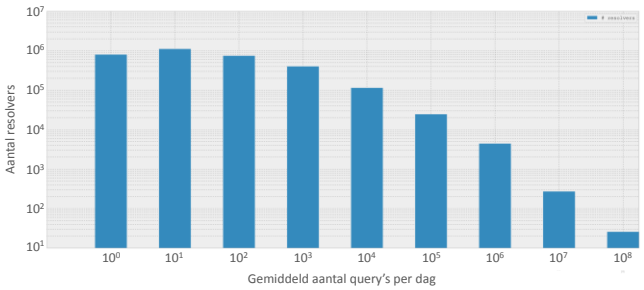
zitten, tijden tussen opeenvolgende query's, gebruikte portnummers en aantallen netwerkhops tussen de resolver en de autoritatieve nameserver. Voor een preciezere bepaling van het aantal gebruikers zouden we ook inzicht moeten hebben in het netwerk tussen de resolver en de eindgebruiker.

Figuur 3 toont het gemiddeld aantal query's per dag dat één van onze productienameservers heeft verwerkt in één maand (juni 2014). Op de x-as staan de resolvers (3.211.225 in totaal), op de y-as het gemiddeld aantal query's per resolver per dag. Beide assen hebben een logaritmische schaal. De dataset die we hebben gebruikt bevat ruim 3,74 miljard DNS-query's die we hebben verzameld en geanalyseerd met de R&D-versie (prototype) van het ENTRADA-platform.

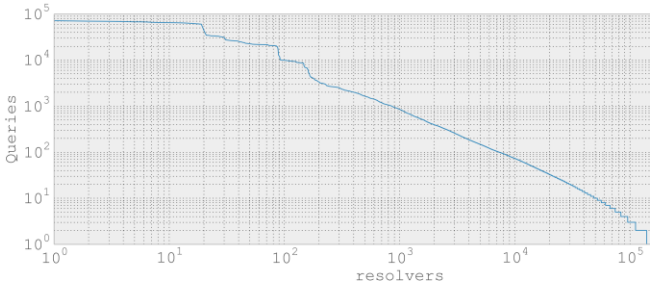
Figuur 3 laat duidelijk zien dat de verdeling van resolvers onevenredig is als het gaat om het aantal query's dat ze versturen. Er is een beperkt aantal resolvers (linker deel van Figuur 3) dat een groot aantal query's verstuurt en dus waarschijnlijk een groot aantal gebruikers bedient. De top 100 van resolvers verstuurt bijvoorbeeld 28% van het totaal aantal query's dat de nameservers ontvangen en de resolver op plek 100 verstuurt gemiddeld 117.000 query's per dag. Dit is ook te zien in Figuur 4, dat het aantal resolvers uitzet tegen het aantal query's wat we ontvangen. Iedere staaf in Figuur 4 geeft het aantal resolvers aan dat $10^{N-1}+1$ tot en met 10^{N} query's verstuurt (N=1…8). De meest linker staaf is het aantal resolvers dat 1 query verstuurt.

Met behulp van reverse DNS zien we dat resolvers die veel query's versturen vaak van grote ISP's of van grote bedrijven zijn. Voor deze situatie is het dus onwaarschijnlijk dat het IP-adres van de resolver een persoonsgegeven is. Tussen de topgebruikers vinden we ook resolvers van 'domainers' die proberen te achterhalen welke domeinnamen er in de .nl-zone zitten. Zij maken daarvoor vaak gebruik van een klein aantal automatische systemen, waardoor het IP-adres van de resolver mogelijk een persoonsgegeven is.

Veruit het grootste deel van het aantal query's in Figuur 3 bestaat echter uit resolvers die een beperkt aantal query's versturen en dus waarschijnlijk een klein aantal



Figuur 4. Aantal resolvers per aantal DNS-query's.



Figuur 5. Aantal DNS-query's waarbij de gezochte domeinnaam een IP-adres bevat.

gebruikers bedienen. Het aantal resolvers dat bijvoorbeeld 100 query's per dag of minder verstuurt is 83% van het totaal. Deze resolvers bedienen waarschijnlijk een beperkt aantal gebruikers of draaien zelfs op de machines van eindgebruikers. Het is daarom bij veruit het grootste deel van de resolvers waarschijnlijk dat het IP-adres een persoonsgegeven is.

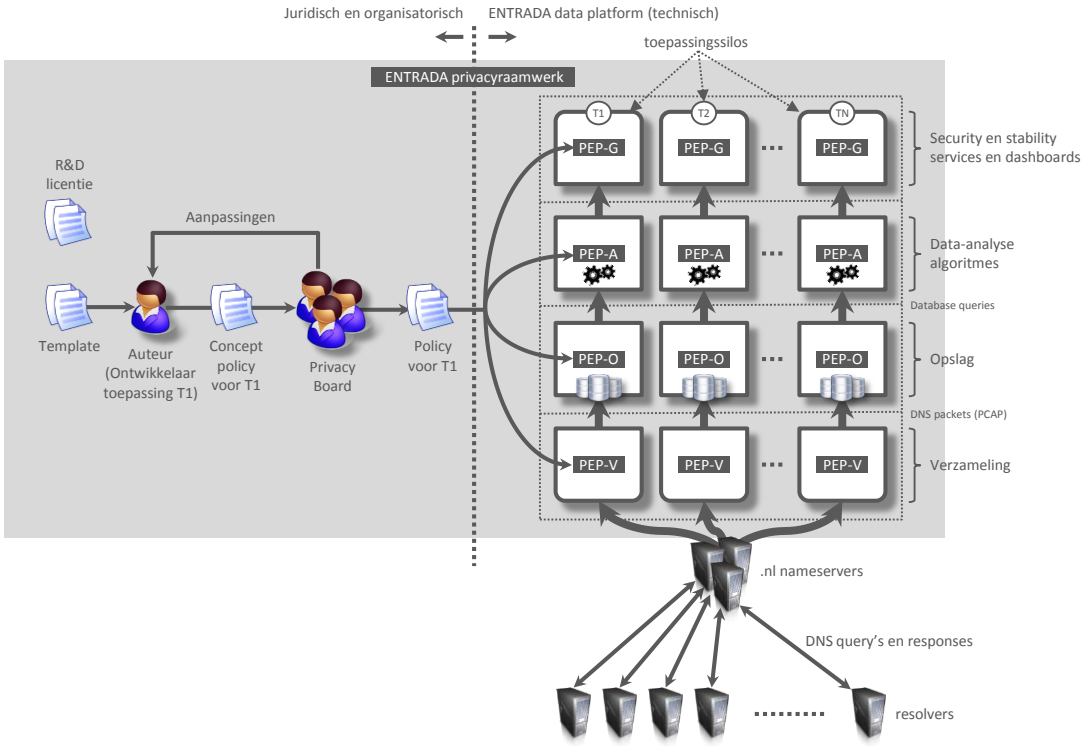
C. Gezochte domeinnamen

Ook de domeinnaam waar een eindgebruiker naar zoekt (zie Figuur 1) kan op zichzelf een persoonsgegeven zijn. Een voorbeeld is een domeinnaam met daarin de naam van een natuurlijk persoon, bijvoorbeeld www.voornaam-achternaam.nl. In dit geval gaat het om persoonsgegevens van de eigenaar van de domeinnaam en niet om persoonsgegevens aan de kant van de resolver. Een platform als ENTRADA zou daar door analyse van de opgeslagen DNS-querydata extra informatie aan kunnen koppelen die als persoonsgegevens van de domeinnaamhouder zou kunnen worden beschouwd. Bijvoorbeeld vanaf welke IP-adressen en op welke tijden en met welke frequentie een domeinnaam benaderd wordt. We vragen ons af hoeveel relevante informatie dit op zou leveren over een houder, maar het blijven naar onze mening persoonsgegevens.

Een gezochte domeinnaam is zonder andere informatie mogelijk ook een persoonsgegeven als het een IP-adres bevat. Dit is een manier die ISP's soms gebruiken om de verbindingen naar hun klanten te identificeren. Voorbeelden die we gevonden hebben zijn:

- <IP adres>.customer.<naam ISP>.nl
- <IP adres>-dsl.<naam ISP>.nl
- <IP adres>-mx.xdsl.<naam ISP>.nl
- <IP adres>-static-<naam ISP>.dsl.ip.<naam ISP>.nl

Waarbij de ISP soms een liggend streepje (-) tussen de nummers in het IP-adres gebruikt in plaats van een punt. Figuur 5 laat zien hoe vaak dit soort query's voorkwam in juni 2014 (y-as). Er waren ongeveer 100.000 resolvers die dit soort query's verstuurden (x-as) met een maximum van ongeveer 100.000 query's (y-as).



Figuur 6. ENTRADA-privacyraamwerk (productie)

Tot slot is een gezochte domeinnaam een persoonsgegeven als het IP-adres in de DNS-query van de resolver een persoonsgegeven is (zie Sectie III.B). Als de gezochte domeinnaam bijvoorbeeld die van een gaysite is, dan zegt dat in dergelijke gevallen iets over het individu achter de resolver. In dit geval is ook alle andere data waarover wij naar aanleiding van zo'n query beschikken een persoonsgegeven. Dit geldt bijvoorbeeld voor het tijdstip waarop een query heeft plaatsgevonden.

IV. ENTRADA-PRIVACYRAAMWERK

Figuur 6 geeft een overzicht van het ENTRADA-privacyraamwerk zoals we dat voorzien voor toekomstige productiediensten en –toepassingen. Het centrale concept is dat van een privacypolicy, die definieert welke data het ENTRADA-platform verwerkt voor een bepaalde toepassing, met welk doel en welke filters daarbij op de persoonsgegevens toegepast worden. Een filter is een operatie op de persoonsgegevens (bijv. pseudonimisering of aggregatie) om te voldoen aan de beginselen van proportionaliteit en subsidiariteit door het vermijden van een overmatige of onnodige verwerking van persoonsgegevens. De filters vormen een essentieel element in het privacyraamwerk, omdat de policy's hiermee op een toetsbare wijze door middel van technische maatregelen afgedwongen worden. In het ENTRADA-privacyraamwerk heeft iedere toepassing een privacypolicy.

Het ENTRADA-privacyraamwerk is gebaseerd op eisen zoals doelbinding en toetsbaarheid (Sectie IV.A) en kent twee organisatorische rollen: policy-auteurs (Sectie IV.A) en een privacyboard (Sectie IV.C). Policy-auteurs specificeren een privacypolicy voor een bepaalde ENTRADA-applicatie en zijn meestal de ontwikkelaars van die applicatie. De privacyboard toetst de policy's en geeft goedkeuring om de toepassing met de bijbehorende privacypolicy te realiseren. De technische componenten van het raamwerk bestaan uit policy enforcement points die goedgekeurde policy's afdwingen (Sectie IV.D) en zogenaamde 'toepassingssilos' die ervoor zorgen dat data altijd gebonden blijft aan het doel waarvoor we het verzamelen (Sectie IV.E). Het raamwerk combineert zo jurische aspecten (de privacypolicy's), organisatorische aspecten (de policyauteurs en de privacyboard) met technische aspecten van privacybeheer (de policy enforcement points en de toepassingssilos). Het privacyraamwerk passen we ook toe op de R&D-versie van het ENTRADA-platform (Sectie IV.F), dat we bijvoorbeeld gebruiken om de privacymechanismes voor de productieversie te ontwikkelen.

Een deel van de concepten die we gebruiken is geïnspireerd op het policyraamwerk van de IETF [22].

A. Eisen

Ons uitgangspunt voor het ENTRADA-privacyraamwerk is de analyse uit Sectie III. We stellen de volgende eisen aan het raamwerk:

- *Doelbinding*: het raamwerk moet het gebruik van persoonsgegevens (IP-adressen van resolvers of gezochte domeinnamen) koppelen aan een specifieke ENTRADA-toepassing met een specifiek doel en deze doelbinding actief afdwingen. ENTRADA-toepassingen hebben uitsluitend tot doel om de stabiliteit en veiligheid van het .nl-domein verder te verhogen. Voorbeelden van doelen zijn het detecteren van botnet-verkeer in DNS-data of het uitvoeren van onderzoek op dit gebied door onderzoeksinstellingen. Gebruik van deze data voor commerciële doeleinden staan we expliciet niet toe.
- *Toetsbaar*: het raamwerk moet bestaan uit technische, organisatorische en juridische concepten en structuren die SIDN in staat stellen systematisch te toetsen welke persoonsgegevens een bepaalde ENTRADA-toepassing nodig heeft voor welk doel en welke privacymaatregelen daar eventueel voor nodig zijn (bijv. anonimisering van IP-adressen). Policy-auteurs moeten met het raamwerk bijvoorbeeld kunnen beschrijven welke persoonsgegevens een ENTRADA-toepassing nodig heeft.
- *Eenvoudig*: het raamwerk en de documentatie die voorkomt uit de toepassing ervan moet zo eenvoudig mogelijk zijn, zodat het bruikbaar is voor policy-auteurs. Daarnaast is eenvoud belangrijk om het raamwerk technisch, juridisch en organisatorisch uitvoerbaar te maken zodat we het uiteindelijk in onze operationele processen en systemen kunnen integreren. Het vergaand automatiseren van het raamwerk via bijvoorbeeld webforms vinden we op dit moment niet nodig, omdat we verwachten dat we het privacyraamwerk slechts af en toe gaan gebruiken, gewoonlijk alleen bij het ontwikkelen van een nieuwe ENTRADA-toepassing of een aanpassing daarvan. Daarnaast zijn we van mening dat enig denkwerk op het gebied van privacy belangrijk is en dat een al te automatische opzet daar niet aan bijdraagt.
- *Uitbreidbaar*: het raamwerk moet generiek genoeg zijn om het te aan te kunnen passen, bijvoorbeeld als op Europees niveau de Data Protection Regulation [17] de Data Protection Directive [16] gaat vervangen waarop de WBP is gebaseerd. Het privacyraamwerk moet ook uitbreidbaar zijn naar andere soorten datastromen die we als .nl-beheerder verwerken zodat we ook daarin vroegtijdig bedreigingen en onregelmatigheden kunnen signaleren. Een voorbeeld is verkeer van het Extensible Provisioning Protocol (EPP) [13].

B. Policy-auteurs

Een policy-auteur is iemand die een privacypolicy schrijft voor een ENTRADA-toepassing. In termen van Figuur 6 betekent dit dat iedere toepassing T1, T2 tot en met TN een policy-auteur heeft die verantwoordelijk is voor het beheer van de policy.

Een privacypolicy heeft de vorm van een tekstdocument waarvan de structuur lijkt op die van het 'meldingsformulier verwerking persoonsgegevens' van het CBP [10]. De onderdelen van een privacypolicy zijn (zie Appendix B voor een voorbeeld):

- *Identifier*: identificeert de policy.
- *Doel*: omschrijving van de ENTRADA-toepassing die de persoonsgegevens nodig heeft, voor welk doel en wat de voordelen zijn voor de stabiliteit en veiligheid van de .nl-zone. Een voorbeeld is een monitoringtoepassing die als doel heeft automatisch botnets te detecteren in DNS-verkeer en zo het .nl-domein veiliger maakt.
- *Persoonsgegevens*: de typen persoonsgegevens waar deze policy op van toepassing is. Voor DNS-verkeer is dit 'IP-adres', 'gezochte domeinnaam' of beide (zie Sectie III).
- *Filters*: beschrijving van welke filters deze policy toepast onder welke omstandigheden en op welke typen persoonsgegevens. Voorbeelden van filters zijn pseudonimisering, verwijderen van de persoonsgegevens of geen filtering.
- *Retentie*: de duur waarvoor we de persoonsgegevens opslaan die de toepassing nodig heeft. Het ENTRADA-platform verwijdert de persoonsgegevens daarna of bewaart ze in geanonimiseerde vorm.
- *Toegang*: beschrijving van welke personen of systemen toegang krijgen tot de data en onder welke voorwaarden. Bij een systeem hoort ook een beschrijving van hoe de beveiliging daarvan gewaarborgd is en hoe het de data verkrijgt.
- *Type*: soort policy, dat aangeeft of dit een policy is voor R&D-doeleinden of voor een dienst die bij SIDN in productie is. Privacypolicy's voor R&D (zie Sectie IV.F) zullen typisch geen of weinig filters kennen, bijvoorbeeld om de privacymechanismes zelf te kunnen ontwikkelen en evalueren. Bij productieservices weten we precies welke persoonsgegevens nodig zijn en kunnen we privacypolicy's strikt toepassen.

- *Andere beveiligingsmaatregelen*: beschrijving van eventuele additionele beveiligingsmaatregelen die niet in eerder genoemde onderdelen passen.

Policy-auteurs maken gebruik van het ENTRADA policytemplate om een nieuwe policy te schrijven. Het template is een tekstdocument dat de structuur van een policy voorschrijft en bij ieder element een toelichting geeft. Het template zorgt ervoor dat ENTRADA-policy's dezelfde structuur hebben en inhoudelijk maximaal gelijkvormig zijn. Dit vergemakkelijkt het schrijven van een policy, de evaluatie daarvan door de privacyboard (zie Sectie IV.C) en de publicatie van de policy.

Het ENTRADA-policy template definieert per type persoonsgegeven (IP-adres of gezochte domeinnaam) ook de verzameling filters die policy auteurs kunnen gebruiken. Het template legt per filter uit wat de voor- en nadelen van een filter zijn, zodat policy-auteurs een onderbouwde keuze kunnen maken voor een bepaald filter (zie Appendix A).

Het ENTRADA-policytemplate onderscheidt vier soorten filters, één voor elk van de stadia van verwerking van persoonsgegevens in het ENTRADA-platform (zie Figuur 6): verzameling (van DNS-verkeer op de .nl-nameservers), opslag (in een database), analyse (door algoritmes en combinatie met andere bronnen) en gebruik (door ENTRADA-services en toepassingen). Voorbeelden van filters voor IP-adressen zijn: het negeren van IP-adressen als querydata wordt verzameld (verzamelingsfilter), IP-adressen gedeeltelijk op 0 zetten voordat de verzamelde data opgeslagen wordt (opslagfilter), aggregatie van data waarbij brondata ouder dan bijvoorbeeld een dag verwijderd wordt (analysefilter) en IP-adressen niet tonen als data opgevraagd wordt (gebruiksfilter).

Privacypolicy's passen we ook toe voor toepassingen waarbij we data delen met derden, zoals met AbuseHUB [19] om botnets op te ruimen.

C. Privacyboard

De privacyboard is een orgaan binnen SIDN dat verantwoordelijk is voor het evalueren van de privacypolicy van een ENTRADA-toepassing en dat beoordeelt of het doel van de toepassing de middelen rechtvaardigt (validatie). De board maakt daarbij een afweging tussen de bijdrage van de ENTRADA-toepassing aan de stabiliteit en veiligheid van .nl aan de ene kant ('het belang of de fundamentele rechten en vrijheden van de betrokkene' [15]) en de privacy van .nl-gebruikers aan de andere kant. In Figuur 6 keurt de privacyboard de privacypolicy voor toepassing T1 goed, waarna het ENTRADA-platform de privacypolicy technisch afdwingt.

De board bestaat uit een juridisch expert, een technisch expert en een voorzitter. De privacyboard publiceert goedgekeurde privacypolicy's en de onderbouwing daarvan op de website van SIDN. Dit zorgt voor maximale transparantie en stimuleert de board om welafgewogen beslissingen te nemen.

De privacyboard toetst privacypolicy's voordat we een nieuwe dienst in productie nemen. De board is daarnaast verantwoordelijk voor het beoordelen van updates van privacypolicy's en het actualiseren van het ENTRADA-policytemplate, bijvoorbeeld de lijst van privacyfilters in de template.

D. Policy Enforcement Points

Een Policy Enforcement Point (PEP) is een softwarecomponent in het ENTRADA-platform die de filters van een privacypolicy realiseert voor een specifieke toepassing.

We onderscheiden vier soorten PEP's, één voor elk van de lagen in het ENTRADA-platform (zie Figuur 6):

- PEP-V: realiseert privacypolicy's voor het *verzamelen* van DNS-data, bijvoorbeeld om IP-adressen te verwijderen nog voordat het platform de DNS-data opslaat. De PEP-V werkt direct op de vragen en antwoorden die de .nl-nameservers afhandelen.
- PEP-O: realiseert privacypolicy's voor de *opslag* van DNS-data, bijvoorbeeld om opgeslagen gegevens na een bepaalde periode te aggregeren. De PEP-O werkt op de databases waarin we de DNS-data opslaan, zoals Hadoop [7].
- PEP-A: realiseert privacypolicy's voor de *analyse* van DNS-data, bijvoorbeeld om er voor te zorgen dat analysealgoritmes alleen informatie produceren die niet tot individuen te herleiden is.
- PEP-G: realiseert privacypolicy's voor het *gebruik* van DNS-data door services en applicaties, bijvoorbeeld om data te delen met initiatieven zoals AbuseHUB [19].

E. Toepassingssilo's

Naast de vier lagen in het ENTRADA-platform (zie Sectie IV.D) onderscheiden we ook zogenaamde toepassingssilo's. Een toepassingssilo zorgt ervoor dat de persoonsgegevens in het ENTRADA-platform altijd gebonden blijven aan het specifieke doel waarvoor we ze verzamelen (de toepassing) en dat ze niet terechtkomen in andere silo's (toepassingen) die een ander doel hebben.

In het ENTRADA-platform bestaat een toepassingssilo uit de toepassing, alle opgeslagen persoonsgegevens die de toepassing nodig heeft en de bijbehorende privacypolicies. Dit kan bijvoorbeeld door het ENTRADA-platform zo te configureren dat silo's ieder in een eigen (virtuele) machine draaien. Dat minimaliseert de noodzaak voor speciale technische maatregelen in het platform, waardoor het

platform zo eenvoudig mogelijk blijft en we de scheiding van silo's vooral organisatorisch regelen.

F. Research en development

Het ENTRADA-platform en de concepten van het privacyraamwerk hebben een hoog innovatief gehalte. Gedegen research en development (R&D) is daarbij onontbeerlijk, bijvoorbeeld om algoritmes te ontwikkelen die botnets detecteren in DNS-verkeer of om nieuwe privacyfilters te ontwikkelen.

Om deze reden maken we een expliciet onderscheid tussen productie en R&D, waarbij we voor productie strikt de aanpak van Figuur 6 volgen. Voor R&D maken we echter gebruik van een flexibeler regime, omdat het doel daar is om te onderzoeken hoe we een ENTRADA-toepassing kunnen realiseren (bijv. met welke mechanismes, algoritmes en privacypolicy's), evalueren en daarna eventueel in productie kunnen nemen. Het doel is niet om de toepassing beschikbaar te maken aan .nl-gebruikers, behoudens pilots van ENTRADA-toepassingen waar .nl-gebruikers vrijwillig aan meewerken.

Ons R&D-regime is flexibeler dan voor productie, omdat we:

- Toepassingssilo's gebruiken met 'poreuze wanden'. Dit betekent dat we persoonsgegevens delen tussen verschillende toepassingen in onze lab-omgeving, maar uitsluitend voor R&D-doeleinden. Dit geldt ook voor het delen van data voor onderzoek met onze (academische) R&D-partners, waarbij we waar nodig de data eerst pseudonimiseren of anonimiseren. Voor deze situaties sluiten we met deze partijen een bewerkersovereenkomst.
- DNS-data en de persoonsgegevens daarin voor alle ENTRADA-toepassingen even lang opslaan in plaats van de toepassingsspecifieke opslagperiode die we in productie gebruiken (zie Sectie IV.B). In artikel 10 lid 2 van de WBP wordt bepaald dat gegevens langer bewaard mogen worden mits deze voor historische, statistische of wetenschappelijke doeleinden worden bewaard. Hierbij wordt geen specifieke limiet genoemd. Wij hebben er voor gekozen een opslagtermijn te hanteren van 18 maanden, zodat we voldoende tijd hebben om een heel jaar te analyseren en daarover te rapporteren. Data die ouder is dan 18 maanden anonimiseren we of gooien we weg. De periode van 18 maanden is een 'sliding window', waarbij de privacy board incidenteel toestemming kan geven het window te vergroten voor specifieke R&D-doeleinden.

Bij de overgang van een ENTRADA-toepassing van R&D naar productie start de toepassing in productie in een lege silo (d.w.z. zonder DNS-data). Op deze manier zorgen we ervoor dat eventuele persoonsgegevens die we hebben gebruikt voor het ontwikkelen van de toepassing niet voor andere doeleinden wordt gebruikt (het leveren van een op ENTRADA gebaseerde productiedienst in plaats van onderzoek en ontwikkeling).

V. Realisatie

We zijn het ENTRADA-privacyraamwerk op dit moment aan het inrichten. We beginnen met het aanmelden van de geplande handelingen bij het College Bescherming Persoonsgegevens, zoals beschreven in hoofdstuk 4 van de WBP. Daarnaast werken we intern aan de oprichting van de privacyboard, waarbij we de verantwoordelijkheden van de board incrementeel uitbreiden en de board de eerste tijd gaan 'testen' met het prototype van het ENTRADA-platform.

Op technisch vlak hebben we het ENTRADA ontworpen op basis van een 'plug-in' architectuur. Dit betekent dat we de filters die nodig zijn om privacypolicy's af te dwingen eenvoudig aan het platform toe kunnen voegen en zo privacy 'by design' inbouwen (bijv. een plug-in om IP-adressen te anonimiseren). Het ENTRADA-platform hebben we gerealiseerd in de vorm van een Hadoop-cluster.

Het prototype van het platform werkt op dit moment alleen in een afgeschermde lab-omgeving. Vanwege het experimentele karakter verwachten we dat het nog enige tijd gaat duren voordat we een ENTRADA-achtig systeem voor onze operationele dienstverlening in kunnen gaan zetten, maar het privacyraamwerk hebben we tegen die tijd alvast ontwikkeld en ingeregeld.

VI. Gerelateerd werk

Krishnan en Monrose [14] bespreken de privacy-implicaties van DNS-prefetching. Hierbij resolvet een browser (bijvoorbeeld Google Chrome) al tijdens het invoeren van een zoekterm in de adresbalk of tijdens het laden van een pagina de domeinnamen die op de pagina voorkomen. Het voordeel is dat webpagina's zo sneller laden, wat de 'browserbeleving' van eindgebruikers verbetert. Het onderzoek van Krishnan en Monrose laat zien dat DNS-prefetching een voorbeeld is van de privacyrisico's rondom het gebruik van domeinnamen. De browser zal door het opvragen van alle domeinnamen in een pagina, in een korte periode veel extra context informatie toevoegen aan de cache van de resolver, waardoor de resolver zich potentieel een beeld kan vormen van de zoekopdracht van de gebruiker. Deze methode is minder praktisch wanneer slechts een deel van de query's uitkomt bij de .nl-nameservers (door caching bij resolvers) of wanneer er domeinnamen worden gebruikt waarvan de woorden in de naam geen relatie hebben tot het zoekonderwerp. Het

onderzoek Krishnan en Monrose verschilt van dat van ons omdat het enkel de technische mogelijkheden voor privacybescherming bespreekt en de juridische en organisatorische aspecten buiten beschouwing laat.

Project Turris [24] is een dienst van het Tsjechische CZNIC, de beheerder van het .cz-domein. Turris analyseert (DNS-) dataverkeer om aanvallen op het internet te detecteren en bestrijden en maakt daarvoor gebruik van een speciale router die gebruikers in hun thuisnetwerk plaatsen. Omdat het hier om het dataverkeer van eindgebruikers gaat, heeft CZNIC hiervoor een privacypolicy ontwikkeld [25]. In ons raamwerk zou dit een specifieke policy van beveiliging en aggregatie zijn. Een verschil met ons ENTRADA-privacyraamwerk is dat gebruikers bij het Turris-project expliciet toestemming geven, omdat ze een leasecontract afsluiten met CZNIC. Een ander verschil is dat het om veel gedetailleerdere data gaat dan bij ENTRADA, omdat Turris gegevens verzamelt van al het internetverkeer, dat direct gekoppeld kan worden aan individuele gebruikers. Overeenkomsten zijn de manier waarop data beveiligd opgeslagen wordt en hoe ze aggregatie en beveiligingsmaatregelen toepassen voordat data met gebruikers gedeeld wordt.

Leenes geeft in een expertopinion-stuk [28] een overzicht van de toelaatbaarheid van de verwerking van gegevens van botnets door SURFnet, de organisatie die de netwerken van hogescholen, universiteiten en andere wetenschappelijke instellingen in Nederland met elkaar verbindt. Leenes beschrijft om welke data het gaat, wat de privacyrechtelijke afwegingen zijn, en welke acties er ondernomen kunnen worden. De dataset die besproken wordt bestaat niet uit DNS-data, maar uit botnetdata. Dit is een specifiekere dataset, maar wel een die veel meer persoonsgegevens bevat. De focus van het stuk ligt op de juridische aspecten.

VII. Conclusies en toekomstig werk

Toepassingen die DNS-data opslaan en automatisch analyseren hebben de potentie om de veiligheid en stabiliteit van het nationale .nl-domein verder te verhogen. Hiervoor hebben we een privacyraamwerk ontwikkeld, omdat een deel van de DNS-data bestaat uit persoonsgegevens (IP-adressen van resolvers en gezochte domeinnamen). Ons raamwerk is uniek omdat het (1) privacy afdwingt voor 'DNS big data' toepassingen en (2) omdat het juridische, organisatorische en technische aspecten van privacybeheer daarvoor integraal combineert. We vinden een gedegen en transparante aanpak op dit gebied bijzonder belangrijk omdat .nl een publieke infrastructuur vormt met een kritische functie voor de Nederlandse economie en samenleving.

Op technisch vlak bestaat ons toekomstige werk bijvoorbeeld uit het ontwikkelen en evalueren van mechanismes om preciezer onderscheid te kunnen maken tussen resolvers met een klein en met een groot aantal gebruikers, bijvoorbeeld door meerdere indicatoren (zie Sectie III.B) te combineren of door het inzetten van machine learning technieken.

Vanuit een juridisch perspectief gaan we onderzoeken hoe we onze (verrijkte) DNS-data kunnen delen op basis van een licentie die gebruikt maakt van (delen van) onze privacypolicytemplate. Daarnaast gaan we bestuderen wat de impact is van de overgang van de Europese Data Protection Directive naar de Data Protection Regulation. De huidige WBP is de Nederlandse implementatie van de Directive en de Data Protection Regulation wordt op een aantal punten strenger. Het is niet langer een richtlijn, maar een verordening met directe werking. Over de voorstellen wordt nog gediscussieerd en het is nog niet duidelijk welke maatregelen er anders zullen zijn in de nieuwe regelgeving.

Tot slot willen we het privacyraamwerk ook toepassen op andere soorten verkeer die wij als nationale registry verwerken, zoals EPP-verkeer.

Dankwoord

We bedanken Arnold Roosendaal (TNO), Simon Hania (TomTom en lid RvT SIDN) en de onderzoekers van het Privacy & Identity Lab voor hun feedback op de conceptversie van dit artikel waarmee we het verder hebben kunnen verbeteren.

Referenties

[1] C. Dietrich, C. Rossow, F. Freiling, H. Bos, M. van Steen, and N. Pohlmann, "On Botnets that use DNS for Command and Control", 7th European Conference on Computer Network Defense (EC2ND '11), Gothenburg, Sweden, September 2011, http://www.syssec-project.eu/m/page-media/3/dietrich-ec2nd11.pdf

[2] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vign, "The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns", 4th USENIX conference on Large-scale exploits and emergent threats (LEET'11), Boston, USA, March 2011, https://iseclab.org/papers/cutwail-LEET11.pdf

[3] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi, "EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis", ISOC Network and Distributed System Security Symposium (NDSS 2011), San Diego, California, Feb 2011, http://www.syssec-project.eu/media/page-media/3/bilge-ndss11.pdf

[4] M. Antonakakis, R. Perdisci, W. Lee, N. Vasiloglou, and D. Dagon, “Detecting Malware Domains at the Upper DNS Hierarchy”, 20th USENIX Security Symposium, San Francisco, California, Aug 2011, https://www.usenix.org/legacy/event/sec11/tech/full_papers/Antonakakis.pdf
[5] M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee, and D. Dago, “From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware”, 21st USENIX Security Symposium, Bellevue, WA, Aug 2012, https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final127.pdf
[6] F. Alizadeh and R. Oprea, “Discovery and Mapping of the Dutch National Critical IP Infrastructure”, M.Sc. thesis, University of Amsterdam, August 2013
[7] Hadoop Homepage, http://hadoop.apache.org/
[8] S. Madden, “From Databases to Big Data”, IEEE Internet Computing, Volume 16, Issue 3, May-June 2012
[9] G.-J. Zwenne, “De verwaterde privacywet”, oratie, Universiteit Leiden, april 2013, http://zwenneblog.weblog.leidenuniv.nl/files/2013/09/G-J.-Zwenne-De-verwaterde-privacywet-oratie-Leiden-12-apri-2013-NED.pdf
[10] Meldingsformulier verwerking persoonsgegevens, College Bescherming Persoonsgegevens, http://www.cbpweb.nl/Pages/ind_melden_formulier.aspx
[11] D.-E. Smørgrav, “Local caching resolver in FreeBSD 10”, September 2013, http://blog.des.no/2013/09/local-caching-resolver-in-freebsd-10/
[12] DNSSEC Trigger Project, NLnet Labs, http://nlnetlabs.nl/projects/dnssec-trigger/
[13] S. Hollenbeck, “Extensible Provisioning Protocol (EPP)”, RFC 5730, August 2009
[14] S. Krishnan and F. Monrose, “DNS prefetching and its privacy implications: when good things go bad,” in USENIX Conference on Large-Scale Exploits and Emergent Threats (LEET), 2010, https://www.usenix.org/legacy/event/leet10/tech/full_papers/Krishnan.pdf
[15] Wet bescherming persoonsgegevens (WBP), http://www.cbpweb.nl/pages/ind_wetten_wbp.aspx
[16] Data Protection Directive, oktober 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[17] Data Protection Regulation, januari 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[18] SIDN Labs homepage, www.sidnlabs.nl
[19] AbuseHUB homepage, www.abuseinformationexchange.nl
[20] P. Mockapetris, “Domain Names – Concepts and Facilities”, RFC 1034, November 1987
[21] P. Mockapetris, “Domain Names -- Implementation and Specification”, RFC 1035, November 1987
[22] B. Moore, et al., “Policy Core Information Model—Version 1 Specification”, IETF RFC3060, February 2001
[23] C. Hesselman, “.nl DNSSEC Deployment”, DNSSEC Workshop at ICANN45, Toronto, Canada, October 2012, http://ccnso.icann.org/pt/node/34637
[24] Homepage Project Turris, https://www.turris.cz/en/
[25] Turris privacy policy, https://www.turris.cz/en/privacy
[26] M. Davids, “A Resolver Reputation System Based on Interpreting DNS Traffic Characteristics”, 6th CENTR R&D Workshop, Paris, France, June 2014, https://centr.org/RD6-Davids-Resolver_Reputation_System
[27] P. Ohm, “Broken Promises of Privacy”, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006
[28] R. Leenes, “Acties tegen botnets door SURFnet en bij SURFnet aangesloten instellingen: privacy & data protectie aspecten”, oktober 2013, http://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/expert_opinion_botnets_leenes_oktober_2013.pdf

APPENDIX A: MOGELIJKE FILTERS

Een filter is een operatie op de persoonsgegevens in DNS-data (IP-adres of gezochte domeinnaam) die erop gericht een overmatige verwerking op toetsbare wijze tegen te gaan. Een van de onderdelen van een ENTRADA privacypolicy is een beschrijving van welke filters bij een specifieke ENTRADA-toepassing horen (zie ook Sectie IV.B). In deze appendix bespreken we een aantal voorbeelden van dergelijke filters.

A. Whitelist

Op de whitelist staan alle resolvers waarvan bekend is dat deze niet van een thuisgebruiker zijn. Dit zijn resolvers van bijvoorbeeld ISP’s, Google en OpenDNS. DNS-verzoeken die niet van deze resolvers afkomstig zijn, worden niet of geanonimiseerd opgeslagen in het ENTRADA platform. Dit kan op een statische manier met een lijst die alleen wijzigt als er nieuwe resolver wordt gevonden. Of op een dynamische manier waarbij alle resolvers potentieel op de lijst terecht kunnen komen, maar dit alleen wordt gedaan als de resolvers een bepaalde hoeveelheid query’s versturen.

Voordelen van whitelisting: zekerheid dat de opgeslagen data niet kan worden gebruikt om een profiel

van een specifiek persoon samen te stellen. Nadelen: (1) detecteren van botnets met een ingebouwde resolver wordt moeilijker of onmogelijk, (2) detecteren van botnets of andere activiteiten die gebruik maken van een open resolver wordt moeilijk of onmogelijk en (3) missen van data is goed mogelijk als de lijst niet actueel genoeg is.

B. Blacklist

Op de blacklist staan alle resolvers waarvan door de eigenaren is aangegeven dat de query's van deze resolvers niet mogen worden opgeslagen.

Voordelen van blacklisting: een gebruiker kan zelf aangeven of query's van een resolver worden opgeslagen. Nadelen: (1) de nadelen van whitelisting gelden ook voor blacklisting, (2) het opt-out principe verwacht actie van de gebruiker en dat is lastig omdat DNS een infrastructuurdienst is waar de meeste eindgebruikers niet bekend mee zijn en (3) als ISP's hun resolvers gaan blacklisten, dan mist het ENTRADA platform een grote hoeveelheid data, wat het nut ervan (verhogen veiligheid en stabiliteit) mogelijk teniet doet.

C. Geen anonimisering

De querydata wordt niet geanonimiseerd voordat deze wordt opgeslagen.

Voordelen van niet anonimiseren: er is geen beperking m.b.t. tot de onderzoeksmogelijkheden van de data, wat maximale mogelijkheden biedt voor een veilige en stabiele dienstverlening. Nadelen: (1) de data kan mogelijk worden gebruik om een profiel te ontwikkelen van een persoon, als deze persoon gebruik maakt van een privé resolver, (2) de data moet beveiligd worden zodat alleen bevoegd intern personeel ermee mag werken en (3) delen van de data met derden vereist een extra anonimiseringslag of een geheimhoudingsovereenkomst.

D. Anonimisering bij delen

Het filter anonimiseert de data op het moment dat deze met derden wordt gedeeld.

Voordelen van anonimiseren bij delen: het analyseren van de niet geanonimiseerde data biedt meer mogelijkheden en dat blijft intern mogelijk. Nadelen: (1) data goed anonimiseren is niet triviaal en (2) het is voorstelbaar dat de data zijn onderzoekswaarde verliest op het moment dat deze geanonimiseerd is.

E. Aggregatie van adres

Door het toevoegen van ruis moet het onmogelijk worden om query's van een specifiek IP-adres te herkennen. De data wordt geaggregeerd naar een hoger niveau, zodat individuele query's niet meer te achterhalen zijn. De laatste x bits van een bron IP-adres kunnen op nul worden gezet. 192.0.2.189 wordt dan bijvoorbeeld 192.0.2.0 als de laatste 8 bits op nul worden gezet.

Voordelen van adresaggregatie: eenvoudig en snel te implementeren. Nadelen: (1) opvolging van gedetecteerde abuse wordt onmogelijk omdat niet meer is te achterhalen vanaf welk specifiek adres de abuse afkomstig is en (2) onderzoek [27] toont aan dat met behulp van de overige attributen en externe datasets het mogelijk kan zijn om toch data te herleiden naar een specifieke persoon.

F. Aggregatie van adres op autonoom netwerkniveau

Dit lijkt op het aggregeren van IP-adressen, maar nu worden de adresdelen niet simpelweg op 0 gezet, maar geaggregeerd naar het netwerk waar het vandaan komt. In veel gevallen kan dit op hetzelfde neerkomen, als bijvoorbeeld de laatste 8 bits worden gewist en het gaat om een /24 netwerk, maar dit hoeft lang niet altijd het geval te zijn.

Voordelen van deze vorm van adresaggregatie: (1) is net wat specifieker dan algemene aggregatie en (2) is relatief eenvoudig te implementeren. Nadelen: (1) vereist een opzoekslag om het netwerk te achterhalen en (2) verlies van individuele adressen kan voor sommige doelen opvolging verhinderen.

G. Aggregatie algemeen

Aggregatie algemeen is vergelijkbaar met aggregatie van adres (zie Appendix A.E), maar is iets algemener gedefinieerd. In plaats van het adres wordt juist andere data geaggregeerd. Een voorbeeld is dat er per adres het aantal query's wordt geteld. In dat geval wordt alle andere data geaggregeerd.

Het voordeel van deze vorm van aggregatie is dat het eenvoudig toe te passen is. Nadelen zijn: (1) er moet zeer specifiek bekend zijn welke data er nodig is en (2) er moet nog verder gedefinieerd worden hoe deze methode toegepast wordt.

H. Distributie (distributed privacy preservation)

Distributie is het partitioneren van data over verschillende entiteiten (servers) waarbij de data op één entiteit onvoldoende is om het gedrag van een specifiek adres te profileren. Bij horizontaal partitioneren worden de query's verdeeld over verschillende entiteiten. Bij verticale partitionering worden de attributen van een query verdeeld over verschillende entiteiten.

Voordeel van dit soort filter is dat partitionering relatief eenvoudig realiseerbaar is door meerdere databases te gebruiken. Nadelen zijn: (1) op het moment dat de afzonderlijke databases groot genoeg worden, kan daar mogelijk alsnog een profiel uit worden opgebouwd. Er moet dus een limiet zijn aan het aantal query's in een database. Dit kan leiden tot een veelvoud van databases en

bijbehorende complexiteit, (2) partitioneren zal in de praktijk ervoor zorgen dat efficiënte analyse van de data moeilijker wordt omdat de data op enig moment weer gelinkt moet worden. Op dat moment worden de privacyvoordelen mogelijk ook weer weer teniet gedaan.

I. Vervanging

Attributen waarmee personen kunnen worden geïdentificeerd worden vervangen door een andere waarde. Om analyses over langere tijd mogelijk te maken moet de vervanging 1 op 1 zijn. Een attribuut waarde x moet altijd dezelfde vervangende waarde y krijgen.

Voordelen van vervanging: als de relatie tussen attribuut x en vervanging y wordt bewaard dan kan later als nodig de originele waarde van x worden achterhaald. Nadelen: de vervanging voor attribuut x moet bijgehouden worden zodat de volgende keer dat attribuut x vervangen moet worden, dezelfde vervangende waarde gebruikt kan worden. Dit moet bijgehouden worden, dit wordt lastig op het moment dat verwerken van nieuwe data parallel wordt uitgevoerd.

J. Willekeurige modificatie

Het modificeren van privacygevoelige attributen door er willekeurige data aan toe te voegen. De methode voor modificatie van een IP-adres kan anders zijn dan die voor een zoekterm. IP-adres 192.0.2.189 wordt dan bijvoorbeeld 203.0.113.044.

Voordelen van willekeurige modificatie: relatief eenvoudig te implementeren. Nadelen: (1) onbekend hoe moeilijk het is om de data te de-randomizen, (2) opvolging geven aan gedetecteerde abuse is niet effectief omdat niet meer is te achterhalen vanaf welk specifiek adres de abuse afkomstig is en (3) mogelijkheden voor onderzoek worden negatief beïnvloed, herkennen van patronen op basis van bron en zoekterm worden bijna onmogelijk.

K. Weglaten van attributen

Weglaten van privacygevoelige attributen zoals bron IP-adres en zoekterm.

Voordelen: relatief eenvoudig te implementeren, Nadelen: (1) onbekend hoe moeilijk het is om de data te de-randomizen, (2) opvolging geven aan gedetecteerde abuse is niet effectief omdat niet meer is te achterhalen vanaf welk specifiek adres de abuse afkomstig is, (3) mogelijkheden voor onderzoek worden negatief beïnvloed, herkennen van patronen op basis van bron en zoekterm worden bijna onmogelijk.

APPENDIX B: VOORBEELD POLICY

De policy ‘Resolver Reputation R&D’ is een policy die we gaan gebruiken voor het Resolver Reputation systeem [26], een ENTRADA-toepassing die een reputatie aan de resolvers toekent die de .nl name servers bevragen. Hiermee kunnen we bijvoorbeeld resolvers als ‘verdacht’ classificeren omdat ze onderdeel van een botnet lijken te zijn. Ons doel is deze informatie door te zetten naar de AbuseHUB zodat de abusedesks die daarop zijn aangesloten de besmetting kunnen verwijderen. Het Resolver Reputation systeem zijn we aan het ontwikkelen bij SIDN Labs en is nog niet in productie.

A. Identifier

Resolver Reputation R&D

B. Doel

Het doel van resolver reputation is, zoals de naam al suggereert, het geven van een reputatiescore aan de resolvers die .nl-domeinnamen opvragen. Het is een experimenteel project om te bekijken of we automatisch het verschil kunnen zien tussen een ‘fatsoenlijke resolver’ en bijvoorbeeld een geïnfecteerde machine die spam probeert te versturen.

C. Persoonsgegevens

Omdat het hier gaat over specifieke machines worden IP-adressen opgeslagen. Maar verder wordt er voornamelijk naar gegevens over de query’s gekeken; de domeinnamen in de query worden zelf niet opgeslagen, maar wel of deze meer dan 2 labels bevat en welk rrtype is gevraagd. Het aantal query’s wordt bijgehouden, evenals het aantal keer dat specifieke header flags gezet zijn en de response code.

Deze data wordt van de laatste dag bijgehouden, daarna geaggregeerd naar laatste week, maand, en ‘totaal’. Er wordt nog specifiek bijgehouden wanneer de eerste en laatste query’s zijn, maar afgezien daarvan is het niet mogelijk om terug te zien wanneer een specifieke query is geweest, tenzij het adres hooguit twee query’s heeft verstuurd.

D. Filters

De toegepaste filter is ‘Aggreggatie Algemeen’ (zie Appendix A.G). Individuele query’s per IP worden niet opgeslagen, alleen totalen van specifieke eigenschappen van die query’s. Bijvoorbeeld ‘van IP-adres 192.0.2.1 zijn 50 query’s met de header flag TC verstuurd’.

E. Retentie

Van een resolver die 31 dagen niet gezien wordt, wordt alle data uit het systeem verwijderd.

F. Toegang

Vooralsnog is er alleen intern toegang binnen de afgeschermde labomgeving bij SIDN Labs, middels een wachtwoord en een client certificaat mogelijk. Als deze

data uitgebreid wordt naar een productiedienst moet deze policy geüpdatet en opnieuw beoordeeld worden.

Als we data delen met derden zal het ofwel alleen zijn met de netwerkeigenaren waar de adressen toe behoren, ofwel hooguit gaan om 'totalen', dus zonder specifieke IP-adressen.

G. Type

Deze policy is van toepassing op de R&D-fase van het Resolver Reputation project.

H. Andere Beveiligingsmaatregelen

Er zijn geen verdere beveiligingsmaatregelen van toepassing.

DOCUMENT HISTORIE

Versie	Datum	Belangrijkste wijzigingen
1.3	30-sep-2014	Eerste publieke versie
1.4	4-nov-2014	Toepassingssilo's toegevoegd, onderscheid tussen R&D en productie verduidelijkt