No 13, Q1 2014

The.nlyst

LOKALE ANYCAST: SIDN'S NIEUWSTE WAPEN TEGEN DDOS-AANVALLEN

SIDN plaatst als eerste registry DNS-servers 'in het veld'

Anycast is een veelgebruikte techniek om de beschikbaarheid van servers te vergroten. Meer en krachtigere DDoS-aanvallen deden SIDN besluiten om haar DNS-anycast-technologie ook lokaal onder te brengen, bij onder meer grote ISP's en hostingpartijen. SIDN is de eerste registry die gebruikmaakt van zo'n lokale anycast. Erwin Heringa, netwerkbeheerder, en Marc Groeneweg, ICT-projectleider, zijn nauw bij het project betrokken en vertellen er meer over.

Marc Groeneweg, ICT-projectleider

Slachtoffer of medeplichtig

SIDN beschikt over een indrukwekkende DNS-infrastructuur die duizenden DNS-query's per seconde aankan. Een gevolg van zo'n krachtige infrastructuur is dat kwaadwillenden deze kunnen misbruiken om DDoS-verkeer te versterken. Marc Groeneweg: "We zien dit de laatste tijd veel in de gaming-industrie. Gamers lanceren aanvallen op hun tegenstanders of men probeert grote gameplatforms offline te krijgen." Door zogenaamde response rate limiting, het beperken van malafide DNS-verkeer, kan SIDN de overlast al enorm beperken en is het bedrijf niet langer ongewild medeplichtig in DNS-amplificatieaanvallen. Naast de DNS-amplificatieaanvallen tegen derden, is er ook het risico dat SIDN zelf het doelwit wordt van een DDoS-aanval. Marc Groeneweg: "Onze reactie hierop was tot voor kort: meer DNS-capaciteit toevoegen. Hoewel dit nog steeds zinvol is, is het toevoegen van alsmaar meer capaciteit een ratrace die uiteindelijk niet valt te winnen." Daarom ging SIDN op zoek naar een andere benadering. Die werd gevonden in lokale anycast.

Globale anycast: bewezen technologie

Globale anycast is een bewezen en heel effectieve technologie. Het is al tijden in gebruik voor de root-nameservers. Ook SIDN zet het al sinds jaar en dag in om de beschikbaarheid van het .nl-domein te vergroten. De werking is even simpel als doeltreffend. Doordat verschillende servers één IP-adres delen, 'denken' routers dat het dezelfde server is. IP-pakketten worden doorgestuurd naar het 'dichtstbijzijnde' punt. De totale netwerkbelasting wordt dus verspreid over meerdere exemplaren van wat dezelfde server lijkt.

Erwin Heringa, netwerkbeheerder

Lokale anycast

Wat lokale anycast anders maakt, is de inzet van zogenaamde lokale nodes. Door slim om te gaan met routering kunnen deze alleen lokaal benaderd worden. Hierdoor kan wereldwijd DDoS-verkeer, ongeacht de hoeveelheid, ⊕

Voorwoord

Het internet is vandaag de dag hét mondiale medium voor communicatie, informatie-uitwisseling, sociale activiteiten, samenwerken en commercie. Het is een cruciale factor geworden in de economische en democratische ontwikkeling van landen, het succes van bedrijven en de persoonlijke ontwikkeling van individuen. We doen ons werk online, hebben er contact met onze vrienden en delen onze meningen en ervaringen met de hele wereld. We volgen er het nieuws, kijken naar films en televisieprogramma's, regelen onze financiële zaken, spelen games en bestellen er onze kleren, ons eten of een nieuwe smartphone.

Het succes van het internet heeft ook zijn keerzijde. Juist door het belang voor maatschappij en economie, is het steeds vaker een middel of doelwit voor bepaalde regimes, criminelen, terroristen, vandalen of simpelweg onverlaten die willen tonen wat zij kunnen. In 2013 zagen we daar meer voorbeelden van dan ooit. Onder andere de douane, de Belastingdienst, de NS en verschillende Nederlandse banken waren het slachtoffer van DDoS-aanvallen. Door een grootschalige aanval op Spamhaus, een non-profitorganisatie die helpt spam te bestrijden, functioneerden zelfs grote delen van het internet korte tijd trager. Zorgelijke ontwikkelingen, waarbij de aanvaller en de verdediger in een eindeloze strijd dreigen te raken.

Het 'goede nieuws' is dat deze incidenten zorgden voor een sterke toename van de aandacht voor en investeringen in veiligheid en stabiliteit, zowel bij de overheid als bij het bedrijfsleven.

Voor SIDN zijn de eigen security en de veiligheid van het internet belangrijke thema's. Vanwege onze specifieke functie zijn ook wij een doelwit voor kwaadwillenden. Onderdeel van een omvangrijk pakket van beschermende maatregelen is een lokaal 'anycastnetwerk' dat vorig jaar is opgezet. We zijn de eerste registry die op deze manier samenwerkt met internetserviceproviders. In dit nummer leest u hier meer over.
Ook leest u over een nieuwe bewakingsservice voor .nl-domeinnamen en over de wijze waarop registrars omgaan met de dreiging van DDoS-aanvallen.

Alleen als het overal stabiel beschikbaar is en gebruikers zich terecht online veilig voelen, zal het internet zich tot zijn volle potentieel ontwikkelen. Wij zetten ons daar dagelijks voor in!

Roelof Meijer,
Algemeen directeur

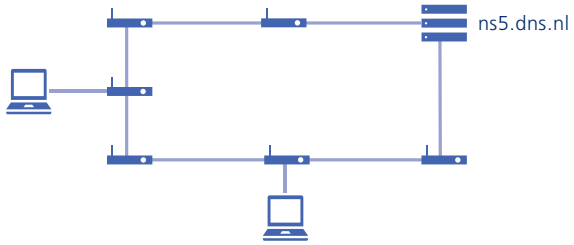
niet bij een lokale node uitkomen. Dat kan alleen lokaal gegenereerd DDoS-verkeer, en dit is veel beter onder controle te krijgen. Bij aanvallen die niet geïsoleerd kunnen worden omdat ze te groot zijn, bieden de lokale anycast-servers extra capaciteit die helpt om de aanval af te slaan. Het systeem voor lokale anycast is door SIDN in eigen huis gebouwd en uitgedacht. Hierdoor heeft het bedrijf veel kennis opgebouwd.

bijvoorbeeld gebruikt kunnen worden door kleinere partijen: lokale anycast-servers die gedeeld worden door een aantal partijen. Een dergelijke server is nu bij AMS-IX geplaatst. Hiervan maken inmiddels verschillende internetbedrijven gebruik.

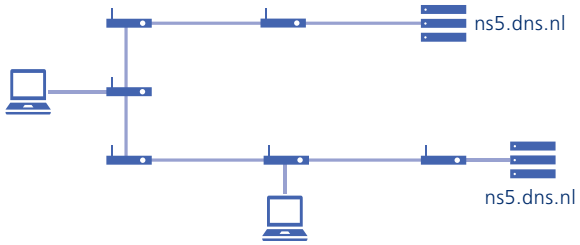
Voor veel partijen interessant

Lokale anycast is relatief eenvoudig uit te voeren en heeft veel voordelen. Men zou dus verwachten dat de techniek al door veel registries wordt toegepast. Toch is SIDN de eerste die dit doet. Erwin Heringa: "Volgens mij was de Duitse registry ooit van plan ermee te beginnen. Zij waren echter bang dat deelnemers een commercieel voordeel zouden krijgen ten opzichte van andere hostingbedrijven. Omdat bij ons in principe elk hostingbedrijf deel kan nemen, hebben we dat probleem niet." De komende tijd plaatst SIDN dan ook meer lokale anycast-servers. Elk hostingbedrijf kan hiervoor in aanmerking komen. SIDN stelt wel een aantal voorwaarden aan partijen die willen participeren. Zo moet een bedrijf bijvoorbeeld een serieus beleid hebben om misbruik tegen te gaan en moet het IPv6-enabled zijn. Wilt u meer informatie over de lokale anycast van SIDN of hierin participeren? Neem dan contact op met onze relatiebeheerder Daniël Federer via daniel.federer@sidn.nl.

Globale anycast: wat routers 'denken'



Globale anycast: hoe het werkelijk is

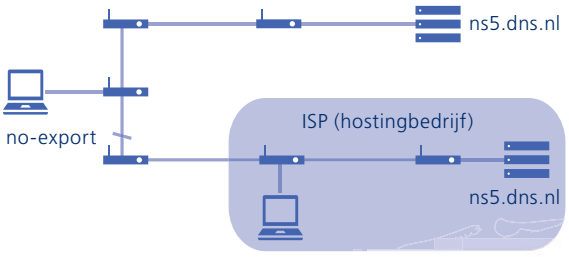


Marc Groeneweg: "We hadden al veel DNS-kennis in huis en hebben nu heel wat bijgeleerd over routering. In dit project komen veel interessante beheeraspecten bij elkaar. Natuurlijk blijven we het systeem verbeteren en verder ontwikkelen. We leren elke dag bij."

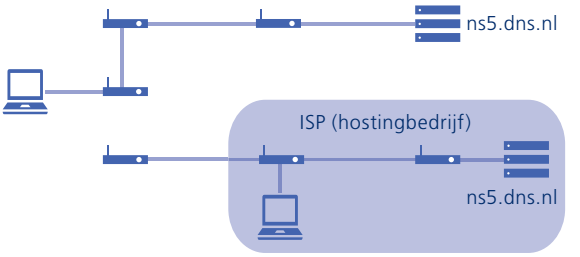
Dedicated en shared nodes

De lokale anycast-technologie van SIDN is met name interessant voor grote ISP's en hostingbedrijven. Erwin Heringa: "Als de .nl-dienstverlening van SIDN door DDoS-aanvallen geraakt zou worden, blijft het .nl-domein voor hen via de lokale anycast-servers beschikbaar." De primeur ging naar hostingleverancier LeaseWeb. Zij deelden van meet af aan de visie van SIDN en stelden meteen de nodige datacenterfaciliteiten beschikbaar. Al snel werden er 'dedicated nodes' geplaatst bij verschillende Nederlandse ISP's, waaronder UPC, KPN en XS4All. Ook zet SIDN zogenaamde 'shared nodes' in die

Lokale anycast: hoe het werkelijk is



Lokale anycast: wat routers 'denken'



“NIEMAND PRAAT ER GRAAG OVER”

Twee registrars over DDoS-aanvallen

Steeds vaker krijgen hostingbedrijven te maken met DDoS-aanvallen. Rob van den Nieuwelaar, directeur van Hosting2GO, en Erik Logtenberg, directeur van VEVIDA en voorzitter van de Vereniging van Registrars, vertellen hoe hun bedrijf omgaat met dit probleem.

Hoe vaak komen DDoS-aanvallen eigenlijk voor?
Erik Logtenberg: “In de laatste helft van 2013 zagen we een flinke toename. Voorheen waren het vooral in het oog springende websites die doelwit waren van een aanval. Nu kan zowat elk bedrijf slachtoffer worden.”

Rob van den Nieuwelaar: “In de media wordt er weinig aandacht aan besteed. Niemand praat er graag over. Bedrijven willen niet laten weten dat ze kwetsbaar zijn. En als je laat weten hoeveel maatregelen je hebt genomen, is dat bijna een uitnodiging voor DDoS’ers om het te proberen.”

Hoeveel last hebben jullie van deze aanvallen?
Erik Logtenberg: “We hebben er waarschijnlijk een paar keer per maand last van. Dat is niet alleen vervelend maar ook kostbaar. Een aanval tegengaan is duur. Die kosten kun je nooit helemaal op je klanten verhalen.”

Rob van den Nieuwelaar: “Daar komt bij dat klanten DDoS-aanvallen niet altijd accepteren als reden dat hun website of e-mail niet beschikbaar is. Een klein deel van de providers misbruikt de term DDoS om een storing of menselijke fout goed te praten. Als we met een DDoS-aanval te maken hebben, kost het soms moeite om klanten te overtuigen dat we de waarheid spreken.”

Rob van den Nieuwelaar, directeur Hosting2GO

Waarom wordt een bedrijf eigenlijk uitgekozen voor een aanval?
Rob van den Nieuwelaar: “We hebben gemerkt dat bepaalde sites vaker doelwit zijn. Zoals pornosites, websites waar je illegale software kunt downloaden of fora waar zeer extreme standpunten worden verkondigd. Een aanval begint vaak met een ruzie op een bepaald forum of het betreft een partij die de website van een concurrent offline wil hebben. In het eerste geval is doorgaans vrij makkelijk te achterhalen wat het doel is, vaak het drukste forum op een server, en houdt de aanval ook niet heel erg lang aan. In het tweede geval is de aanval meestal professioneler, groter opgezet en lastiger te bestrijden. Uiteindelijk is het gewoon terreur.”

Erik Logtenberg, directeur VEVIDA

Erik Logtenberg: “Er is ook regelmatig sprake van afpersing. Een kleine webshop wordt platgelegd en als de aanval is afgeslagen, ontvangen ze een e-mail waarin staat dat ze een volgende aanval kunnen afwenden door een bepaalde hoeveelheid bitcoins te betalen.”

Laten bedrijven zich chanteren?
Erik Logtenberg: “Er zijn vast bedrijven die betalen. Anders zouden criminelen dit nooit doen. Wij raden altijd af om te betalen. Want ook al heb je er één afgekocht, wie kan je garanderen dat een ander niet ook een aanval op zal zetten?”

Kan de politie in zo'n geval niets ondernemen?
Rob van de Nieuwelaar: "Er wordt bijna nooit aangifte gedaan van een DDoS-aanval. Dat is niet vreemd. De politie heeft te weinig kennis op dit gebied, daders zijn moeilijk te achterhalen en bewijsmateriaal is bijna niet te vinden."

Erik Logtenberg: "Als ik met mensen van Justitie spreek, blijkt steeds weer dat ze hier helemaal niet mee bezig zijn. Ze concentreren zich op kinderporno en computercriminaliteit gericht tegen banken. Een afpersingszaak van een paar honderd euro is blijkbaar niet interessant genoeg."

Wat is de schade die een DDoS-aanval teweegbrengt?
Rob van den Nieuwelaar: "Het kost geld. Maar de imagoschade is erger. Voor onze klanten is zo'n aanval erg vervelend. Een gevolg kan zijn dat mensen overstappen naar een andere provider. In de praktijk valt dit gelukkig mee. Men begrijpt wel dat het een sectorbreed probleem is."

Wat voor maatregelen nemen jullie tegen DDoS-aanvallen?
Rob van den Nieuwelaar: "De kleine DDoS-aanvallen worden door onze eigen systemen al automatisch tegengehouden. Tegen de zware aanvallen is op dit moment geautomatiseerd weinig te ondernemen. Dat is mensenwerk."

Erik Logtenberg vult aan: "Tegen bepaalde aanvallen die veel bandbreedte gebruiken, kun je maar één ding doen: je capaciteit drastisch verhogen. Er zijn weinig providers in Nederland die daar zelf de middelen voor hebben, daarom zijn er internationale partijen die deze capaciteit aanbieden. Dit is effectief maar kost wel veel geld."

De NBIP is bezig met een anti-DDoS-dienst waarmee providers de kosten van DDoS-bestrijding kunnen delen. Wat vinden jullie daarvan?
Erik Logtenberg: "Ik ken het niet, maar het klinkt goed. De bedrijven die anti-DDoS-maatregelen aanbieden zijn gewend om met grote afnemers te werken, zoals banken en overheidsinstellingen. Voor hen is geld geen probleem. Voor kleinere providers wel. Het scheelt als je de kosten kunt delen."

Komt er ooit een eind aan DDoS-aanvallen?
Erik Logtenberg: "Dat geloof ik niet. Het principe van een DDoS-aanval, ergens meer verkeer naartoe leiden dan de infrastructuur aankan, is gewoonweg te simpel. Natuurlijk kunnen we bepaalde trucjes tegengaan waarvan DDoS'ers gebruikmaken, maar ze vinden vast wel weer nieuwe."

Rob van den Nieuwelaar: "Ik denk dat we ver kunnen komen. De eerste keer dat we met een aanval te maken hadden, waren onze servers een nacht lang slecht bereikbaar. Zo'n aanval hebben we nu in enkele minuten onder controle. Het blijft dweilen met de kraan open. Maar voorlopig lukt het ons om harder te dweilen dan het lekt."

Erik Logtenberg: "We kunnen in ieder geval een deel van de aanvallen oplossen. Als het criminelen meer kost om een aanval uit te voeren dan het ze oplevert, zullen ze ermee stoppen. Aanvallen die bedoeld zijn om een statement te maken, houd je altijd."

SIDN OPENT DE JACHT OP TYPEFOUTEN

Domeinnaambewakingsservice spoort typosquats op

Onlangs heeft SIDN een succesvolle pilot afgesloten voor de Domeinnaambewakingsservice, een nieuw product van de Nederlandse registry. De pilot werd uitgevoerd in samenwerking met een grote financiële dienstverlener. Daniël Federer, key accountmanager bij SIDN, vertelt er meer over.

Wat is de Domeinnaambewakingsservice?
"Het is een tool om typosquatting te signaleren: een vorm van misbruik gebaseerd op het feit dat mensen zich wel eens vergissen bij het intypen van een web- of e-mailadres, een fenomeen dat ook wel fat fingers wordt genoemd. Denk aan amsterdan.nl in plaats van amsterdam.nl. Soms worden deze domeinnamen gebruikt om mensen naar sites met reclame te leiden, maar regelmatig gaat het om sites met malware of e-mails waarin geprobeerd wordt om mensen onder valse voorwendselen persoonsgegevens te ontfutselen. Phishing begint vaak met een typosquat."

Wat zijn de gevolgen van typosquatting?
"De schade die zulke sites aanrichten kan groot zijn. Met phishing zijn flinke bedragen gemoeid. Maar het belangrijkste is dat zulke vormen van misbruik het vertrouwen van gebruikers schaden. Zeker voor banken of andere organisaties waarvoor vertrouwen essentieel is. Zulke bedrijven willen dan ook graag snel op de hoogte zijn van nieuwe typosquats gerelateerd aan hun domeinnaam."

Hoe werkt de Domeinnaambewakingsservice?
"De Domeinnaambewakingsservice is gekoppeld aan de database met alle .nl-domeinnamen. Het systeem controleert of er domeinnamen geregistreerd zijn die lijken op de bewaakte domeinnaam. Denk bijvoorbeeld aan de toevoeging "mijn" aan een domeinnaam zoals mijndigid.nl. Of een letter extra zoals bijvoorbeeld haaerlem.nl. Elke gebruiker van de Domeinnaambewakingsservice (DBS) krijgt toegang tot een webinterface die een overzicht biedt van recent geregistreerde domeinnamen die aandacht behoeven. Ook kan de gebruiker een e-mailalert ontvangen wanneer er een domeinnaam gevonden is. Zo is hij altijd op de hoogte en kan hij snel reageren en eventueel maatregelen nemen."

Daniël Federer,
key accountmanager

Hoe is deze nieuwe dienst ontstaan?
"Eind 2012 is SIDN een innovatietraject gestart. DBS was de eerste innovatie die hieruit voortkwam. Toen we hiermee bezig waren, heb ik het concept dus getoetst bij een grote financiële dienstverlener. Zij waren direct enthousiast. De pilot was toen snel geregeld. Het moeilijkste bij de ontwikkeling was niet de techniek, maar de vraag welke gegevens we wel en niet konden verstrekken. Wat mag, wat is wenselijk, wat is mogelijk? En wat levert het dan nog op?"

Leverde de pilot nog verrassende zaken op?
"Ja. Tot onze verrassing bleek de service ook zeer nuttig als compliance-instrument. Sommige bedrijven zijn namelijk zelf registrar geworden vanwege een strikt securitybeleid en specifieke (registratie)regels. Regels die niet altijd bekend zijn bij alle afdelingen of vestigingen. Stel dat een marketingafdeling een campagnewebsite start en de domeinnaam elders registreert, dan krijgt het bedrijf hier ook een melding van en kan het actie ondernemen."

Voor wie is de Domeinbewakingsservice interessant?

"Op dit moment vooral voor een kleine groep grotere bedrijven met een sterk merk, een sterke reputatie of een website waar waardevolle gegevens worden verwerkt. Denk aan banken of organisaties met een publieke taak, die vaak zelf registrar zijn. Maar we werken nu ook aan productvarianten waarvan andere organisaties gebruik kunnen maken. Wellicht niet direct in eigen beheer maar juist via een derde partij, zoals bijvoorbeeld de registrar waarmee wordt samengewerkt."

Hoe ontwikkelt de Domeinnaambewakingsservice zich verder?

"Samen met de Vereniging van Registrars gaan we bekijken hoe we het product nog beter kunnen afstemmen op de markt. We willen bijvoorbeeld meer intelligentie toevoegen, in de vorm van risicoprofielen. Daarmee kunnen we typosquats kwalificeren, zodat een bedrijf sneller en beter kan zien of het met een bedreiging te maken heeft. Daarnaast onderzoeken we de mogelijkheden om via DBS ook registraties onder andere topleveldomeinen dan .nl te monitoren."

Waar worden typosquats voor gebruikt?

- Bezoekers trekken. Typosquats worden vaak gebruikt om u naar een bepaalde website te trekken. Zo komt u bijvoorbeeld ongewild terecht op de website van een online casino, een advertentiepagina of soms zelfs op de website van een concurrent van het bedrijf waarvan u eigenlijk de website wilde bezoeken.
- Phishing. Criminelen bootsen de website van een bank of internetwinkel na. Door het maken van een typefout in de url of door te klikken op een link in een phishingmail, komt u op deze website terecht. Eenmaal daar aangekomen wordt u verleid om uw wachtwoord of uw creditcardgegevens op te geven.
- Malware verspreiden. Domeinnamen die sterk lijken op het origineel van bijvoorbeeld een bekend bedrijf worden gebruikt om via een website of e-mail schadelijke software, zoals computervirussen, adware en spyware, te installeren op uw computer.
- Satire en persiflages. Soms worden typosquats gebruikt om u naar een website te leiden waar het bedrijf achter de originele website bespot wordt.

"BINNEN 10 MINUTEN HEBBEN WE DE JUISTE MENSEN BIJ ELKAAR"

Een kijkje bij SIDN's Computer Security Incident Response Team

Hoewel SIDN er alles aan doet om het .nl-domein zo veilig mogelijk te houden, werd het bedrijf op dinsdag 9 juli 2013 getroffen door een hack. Op een van de webservers werden bestanden aangetroffen die daar niet thuishoren. Security officer Bert ten Brinke riep SIDN's Computer Security Incident Response Team (CSIRT) bij elkaar, dat ervoor zorgde dat de gevolgen van de hack beperkt bleven.

Bert ten Brinke, security officer

Snel reageren

Als computersystemen zijn gehackt of er een virus is gesignaleerd, is het zaak om snel en effectief te reageren. Het is dan handig om één aanspreekpunt te hebben. Daarom hebben bedrijven van enige omvang vaak een speciaal team, een computer security incident response

team (CSIRT). Het CSIRT van SIDN staat dag en nacht klaar. "Incidenten vinden tenslotte niet alleen plaats tijdens kantooruren," vertelt Bert ten Brinke. "En veiligheid is voor SIDN van het allergrootste belang. Het is de uitdaging om een eventuele storing zo snel mogelijk op te lossen. Soms is het een klein probleem en kan een van de leden van het CSIRT het alleen af. Bij grotere incidenten werken we in teamverband. Binnen tien minuten hebben we de juiste mensen bij elkaar en kunnen we aan de slag."

Eerst de schade beperken ...

Bij elk incident staat het beperken van de schade voorop. Bert ten Brinke: "Bij de hack in juli hebben we met meerdere mensen de hele nacht doorgewerkt. We hebben de gecompromitteerde server zo snel mogelijk afgesloten en de accounts voor ons domeinregistratiesysteem gereset. Ook hebben we de publicatie van de zonefile, het bestand dat alle domeinnamen .nl-domeinnamen bevat, uit voorzorg uitgesteld, alhoewel dit een separaat systeem is. Gelukkig is de .nl-zone geen moment in gevaar geweest en bleef het mogelijk om domeinnamen te registreren via de EPP interface.

... dan op zoek naar de oorzaak

Dat het probleem is opgelost, betekent niet dat daarmee de oorzaak ook is weggenomen. Twee dagen na het incident liepen alle systemen weer, maar de nasleep duurde langer. Er moest een server opnieuw worden ingericht en men heeft verschillende onderzoeken uitgevoerd, waaronder een forensisch onderzoek. Bert ten Brinke: "Na een incident willen we precies weten wat er is gebeurd en hoe het kon gebeuren. Zo leren we elke keer weer bij." Deze kennis zet het CSIRT om in adviezen waarmee SIDN de security kan verbeteren. Bert ten Brinke: "We kunnen echter nooit garanderen dat er niets meer fout gaat. Het probleem met internetsecurity is namelijk dat je altijd achter de feiten aanloopt. Het is een eindeloos kat-en-muisspel. Wij passen ons aan, criminelen zoeken nieuwe wegen. Waarna het weer aan ons is om het gat dicht te rijden."

Goede communicatie

Bij incidenten als de hack in juli is goede communicatie essentieel, volgens Bert ten Brinke: "Het werkt het best als je open en eerlijk communiceert naar alle betrokken partijen. Het is de kunst om dit te doen zonder dat je informatie geeft waar kwaadwillenden wat mee kunnen." De communicatie van SIDN tijdens het incident in juli 2013 werd positief gewaardeerd door registrars.

Sinds 1988

's Werelds eerste alarmdienst voor computerincidenten werd opgericht in 1988. Aanleiding was de uitbraak van de computerworm Morris. Deze worm verspreidde zich snel over een groot deel van het internet. Servers liepen vast waardoor onder meer e-maildiensten onbereikbaar waren. Het computer emergency response team (CERT) dat hiervoor werd opgericht, bleek een adequate oplossing die al snel op heel veel plaatsen werd overgenomen. Inmiddels hebben vrijwel alle grote organisaties en alle landen een eigen CERT. In Nederland wordt deze functie ingevuld door het NCSC, het Nationaal Cyber Security Centre.

Het CSIRT van SIDN is aangesloten bij het internationale forum FIRST. Hierbinnen hebben teams uit de hele wereld contact, onder meer over technische informatie en best practices.

VOOR ELKE DDOS-AANVAL DE JUISTE OPLOSSING

NBIP maakt DDoS-bestrijding voor providers betaalbaar

De stichting Nationale Beheersorganisatie Internet Providers, kortweg NBIP, ondersteunt internet service providers bij de uitvoering van wettelijke verplichtingen uit de Telecommunicatiewet. Binnenkort introduceert de stichting een anti-DDoS-dienst. Voorzitter Alex Bik vertelt er meer over.

Alex Bik, voorzitter NBIP

Tapbevelen uitvoeren

De NBIP is ruim tien jaar geleden opgericht. Aanleiding was de wijziging van de Telecommunicatiewet in 2002. Alex Bik: "De wet eiste dat providers aan tapbevelen moesten vtoldoen. Als een provider zo'n verzoek krijgt, moet hij het juiste dataverkeer onderscheppen, filteren en volgens bepaalde standaarden doorsturen. Voor zo'n interceptiesysteem is speciale hard- en software nodig. Zeker voor kleine en middelgrote providers is dit duur. Door deze kostbare investeringen gezamenlijk te doen, kunnen providers veel geld besparen. De NBIP is opgericht om dit mogelijk te maken." De stichting begon met tien deelnemers maar ondertussen voert de NBIP tapbevelen uit voor zo'n honderd isp's.

Verplicht optreden tegen DDoS-aanvallen

Ook de nieuwe anti-DDoS-dienst van de NBIP komt voort uit de Telecommunicatiewet. Alex Bik: "Deze wet is onlangs weer gewijzigd. Hij stelt nu ook eisen aan de continuïteit van providers. DDoS-aanvallen brengen die continuïteit in gevaar en daar wil je je tegen wapenen. Voor de bestrijding is kostbare apparatuur nodig. Een investering van vele tonnen. Net als bij tapsystemen is het dus ook hier heel interessant om de kosten te delen, waardoor het goed bij de NBIP past."

Elke aanval een andere oplossing

Niet elke DDoS-aanval is hetzelfde, vertelt Alex Bik. "Je hebt aanvallen die gericht zijn tegen een specifiek onderdeel van een website en er zijn aanvallen die domweg met zoveel mogelijk bandbreedte proberen een dienst plat te leggen. Voor al deze vormen zijn andere oplossingen beschikbaar. Er bestaat niet zoiets als een 'silver bullet'. Voor kleinere providers is het bijna onmogelijk om alle oplossingen in huis te hebben. Dat kunnen wij wel. We hebben de beste oplossingen bijeen gebracht op een centrale locatie, die is aangesloten op AMS-IX. Als een deelnemer wordt aangevallen, trekken we het verkeer voor die deelnemer naar ons toe. We filteren het verdachte verkeer er zoveel mogelijk uit en sturen de rest door. Je zou de dienst kunnen zien als de nationale wasstraat voor dataverkeer."

Succesvolle test

Op dit moment wordt de anti-DDoS-dienst getest. Alex Bik is zeer tevreden over het verloop hiervan: "Het systeem werkt precies zoals we dat bedacht hadden. Vijftien partijen hebben aangegeven dat ze de dienst willen gaan gebruiken. We gaan de anti-DDoS-dienst snel aanbieden en verwachten dat er dan nog veel meer isp's aan zullen haken."

Minder overlast, maar geen eind aan de aanvallen

De anti-DDoS-dienst zal kleine en middelgrote isp's zeker helpen om DDoS-aanvallen sneller af te slaan. Dit betekent echter geen einde aan de aanvallen, zegt Alex Bik. "Ik geloof niet dat we ervoor kunnen zorgen dat er geen DDoS-aanvallen meer worden uitgevoerd. We kunnen er wel zorgen dat ze minder overlast meer veroorzaken. Dat zal de mensen achter de aanvallen ook ontmoedigen."

.NL Analysed

#	TLD		Aantal Q4	Groei	
1	.com	Algemeen	111.839.466	1,1%	=
2	.tk	Tokelau	21.131.593	10,2%	=
3	.de	Duitsland	15.592.379	0,7%	=
4	.net	Algemeen	15.166.881	0,4%	=
5	.cn	China	10.829.480	1,0%	↑
6	.uk	Ver. Koninkrijk	10.550.763	0,7%	↓
7	.org	Algemeen	10.366.672	4,3%	↓
8	.info	Algemeen	5.836.808	-4,6%	=
9	.nl	Nederland	5.388.364	1,0%	=
10	.ru	Rusland	4.918.923	3,1%	=
11	.eu	Europese Unie	3.709.860	-0,5%	=
12	.br	Brazilië	3.310.867	2,8%	=
13	.ar*	Argentinië	2.920.000	2,5%	=

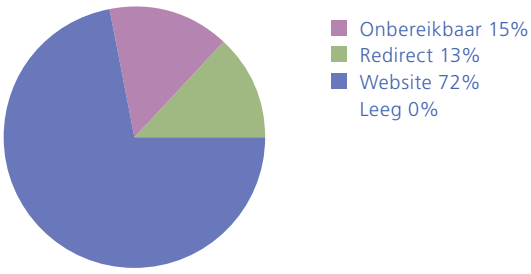
#	TLD		Aantal Q4	Groei	
14	.au	Australië	2.754.959	1,9%	=
15	.fr	Frankrijk	2.716.055	2,3%	=
16	.biz	Algemeen	2.632.683	1,2%	↑
17	.it	Italië	2.630.900	1,5%	↓
18	.pl	Polen	2.461.509	1,6%	=
19	.ca	Canada	2.150.831	1,5%	=
20	.ch	Zwitserland	1.837.020	1,2%	=
21	.us	Ver. Staten	1.796.591	0,4%	=
22	.es	Spanje	1.696.538	1,8%	=
23	.co*	Colombia	1.690.000	4,5%	=
24	.be	België	1.433.990	1,7%	=
25	.jp	Japan	1.356.102	0,8%	=
	* schatting				

Top 25 TLD's

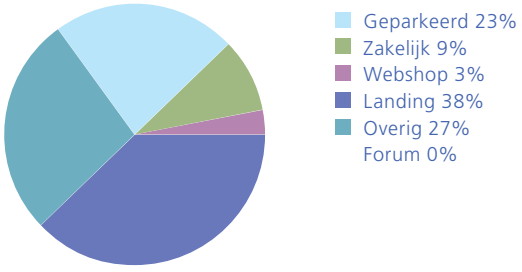
In totaal zijn er in 2013 bijna 271 miljoen domeinnamen geregistreerd, dat is een toename van 20,5 miljoen ten opzichte van 2012. De groei ligt onder het niveau van 2012 (+ 25 mln.) maar wel boven de groei in 2009-2011. De overall groei van domeinnamen blijft sterk maar wordt gedragen door een steeds beperkter aantal TLD's. De meerderheid van de extensies ziet de groei afnemen.

De ccTLD's zijn verantwoordelijk voor 73% van de netto groei, aangejaagd door .tk dat een aandeel van 33% in de totale groei heeft. Opvallend is dat de groei van .tk in het laatste kwartaal de laagste is sinds wij de statistieken bijhouden (Q2 '12). Door deze beperkte horizon is momenteel geen oorzaak aan te wijzen voor de afname van de groei. Aan de andere kant trekt de groei van .cn (China) in het laatste kwartaal juist weer aan.

Gebruik .nl



Classificatie website



Gebruik .nl

Sinds medio 2013 heeft SIDN de beschikking over een analysetool die ons inzicht biedt in het gebruik van .nl-domeinnamen. Om een goed beeld te krijgen van het gebruik wordt frequent een scan uitgevoerd van alle actieve .nl-domeinnamen. Allereerst wordt het gebruik van de domeinnaam op het hoogste niveau in kaart gebracht.

We onderscheiden daarin vier mogelijkheden:

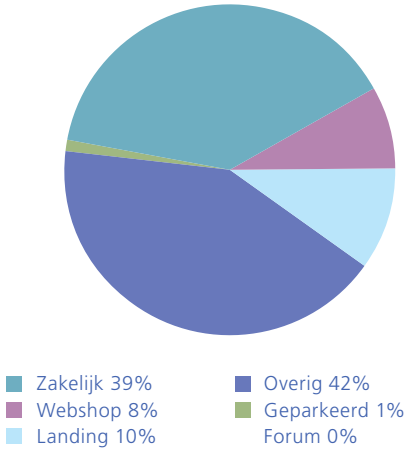
- Website: de domeinnaam is bereikbaar en er is een website aanwezig.
- Redirect: verkeer wordt omgeleid naar een andere domeinnaam.
- Leeg: de domeinnaam is bereikbaar maar er is geen website aanwezig.
- Onbereikbaar: de domeinnaam is onbereikbaar.

Classificatie websites

Van de domeinnamen waarop een website is aangetroffen wordt de inhoud in kaart gebracht, we onderscheiden daarin de volgende categorieën:

- Webshop: dit is een website van een (online) winkel waar goederen te koop aangeboden worden.
- Zakelijk: hieronder vallen de websites van bedrijven en organisaties zonder verkoop.
- Forum: dit zijn de welbekende online discussieplatforms.
- Overig: alle websites waarvan de content niet in een van de andere categorieën te plaatsen is.
- Landing: dit zijn pagina's als 'website in onderhoud' of 'hier komt de website van …'
- Geparkeerd: deze pagina wordt door veel internetproviders geplaatst nadat een domeinnaam geregistreerd is maar de houder nog geen website heeft ingericht.

Type redirect



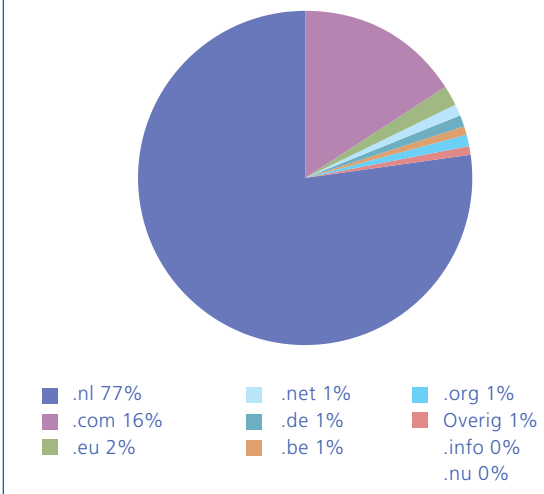
Type redirect

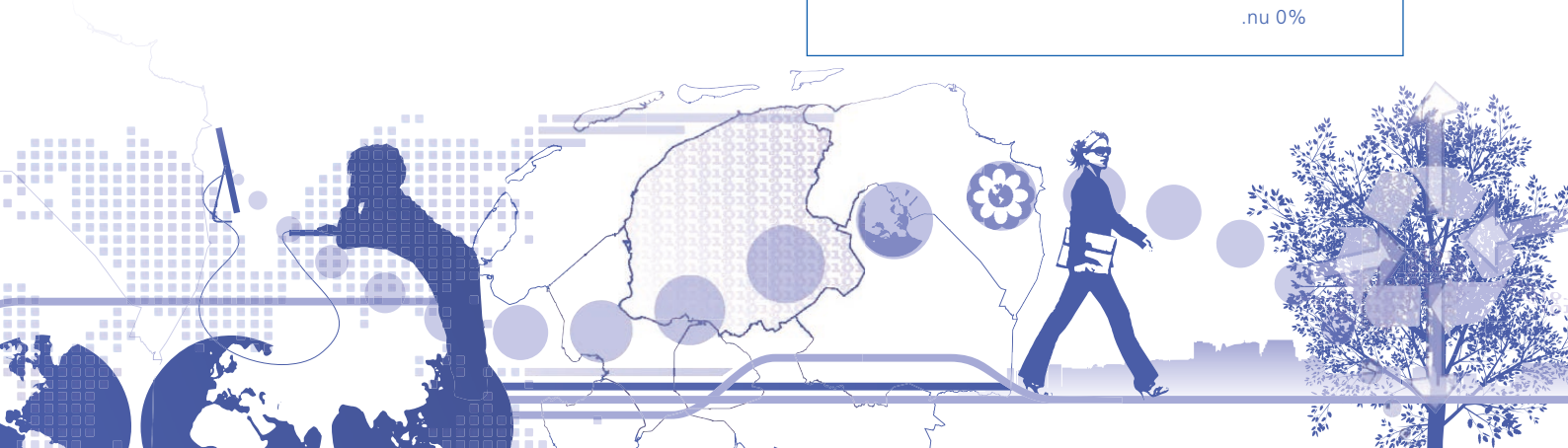
We weten dat veel domeinnaamhouders meerdere domeinnamen registreren voor bijvoorbeeld bescherming van een merknaam of voor toekomstige projecten. Veel van deze domeinnamen bevatten geen website maar verwijzen door naar een andere domeinnaam, dit wordt een redirect genoemd. Met de analysetool brengen we ook deze redirects in kaart. We kijken daarmee naar de domeinnaam waarnaar geredirect wordt. Voor deze analyse hanteren we dezelfde classificatie als voor de websites. Hier zien we, niet geheel verrassend, veel zakelijke websites.

Redirect per TLD

Van de redirects kijken we niet alleen naar de domeinnaam waarnaar verwezen wordt. We kijken ook naar de TLD's, zie de volgende grafiek. Hier zien we duidelijke overeenkomsten met de veel gebruikte extensies binnen Nederland. Natuurlijk .com, wereldwijd de meest gebruikte TLD maar ook de extensies van onze buurlanden .be, .de en natuurlijk .eu. In totaal wordt er doorverwezen naar 110 verschillende TLD's.

Redirect per TLD





Evenementenkalender

In de komende maanden is SIDN, voor zover nu bekend, vertegenwoordigd op de volgende evenementen.

Datum	Evenement	Plaats
27-02 t/m 28-02	13th CENTR Marketing Workshop	Frankfurt, Duitsland
06-03	43rd CENTR Legal & Regulatory Workshop	Rome, Italië
02-03 t/m 07-03	89th IETF	Londen, Engeland
12-03 t/m 13-03	51st General Assembly	Stockholm, Zweden
24-03 t/m 27-03	49th ICANN Meeting	Singapore
01-04 t/m 03-04	World Hosting Days	Rust, Duitsland
12-04	ISP Kartcompetitie	Maarssen

SIDN steunt actie om kinderen te beschermen tegen identiteitshacken

Identiteitshacken is het aan de haal gaan met foto's of andere persoonlijke informatie. Hier worden bijvoorbeeld nep-Twitteraccounts of nep-Facebookprofielen mee aangemaakt. Het blijft niet bij grappig bedoelde fotobewerkingen van politici of BN'ers, maar onschuldige kinderen worden hier de dupe van. Stichting Mijn Kind Online vroeg aandacht voor deze vorm van misbruik met een indringend filmpje. SIDN vindt online bescherming van groot belang en maakte de filmproductie van Mijn Kind Online mogelijk. We willen op deze manier bijdragen aan een veilig internet voor kinderen.

Suggesties

Wilt u graag een onderwerp uitgelicht zien in de The.nlyst? Mailt u dan uw suggesties naar communicatie@sidn.nl.

SIDN wint Internet Innovatie Award

In januari ontving SIDN Labs de ISOC Internet Innovatie Award 2014 voor de ontwikkeling van EPP keyrelay. EPP keyrelay, ontwikkeld door SIDN Labs, biedt een oplossing voor het probleem dat met DNSSEC beveiligde domeinnamen nog niet eenvoudig veilig verhuisd konden worden naar een andere DNS-operator. Bij de oplossing speelt de registry (bv. SIDN) een sleutelrol. Het DNSSEC-sleutelmateriaal van de verkrijgende DNS-operator wordt via de registry naar de latende DNS-operator gestuurd, waarbij gebruik gemaakt wordt van het Extensible Provisioning Protocol, een standaard voor de uitwisseling van informatie tussen registries en registrars. Op deze manier kan de domeinnaam ook gedurende de verhuizing beveiligd blijven met DNSSEC. EPP keyrelay is bij de IETF ingediend als internet draft en wordt zeer waarschijnlijk een nieuwe internetstandaard.

Colofon
The.nlyst is een magazine van SIDN, het bedrijf achter .nl en biedt informatie over internetgerelateerde thema's en over (.nl-) domeinnamen in het bijzonder. Het magazine wordt gratis verspreid onder relaties van SIDN.

Redactieadres
SIDN
Postbus 5022
6812 AR ARNHEM
Nederland
communicatie@sidn.nl

Aan deze editie werkten mee
Rob van den Nieuwelaar, Alex Bik, Erik Logtenberg, Daniël Federer, Erwin Heringa, Marc Groeneweg, Bert ten Brinke, Roelof Meijer, Sean Schuurman van Rouwendal, Marnie van Duijnhoven en Martin Sluijter

Vormgeving & realisatie
ARA, Rotterdam – www.ara.nl

Vertalingen
G & J Barker Translations – www.gandjbarker.co.uk

Oplage
ca. 2.500

Abonnementen
The.nlyst wordt gratis verspreid onder relaties van SIDN. Voor het aanvragen of opzeggen van een abonnement, kunt u mailen naar communicatie@sidn.nl.

ISSN: 2212-2842