The.nlyst
No 9, Q4 2012

SAMENWERKEN IN DE STRIJD TEGEN CYBERCRIMINALITEIT

Een kennismaking met het Nationaal Cyber Security Centrum

In een onopvallend Haags kantoorpand, vlakbij treinstation Laan van NOI en het ministerie van Sociale Zaken en Werkgelegenheid, bevindt zich sinds begin dit jaar het kloppend hart van de Nederlandse strijd tegen cybercriminaliteit: het Nationaal Cyber Security Centrum (NCSC). General manager Elly van den Heuvel vertelt meer over deze publiek-private samenwerking.

Elly van den Heuvel, general manager, NCSC

Toenemend belang cyber security.

"In 2002 werd GOVCERT opgericht; de voorloper van het NCSC. GOVCERT, het Cyber Emergency Response Team van de overheid, hielp overheden en andere organisaties met een publieke taak bij de bestrijding van hacks en besmettingen. Gezien de enorme hoeveelheid cyberdreigingen bleek GOVCERT echter niet voldoende. Van den Heuvel: "Het internet is steeds belangrijker geworden in ons leven. We zijn er afhankelijk van geworden. Incidenten kunnen een enorme impact hebben op onze economie en ons dagelijks leven. Het belang van cybersecurity is daarom ook toegenomen. Een duidelijke strategie op dit terrein ontbrak echter. Tot 2011, want toen kwam het kabinet met de Nationale Cyber Security Strategie. De oprichting van een Nationaal Cyber Security Centrum was een van de zes punten uit deze strategie. Begin 2012 is GOVCERT opgegaan in het NCSC."

Een brede organisatie

Van den Heuvel benadrukt dat het NCSC een compleet andere organisatie is dan GOVCERT. "Het NCSC is geen GOVCERT-plus. We richten ons meer op de nationale veiligheid en de opzet is veel breder omdat we met diverse partijen samenwerken. We zijn een publiek-privaat samenwerkingsverband. Als je iets wilt doen aan veiligheid op internet, kan dat ook niet anders. Het internet is tenslotte

Voorwoord

In de afgelopen decennia heeft het internet zich ontwikkeld tot een wereldomvattend medium dat van cruciaal belang is voor onze maatschappij en economie. Ook onder de huidige economische omstandigheden blijft de internetsector het goed doen. Dagelijks komen nieuwe producten en diensten op de markt. Het aantal gebruikers wereldwijd, op dit moment ruim 2 miljard, stijgt nog elke dag. Het is duidelijk dat het internet zijn volle potentieel nog lang niet heeft bereikt. Voor verdere ontwikkeling is het vertrouwen van gebruikers essentieel. Juist vanwege het grote belang van het internet in ons leven, zakelijk en privé. Dit vertrouwen kan slechts toenemen als gebruikers zich online veilig voelen.
Daarom doet SIDN er alles aan om het .nl-domein nog veiliger te maken. We besteden veel zorg aan onze eigen processen en systemen en waren de eerste registry met een ISO 270001-certificaat, dé standaard voor informatiebeveiliging. Daarnaast nemen wij allerlei maatregelen en initiatieven om de .nl-zone zo veilig mogelijk te maken voor internetgebruikers. Met succes, want van alle landendomeinen met een vergelijkbare omvang is .nl veruit het veiligst*.
Bovendien dragen we op verschillende manieren bij aan een veiliger internet in het algemeen. Bijvoorbeeld door samen te werken in programma's als Digivaardig & Digiveilig of het Platform Internetveiligheid en door het sponsoren van initiatieven als het Steunpunt Acquisitiefraude en het Meldpunt Kinderporno. Maar we doen bijvoorbeeld ook onderzoek naar manieren om je privacy op internet beter te beschermen, onder meer via PI.Lab.

Dit nummer van The.nlyst geeft niet alleen een goed beeld van wat er in Nederland gebeurt op het gebied van cyber security, maar het toont ook de breedte aan van onze aandacht voor veiligheid. We hebben jaren nauw samengewerkt met GOVCERT.NL en doen dat nu met zijn opvolger, het Nationaal Cyber Security Centrum. We zijn intensief betrokken bij de Abuse Information Exchange, een goed voorbeeld van publiek-private samenwerking op dit gebied. En de mensen van Madison Gurkha zijn regelmatig te vinden bij ons of onze relaties om systemen aan de tand te voelen.

Ik wens u veel leesplezier, prettige feestdagen en alvast een goed en vooral veilig 2013. Ook in het komend jaar zullen wij ons inzetten voor een succesvol .nl-domein en de verdere ontwikkeling van het internet.

Roelof Meijer,
Algemeen directeur, SIDN

*Bron: McAfee en APWG

niet in handen van de overheid. Maar liefst 80% van de infrastructuur is van private partijen. We werken samen met bedrijven, wetenschappelijke instellingen, overheden en maatschappelijke organisaties. Nationaal en internationaal."

Deel van de Nederlandse veiligheidsstructuur

GOVCERT viel onder het ministerie van Binnenlandse Zaken. Dit veranderde toen het NCSC werd opgericht. Van den Heuvel: "Toen GOVCERT opging in het NCSC, werden we 'omgehangen' naar het nieuw opgerichte ministerie van Veiligheid en Justitie. Vanaf dat moment vielen we onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Ineens maakten we deel uit van de Nederlandse veiligheidsstructuur. Voor ons voelde dit een beetje als thuiskomen. Alles viel op zijn plek."

Drie taken

"Het NCSC heeft grofweg drie taken. Allereerst proberen we 'situational awareness' te creëren. Het besef dat cybersecurity van belang is en dat de mogelijke schade van incidenten enorm kan zijn. Om dit te bereiken proberen we de grootste dreigingen binnen Nederland in kaart te brengen. Hierdoor kan er focus in het werk worden aangebracht. Met behulp van ons internationale netwerk zetten we ons in om malware vroegtijdig op te sporen zodat incidenten kunnen worden voorkomen of de schade beperkt kan worden. Daarnaast hebben we een operationeel coördinerende rol bij incidenten waarbij de nationale veiligheid in gevaar kan komen, bijvoorbeeld als een energiebedrijf gehackt is. Ten slotte houden we ons bezig met incident respons en crisismanagement bij calamiteiten. Je kunt hierbij denken aan situaties als de hack bij Diginotar."

Nationale veiligheid

Het takenpakket van het NCSC is breed maar heeft grenzen. Van den Heuvel: "Organisaties zijn zelf verantwoordelijk voor hun security en de eerstelijns hulpverlening. Wij helpen als problemen sector-overschrijdend zijn, als de nationale veiligheid in het geding is of als publieke organisaties er zelf niet uitkomen. Ik vind het heel mooi dat je steeds meer ziet dat sectoren hun krachten bundelen als het gaat om security en samenwerken om incidenten te bestrijden. Voorbeelden daarvan zijn de Informatiebeveiligings Dienst (IBD) van de gemeenten en het CIP van een aantal grote uitvoeringsorganisaties."

Samenwerking

Samenwerking is de kracht van het NCSC. Van den Heuvel: "Bij de start van het centrum hebben we hard nagedacht hoe we deze samenwerking het best konden vormgeven. We zijn uitgekomen op een systeem waarin we mensen fysiek naar het NCSC toehalen. Publieke en private organisaties vaardigen 'liaisons' af. Die zijn minstens een dag per week aanwezig bij het NCSC. Het publieke liaisonschap is het afgelopen jaar vormgegeven. Mensen kunnen zo makkelijker informatie delen en omdat ze elkaar kennen, werken ze beter samen. Ik vind het ook heel verrassend dat iedereen zich wil inzetten voor de nationale zaak. Het is echt een community."

De Nationale Cyber Security Strategie

Het thema van de Nationale Cyber Security Strategie is 'Slagkracht door samenwerken'. De strategie bestaat uit zes punten:

1. inrichten van een Cyber Security Raad en Nationaal Cyber Security Centrum;
2. opstellen van dreiging- en risicoanalyses;
3. vergroten van de weerbaarheid van vitale infrastructuur;
4. responscapaciteit vergroten om ICT-verstoringen en cyberaanvallen te pareren;
5. intensiveren van de opsporing en vervolging van cybercrime;
6. stimuleren van onderzoek en onderwijs.

Een bijzonder model

"In het buitenland vindt men ons model zeer aansprekend. De manier waarop we werken is niet uniek, maar de invulling wel. Het commitment van private partijen is hier heel hoog, dat blijkt wel uit het aantal captains of industry dat plaats heeft in de Cyber Security Raad. Dat zie je in andere landen eigenlijk niet. Ook uniek is het feit dat we elk jaar, samen met onze partners, een Cyber Security Beeld opstellen. Hierin worden de belangrijkste bedreigingen benoemd. Op basis hiervan kan Nederland prioriteiten stellen in het cybersecurity-beleid."

De grootste bedreigingen

"De belangrijkste dreigingen waar bedrijven en overheidsorganisaties op dit moment mee te maken hebben, zijn cybercriminaliteit en spionage. Daarnaast baren botnets ons blijvend zorgen. Zeker vanwege kwaliteit van social engineering die criminelen toepassen: de nep websites en andere trucs waarmee ze gebruikers verleiden om op een link te klikken, worden steeds beter. Tot slot maken het toenemende gebruik van mobile devices en het opslaan van data in 'de cloud', de beveiliging de komende jaren nog veel complexer."

SIDN over de samenwerking

Bert ten Brinke is een van de twee liaisons die vanuit SIDN bij het NCSC betrokken is. Ook hij is erg enthousiast over de samenwerking binnen het centrum: "Cyber security kan niet zonder samenwerking. Criminelen vinden steeds weer nieuwe manieren om samen te werken, dus moeten de bestrijders ook de handen ineen slaan. Een mooi voorbeeld? In maart 2012 werd er tijdelijk een gevaarlijk virus verspreid via NU.nl. Op dat moment gingen bij het NCSC en bij SIDN alle alarmbellen rinkelen. Dat we dit virus snel konden bestrijden, kwam door een goede samenwerking binnen het NCSC. Een ander voorbeeld is het Dorifel-virus dat afgelopen zomer bankgegevens van meer dan 1.600 Nederlanders stal. Bij het NCSC zag ik een interessante presentatie van iemand die software had gemaakt om dit virus te bestrijden, zeg maar het antivirus. Ik heb hem uitgenodigd om deze presentatie ook te geven tijdens een bijeenkomst met enkele peer-registries. Zo draagt de samenwerking met het NCSC eraan bij dat kennis sneller gedeeld wordt."

Een belangrijke taak

Bert ten Brinke: "Als registry levert SIDN een cruciaal onderdeel van de online infrastructuur in Nederland. Vanuit die positie werkten we al nauw samen met GOVCERT. We kregen van hen informatie over dreigingen en GOVCERT kon bijspringen bij problemen. Nu is de samenwerking veel breder geworden en de slagkracht groter. De samenwerking voelt goed, omdat onze strategische doelen overeenkomen. Net als het NCSC zet SIDN zich ook in voor een veilig internet voor iedereen. Een enorm belangrijke taak, want zonder internet draait de wereld door, maar staat ons leven stil."

De Nationale Cyber Security Raad

De Raad geeft de regering en private partijen gevraagd en ongevraagd advies over digitale veiligheid en stelt prioriteiten in de aanpak van ict-bedreigingen. In de Raad zitten afgevaardigden van overheden, bedrijfsleven, wetenschap en maatschappelijke organisaties. Het voorzitterschap is in handen van Eelco Blok, ceo KPN, en Nationaal Coördinator Terrorismebestrijding Erik Akerboom.

Bert ten Brinke,
security officer, SIDN

EEN CONSTANTE WAPENWEDLOOP MET HACKERS

WALTER BERGERS VAN MADISON GURKHA OVER CYBER SECURITY

Walter Bergers noemt zich ook wel 'ethisch hacker'. Voor Madison Gurkha, het bedrijf waarvan hij mede-eigenaar is, probeert hij in te breken in bedrijfssystemen. Zo legt hij feilloos de zwakke punten in de beveiliging bloot. Madison Gurkha geeft onder meer beveiligingsadviezen en ondersteunt bedrijven die te maken hebben met een lek.

Walter Belgers,
partner, principal security consultant

Hebben bedrijven wel voldoende aandacht voor beveiligingsrisico's?

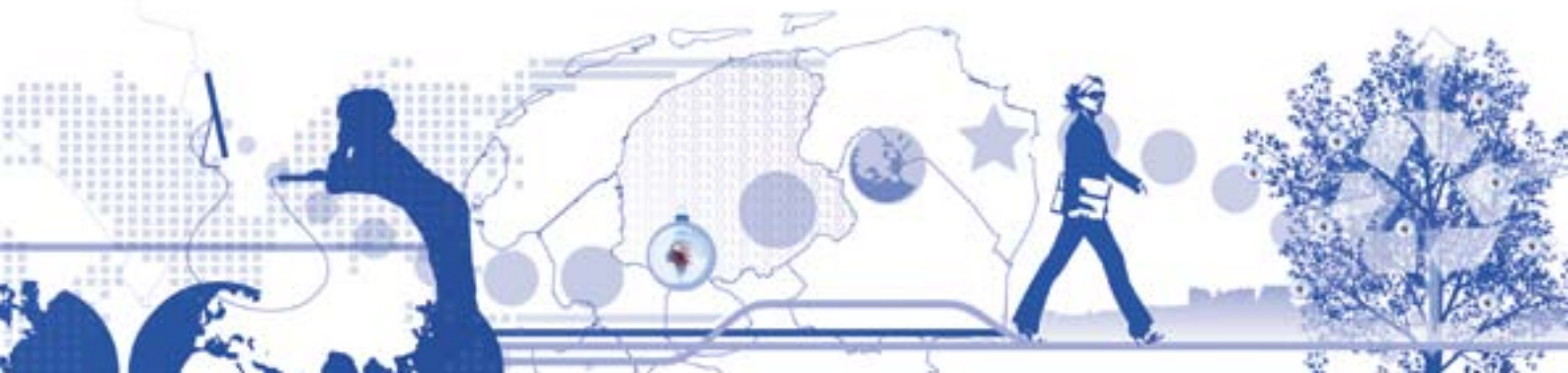
"Vooral in een vroeg stadium van een project is er te weinig aandacht voor veiligheid. De focus ligt dan op de functionaliteit. Een projectleider werkt met een lijst functionele specificaties, niet met security-vereisten. Op zich is dat niet zo gek, beveiliging levert immers niet direct iets op, het kan alleen in een later stadium zorgen voor minder verliezen. Maar er is ook gewoonweg te weinig bewustzijn. Ondernemers denken er niet over om hun brandverzekering op te zeggen, terwijl de kans op brand veel kleiner is dan de kans dat ze op een of andere manier met computercriminaliteit te maken krijgen."

Worden bedrijven zich wel meer bewust van die risico's?

"Gelukkig wel. Elke hack die in het nieuws komt draagt daaraan bij. Bedrijven die een keer negatief in het nieuws komen vanwege een lek, worden in ieder geval wel wakker. Zo werkt het nu eenmaal. Mensen kopen ook pas een tweede fietsslot als hun fiets een keer gejat is."

Waar moeten bedrijven op letten?

"Er zijn drie momenten waarop iets mis kan gaan: bij de bouw of de aanschaf van een nieuwe computersysteem, bij de configuratie daarvan en bij het onderhoud. Veel systemen zijn te goed van vertrouwen. Als je een nieuwe webapplicatie bouwt zou je ervan uit moeten gaan dat alles dat van buiten komt niet te vertrouwen is. Dit gaat nog vaak mis. En als je eenmaal een nieuw systeem hebt, moet je het nog configureren voordat je het gebruikt. Wachtwoorden instellen, onnodige programma's verwijderen, enzovoorts. Deze stap wordt regelmatig vergeten. Tot slot moet je zorgen dat je systeem up-to-date blijft. Eigenlijk kom ik in elk bedrijf waar ik binnenkom wel verouderde onderdelen tegen."



Zie je trends in cybercriminaliteit?

"In de jaren '80 braken veel hackers in voor de kick, gewoon om te bewijzen dat het kon. In de jaren '90 kwamen er steeds meer mensen die er geld mee wilden verdienen. Nu zijn het keiharde criminelen die zich ermee bezighouden. Cybercriminaliteit is ook steeds georganiseerder. Een andere trend is dat medewerkers van bedrijven steeds vaker mobiel werken. Het is heel gewoon om met je mobiele telefoon of de laptop van thuis op het bedrijfsnetwerk te komen. Dit brengt enorme risico's met zich mee. Bedrijven zouden dat voor een deel op kunnen lossen door werknemers alleen maar toegang te geven tot de netwerkonderdelen die voor hen interessant zijn, in plaats van tot het hele netwerk. En een laatste trend is cyberoorlog en -terrorisme. Ik geloof niet in een aanval alleen op internet, maar cyberwarfare zal zeker onderdeel zijn van toekomstige conflicten."

Welke technische ontwikkelingen zijn van invloed op cybersecurity?

"Computers zijn de laatste tijd steeds minder general purpose-apparaten. Een tablet is eigenlijk een black box met een browser. Als gebruiker kun je niet zien wat het apparaat doet, laat staan dat je iets kunt veranderen aan de instellingen. Daar komt bij dat er slechts een klein aantal besturingssystemen overblijft op de markt. Dit betekent dat een lek in een van die systemen direct een enorme impact heeft."

Wat is meestal het zwakste punt in een bedrijf?

"Tegenwoordig is de techniek vaak zo goed dat de mens duidelijk de zwakste schakel is. Criminelen richten zich steeds vaker daarop. En daar worden de slimste dingen voor verzonnen. Er is bijvoorbeeld een virus dat een venster opent zodra iemand gaat internetbankieren. Dit lijkt een pop-up waarop reclame wordt gemaakt voor een zeer aantrekkelijke depositorekening. Gebruikers denken geld te storten op deze rekening, maar maken het in werkelijkheid over op de rekening van een criminele bende. Een ander trucje zijn give-aways met een usb-aansluiting, zoals een toetsenbordje of een grappig robotje. Zodra je ze aansluit, besmetten ze je computer. Zo verzinnen criminelen steeds weer wat nieuws. Ons werk is een constante wapenwedloop met hackers. Aanvallers en verdedigers proberen elkaar steeds weer een stapje voor te zijn."

Madison Gurkha
Your Security is Our Business

ABUSE INFORMATION EXCHANGE: EEN NIEUW WAPEN TEGEN BOTNETS

ISP's, SIDN en overheid slaan handen ineen

Zonder dat gebruikers het merkten waren er van begin 2009 tot halfweg 2010 tussen de 450.000 en 900.000 Nederlandse computers besmet en onderdeel van botnets. Mogelijk waren het er zelfs meer. Dit bleek uit een onderzoek dat de TU Delft in 2010 uitvoerde in opdracht van het ministerie van Economische Zaken. Dit onderzoek was de aanjager voor Abuse Information Exchange, een samenwerking tussen zeven ISP's, SIDN en het ministerie van EZ.

Bots zijn kleine computerprogramma's die op de achtergrond draaien en voor computergebruikers bijna niet waarneembaar zijn, ze worden verspreid via spyware, trojaanse paarden en andere malware.
Door grote aantallen bots te verbinden in een botnetwerk, kunnen criminelen illegale acties uitvoeren. Zoals het versturen van spam, het platleggen van websites via zogenaamde DDoS-aanvallen, en in toenemende mate identiteitsfraude. De maatschappelijke schade van botnets is moeilijk in cijfers uit te drukken omdat veel verborgen blijft. Ook omdat bijvoorbeeld bedrijven die gechanteerd worden met de dreiging van een DDoS-aanval, dit niet altijd aan de grote klok willen hangen. Maar misschien nog belangrijker dan de directe schade is de beschadiging van het vertrouwen in ICT.

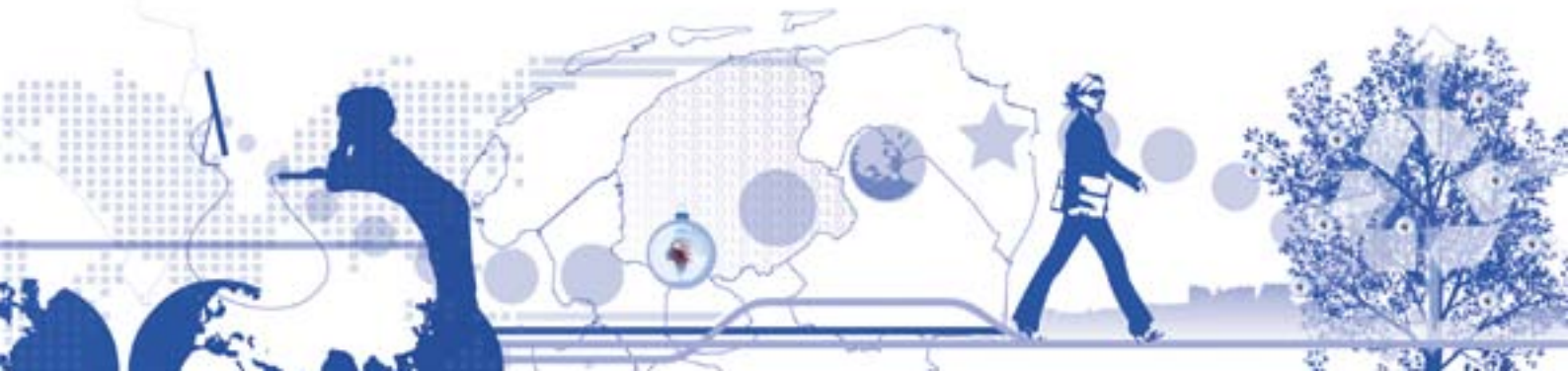
Thomas de Haan, vanuit het ministerie van EZ betrokken bij Abuse Information Exchange: "Minder vertrouwen bij de consument leidt tot minder gebruik van ICT. En dat zal onze economische groei remmen. ICT draagt namelijk voor meer dan de helft bij aan de economische groei in Europa."

Moeilijk aan te pakken

Botnets hebben al geruime tijd de aandacht van de

Thomas de Haan, Senior beleidsmedewerker, ministerie van EZ

Nederlandse overheid, maar opsporing en vervolging zijn moeilijk. Thomas de Haan: "Het KLPD heeft specialisten die zich hiermee bezighouden. Het vinden van de makers van botnets is echter technisch complex en arbeidsintensief. En als je ze eenmaal hebt gevonden zitten ze vaak in het buitenland en zijn moeilijk aan te pakken. Toch zijn er wel successen, zoals de uitschakeling van het Bredolab-netwerk, een botnet dat wereldwijd 30 miljoen computers besmette, in 2010. Dit werk blijft belangrijk. Als je de bron van het kwaad niet aanpakt blijft het dweilen met de kraan open. Maar met 'schonere' computers en bewuste gebruikers wordt het voor de makers wel steeds moeilijker om voet aan de grond te krijgen."



Onderzoek TU Delft

In 2010 liet het ministerie van EZ de TU Delft een onderzoek uitvoeren naar het botnetprobleem. Gert Wabeke, manager bij KPN en voorzitter van Abuse Information Exchange: "De belangrijkste uitkomst was dat we slechts een klein gedeelte van de besmettingen zien. Als een computer besmet raakt, gaat er tenslotte niet ergens een bel af. Dit leidt op zijn beurt tot een beperkte aanpak van botnets. Met een kleine groep ISP's zijn we bij elkaar gaan zitten en hebben we gekeken wat we hieraan kunnen doen. We vonden dat we in ieder geval de informatie-uitwisseling konden verbeteren. Hieruit is Abuse Information Exchange voortgekomen.

Gert Wabeke, manager Lawful Intercept, KPN

Het idee erachter is om alle verschillende informatiebronnen te combineren, bijvoorbeeld signalen die we krijgen van partijen zoals Spamhouse of het NCSC. Abuse Information Exchange is één centraal punt waar alle informatie over botnetbesmettingen verzameld en verspreid wordt. Dit zal er niet alleen voor zorgen dat we meer besmettingen aan kunnen pakken, maar het zorgt ook voor een kwalitatief betere aanpak."

Steeds bredere samenwerking

Nederland kent honderden partijen die met botnets te maken hebben: ISP's, hostingpartijen, registrars, enzovoorts. Slechts zeven grote ISP's werken samen in Abuse Information Exchange. Gert Wabeke: "Natuurlijk zou het beter zijn als er meer partijen meededen. Maar dat betekent niet dat je maar moet wachten totdat je alle partijen bij elkaar hebt. Op een gegeven moment moet je gewoon beginnen. We zijn heel blij dat er zich nu al steeds meer organisaties melden die hun informatie graag met ons delen of gebruik willen maken van onze kennis."

Unieke aanpak

Ook in andere landen maakt men zich zorgen over botnets. Zo is er bijvoorbeeld een Europees programma in de maak. Daarnaast hebben verschillende landen programma's opgezet, zoals Japan, Taiwan en Duitsland. De Nederlandse aanpak is echter uniek.

Cristian Hesselman, manager research bij SIDN en namens SIDN bij het project betrokken: "In Duitsland werken ze met een centrale helpdesk. ISP's melden daar besmettingen bij hun klanten en dragen hen waar nodig over aan de centrale helpdeks die verder assisteert bij het verwijderen van de bot. Wij kiezen voor een model waarbij ISP's altijd zelf hun klanten helpen bij het verwijderen van botnetsoftware en gebruik maken van een centrale informatiedienst, Abuse Information Exchange.
Deze dienst concentreert zich op het verzamelen, correleren en doorgeven van botnetmeldingen. Op deze manier hoeft alleen de informatievoorziening van de Abuse Information Exchange uniform te zijn, waardoor we flexibeler zijn en het eenvoudiger is voor andere partijen, zoals registrars of hostingbedrijven, om aan te haken."

Rol SIDN

De rol van SIDN in Abuse Information Exchange is meerledig. Cristian Hesselman: "Allereerst zijn we leverancier en afnemer van informatie. Vanuit de aard van ons werk als registry zien we soms een besmetting voorbijkomen. En als er een botnet is die het DNS bedreigt dan willen we dat natuurlijk als eerste weten. Daarnaast zijn we technisch beheerder van het systeem. Wij zorgen ervoor dat Abuse Information Exchange een goedlopende online service wordt."

Cristian Hesselman, manager research, SIDN

Aanpak op drie assen

Het gevecht tegen botnets wordt gevoerd op drie fronten. Thomas de Haan: “Allereerst zijn er de bronnen, dit zijn veelal servers in het buitenland. De aanpak hiervan is een kwestie van internationale samenwerking en van de lange adem. Daarnaast zijn er de besmettingshaarden, zoals websites met malware. En dan zijn er nog de besmettingen zelf. Ik verwacht dat Abuse Information Exchange, door haar unieke positie, opgebouwde kennis en expertise in de toekomst op alle fronten nuttig zal zijn, niet alleen bij het aanpakken van besmettingen.“

Enkele bekende botnets

Grum Was verantwoordelijk voor maar liefst 18 miljard spamberichten per dag – 18% van alle spam in de wereld. Werd in juli 2012 neergehaald, maar wist helaas een herstart te maken.

Lethic Maakt gebruik van encryptie waardoor de bron extra moeilijk is op te sporen. Neemt ongeveer 28% van alle spam in de wereld voor zijn rekening.

Zeus Een toolkit om eenvoudig een botnet op te zetten. Het enige wat je moet doen is mensen verleiden om een programma te openen en zo de trojan te starten die Zeus in werking zet.

SpyEye Een succesvol botnet dat zich specifiek richt op het stelen van bankinformatie.

TDL-4 (TDSS of Alureon) Een zeer geavanceerde bot die zich verstopt in de systeembestanden van een computer, waardoor het nauwelijks te vinden is.

Flashback Een botnet dat zich richt op Macgebruikers. Probeert gebruikers hun wachtwoorden te ontfutselen, zodat cybercriminelen hun accounts kunnen overnemen.

.NL Analysed

	TLD		Aantal Q3*	Groei	
1	.com	Algemeen	104.866.127	1,3%	=
2	.de	Duitsland	15.202.243	0,7%	=
3	.net	Algemeen	14.831.792	0,6%	=
4	.tk	Tuvalu	12.691.637	18,1%	↑
5	.uk	Ver. Koninkrijk	10.243.649	0,9%	↓
6	.org	Algemeen	10.085.123	0,9%	↓
7	.info	Algemeen	7.514.932	-3,9%	↓
8	.cn	China	5.709.234	43,3%	=
9	.nl	Nederland	5.039.845	1,4%	↓
10	.ru	Rusland	4.023.640	4,0%	↓
11	.eu	Europese unie	3.663.898	1,8%	↓
12	.br	Brazilië	3.061.952	3,5%	↓
13	.ar*	Argentinië	2.632.213	2,3%	↓

	TLD		Aantal Q3*	Groei	
14	.au	Australië	2.525.707	2,7%	↓
15	.it	Italië	2.448.185	1,5%	↓
16	.fr	Frankrijk	2.442.463	3,2%	=
17	.pl	Polen	2.390.614	0,7%	↓
18	.biz	Algemeen	2.210.317	-1,5%	↓
19	.ca	Canada	1.972.688	1,7%	↓
20	.us	Ver. Staten	1.743.016	0,6%	↓
21	.ch	Zwitzerland	1.734.170	1,5%	↓
22	.es	Spanje	1.596.547	2,1%	↓
23	.be	België	1.319.016	1,3%	↓
24	.jp	Japan	1.307.023	0,9%	↓
25	.co*	Colombia	1.304.516	2,2%	↓
	* schatting				

Het derde kwartaal viel qua groei tegen, bijna alle TLD's noteerden een lagere groei ten opzichte van het tweede kwartaal. De totale groei in dit kwartaal is uitgekomen op 6,4 miljoen domeinnamen, tegen 7,2 miljoen in het tweede kwartaal. Positieve uitschieters zijn .tk, .cn, .ru, .br en .fr, zij groeiden sterker dan de andere TLD's van vergelijkbare omvang.

Sinds enkele maanden publiceert de .tk-registry cijfers over het domein. Zij nemen nu de derde positie overall in en zijn de 2e ccTLD, na .de. Als het domein van Tuvalu de huidige groei weet vast te houden zullen ze binnen enkele maanden de eerste positie van Duitsland overnemen. De groei van .cn lag in het derde kwartaal weer op het niveau van de periode 2007-2008 toen de liberalisatie van het registratiebeleid zorgde voor een zeer sterke toename van het aantal geregistreerde domeinnamen. Door deze grote toename is .cn het .nl-domein voorbijgestreefd en zijn zij nu de 4e ccTLD.

DNSSEC

Sinds de vorige editie van The.nlyst is het aantal DNSSEC .nl-domeinnamen meer dan verdubbeld naar ruim 1,3 miljoen. We zijn uiteraard erg trots op deze stormachtige groei. Echter, het risico dat er iets fout gaat wordt groter naarmate er meer domeinnamen met DNSSEC beveiligd worden. Om domeinnaambeheerders de mogelijkheid te bieden fouten op te sporen in gesignde domeinnamen heeft Miek Gieben (technisch adviseur bij SIDN) in het kader van SIDN Labs de DNSSEC-checker ontwikkeld. Deze checker is te vinden op: http://check.sidnlabs.nl:8080/form. De tool biedt ons de mogelijkheid een vinger aan de pols te houden, periodiek wordt middels een steekproef gecontroleerd hoe het staat met de kwaliteit van de DNSSEC-domeinnamen. Nevenstaand diagram laat de uitkomsten zien van een controle van 50.000 willekeurig gekozen DNSSEC .nl-domeinnamen.

Slechts een fractie van de gesignde domeinnamen is niet correct beveiligd met DNSSEC, deze hebben als status 'bogus'. Geëxtrapoleerd naar de hele zone komt dat uit op circa 8.000 foutief beveiligde domeinnamen.

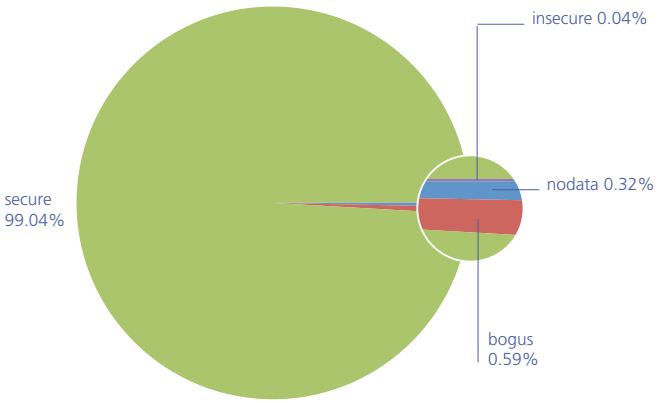
Toelichting:

secure: de domeinnaam is correct beveiligd met DNSSEC

bogus: de domeinnaam is niet correct beveiligd met DNSSEC

insecure: de domeinnaam is niet beveiligd met DNSSEC

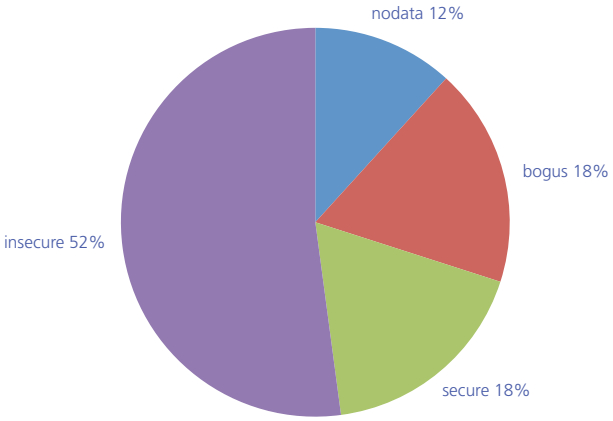
nodata: de domeinnaam komt niet voor in het DNS, er bestaat geen name server voor dit domein.

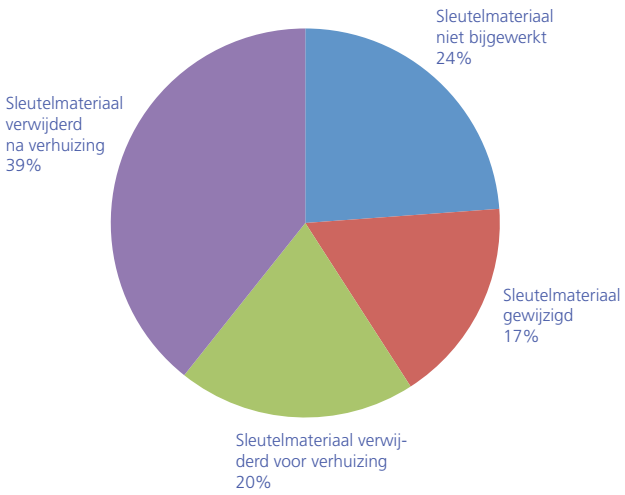


DNSSEC-verhuizingen

Een belangrijke oorzaak van het aantal 'bogus'-domeinnamen is het verhuizen van domeinnamen. Sinds 1 juni 2012 zijn er iets meer dan 10.000 DNSSEC-domeinnamen verhuisd. Al deze domeinnamen zijn middels de DNSSEC-checker gecontroleerd, onderstaand diagram toont de uitkomsten van deze controle.

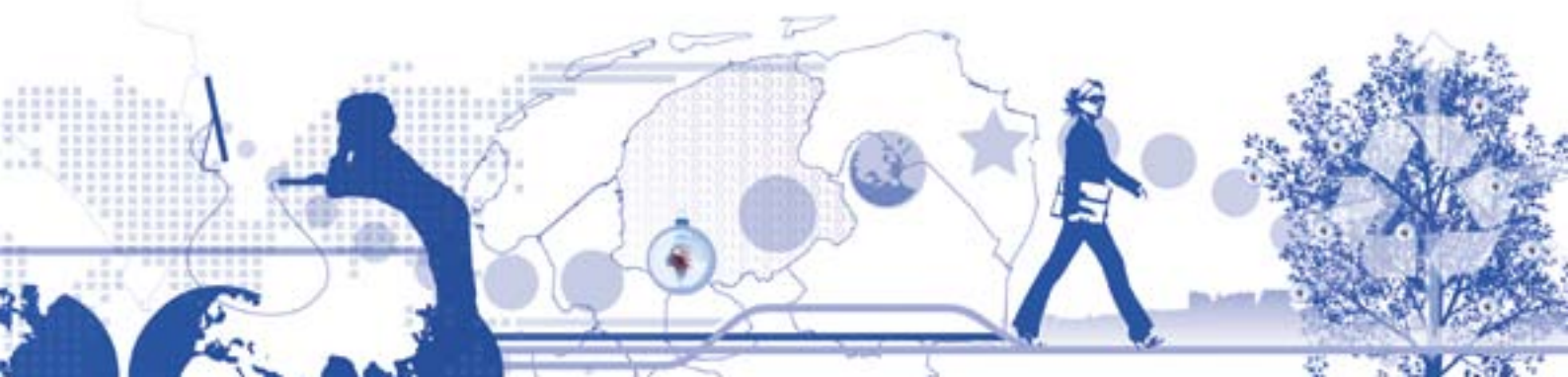
Meer dan de helft van de verhuisde domeinnamen heeft na verhuizing geen sleutelmateriaal meer, deze domeinnamen zijn dus niet meer beveiligd met DNSSEC, zij zijn overigens nog wel bereikbaar. Dat geldt niet voor de 18% die 'bogus' zijn, deze domeinnamen zijn feitelijk stuk en zijn dus onbereikbaar voor bezoekers die DNSSEC-validatie aan hebben staan. (zie linker taartdiagram)





Uit de logging van het domeinregistratiesysteem blijkt dat in bijna een kwart van de DNSSEC-verhuizingen het sleutelmateriaal niet bijgewerkt wordt, zie het diagram hierboven. Daar staat tegenover dat driekwart van de registrars wél iets doet met het sleutelmateriaal. Enkele registrars verwijderen het sleutelmateriaal voordat de domeinnaam verhuist, door deze proactieve houding zorgen zij ervoor dat de domeinnaam ook na verhuizing bereikbaar blijft.

(zie rechter taartdiagram)



Suggesties

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

Evenementenkalender

SIDN is vertegenwoordigd op tal van nationale en internationale evenementen. We doen dit vanuit onze taak als registry van het .nl-domein en vertegenwoordigen daarbij de Nederlandse internetgemeenschap en de .nl-registrars. Ook organiseren wij zelf geregeld bijeenkomsten. In de komende maanden is SIDN, voor zover nu bekend, vertegenwoordigd op de volgende evenementen:

Datum	Evenement	Plaats
15-02	40th CENTR Legal and Regulatory Workshop	Zürich, Zwitserland
13-03	28th CENTR Administrative Workshop'	Lissabon, Portugal
14-03 t/m 15-03	49th CENTR General Assembly / 2013 Annual General Meeting	Lissabon, Portugal
17-03 t/m 22-03	86th IETF Meeting	Orlando, Florida, Verenigde Staten

Rectificatie

In de vorige editie van The.nlyst stond een onjuistheid in het artikel over .nl-registrar InterNetX (pagina 4). In het antwoord van Claus Barche op de vraag 'Verwachten jullie veel innovatief gebruik van de nieuwe top level domeinen?' staat ten onrechte dat InterNetX de back-end systemen voor .gmbh gaat leveren. InterNetX gaat een API voor de back-end systemen voor .gmbh leveren.

Onjuiste adressering

Bij de samenstelling van de verzendlijst voor de vorige editie van The.nlyst is een fout gemaakt met als gevolg dat verkeerde bedrijfsnaam aan het adres is gekoppeld. Onze excuses hiervoor. Voor het merendeel zijn de magazines wel correct bezorgd. Mocht u nummer 8 onverhoopt toch niet ontvangen hebben, mailt u dan naar communicatie@sidn.nl. Wij sturen u het magazine dan alsnog toe.

Wist u dat...

...de supportafdeling van SIDN sinds kort ook bereikbaar is via Twitter. Stel uw vragen via @SIDNsupport.

twitter FOLLOW US

Colofon
The.nlyst is een platform voor informatie over (.nl-)domeinnamen en wordt vier keer per jaar gratis verspreid onder relaties van SIDN.

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

Aan deze editie werkten mee
Elly van den Heuvel, Walter Belgers, Gert Wabeke, Thomas de Haan, Cristian Hesselman, Bert ten Brinke, Roelof Meijer, Lycke Hoogeveen, Sean Schuurman van Rouwendal en Martin Sluijter

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

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

Aantal
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